미국 해사 사이버안보 정책과 한국에의 시사점

김소정 | 국가안보전략연구원
배선하 | 국가보안기술연구소, 교신저자

| 목차

해사 분야는 국가 안보적 측면에서 다양한 영향력을 투사할 수 있는 플랫폼이면서, 동시에 물류 흐름과 공급망 안전성을 보장할 수 있는 최일선의 영역이다. 최근 제조, 자동차 등 전통적인 산업 분야에 ICT 기술이 도입되고, 조선 및 해양 산업에도 ICT 기술 활용이 확대되면서 디지털 전환이 급속도로 이루어지고 있다. 또한, 스마트 선박, 스마트 항만 등 새로운 기술이 발달하고, IT와 OT 간의 경계가 모호해지면서 해사 분야의 사이버안보 위협이 증대되고 있다. 위성통신 기술에 기반하는 6G 시대에는 해사 시스템의 인터넷 접속이 급격히 증가하고 IoT 등 공격벡터 확대가 예상되며, 이에 해사 분야의 사이버안보 위협은 국가안보를 넘어서 글로벌 안보 이슈로 부상하고 있다.
미국은 트럼프 정부부터 국가사이버전략을 통해 국가안보 및 경제 분야에 해사의 중요성을 강조하고, 다른 기반시설과 해사의 사이버보안 격차를 줄이고 취약성을 완화하기 위한 다양한 정책을 추진 중이다. 또한, 최근 글로벌 해사 사이버안보에서 위험관리체계가 핵심적 요소로 다뤄지고 있는데 위험관리체계는 미 연방정부에서 처음 제안되고 적용이 확대되고 있는 사이버안보 체계이다. 이하에서는 미국의 해사 사이버안보 정책과 핵심 조직인 해안경비대 사이버사령부의 임무와 기능을 분석했다. 그리고 한국의 해사 사이버안보 정책 및 조직 현황을 분석하고, 미국과의 비교를 통해 우리나라 해사 사이버안보를 위한 정책 개선방향을 제안한다.

| 주제어 해사 사이버안보, 항만 및 선박 사이버보안, 미국 해사 사이버안보 정책, IMO, 해안경비대 사이버 전략

Ⅰ. 서론

1. 연구배경 및 필요성

국가 및 국가지원 조직의 선거공작, 기반시설 공격, 사이버 스파이(espionage) 활동을 통한 지식재산권 도용 등 정치적· 경제적 이익을 위한 악의적인 사이버 활동이 증가하고, 주요 기반시설에 대한 사이버 위협은 국가안보에 막대한 위해 요소가 되고 있다(김소정 2022). 동시에 국가 주요 기반시설 등에는 새로운 기술이 속속 접목되고 있다. 스마트 제조 분야에서는 스마트 센서, 3D 프린팅, 에너지 절감 기술 등 다양한 ICT 기술을 공장 자동화·최적화에 활용하고 있고,[1] 스마트 조선 분야에서도 사물인터넷(IoT), 인공지능(AI), 센서 및 센싱 네트워크, 블록체인 등의 기술이 도입되고 있다. 스마트 선박 분야는 자율운항선박과 더 나아가 무인선박의 형태로 발전해 나가고 있다. 이렇듯 OT 분야가 디지털화되면서 OT 시스템 자체가 인터넷에 연결되거나 IT 시스템과 OT 시스템 간 망 연계가 증가하고 있다. 더욱이 IT 시스템 침해가 OT 사이버 공격의 시작점이 되는 경우가 많은데, IT와 OT 간의 경계가 모호해지면서 주요 기반시설의 사이버안보 위협은 더욱 증대되고 있다.

항해 승객의 안전한 운송과 대부분의 국제 무역을 촉진하는 역할을 담당하는 해상 운송 시스템(MTS, Maritime Transportation System) 역시 국가의 기간산업으로 세계 경제에 글로벌 공급망 측면에서 가장 중요한 산업 중 하나다. 미국의 경우 MTS는 국내

1) 한국정보통신기술협회, “정보통신용어사전, 스마트 자동차” http://word.tta.or.kr/mobile/dictionaryView.do? word_seq=060993-2 (검색일: 2024.1.9.)

총생산(GDP)의 4분의 1을 공급하며, COVID-19 대유행 이전에 상업용 해운은 물동량 기준으로 전 세계 무역의 80% 수준, 금액 기준으로 전 세계 무역의 70% 이상을 이동했고(UNCTAD 2018), 팬데믹 이후에는 4.1%까지 성장했다(UNCTAD 2020).

이렇듯 전 세계 물류 이동의 큰 부분을 차지하는 해사 분야에도 육상과 선박의 통신 연결, 선원들의 IT 기기 활용이 확대되면서 사이버 위협이 증가하고 보안이 취약해짐에 따라(원병철 2022), MTS의 효율적인 운영이 위험에 처해 있는 상황이다. 위성통신 기술에 기반하는 6G 시대가 도래하면 해사 시스템의 인터넷 접속이 급격히 증가할 것이며, 이제 해사 분야의 사이버안보 위협은 국가 안보를 넘어서 글로벌 안보 이슈로 부상하고 있다.

대표적인 해사 사이버 공격 사례를 살펴보면 2017년 Maersk Line 사의 낫펫야 랜섬웨어 공격이 있다. 당시 Masesk Line 터미널 IT 시스템에 랜섬웨어 공격이 발생하여 약 3주간 선박의 정상적인 하역에 어려움을 겪었으며, 약 3,000억 원의 재정적 손실이 발생했다(Andersen 2017). 또한 2021년 5월에 발생한 미국 콜로니얼 파이프라인社의 랜섬웨어 공격이다. 당시 다크사이드 공격 그룹이 이메일 피싱 기술을 이용해 IT 망을 먼저 침해하고, 이를 기반으로 OT 영역으로 이동했다(김선애 2021). 이외에도 전 세계의 해사 기자재 업체, 터미널 등에 다수의 사이버 공격이 발생했으며, 2017년 이후 전 세계적으로 해사 시설 필수 운영시스템(OT, Operation Technology)에 대한 사이버 공격이 900% 증가한 것으로 나타났다(한국선급 2021a).

우리나라도 예외는 아니다. 2021년 6월 잠수함을 건조하는 대우조선해양을 비롯한 방위산업체들이 해킹 시도를 당했다. 대우조선해양의 경우 한국 최초 3,000톤급 잠수함인 도산안창호함을 비롯해 안무함 등 우리나라의 주력 잠수함을 건조하는 핵심 방산기업으로, 지난 2016년에도 북한 추정 해커 그룹에 의해 잠수함 관

련 핵심기술 등 1~3급 군사기밀 60여 건을 포함한 4만여 건의 내부 자료를 탈취당한 바 있다(원병철 2021). 또한, 2023년 국정감사를 통해서 알 수 있듯이, 최근 5년간(2018년~2022년) 4개 항만공사(부산, 인천, 울산, 여수) 대상 정보 유출, 시스템 권한 획득 등 총 449건의 사이버 공격이 발생한 것으로 확인되었고, 2018년 41건에서 지난해 227건으로 5.5배 폭증했다(박종서 2023).

이렇듯 해사 분야 사이버안보 필요성이 제기되고 있음에도, 한국에서는 그 중요성이 상당히 늦게 인식되었다. 국제해사기구(IMO, International Maritime Organization)가 선박의 안전관리 규제에 사이버보안 위협 대응 개념을 적용한 규제를 포함하고, 국제표준화하면서 논의가 시작되었으며, 선박 등의 운항을 위한 최소한의 해사 분야 사이버보안 기준을 준수하는 데 급급한 실정이다. 이로써 현재 주를 이루는 해사 분야 사이버보안 이슈는 선박 등에 발생할 수 있는 사이버보안 위협 대응으로 한정되어 있다. 그러나 해사 사이버안보 강화를 위해서는 선박 외에도 화물관리 업체, 터미널 및 하역사 등의 항만시설, 운송사 등 관련한 다양한 이해관계자 전반에서 사이버안보 수준 제고가 요구되며, 해사 분야를 국가 차원에서 안전보장을 위한 필수 보호 영역으로서 인식하고, 주요 기반시설 관점에서 국가 차원의 종합적인 정책 수립 및 추진이 필요하다.

이에 반해 미국은 해사 분야 사이버안보를 국가안보 요소로 인식하고 주요 기반시설 사이버안보 강화 측면에서 접근하고 있으며, 이를 위해 국가 차원에서 적극적인 활동을 수행하고 있다. 특히, 해안경비대를 해사 사이버안보 총괄기관으로 명시하고, 2015년에는 해안경비대 사이버안보 전략을 발표하였으며, 2020년에는 백악관이 국가전략 수준의 계획을 발표한 바 있다. 특히, 범죄자의 랜섬웨어 사용, 적대국의 전술역량 향상, 피싱 공격 증대 등 환경 변화에 대응하기 위한 해안경비대 사이버사령부의 임무는 우리나

라의 해군이나 해경에 비해 그 범위나 영향력이 훨씬 광범위하다. 해안경비대 사이버사령부는 항만에서의 위험을 시설 접근 제한, 터미널 본부 데이터 관리, 랜섬웨어 대응, 운영시스템 보호, 위치 기반시스템 보호, 선박 보안 등 다양한 분야가 포함되는 포괄적인 개념으로 인식하고, 이러한 위험 인식에 기반하여 정보수집, 사이버 작전, 평가 등의 업무를 수행하고 있다.

이에 본 고에서는 국가 차원에서 해사 사이버안보를 강화해 나가고 있는 미국의 정책문서들을 살펴보고, 해양경비대 사이버사령부의 조직체계와 임무를 살펴보고자 한다. 또한, 한국의 해사 사이버안보 정책 동향을 살펴보고, 이를 기반으로 한국의 정책 개선 방안을 제안하고자 한다.

2. 연구방법 및 범위

본 논문에서 말하는 해사 사이버안보는 선박뿐만 아니라 해운선사, 항만시설 운영자, 화주/포워더, 조선사 등 해상물류 관계자, 해안 경찰, 해군 등 해사 전반에 걸친 이해관계자의 사이버공간을 악의적인 사이버 활동으로부터 안전하게 보호하는 것을 의미한다. 이에 선박, 선사 시설, 조선사 시설, 항만시설 및 관련 물류 시설 등 다양한 주요 기반시설의 예방 및 보안과 사이버 작전 및 사이버 위협에 대한 능동적 대응 등 포괄적인 측면에서 해사 사이버안보 정책을 살펴보고자 한다. 기존 한국의 선박 보안 중심 해사 사이버안보 정책의 변화를 위해 선박에 대한 사이버보안뿐만 아니라 주요 기반시설의 관점에서 국가 차원의 해사 사이버안보 강화 정책과 부처 및 기관의 역할에 초점을 맞추었다.

