해양산업 디지털전환을 위한 사이버보안 전문 인력양성 방안연구

† 유진호 · 임정규* · 박개명*

*,† 한국선급 책임검사원

A study on the development of cybersecurity experts and training equipment for the digital transformation of the maritime industry

† *Jinho Yoo · Jeounggye Lim* · Kaemyoung Park**

,† Korean Register, Busan 46762, Korea

요 약 : 해양산업 디지털 전환에 따른 사이버 위협이 증가함에 따라 선박 및 항만 종사자들에 대한 사이버보안 교육훈련과 전문인력양성 필요성이 증가하였다. 선원의 교육훈련은 IMO의 STCW 협약과 연관되어 교육훈련 관리 및 자격증명이 이루어져야 하고, 선박과 항만의 OT시스템 특성을 반영한 사이버보안 교육훈련 시스템 개발이 필요하다. 본 논문에서는 IMO 사이버 리스크 관리 가이드라인 기반 훈련모델 개발, 해양산업 위협의 특성 기반 사이버보안 훈련모델 개발, AR/VR 및 메타버스를 활용한 사이버보안 훈련 효과 향상을 목표로 해양산업 디지털전환에 따른 사이버보안 전문인력 양성 시스템 개발방안을 제시하였다.

핵심용어 : 해상 사이버보안, 전문인력 양성, 선원교육, 자율운항선박, 스마트 항만

Abstract *: As cyber threats in the maritime industry increase due to the digital transformation, the needs for cyber security training for ship's crew and port engineers has increased. The training of seafarers is related to the IMO's STCW convention, so cyber security training also managed and certified, and it is necessary to develop a cybersecurity training system that reflects the characteristics of the OT system of ships and ports. In this paper, with the goal of developing a training model based on the IMO cyber risk management guideline, developing a cyber security training model based on the characteristics of maritime industry threats, and improving the effectiveness of cyber security training using AR/VR and metaverse, A method for developing a system for nurturing cyber security experts is presented.*

Key words *: Maritime cyber security, professional manpower training, crew training, MASS, Smart ports*

1. 서 론

세계 각국은 해양산업의 디지털 전환(Digital Transfomation)을 통해 국가경쟁력을 높이기 위한 여러 가지 시도를 하고 있다. 유럽은 'Horizon 2020', 'Horizon Europe' 등의 프로그램을 통해 해양 환경오염 저감