이에 사이버보안프레임워크(CSF, Cyber Security Framework) 및 위험관리체계(RMF, Risk Management Framework) 등 해사 분야 사이버안보 정책에서 글로벌 표준을 이끌어 나가고 있는 미

국의 해사 사이버안보 정책을 중심으로, 국제기구 및 선주협회·화주협회 등 국제협회와 협력하여 국가 차원에서 펼쳐야 하는 해사 사이버안보 정책 방향과 주요 기관이 맡아야 하는 책임 및 역할을 살펴보고자 한다.

주요하게 검토한 미국의 정책문서는 <표 1>과 같고, 선행연구로는 해사 사이버안보 관련 국제협회 사이버안보 정책 동향과 국내 주요 연구결과를 살펴보았다. 이를 기반으로 미국과 한국의 해사 사이버안보 정책 비교를 통해 한국의 해사 사이버안보 정책 개선 방안을 제안한다.

<표 1> 미국 해사 사이버안보 관련 주요 정책보고서

구분	주요 정책	연도
1	해안경비대 사이버안보 전략	2015
2	국가 해사 사이버안보 강화 계획	2020
3	해안경비대 2021 사이버 전략 전망(Cyber Strategic Outlook)	2021
4	사이버 동향 및 해상환경 보고서	2021

Ⅱ. 선행연구

1. 국제협회 및 기구 해사 사이버안보 정책

해사 사이버안보 정책은 해운산업이 국경을 넘나드는 국제산업이라는 특징으로 인해 국제협회를 주도로 이루어지고 있으며, 이러한 국제협회에는 선사, 화주, 선급 등 민간기업이 참여하고 있다. 또한, UN 회원국들을 중심으로 한 국제기구인 국제해사기구(IMO)가 있다. 발틱국제해사위원회(BIMCO, The Baltic and Intern

ational Maritime Conference)가 2016년에 최초로 선박 사이버 보안 지침을 발표하고, 2017년에 IMO가 해사 사이버 위험관리 지침을 승인하였으며, 이후로 국제선급협회(IACS, International Association of Classification Societies), 디지털컨테이너선사협회(DCSA, Digital Container Shipping Association), 국제정유사해운포럼(OCIMF, Oil Companies International Marine Forum), RIGHTSHIP 등 다양한 국제협회에서 해사 사이버안보 강화를 위해 정책을 제·개정하고 있는 상황이다.

IMO는 UN 산하의 해운과 조선에 관련된 국제적인 문제를 다루기 위한 국제기구로 전 세계 175개국이 회원국으로 참여하고 있으며, 미국과 캐나다를 중심으로 해사 사이버보안에 대한 논의가 진행되고 있다. 2021년 1월부터 IMO 지침 MSC.428(98)에 따라 국제안전관리규약(ISM, International Safety Management) Code 레벨에서 사이버 위험을 관리하도록 하였으며(IMO 2017),[2] 해사 사이버 위험관리 가이드라인을 발표했다. 이에 따라 선주사 및 관리사는 기존 선박 안전관리시스템(SMS, Safety Management Systems)에서 적절한 사이버 위험관리를 의무적으로 수행해야 하며, 사이버 위험에 대한 통합관리 여부를 적합성 인증 시 평가받는다.

사이버 위험관리 가이드라인은 운송 프로세스 및 절차의 디지털화·통합·자동화와 관련하여 직면한 그리고 새로운 위협과 취약점으로부터 운송을 보호하기 위해 개발되었으며, IT 의존도가 높아짐에 따라 해운업계의 사이버 위험관리 필요성이 높아졌음을 강조했다. 이에 미국 국립기술표준원(NIST, National Institute of Standards and Technology)에서 제안한 사이버보안프레임워크(CSF,

2) IMO의 ISM Code는 국제항해에 취항하는 일정 규모 이상의 선박에 모두 적용되며, 기국 정부에 선박 및 선사에 대한 정기적인 검사를 의무화하고 증서를 발급하도록 하였으며, ISM Code를 준수하지 않는 회사 및 선박은 기준미달로 지적되어 항해가 제한됨

Cyber Security Framework)에 따라 사이버 위험관리 프레임워크를 식별-보호-탐지-대응-복구 5가지 단계로 해사 환경에 맞춰 수행하도록 권고하고, 이를 통해 사이버 복원력(resilience)을 구축하도록 했다(IMO 2022).

단계별 활동은 다음과 같다. 식별 단계에서는 사이버 위험관리를 위한 직원의 역할과 책임을 정의하고, 시스템이 중단될 경우 선박 운영에 위험을 초래하는 시스템, 자산, 데이터, 기능을 식별한다. 보호 단계에서는 사고로부터 보호하고, 운송 작업의 연속성을 보장하기 위해 위험 제어 프로세스, 조치, 비상계획을 이행한다. 탐지 단계에서는 적시에 사이버 사고를 탐지하기 위해 필요한 활동을 개발·이행한다. 대응 단계에서는 복원력을 제공하고, 사이버 사고로 인해 손상된 운송 및 서비스 시스템을 복원하기 위한 활동과 계획을 개발·이행한다. 복구단계에서는 사이버 사고의 영향을 받은 운송 작업에 필요한 사이버 시스템을 백업하고 복구하기 위한 조치를 식별한다(IMO 2022).

IACS는 IMO에 기술적인 자문을 제공하고, 국제법규에 대한 해석을 제공하는 기관으로 11개국의 선급이 참여하고 있으며, 한국선급도 그중 하나다. IACS는 2018년에 선박 사이버보안 권고사항을 발표하였으며(O'Dwyer 2018), 2022년에는 선박 및 기자재시스템 사이버 복원력 달성을 위한 통합 요구사항을 발행했다. 이에 따라 2024년 건조되는 선박에는 의무적으로 적용될 예정이다(Maritimecyrpus 2022). 또한, DCSA는 2019년에 선박 사이버 위험관리 업무 지침을 발표하였으며(DCSA 2023), BIMCO의 선박 가이드라인을 NIST CSF에 맞춰 이행하는 방안을 제시하였다.

OCIMF은 2017년부터 탱커운영 및 자체평가(TMSA, Tanker Management and Self Assessment)에 사이버안보 항목을 추가하였으며, 2022년부터는 사이버보안 위험관리를 위한 회사 절차, 선박에 탑재되는 주요 IT/OT 시스템 목록을 요구하고 있다. 화물

의 안전한 운송을 위해 선박 검사를 통해 안정성이 높은 선박을 선정하고 계약하기 위한 단체인 RIGHTSHIP은 2017년 검사질의서(RisQ, Rightship Inspection Ship Questionaire)에 사이버보안 항목을 추가하고 선박 검사에 적용하고 있으며, 2023년 2월에는 RisQ 3.0을 발표하고 사이버안보 관련 검사 문항을 보강한 바 있다(Circulars 2023).

이렇듯 해사 분야 주요 국제협회의 사이버안보 정책은 선박을 중심으로 한 정책 이행 및 표준 준수가 강조되고 있으며 선박 검사를 통해 규제 준수 여부를 평가한다. 최근 선박에서 선사로 규제 및 심사 대상이 확대되고 있으나 해사 분야 사이버안보 이해관계자를 포괄적으로 고려하기에는 한계가 있다.

2. 국내 선행연구

유지운(2022)은 인공지능 기술 발달에 따라 스마트 선박, 자율운항 선박기술이 함께 발전해 가고 있으나 사이버보안을 고려하여 설계되지 않아 잠재적 사이버 위협에 노출되어 있음에 주목했으며, 발생 가능한 사이버 공격 시나리오를 제안했다. 또한, 자율 운행 차량에 비해 자율 운항 선박에 관한 사이버보안 연구가 상대적으로 많이 진행되지 않고 있음을 지적했다. 강남선(2018)은 선박 사이버보안 현황을 파악하고, 미국과 영국의 선박 및 해운 사이버보안 가이드라인을 분석한 결과 가이드라인에서 사이버보안에 대한 인식개선, 내부절차 및 기술, 교육 등을 강조하고 있다고 밝혔다. 그리고 이를 기반으로 기술적 요구사항을 준수하는 방안을 제시하였다. 그러나 정책적 개선 방안은 다루지 않았다. 김영곤(2021)은 최근 증가하고 있는 해운업계에 대한 사이버 공격에 주목하고, 선박에 다양한 통신기술이 적용되고 디지털화되면서 사이버보안 위협이 증가하고 있다고 언급했다. 조용현(2019)은 최근 운항

하고 있는 선박에 IT, OT가 융합되고 있어 보안 요소에 대한 고려가 요구된다고 언급했으며, IMO, BIMCO, OCIMF 등 주요 국제기구에서 발표한 사이버보안 정책 동향을 소개하였다. 그리고 이를 기반으로 선박의 위협을 모델링하고, 사이버보안 요구사항을 제시하였다. 그러나 앞의 4가지 선행연구는 모두 기술적인 요구사항 및 개선 방안에 초점이 맞춰져 있다.

박한선 외(2019)는 해상 사이버보안 체계 강화 방안 연구를 위해 해상 분야 사이버 취약점과 일본, 중국, 미국 등 국내외 사이버보안 관련 법·정책 현황을 분석하여 관리적·물리적·기술적 보안 영역별 위험 요소에 대한 위험도를 식별하고, 이를 기반으로 우리나라 해상 사이버보안 대책 마련을 위해 해상 사이버보안 관리 지침 제정과 법제도 마련, 기술 및 인증 체계 마련, 인력양성 정책 마련을 제안했다. 그러나 당시에는 국가별 해사 분야 사이버안보 정책이 거의 없어 국가사이버안보전략, 전자정부 보호, 개인정보보호 등 포괄적인 사이버안보 정책에 초점을 맞춰 분석하여, 국가별로 주요 기반시설 관점에서 해사 분야 사이버안보 정책을 강화해 나가는 방안에 대해서는 면밀한 검토가 이루어지지 않았다는 한계가 있다.

이에 본 고에서는 미국이 국가안보 차원에서 추진하고 있는 해사 사이버안보 정책과 이를 조직체계를 살펴보고, 한국의 해사 사이버안보 정책 체계와 비교·분석을 통해 국내 해사 사이버안보 강화를 위한 개선 사항을 제안하고자 한다.

Ⅲ. 미국 해사 사이버안보 정책 및 조직

1. 미국 해사 사이버안보 정책

1) 해안경비대 사이버안보 전략(2015)

2015년 해안경비대는 해안경비대 사이버 전략(United States Coast Guard Cyber Strategy)을 발표하였다. 동 전략에 따르면, 해안경비대는 2013년 해안경비대 내 사이버사령부(Cyber Command)를 설립했고, 사이버사령부는 사이버공간 방어, 작전 수행, 인프라 보호라는 3대 임무를 갖는다. 동 전략은 2023년까지 사이버사령부가 수행할 주요 임무 영역을 사이버공간 방어, 운영 보장 및 인프라 보호 3개로 제시하고 있다(The Coast Guard 2015).

첫째, 해안경비대는 해안경비대 전반적인 임무 성공을 위해 해안경비대 사이버사령부의 IT 시스템과 네트워크를 보호하여; 정보 인프라를 보호하고 보다 탄력적인 해안경비대 네트워크를 구축할 책임을 갖고 있다. 이는 시스템 및 네트워크 식별 및 강화(위험관리, 시스템 계획 및 획득 시 사이버보안 고려), 사이버 위협 이해 및 대응(사이버 전문인력 양성, 사이버 정보수집의 효율적이고 효과적인 시행 촉진, 정보 기반 사이버공간 방어), 운영 측면의 회복성 강화(임무 중심의 사이버공간 작전 보장, 해양경비대 문화에 사이버보안 포섭) 활동을 시행한다.

둘째, 사이버 영역 내에서 효과적으로 운영하기 위해 해안경비대는 다양한 사이버 역량과 권한을 개발하고 활용한다. 해안경비대 정보 통신 네트워크 및 시스템 내외부 사이버공간 작전은 적을 탐지, 억제, 무력화 및 물리치는 데 도움이 될 수 있으므로, 강력

한 정보·법 집행·해사 및 군사 사이버 프로그램을 활용하여 해안경비대 작전의 효율성을 높이고 중요한 해사 인프라를 대상으로 하는 악의적인 활동을 억제, 방지 및 대응한다. 이를 위해 사이버 공간 작전을 임무 계획 및 시행에 포함(사이버 인식 통합, 역량 강화)시키고, 해안경비대 전 임무 수행 시 사이버 역량 활용(사이버공간 작전 지원을 위한 정보활동 강화, 작전 수행을 위한 사이버 역량 활용 강화) 방안을 마련·시행한다.

셋째, 사이버 시스템을 통해 MTS는 전례 없는 속도와 효율성으로 작동할 수 있고 동일한 사이버 시스템도 잠재적인 취약점을 생성할 수 있기에, 해상 주요 인프라와 MTS는 경제, 국가안보 및 국방에 필수적으로 보호해야 할 대상이 된다. 해상 운송 부문 특정 기관으로서 해안경비대는 공격, 사고 및 재난으로부터 해사 주요 기반시설을 보호하는 데 필요한 노력을 통합 주도한다. 이를 위해 위험 평가, 사이버 위험에 대한 인식 제고 및 관리 촉진(항만 전반의 사이버보안 위험 평가 툴 및 방법론 개선, 사이버보안 정보공유 개선), 예방 MTS 내 사이버보안 취약점 감소(선박 및 시설의 사이버 취약점 경감, 교육 및 훈련에 사이버보안 포함) 활동을 시행한다.

동 문서에서 제시하고 있는 해안경비대 사이버사령부의 임무는 자체 네트워크 및 인프라 보호, 사이버공간을 수단으로써 활용한 작전 시행 및 법 집행 역량 확보, 해상 주요 인프라 및 MTS 위험 평가 및 예방 활동 시행으로 요약할 수 있다.

2) 국가 해사 사이버안보 강화 계획(2020)

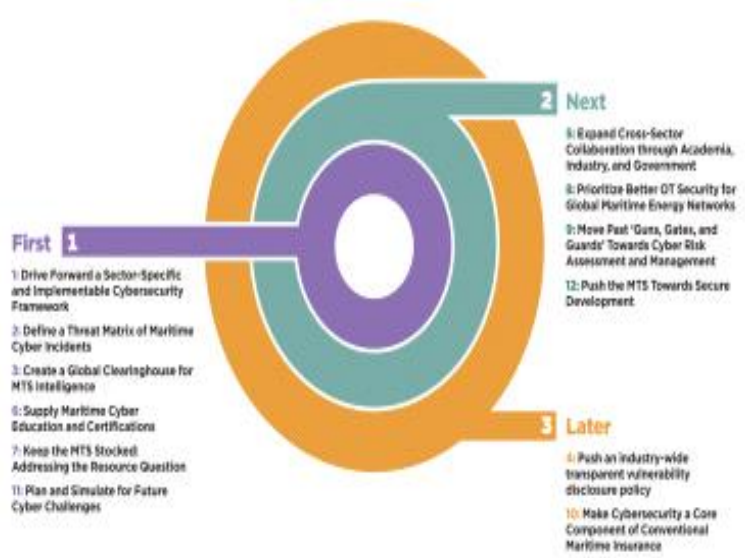
<표 2> 국가 해사 사이버보안 강화 계획 주요 내용

구분	주요 조치
위험 및 표준	PA1. 유관 기관 책임 및 역할 재식별 - NSC 중심의 정책 조정 프로세스를 통해 법제상 격차 식별, MTS 사이버보안 표준을 위한 책임과 역할 효율성 저하 요소 식별
	PA2. 해사 사이버보안 표준 및 모범사례 정보제공을 위한 위험 모델링 방법 개발 - 해안경비대는 해사 사이버보안 이해당사자에게 제공된 사이버보안 보고 가이드라인(2016, 2020) 구체화 및 분석 - 해사 사이버 사고 보고 사례 수집을 통해 공격 경향과 공격 요소 등을 식별하고, 상황 인식 제고를 통한 해사 사이버 위험 감소 추진 - NIST 중심으로 국내외 이해당사자들의 의견을 수렴하여 국제 항만 OT 위험 프레임워크를 개발하고 국제적인 사용 촉진 추진
	PA3. 항만서비스 계약 및 임대 시 사이버보안 요구사항 강조 - 연방기관 및 GSA는 해사 분야 기반시설 관련 계약 체결 시 적용 가능한 강제성을 띠는 요구조건 개발
	PA4. 주요 선박 및 항만 시스템의 사이버보안 위험 식별, 우선순위 선정, 경감, 조사를 위한 절차 개발 - 국방부 및 국토안보부는 항만 사이버보안 평가 프레임워크 개발 - 국토안보부는 해사 주요 기반시설 보호 자금지원 및 프로젝트 시행 - 해사 수사 시 활용 가능한 사이버 포렌직 프로세스 구축
정보 공유	PA1. 해상 산업계와 정보공유 강화 - 국내외 이해관계자들과의 협력 강화 - 해사 사이버보안 사고 신고 및 처리를 위한 정책 및 절차 개발
	PA2. 적절한 비정부단체와의 정보공유 강화 - 필요한 국제사회 및 기관과의 정보공유 확대
	PA3. 해사 사이버보안 정보수집 우선순위 설정 - 해사 사이버안보를 위협하는 적에 대한 평가 및 위험 모델링이 가능한 관련 정보공유 확대, 이를 위한 정보수집 및 요구사항 우선순위 설정
인력 양성	PA1. 항만 및 선박 시스템 특화 전문인력 양성 - 관련 커리어패스 개발, 훈련 및 교육 기준 개발 등
	PA2. 인력양성을 위한 민관협력 강화
	PA3. 양성된 인력의 적극적 활용 방안 모색

출처: 저자 작성

미국 정부는 2020년 12월에 “국가 해사 사이버안보 강화 계획 : 항만 안보를 위한 국가 계획(NATIONAL MARITIME CYBERS ECURITY PLAN : To The National Strategy for Maritime Security)을 발표하여 해사 부문의 사이버보안 부족 문제를 해결하고자 했다(The White House 2020b). 미국은 국가사이버전략(National Cyber Strategy of the United State of America 2018)에서 미국 경제에 있어 해상 무역 및 운송의 중요성을 강조하고 해사 사이버보안 향상을 위한 노력을 추진할 계획이 명시되어 있으며, 전략이행계획(2019)에서도 이를 위한 활동을 담고 있다. 동 전략에 따르면 미 정부는 국가사이버전략(2018) 이행계획에 따라 해사 부문 위험 완화를 위해 공공 및 민간부문 전체에서 과제를 추진하며, 해사 분야 사이버보안 실태를 검토하고, 해사 OT 부문의 전반적인 사이버보안 향상하고자 한다. 동 계획은 구현 계획이라기보다는 로드맵에 가깝고(Kollars et al. 2021), 복잡한 MTS 전반에 걸쳐 사이버안보 수준을 향상하기 위한 노력을 지속 및 확장하여 전체적인 MTS 내 사이버보안 태세를 개선하고자 한다. 동 계획 시행 조치를 도식화하면 아래 <그림 1>과 같다. 국가 해사 사이버보안 강화 계획 주요 내용은 <표 2>에서 정리하였다.

<그림 1> 국가 해사 사이버보안 강화 계획 단계별 임무



출처: Loomis et al. 2021

2021년 발표된 상기 전략 이전에 미 백악관이 의견 수렴을 위해 일부 제한 공개했던 버전에서는 해사 분야 CERT 설립, NIST의 관련 지침 등 제·개정, 국제협력 강화를 골자로 하고 있다(The White House 2020a). 초안은 해사 부문 사이버보안 환경은 다른 주요 기반시설의 보안에 비해 적절한 재원이 공급되지 않아 악성 사이버 활동에 취약하며, 관련 표준이나 감독기관이 부재하여 사이버 공격이 증가하고 피해가 확대되고 있다는 점을 문제로 식별하고 있다. 제안하는 활동은 1) 국립표준기술연구소 지침 및 가이드 배포, 2) 정보공유 및 협력, 3) 항만 장비 취약점 평가, 4) 해안경비대 인력 확충의 4가지이다.

첫째, NIST가 미국 정부 기관, 국제파트너 및 업계 이해관계자와 협력하여 해사 OT 부문에 NIST 사이버보안 프레임워크를 적

용하고, 관련 지침 및 가이드를 배포하도록 한다. NIST 문서는 위험 평가를 위한 기준이 될 수 있으며, 해안경비대는 이를 기반으로 해상 운송시스템과 항만에 적합한 위험관리 지원 제공이 가능하다. 둘째, 해사 환경에 대한 사이버 위협과 취약성에 대하여 글로벌 이해관계자 간 신속한 정보공유를 위한 해사정보공유센터 또는 정보공유 분석조직 창설을 장려하고 있다. 이를 통해 해사 부문 사이버보안 취약성과 위험에 대한 글로벌 인식을 제고하고자 한다.

셋째, 국토안보부(DHS, Department Homeland Security)와 미국에너지부 국립연구원(Department of Energy and the National Laboratories)과 협력하여 주요 항만 기술에 대한 위험 평가와 중요한 OT 시스템의 취약성 식별 및 평가를 수행하고, IT 시스템과 OT 시스템을 식별하고, 모니터링되지 않는 장비를 식별하고자 한다. 넷째, 해안경비대의 사이버 인력을 증강하고, 역할 및 책임을 검토하여 해안경비대에 해사 부문 사이버보안 책임을 부여하고자 한다. 이를 통해 해안경비대가 책임 이행을 위한 인력구축 및 자원확보를 할 수 있도록 한다.

2개 버전의 문서 모두 해사 분야 사이버보안 활동 강화를 적극적으로 추진할 것으로 요구하고 있는데, 이는 특히 신기술의 적용과 적성 국가 후원 및 직접 지시를 받은 테러 혹은 지재권 탈취 목적의 악의적 행위가 늘어나면서 더욱 강화된 것으로 보인다. 2020년 공개된 버전의 계획 문서가 로드맵 제시에 가까운 문서임에도 불구하고, 전략 및 정책 수준의 보완, 유관 기관의 업무수행 근거 재정비, 표준 및 모범사례 공유, 위험 모델링 방법론 제시, 제3자와의 계약 시 사이버보안 측면의 고려, 위험 대응을 위한 절차 마련, 정보공유 및 인력양성 추진 등 전방위적인 역량 강화에 적극적임을 알 수 있다.

3) 해안경비대 2021 사이버 전략 전망(Cyber Strategic Outlook)

2021년 해안경비대는 사이버공간 보호 및 작전을 위한 새로운 비전 문서인 “미국 해안경비대의 사이버 전략 전망(Cyber Strategic Outlook) : 사이버공간 보호 및 작전을 위한 비전(The United States Coast Guard’s VISION To Protect and Operate in Cyberspace)”을 발표했다(The Coast Guard 2021b).

앞에서 살펴본 2015년 미국 해안경비대의 사이버 전략은 사이버공간을 미국 해안경비대의 새로운 작전 영역으로 설정했다. 2021 사이버 전략 전망은 2020년 발표된 정부 차원의 계획 문서와 함께, 2015년 해안경비대 사이버사령부 전략문서의 토대를 재확인하고 동일한 정신, 입증된 교리 및 운영 개념, 그리고 기존의 다른 작전 영역에서의 경험을 사이버공간에서 그리고 사이버공간을 통한 운영에 적용하고 있다. 미국 해안경비대 네트워크 및 정보의 탈취, 해사 주요 기반시설에 대한 공격, 네트워크 악용 및 허위정보 활동으로 미국의 민주적 절차를 약화시키는 적대적 노력을 포함한 일련의 사건들로 사이버공간 보호 필요성은 전례 없이 강화되고 있다. 이에 DHS, 국방부(DOD, Department of Defense), 정부 파트너, 외국 동맹국 및 해양 산업과 긴밀히 협력하여 사이버공간에서, 그리고 사이버공간을 통해 전달되는 위협으로부터 MTS를 보호하는 것을 그 목적으로 한다.

동 비전 문서에 따르면 해안경비대 사이버사령부는 이 전망에 대응하는 미국 해안경비대 조치는 네 가지 노력으로 구성된다.

- 기관의 임무 플랫폼 방어·운영 : 안전하고 탄력적인 정보 기술 및 운영 기술 네트워크 확보를 통해 해안경비대 사이버사령부의 모든 임무 지원, 모든 미국 해안경비대 기술을 포함하여 국방부 정보 네트워크(DODIN)의 일부인 미국 해안경비대 EMP(Enterprise Mission Platform)를 방어하고 운영하여 적의

간섭과 침해 대응

- 해상 운송 시스템 보호 : 미국 해안경비대는 MTS에 대한 사이버 위험을 식별하고 관리하기 위해 예방 및 대응 활동에 프레임워크, 표준 및 모범사례 사용, 사이버 위험관리, 책임, 통합 대응 계획의 개발 및 구현을 촉진하여 거버넌스 주도
- 주요 인프라 보호 : 미국 해안경비대 정보국은 사이버 위험 식별 및 완화, MTS를 위험에 빠뜨리는 사이버 행위자 및 위해 그룹 능력에 대한 특성화 및 인식 제공, 위협 집단 및 개인의 전문 지식·평가 등 시행, 이를 통한 선제적 사고 대응
- 사이버공간에서 그리고 사이버공간을 통해 작전 수행 : 선진화된 사이버공간에서의 다양한 역량을 투사함으로써 해안경비대 사이버사령부의 임무 수행 지원, 해안경비대는 전통적인 임무에 사이버 계획을 포함하고 임무 성공을 위해 서비스의 고유한 권한, 능력 및 인력을 결합하는 사이버공간 작전 실행, 범죄 행위자 및 적들에게 유효한 비용 부과 유도하기 위한 법·집행 활동 및 군사 활동 지원

기본적으로 동 문서는 2015년 발표된 해안경비대 사이버 전략 문서의 후속 문서로 보아야 한다. 다만 2015년 문서에서 정한 3대 임무를 향후 10년 동안 지속할 것으로 명시하고 있기에, 전략이라는 명칭을 쓰지 않고 전략 전망 보고서 형태로 발표한 것으로 추측된다.

해안경비대에서 발표한 두 문서에서 해안경비대 사이버사령부의 임무는 크게 달라진 것으로 보이지는 않는다. 다만, 2021년 문서 발표 이전 러시아의 크리미아반도 합병, 2016년 미 대선 개입, 소프트웨어 공급망 보안 이슈 발생 등에 따라 사이버공간을 수단으로 혹은 직접적 목적으로 발생한 사이버 공격 행위에 대한 해사 분야에서의 안보 확보를 위한 노력을 강조하고 있다는 점에서 약간의 발전이 있었다고 볼 수 있다. 또한, 주요 보호 대상인 인프라

에 MTS와 이를 통한 업무 전반을 식별하고, 위협요인에 대한 객관적이고 전문적인 평가 및 대응을 명시하고 있다는 점에서 업무가 전반적으로 성숙해 가고 있는 것으로 판단할 수 있다. 이하에서 설명하는 2021년 사이버 동향 및 해양 환경 보고서는 보다 심층적으로 사이버 분야 위험과 해안경비대 사이버사령부의 임무를 보여주고 있다.

4) 2021 사이버 동향 및 해양 환경 보고서

2021년 해안경비대 사이버사령부는 사이버 동향 및 해양 환경 보고서(2021 Cyber Trends and Insights in the Marine Environment)를 발표했다. 동 보고서에 따르면 MTS 대상 공개된 취약점 제거, 내부적으로 악용 가능한 취약점 제거 및 소셜 엔지니어링상 취약점에 대해 조치 결과를 요약하고 있다. 이들은 취약점 제거, 패스워드 정책 검토, 다중 인증 체계 점검, 계정 관리, 네트워크 침입 탐지, 네트워크 분리, 취약점 스캐닝, 소프트웨어 업데이트, 사용자 훈련 등 다양한 분야를 점검하고 이에 대한 조치 시행 및 개선 활동을 수행했다(The Coast Guard 2021a). 이는 동 부서가 해사 사이버보안 강화를 위한 조치 결과를 공유하고, 동시에 이해당사자들에게 관련 정보를 제공함으로써 교육자료로써도 활용되고 있다.

특히, 범죄자의 랜섬웨어 사용, 적대국의 전술역량 향상, 피싱 공격 증대 등 환경 변화에 대응 등 해안경비대 사이버사령부의 임무는 범위나 영향력 측면에서 훨씬 광범위하다. 해안경비대 사이버사령부에 따르면, 항만에서의 위험은 시설 접근 제한, 터미널 본부 데이터 관리, 랜섬웨어 대응, 운영시스템 보호, 위치기반시스템 보호, 선박 보안 등 다양한 분야가 포함되어 있다.

동 문서는 해안경비대 사이버사령부가 인식하는 해사 분야 사이

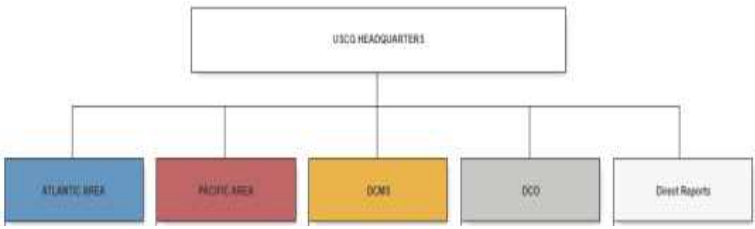
버 위험 인식을 구체적으로 보여준다는 점에서 큰 의의를 가진다. 동 인식은 2015년과 2021년 제시한 전략문서에서 식별한 임무 내용을 구체적으로 설명함으로써 앞으로 우리의 임무 설정 시 크게 참고할 수 있을 것이다. 또한, 동 보고서는 실제 기관 자체의 사이버보안 향상을 위한 다양한 노력 외에 유관 기관 및 민간업체 등 해사 시설을 사용하고 시스템상 연계될 수 있는 모든 기관을 대상으로 취약점 제거, 적절한 사이버보안 정책 사용 유도 등 긍정적 활동을 시행함으로써 적극적으로 사이버보안 위험 요소를 최소화하는 노력을 했다는 점에서 고무적이다.

2. 미국 해사 사이버안보 조직체계 및 기능

1) 해안경비대 조직체계

해안경비대의 조직도는 아래와 같다. 본 논문에서 살펴보고 있는 사이버 분야 임무는 사이버사령부가 수행하는 것으로 확인되며, 이는 DCO(Deputy Commandant for Operations) 산하에 존재한다.

<그림 2> 미 해안경비대 조직도



출처: 미국 해안경비대(The Coast Guard) 홈페이지
(최종접속일 : 2022년 11월 22일) https://www.uscg.mil/Units/Organization/

2) 해안경비대 사이버사령부 조직체계

사이버공간의 보안을 보장하고 적보다 우위를 유지하며 국가의 중요한 해사 인프라를 보호한다는 비전을 가진 사이버사령부(CG-791 조직)의 임무는 아래와 같다.

- 해안경비대 사이버공간 방어: 해안경비대 기업 임무 플랫폼을 운영 및 조종하여 DoD 정보 네트워크(DODIN, DOD Information Network)의[3] 우리 부분을 공격적으로 방어하면서 모든 영역에서 해안경비대 임무 실행을 보장
- 해안경비대 작전 활성화: 사이버공간에서 그리고 사이버공간을 통해 해상, 공중, 지상 및 우주에서 해안경비대 작전 활성화
- MTS 보호: 사이버공간에서, 사이버공간을 통해 효과와 기능을 제공하여 해사 주요 기반시설 보호

이는 2015년과 2021년 전략문서에서 제시한 임무 영역을 명확히 구현하였다. 해안경비대의 사이버사령부는 크게 정보, 작전, 평가 및 인가, 작전 지원의 4개 부서로 구성되어 있고 해당 부서별 임무는 아래와 같다.

3) 국방부 정보네트워크(DODIN)은 전 세계적으로 상호 연결된 국방부의 전자 정보 기능 및 관련 프로세스의 집합을 말하며, 통신 및 컴퓨팅 시스템 및 서비스, 소프트웨어, 데이터, 보안 서비스 및 기타 관련 서비스 및 국가보안시스템을 포함 (https://csrc.nist.gov/glossary/term/department_of_defense_information_networks)

(1) 사이버 인텔리전스(CGCC-2)

CGCYBER 인텔리전스 부서인 CGCC-2는 CGCYBER 운영 부서(CGCC-3), CGCYBER/CGCYBER 차장, 기획 및 정책 부서(CGCC-5)에 내부적으로 인텔리전스 지원을 제공한다. CGCC-2는 또한 해안경비대 정보부 구성 요소, 정보공동체(Intelligence Community, IC) 구성 요소, 그리고 요청에 따라 국토안보부(DHS), 국방부(DOD), 해안경비대 내의 리더십과 협력한다.

(2) 운영 부서(CGCC-3)

CG CYBER 운영 부서는 CGCC-33 네트워크 운영 및 보안 센터와 CGCC-35 미래 운영 부서로 구성된다. CGCC-3은 또한 사이버 보호 팀, 사이버보안 운영 센터 및 해사 사이버 준비 부서의 상위 사령부이기도 하다.

CGCC-3의 임무에는 사이버 보호 팀(CPT), 사이버보안 운영 센터(CSOC) 및 해사 사이버 준비국(MCRB)이 포함된다. CPT는 해상 운송 시스템(MTS)에 사이버보안 서비스를 제공하는 책임을 맡은 해안경비대의 배치 가능한 부대이다. MCRB는 상업용 해상 운송 커뮤니티의 사이버보안 담당이다.

(3) 평가 및 승인(CGCC-AA)

CGCC-AA는 해안경비대가 해안경비대(CG) 정보 기술(IT)에 대한 평가 및 승인을 수행 방법을 표준화하기 위해 모든 A&A 기능의 프로세스를 수립한다.

(4) 운영 지원

CG CYBER 운영 지원 부서는 전반적인 지원 및 관리를 담당한다. 조직 내 인력과 연간 예산을 관리하고, 조달, 자원 할당 및 배치를 담당하며, 통관 및 개인 보안 조치 등 조직 내 보안관리를 수행한다. 그리고 교육 및 연습 방안을 개발하고, 일정을 수립한다.

해안경비대 사이버사령부의 조직체계와 업무 범위를 살펴보면 다음과 같은 점을 알 수 있다. 첫째, 미국은 주요 기반시설 보호를 위한 영역별 사이버보안 임무를 별도 담당 기관을 정해 근거를 명확히 하고 있다. 이는 유관 기관 간 업무중복 및 관할권 분쟁 등이 발생할 가능성을 사전 차단하고, 업무의 효과적이고 효율적인 시행을 가능하게 한다.

둘째, 정보통신기술을 활용한 사이버 작전을 해당 기관의 임무 수행 범위에 긍정적으로 고려하고 있으며, 동시에 해당 기관의 자원을 활용해 사이버 작전을 수행하는데도 전적으로 지원하고 있다는 점을 알 수 있다. 이는 사이버 기술이 수단 및 도구적 의미로써도 역할을 갖고, 보호 대상으로써도 그 역할을 갖는 점을 보여준다. 앞으로 우리나라의 해사 사이버안보 업무 범위 설정에도 양측면을 모두 고려해야 할 것이다.

셋째, 관련 정보의 수집 및 활용, 공유에 있어 범위를 확장하였으며, 해사 시설을 사용하는 민간기업에도 정보를 제공하고, 사이버보안 위협 요소 제거에 도움을 줌으로써 실질적인 사이버보안 수준 향상 및 안보 역량 강화에 직접적으로 지원하고 있다는 점이다. 최근 국가정보원이 민간 방산업체를 대상으로 위협 정보를 적극적으로 공유하는 등 우리나라 타 부처에서도 정보공유 대상을 확대하고 있는바, 해상 항만 분야 사이버안보 수준 제고 시 민간

기업 대상 정보 및 기술 서비스 제공을 적극적이고 확장적으로 고려할 필요가 있다.

넷째, 사이버사령부 내 평가 및 인가 부서가 별도로 존재하고, 이를 조달 체계와 연계시키는 노력이 보이는바, 사용되는 정보시스템의 무결성 및 기밀성 평가 및 인증, 통합 보안 시스템 구축, 사이버보안 인증 기술, 통합 소프트웨어의 적합성 인증 기술, 무결성 검증 기술, 시험 평가 방안 기술, 보안 내재화 등 다방면으로 사이버보안 수준 향상을 지원할 수 있는 업무 영역을 발굴하고 정착시켜야 할 것이다.

3. 소결

미국은 2010년대 초부터 해사 사이버안보 강화 노력을 시작했다. 국가가 안전보장을 위한 영역으로 사이버가 그 중요성을 인지하고 제5의 전장으로 사이버공간을 식별한 2010년 즈음을 기점으로, 항만의 사이버보안 강화를 위한 미국의 활동은 본격적으로 시작됐다. 2013년, 해안경비대(Coast Guard)가 사이버사령부를 설립한 것을 기점으로 2015년, 2020년, 2021년 주요 정책문서를 발표함으로써 체계적으로 해사 사이버안보 활동을 수행 중인 것으로 판단된다.

특히, 항만시설 및 선박 대상 랜섬웨어 공격 등 위협 방식 변화에 따라, 항만시설 접근 통제, 터미널 본부 내 혹은 선박 등과의 데이터 관리, 랜섬웨어 대응, 운영시스템 보호, 위치기반시스템 보호, 선박 보안 등 다양한 분야를 모두 업무 범위에 포함시키고 있음을 확인할 수 있었다. 해안경비대 내 사이버사령부를 두고, 휘하에 정보, 작전 및 평가 등의 업무를 수행하게 함으로써 이들 활동을 뒷받침하고 있다.

Ⅳ. 한국 해사 사이버안보 정책 및 조직

1. 한국 해사 사이버안보 정책

한국은 스마트 선박, 스마트 항만 등 해사 분야에서 IoT, AI 등 신기술을 적극적으로 도입하고 디지털 전환을 촉진하여, 이를 통해 국가 물류 네트워크를 효율화하고, 속도를 향상하고자 한다. 2022년 디지털 전략에 따르면 정부는 2029년까지 스마트 항만을 완성할 계획이며, 이를 위해 디지털 트윈[4] 기술 기반으로 항만 자동화 테스트베드를 구축하고, 스마트 보안 심사 도입 및 데이터 통합, 기관 간 공유 활성화를 통해 항만 보안을 강화하기 위한 항만보안 종합정보 플랫폼을 구축할 계획이다. 또한, AI 기술을 활용한 스마트 물류 시설 도입을 추진한다. 그리고 초고속 해상통신망 구축을 통해 선박 간 통신체계를 구축하고, 2025년까지 선원 없이 원격제어가 가능한 수준의 선박 자율운항 기술을 개발하며, 이를 위한 법·제도적 기반을 마련한다. 해상안전을 위해서는 디지털 교통망 지도 구축, 빅데이터 기반 안전 정보 제공, 실시간 모니터링을 통해 디지털 해상교통망을 구축할 계획이다(관계부처 합동 2022).

이렇듯 해사 분야에 디지털 전환은 가속화되고 있지만, 비용 절감, 효율 향상에 초점이 맞춰져 해사 분야 사이버안보 정책 및 기술개발은 더딘 상황이다. 선급을 중심으로 국제협회에서 주도하는 선박에 대한 규제 및 표준을 적용하는 방안 마련 등에 국한되어 있다. 4장에서는 한국의 해사 관련 법령에서 사이버안보 관련 내

4) 가상공간에 현실 공간 및 사물의 쌍둥이(Twin)를 구현하고 시뮬레이션을 통해 현실 분석 및 예측을 가능하게 하는 기술을 말함

용을 분석하고, 최근 발표된 「해사 사이버안전 관리지침」을 살펴본다. 또한, 한국선급의 IMO 및 국제협회의 규제 및 표준 적용을 위한 지침 및 방안들을 살펴본다.

1) 관련 법령

한국은 해사 사이버안보와 관련하여 「주요정보통신기반보호법」, 「국가사이버안전관리규정」, 「사이버안보 업무규정」에 따라 항만시설 등이 주요 기반시설로 지정되어 자체적인 보안관리를 시행하고 있다. 해양수산부는 위의 3가지 법률에 기반하여 해양수산 사이버안전센터(OCSC, Oceans & Fishers Cyber Security Center) 운영 규정을 제정하고 설립·운영하고 있으며, 정보통신기반시설의 취약점 분석·평가, 보호 대책 수립·지원, 사이버침해 사고 대응, 조사 및 복구 지원, 보안관제 등의 임무를 수행한다. 그러나 주요정보통신기반보호법 및 국가사이버안전관리규정은 주요 정보통신기반시설과 국가정보통신망의 보호를 목적으로 하고, 해사 분야 및 선박 등의 안전관리에 특화된 별도의 규정이 없어 국제성이 강한 해상환경에 적합하지 않다는 문제점이 있다.

또한, 해사안전법, 국제항해 그리고 선박 및 항만시설의 보안에 관한 법률에 따라 선박 및 항만시설에 국제 규제 이행 및 표준을 적용하고 있다. 해사안전법은 선박의 안전운항을 위한 안전관리 체계를 확립하여 해사 안전 증진과 선박의 원활한 교통에 이바지가 목적이고[5], 국제항해선박 및 항만시설의 보안에 관한 법률은 국제항해 관련 보안 위협 방지를 목적으로 하여 물리적 보안에 대한 심사·보호 조치는 강조하고 있으나, 사이버 관련에서는 별도의 명시된 규정이 없다는 한계가 있다.

5) 해사안전법 제1조(목적)

2) 한국선급, 해상 사이버보안 시스템 지침(2021)

한국선급은 국내에서 유일한 국제선박검사기관으로 국제 해사법규 및 협약에 따라 정부를 대행하여 검사를 수행하고 있다. 한국선급은 현조선, 신조선, 기자재 및 시스템 체계로 구분하여 사이버보안 정책을 추진 중이며 현조선의 경우 선박을 계속 운용하는 상황이기에 시스템 변화가 어려워, 정책 가이드라인 제공, 선원 교육, 운영상의 위험 식별 등을 지원한다. 신조선은 다양한 사이버보안 시스템 적용, 테스트가 가능하여 이를 진행하고 있으며, 내부 기자재 및 시스템의 경우 조선소 차원에서 모두 보안을 적용하기는 어려워 별도로 사이버보안을 지침을 마련하여 적용하도록 하고 있다(임정규 2020).

한국선급은 발틱국제해운협회(BIMCO)에서 2016년 최초로 선박 사이버보안 가이드라인을 발간한 데 이어 2017년 IMO가 MSC.428(98) 해사 사이버위험 관리 가이드라인을 제정하면서, 이에 대한 대응을 위해 선박 및 회사의 IT와 OT 기술·서비스가 내외부적 사이버위협으로부터 강화하도록 2017 해상 사이버보안 가이드라인을 발간하였다. 이후 2020년에는 해상 사이버보안 시스템 지침을 발간하고, 지속적으로 개정·보완하고 있다.

해상 사이버보안 시스템 지침은 국제 선박 및 항만시설 보안 규칙(ISPS Code, International Ship and Port Facility Code)과 국제안전관리규약(ISM Code, International Safety Management Code) 등 국제협약 이행에 대한 인증심사를 수행하고 기준을 제공한다(한국선급 2021b). 동 지침은 회사 및 선박의 사이버보안 시스템에 대한 선급검사 관련 요건을 포함하고 있으며, 선주 및 조선소에 대한 사이버보안 인증 신청을 의무화하고 있다. 이를 위해 회사 사이버보안 시스템과 선박 사이버보안 시스템에 대한 요건 및 조직 절차를 각각 규정하고, 필수 요건을 제시하였다. 지침은

사이버보안 적합성을 3단계로 구분하고, 단계별로 관련 요건을 갖추도록 하고 있으며, 1단계에서는 기본적인 사이버보안 정책·지침 마련, 인력관리 및 교육훈련 방안, 위험관리 계획 및 평가, 데이터 중요도 분류, 접근권한 관리, 사고 대응 및 복구 정책 수립, 암호화, 원격접속 보안, 외부자 보안 방안 등을 갖추도록 하고 있다. 2단계에서는 침해사고 분석 및 대응 방안 마련, 침투테스트, 이상징후 모니터링 등을 수행하고 결과를 제출하도록 하고 있다. 3단계에서는 사이버보안 심사 정책 관리, 협의체 구성, 소프트웨어 소스코드 보안 요구사항 마련 등을 요구한다(한국선급 2021b).

2022년에는 지침에서 사이버보안 시스템 수준 및 요건을 선주의 요청에서 회사나 선주의 요청으로 변경하고, 단순히 사이버보안 시스템이 아닌 사이버보안 관리체계를 갖출 수 있도록 수정하였다.

3) 한국선급, 해사 사이버 인증 서비스

한국선급은 선박 도면, 설비, 각종 규격에 대한 검사·인증 업무를 담당하고 있으며 사이버보안 시스템에 대한 인증 업무도 포함한다. 한국선급의 홈페이지에 따르면 해사 사이버 인증 서비스는 해운회사, 선박, 제품 등 해사 산업 관련된 모든 영역에서 사이버 위협으로부터 안전한지를 검사 및 인증하는 서비스이다.

크게 선박 및 회사 사이버보안 인증, 사이버보안 형식 승인, 소프트웨어 적합성 인증 3가지로 나뉜다. 선박 및 회사 사이버보안 인증은 IMO 사이버 위험관리 권고 이행을 위해 사이버보안 국제표준(ISO 27001, NIST, IEC 62443 등)뿐만 아니라 IMO, BIMCO, DCSA 등 국제협회 및 기구에서 권고하는 사이버 위험관리체계를 기반으로 설계되어 사이버 위협 식별, 위험관리를 지원한다. 사이버보안 형식 승인은 선박에 탑재되는 제품(시스템)에 대한 사

이버보안 형식을 승인하는 것으로 사이버보안 기본요소인 무결성, 가용성, 기밀성 관점에서 인증한다. 소프트웨어 적합성 인증은 선박에 탑재되는 제품(소프트웨어)의 잠재적 결함을 검증하는 서비스이다.[6)]

4) 해사 사이버안전 관리지침(2023)

해양수산부는 2023년 4월 선박의 사이버 안전과 보안에 대한 정부와 민간의 역할을 규정한 「해사 사이버안전 관리지침」을 고시로 제정하고 시행계획을 밝혔다. 지침은 선박의 사이버 안전과 보안을 확보하고 해운선사를 지원하기 위한 정부의 역할과 해운선사가 사이버안전 관리체계를 구축할 때 고려해야 하는 사항을 포함한 권고적 성격의 규정이다(이경성 2023).

지침에 따르면 정부는 해사 사이버안전 대책 수립·시행하고 해사 사이버안전 진단 및 실태 평가를 실시할 수 있다. 또한, 교육·훈련, 기관 간 협력체계를 구축한다. 해운선사에 사이버안전 관리조직 구성 시 고려해야 할 수준, 자산관리 및 업무분담 방안, 사이버안전 위험성 평가 시 고려 사항, 보호·탐지·대응·복구·조치 등 NIST 사이버보안 체계에 따른 보호조치 수립 시 고려 사항 등을 제시하였다. 다만, 해운선사는 사이버 공격 또는 위협 발생 시 피해 최소화 조치를 수행 후 해양수산부로 사고를 지체 없이 통보하도록 하고, 해양수산부는 관련 부서와 기관에 정보를 공유하고, 사고 대응, 복구 지원, 사고원인 조사 등을 지원할 수 있도록 하였다. 또한, 활용 가능한 국제표준 및 산업표준 목록을 제시하여 선박소유자가 참고할 수 있도록 하였다(해양수산부 2023). 그러나 지침이 권고적 성격에 그쳐 선박소유자는 해사 사이버안전 위험성

6) 한국선급. 2023. “인증서비스”. https://www.krs.co.kr/kor/Content/CF_View.aspx?MRID=847&URID=153 (검색일: 2023.11.20.)

을 평가하고, 사이버안전 관리체계를 구축해야 할 의무가 없다는 한계가 있다.

2. 한국 해사 사이버안보 조직체계 및 기능

한국의 해사 분야 사이버안보 조직체계를 주요 정보통신기반시설 분야, 국방 분야, 수사 분야 관점에서 바라보면 <그림 3>과 같다. 국가정보원이 관계 중앙행정기관인 해양수산부와 협력하여 주요 기반시설 지정, 보호 대책 수립, 취약점 분석을 수행하며, 해양수산부는 산하에 해양수산 사이버안전센터를 두고 참여 기관의 보안관제, 사고 대응, 정보공유 업무를 수행한다. 그러나 해양수산 사이버안전센터도 별도의 전문성을 보유하지 못하고, 보안관제 용역업체에 위탁 운영되는 실정이다.

한국선급은 해양수산부가 설립을 허가한 비영리법인으로 한국정부 및 각국 정부로부터 권한을 위임받아 선박 및 선사에 대한 검사 업무를 수행하며, 해당 업무에 사이버안보를 포함한다. 다만 국제협회 및 기구에서 권고하는 규제 및 표준을 중심으로 검사 및 인증을 수행하고, 선박 및 선사에만 초점이 맞춰져 있는 상황이다.

<그림 3> 한국의 해사 분야 사이버안보 조직체계

출처: 저자 작성

해군은 해군 전장 환경을 고려한 함정 및 무기체계 사이버안보 강화 임무 및 사이버 작전 수행 업무를 보유하고 있다. 2015년에 국방망, 인터넷망 관제, 취약점 점검, 침해사고 조사·분석 등 해군 자체 사이버보안 강화를 위한 목적으로 설립된 사이버방호센터를 2019년 대우조선해양 사고 이후 해사 안보를 위한 사이버 작전 대응태세 확립을 위해 사이버작전센터로 변경하고, 해군본부 직할 부대로 전환하면서 해군 사이버 작전 콘트롤타워 등 임무를 확대했다(김민진 2021; 노성수 2021). 그러나 최근 해군이 추진하는 사이버보안 관련 사업을 살펴보면 함정 탑재 체계에 실시간 모니터링 강화를 위해 함정 사이버 방호 원격 관제 체계 시범 구축 사

업 및 함정 통합 사이버 방호 체계 추진, 사이버 전문가 양성을 위해 사이버 모의 체계 구축 사업을 추진 등 여전히 사이버 방호 태세 구축에 초점이 맞춰져 있다는 것을 알 수 있다(김영환 2023).

해양경찰청은 해사 사이버 위협이 증대하면서 사이버범죄 대응과 예방을 위해 사이버수사과를 신설하고(해양경찰청 2023a), 사이버수사 플랫폼을 구축할 예정이다(해양경찰청 2023b). 해양경찰청은 국가 안보적 차원의 해사 사이버범죄 예방과 피해 확산 방지, 신속한 범인 검거 등의 임무를 맡고 있으며, 이를 통해 종합적인 대응체계를 마련할 예정이다. 이를 위해 최신 과학수사 시설·장비를 도입하고, 경찰청 등 사이버수사 담당 기관과 협력을 확대할 계획이다. 그러나 현실적으로 해양경찰청 본청 및 지방청을 합쳐 전종 요원은 8명으로 인력이 매우 부족한 실정이다.

Ⅴ. 결론

지난 9월 개최되었던 “사이버공간 국제 평화안보체제 구축에 관한 학술회의(GCPR)”에서 미 해군대학 크리스 뎀착 교수는 34개 민주국가가 해양과 인접하고 있고, 해사의 중요성이 국가별 안보 전략 수립에 필수적임을 강조했다. 특히, 해사 안보는 사이버안보와 불가분의 관계가 있으며, 공급망 강화 측면에서 전·평시를 가리지 않고 그 중요성이 높다고 강조했다(Demchack 2023). 우리나라보다 선제적으로 해사 사이버안보 활동을 추진해 온 미국도 이들 활동의 제도적 보완 및 개선이 필요하다고 식별하고 있다는 점에서 앞으로 우리나라의 해사 사이버안보를 강화하는 활동에 많은 시사점을 주고 있다.

3장과 4장에서 살펴본 미국과 한국의 해사 사이버안보를 위한 전략 및 정책, 시행부서의 조직체계와 업무 범위를 토대로 한미 양국 정책을 국가전략 및 계획 존재 여부, 주요 기반시설 관리 여부, 주요 조직체계 및 기능, 사이버 작전 및 임무 수행, 위협 정보 공유 방안 5가지로 나누어 비교·분석해 보았고 결과는 <표 3>과 같다. 이를 기반으로 한국 해사 분야 사이버안보 정책 개선 방향 5가지를 제안하고자 한다.

첫째, 국가 사이버안보 정책의 최상위 지침인 국가사이버안보전략 및 기본계획 수준에서 국가 차원의 해사 사이버안보를 위한 목표 및 비전을 명확히 하고, 이를 위한 구체적인 계획 수립이 필요하다. 국가전략 수준에서 해사 사이버안보를 고려하고 있는지에 대해 양국을 비교해 보면, 미국은 2018년 국가사이버전략에서 미국 경제 안보에 있어 해사 사이버안보의 중요성을 강조하고 이를 기반으로 2020년에는 해사 사이버안보 강화 계획을 발표하였으며, 공공 및 민간 부문 전체에서 해사의 특징을 고려한 사이버보안 실태 검토, 위험관리 체계 구축을 추진하고 있다. 그러나 우리나라의 국가사이버안보전략 및 기본계획에서는 별도로 해사 안보의 중요성이 고려되고 있지는 않다. 이는 한미 양국의 해사 사이버안보의 중요성에 대한 인식을 반영하는데, 아직까지 한국은 국가안보를 위한 필수 보호 영역으로서 해사 분야 사이버안보 강화 정책 추진이 필요하다는 인식의 비중이 높지 않다는 것을 알 수 있다. 이에 한국의 해사 사이버안보 정책이 전반적으로 개선되기 위해서는 전략 및 기본계획 수준에서 정부가 이에 대한 목표와 의지를 드러내고 공공·민간 전반에서 해사 사이버안보 강화를 위한 활동이 이루어질 필요가 있다.

둘째, 해사 분야에 특징을 고려한 주요 기반시설 사이버안보 계획이 마련되어야 할 것이다. 주요 기반시설 보호 관점에서 한미 양국을 비교해 보면 미국은 해사 분야를 다른 주요 기반시설과 차

이가 있다는 것을 인식하고, 다른 주요 기반시설 사이버안보 현황과의 격차를 식별한 뒤 해사 분야 특징을 고려한 주요 기반시설 보호 계획을 수립·추진하고 있다. 반면, 한국은 유관 부처를 포함하여 기술적 측면에서 선박 보안 강화를 위한 연구 활동이나 해경 및 해군 등 주요 실무자들별 사이버안보 역량 확보를 위한 연구는 추진되고 있으나 해사 분야에 특화된 주요 기반시설 방안은 마련되어 있지 않은 상황이다(김소정 2023).

더욱이 다른 주요 기반시설도 민간부문에 의해 운영되는 비중이 높은 미국과 달리 한국은 대부분의 주요 기반시설이 공공부문에 운영되고 있다. 이에 따라 미국의 주요 기반시설 사이버안보 정책은 과거부터 민간부문 운영자와 협력, 정보공유 방안, 정부 정책 및 표준을 민간부문에 적용할 수 있는 방안 등을 강조하고, 이러한 운영환경을 고려하여 정책이 마련되어 왔다. 그러나 한국은 2022년 기준으로 공공부문 주요 기반시설이 65%에 달해(국가정보원 2023, 102), 망분리 등 공공부문 운영환경에 초점을 맞춰 주요 기반시설 보호 정책이 추진되고 있다. 다른 주요 기반시설 부문에 비해 해사 분야는 국내에서도 민간부문의 범위가 넓고, 특히, 국제성이 있다는 차별점이 있다. 이에 기존 한국의 주요 기반시설 보호 정책으로는 한계가 있고 해사 분야의 특징을 고려한 개선된 보호 계획이 요구된다.

셋째, 우리나라 해사 시설의 사이버안보를 위한 부처 및 기관의 역할과 책임의 재설정, 그리고 이를 뒷받침할 수 있도록 실질적인 인력과 자원확보 방안이 마련되어야 할 것이다. 한미 양국의 해사 사이버안보를 위한 주요 조직체계 및 기능을 비교해 보면, 미국은 해안경비대에 해사 사이버안보 총괄 업무를 부여하고, 국토안보부, 국방부, 해양청 등 유관 기관과 협력하도록 하여 조정통제가 가능한 일원화된 운영체계를 구축하고, 임무의 범위를 확장하였다. 또한, 해안경비대가 실질적인 책임을 이행할 수 있도록 백악관 차원

<표 3> 한미 해사 사이버안보 정책 비교

	미국		한국	
국가전략·계획 존재 여부	2018년 국가사이버전략에 따라 2020년 국가해사사이버안보강화계획 발표		해사 사이버안보를 위해 특화된 국가전략 및 계획 없음	
주요 기반시설 관리 여부	주요 기반시설로 관리 다른 주요 기반시설과의 차이점과 격차를 식별하고, 해사 분야 주요 기반시설 사이버안보 강화를 위한 계획 마련 및 현재 추진 중		주요 기반시설로 관리 그러나 해사 분야 특징을 고려한 별도의 규정 및 제도 부재	
주요 조직체계 및 기능	국토안보부	주요 기반시설 사이버안보	국가정보원	주요 정보통신기반시설 및 공공기관 사이버안보
	해양청(MARAD)	미국 교통부 산하 해사 서비스 및 선박관리 기관	해양수산부	해사 분야 보안관제, 해사 분야 주요 기반시설 사이버안보
	해안경비대	해사 사이버안보 총괄기관 주요 기반시설 보호, 사이버 작전	해군	해군 사이버안보, 사이버 작전
	미국선급협회(ABS)	선박, 선사 등 해양구조물 사이버보안 규제·표준 마련, 인증·평가	한국선급	선박, 선사 등 해양구조물 사이버보안 규제·표준 마련, 인증·평가
	국토안보수사국(HSI) 및 연방수사국(FBI)	사이버범죄 수사	해양경찰청	해양 분야 사이버범죄 수사
사이버 작전 및 임무 수행	해안경비대 임무 기능에 사이버 작전 활성화를 부여하고, 공식적인 전략에서 사이버 작전 수행 역량 확대 계획 발표		해군부대 조직으로 사이버작전센터를 신설하고, 사이버 작전 임무 수행 계획을 밝혔으나, 별도의 구체적인 전략이나 계획을 포함한 공식 문서 부재	
위협 정보공유 방안	주요 기반시설 정보공유 및 분석 확대를 위한 ISAC 구축 및 운영 국토안보부, 연방수사국, 해안경비대 간에 정보 커뮤니티 구축 해사 기업 사이버 사고 보고 의무화 민관 간 정보공유 촉진을 위해 비기밀 분류 정보·허용 가능한 기밀정보 체계 구축		공공기관 간 사이버 위협 정보공유를 위한 시스템 운영 주요 정보통신기반시설 사고 보고 의무화 해운선사는 선박사고 발생 시 해양수산부에 통보	

출처: 저자 작성

에서 해안경비대의 인력확충, 자원확보 계획을 약속했다.

그러나 한국은 미국이 인식하고 있는 임무 범위 중에서도 일부만 위협으로 인식하고 있으며, 그마저도 총괄기관이 부재하고 다부처가 접근하여 체계화된 대응에 한계가 있다. 이에 사이버보안에 대한 전문성을 갖춘 정부 부처 및 기관에서 해사 사이버안보 업무를 총괄하고, 해당 기관이 실질적인 임무를 수행할 수 있도록 자원확보 방안 수립이 필요하다.

넷째, 해사 사이버안보를 위해 ICT를 활용한 사이버 작전을 긍정적으로 고려하고 이를 위한 역량을 강화할 필요가 있다는 것이다. 사이버 작전 및 임무 수행 관련 한미 양국 정책을 비교해 보면, 미국은 공식적인 전략을 통해 사이버공간에서 적의 탐지, 억제, 무력화를 해안경비대의 주요 임무로 설정했다. 그리고 ICT 기술을 활용하여 사이버 작전의 효율성을 높이고, 해사 주요 기반시설을 대상으로 하는 악의적인 활동을 억제, 방어, 대응하도록 하였으며, 작전 역량 강화 방안을 추진하고 있다. 이는 사이버 기술이 수단 및 도구적 의미로도 역할을 갖고, 보호 대상으로도 그 역할을 갖는다는 점을 보여준다.

반면, 한국은 2019년에 해군 내 사이버작전센터를 설립하고, 사이버 작전 임무 수행 계획을 밝혔으나 공식적인 전략이나 계획이 없어 구체적인 내용을 확인하기는 어렵다. 다만, 2013년 해안경비대 사이버사령부를 창설한 미국에 비해 사이버작전센터 설립이 다소 늦게 이루어졌다는 것을 알 수 있다. 정부가 국가사이버안보전략 개정 시 사이버 위협에 능동적·공세적 대응을 위한 방향성을 강조할 계획을 밝힌 만큼(황국상 2023), 관련하여 해군의 사이버 작전 수행을 위해 명확한 임무와 권한을 부여하고, 해사 환경의 특수성을 고려한 해군 사이버작전 수행 체계 구축, 전문인력 양성, 기술개발 등 역량 강화 방안이 마련되어야 할 것이다. 다만, 미국은 해안경비대 또한 군 기관으로, 현재 우리나라에 대입 가능한

조직적 구조가 아니므로, 무턱 댄 접목보다는 한국 실정에 맞도록 개념을 설정하고, 역할과 책임을 구체화 작업이 필수적으로 선행되어야 할 것이다.

다섯째, 위협 정보와 인텔리전스 공유를 확대하여 해사 시설을 사용하는 민간기업에도 정보를 공유하고, 사이버보안 위협 요소 제거에 도움을 줌으로써 시장의 자체적인 사이버보안 수준 향상을 지원해야 한다. 한미 양국의 위협 정보 공유 방안을 비교해 보면, 미국은 국토안보부, 연방수사국 등 주요 사이버보안 정부 기관과 해안경비대 간에 정보 커뮤니티를 구축하고, 해사 기업의 사이버 사고 보고를 의무화하는 등 정보공유를 확대해 나가고 있다. 또한, 정부 기관 이외에도 민간부문 파트너와 정보공유 촉진을 위해 비기밀 분류 정보 또는 허용 가능한 기밀정보 체계를 구축하는 등 정부의 사이버위협 정보 및 인텔리전스를 공유해 위협 예방을 지원하고 있다.

한국도 주요정보통신기반보호법에 따라 주요 기반시설 사이버 사고 발생 시 보고가 의무화되어 있으며, 개정된 해사 사이버안전 관리지침에 따라 해운선사는 사이버사고 발생 시 해양수산부에 보고하도록 했다. 또한, 국가사이버위협정보공유시스템을 통해 국가정보원을 주도로 주요 공공기관에 사이버 위협 정보를 공유하고 있다. 그러나 항만 및 해사 분야에는 공공기관뿐만 아니라 다수의 민간기업이 관련되어 있어 민간부문까지 정보공유의 범위가 확대될 필요가 있으며, 이를 위한 정보 분류, 공유체계 구축 등 세부 방안이 마련되어야 할 것이다.

마지막으로 이 모든 것을 추진할 수 있는 조직, 예산, 인력 측면의 보강이 필요하며 특화된 전문인력을 다수 양성 및 확보하는 방법에 대한 고민이 필요하다. 또한, 실무적인 문제를 해결하기 위한 다양한 기술 해결책들에 대해 긍정적인 자세를 보여야만, 새로운 기술 발전이 위협이 아닌 우리를 위한 도구가 될 수 있을 것이다.

〈참고문헌〉

강남선. 2018. “선박 사이버보안에 대한 기술적 분석.” 『한국마린엔지니어링학회지』 42권 6호, 463-471.

관계기관 합동. 2019. “19년 스마트 해상물류 체계 구축전략.”

관계부처 합동. 2022. “대한민국 디지털 전략.”

국가정보원. 2023. “2023 국가정보보호백서.”

김경식. 2017. “패권경쟁과 해군력의 역할.” 『STRATEGY 21』 통권 41호, 108-152.

김민진. 2021. “방산명가 대우조산해양, 함정 사이버보안 기술개발 고삐 쥔다.” 『부산일보』(11월 22일).

김선애. 2021. “IT에서 시작되는 OT타깃 공격.” 『DataNet』(9월 10일).

김소정. 2022. “미국의 사이버공격 대응정책과 한국에의 시사점; 솔라윈즈 해킹 대응 사례를 중심으로.” 『국가안보전략연구원 연구보고서』 04.

김소정. 2023. “해양 사이버안보 현황과 대응 방안.” 『국가안보전략연구원 이슈브리프』 476호, 11.

김엘진. 2021. “디지털 해운시대의 과제. 선박 사이버 보안.” 『현대해양』(12월 11일).

김영곤. 2021. “해운업계에서 사이버공격의 증가에 따른 사이버 위험관리 방안에 관한 연구.” 『지역산업연구』 제44권 제3호, 345-371.

김영환. 2023. “함정 사이버보안 발전방향.” 해양·선박사이버보안워크숍. 9월.

남영수. 2019. “위기의 해운. 디지털의 습격①~⑤.” 『ESG 얼라이언스』. https://clomag.co.kr/article/3196

노성수. 2021. “해군 사이버작전센터를 가다 – 사이버작전의 심장 함정·육상 정보체계 위협 방어.” 『국방일보』 (07월 07일).

박종서. 2023. “신정훈 의원. 항만 사이버공격 지난해 227건, 2018년 比 5.5배 증가 … 해양사이버 수사 대응체계 구축 필요.” 『시사일보』(10월 22일).

박한선 외 3명. 2019. “해상 사이버 보안체계 강화방안 연구.” 『한국해양수산개발원 기본연구』 2019-16.

안종우. 임정규, 박개명. 2019. “해양 사이버보안 동향 분석 및 해사 사이버보안 시스템 구축.” 한국항해항만학 춘계 학술대회.

원병철. 2021. “2021년을 괴롭혔던 ‘사이버보안 사건·사고’ 어떤 것들이 있었나? 上.” 『보안뉴스』(12월 28일).

원병철. 2022. “2022년 해양선박 보안을 위한 4가지 고려사항.” 『보안뉴스』(3월 22일).

유지운. 2022. “자율 운항 선박의 인공지능 잠재적 사이버 위협과 보안.”, 『정보보호학회논문지』 vol. 32, no. 2, 447-463.

이경성. 2023. “해수부, 선박 사이버안전 관리 지침 제정.” 『물류신문』(04월 22일).

이근홍. 2022. “대우조선해양, 선박·함정 사이버보안 기술 국산화 나서.” 『문화일보』(10월 24일).

임정규. 2020. “해사 사이버보안 동향 및 선박 사이버보안 인증 현황과 미래.” 해양산업통합클러스트 워킹그룹 세미나. 2월.

임정규 외. 2020. “해상 사이버 보안 동향 및 선박 사이버 안전 체계 구축 방안.” 한국선급(KR) 기술정책제언연

구집.
조용현. 2019. “위협 모델링을 이용한 선박 사이버보안 요구사항 연구.” 『정보보호학회논문지』 vol. 29, no. 3, 657-673.
한국선급. 2021a. “한국선급 사이버보안 뉴스레터” vol. 42.
한국선급. 2021b. “해상 사이버보안 시스템 지침” GC-24-K.
해양경찰청. 2022. “2022년 주요업무계획.”
해양수산부. 2023. “해사 사이버안전 관리지침.”
해양경찰청. 2023a. “사이버수사 전담조직 신설.” 『보도자료』 (03월 15일).
해양경찰청. 2023b. “해양사이버범죄 대응을 위한 사이버수사 홈(플랫폼) 구축.” 『보도자료』(6월 13일).
황국상. 2023. “국정원 국가 사이버 안보전략, 위협주체 명시·적극대응 방향성 제시해야.” 『머니투데이』(07월 12일).
Andersen. 2017. “머스크 해킹으로 최대 3400억원 손해봐.” 『Naked Denmark』(8월 17일).
Cimpanu, Catalin. 2020. “UN Maritime Agency Says It Was Hacked.” *ZDNet*(10월 6일)
Circulars. 2023. “Revision of the Rightship Inspection Questionaire.” https://sqemarine.com/revision-of-the-rightship-inspection-questionnaire-risq-3-/ (검색일: 2023.11.20.)
DCSA. 2023. “Cyber Security.” https://dcsa.org/standards/cyber-security/ (검색일: 2023.11.20.)
Demchack, Chris. 2023. “Maritime Cybersecurity.” GCPR. September.

EUROPA. “International Legal Framework Applicable to th e Maritime domain : Safe Operations of Ships & #8211; SOLAS Convention.” https://emsa.europa.eu/e-learning/cybersec/AMC 003/story_html5.html (검색일 : 2022.11. 22.)

IMO. 2017. “Resolution MSC.428(98) – Maritime Cyber Ri sk Management in Safety Management System.”

IMO. 2022. “MSC-FAL.1/Circ.3/Rev.2-Guidelines on Mariti me Cyber Risk Management.”

Kim, So Jeong, and Sunha Bae. 2021. “Korean Policies of Cybersecurity and Data Resilience.” *CEIP*.

Kollars, Nina A., Sam J. Tangredi, and Chris C. Demchak. 2021. “The Cyber Maritime Environment: A Sha red Critical Infrastructure and Trump’s Maritime Cybersecurity Plan.” *War on the Rocks*.

Loomis, William, Virpratap Vikram Singh, Dr. Gary C. Kes sler, and Dr. Xavier Bellekens. 2021. “Raising t he colors: Signaling for cooperation on maritime cybersecurity.” *Atlantic Council*.

Maritimecyprus. 2022. “Maritime Compliance.” https:// m aritimecyprus.com/2022/06/29/maritime-complian ce-iacs-unified-requirements-for-cyber -securit y-mandatory-from-1-jan-2024/ (검색일: 2023.1 1.20.)

O’Dwyer, Rob. 2018. “ISAC Issues Cyber Recommenda tio ns.” https://smartmaritimenetwork.com/2018/ 09/ 27/iacs-issues-cyber-recommendations/ (검색일:

2023.11.20.)
The Coast Guard. 2015. “United States Coast Guard Cyber Strategy.”
The Coast Guard. 2021a. “2021 Cyber Trends and Insights in the Marine Environment.”
The Coast Guard. 2021b. “The United States Coast Guard’s VISION To Protect and Operate in Cyberspace.”
The White House. 2018. “National Cyber Strategy of the United State of America 2018.”
The White House. 2020a. “Maritime Port Operational Technology Systems Cybersecurity Information Paper.”(비공개 초안)
The White House. 2020b. “National Maritime Cybersecurity Plan : To The National Strategy for Maritime Security.”
UNCTAD. 2018. “UNCTAD Review of Maritime Transport 2018.”
UNCTAD. 2020. “UNCTAD Review of Maritime Transport 2020.”
United States Coast Guard. 2023. “CGCYBER.” https:// www.dco.uscg.mil/Our-Organization/CGCYBER/ (검색일: 2023.11.20.)

논문접수일 : 2023년 11월 20일
논문심사일 : 2023년 12월 26일
게재확정일 : 2024년 1월 26일

Study on U.S. Maritime Cybersecurity Strategy and Its Implications for the ROK

| So Jeong KIM Institute for National Security Strategy
| Sunha Bae National Security Research Institute, Corresponding author

| Abstract

The maritime sector has evolved into a crucial platform projecting diverse influences from a national security perspective, concurrently serving as the frontline domain ensuring the safety of logistics flows and the resilience of the supply chain. However the maritime and shipbuilding industries have also witnessed an expansion in the utilization of ICT, driving a rapid digital transformation. Emerging technologies like smart ships and smart ports are advancing, and the blurred boundaries between IT and OT are intensifying cyber threats in the maritime sector.

The U.S. has emphasized the significance of maritime affairs in national security and the economic domain. The U.S. is actively pursuing various policies to underscore the importance of maritime security and bridge the cybersecurity gap between maritime infrastructure and other critical sectors, aiming to mitigate vulnerabilities. We analyzes the maritime cybersecurity strategy and policy documents of the U.S. and examines the policy landscape and organizational status of maritime cybersecurity in Korea. Based on this, we proposes policy directions for enhancing maritime cybersecurity in our country.

| Keyword Maritime Cybersecurity, US Coast Guard Cyber Command, International Maritime Organization, US Coast Guard 2015 Strategy, US Coast Guard 2021 Outlook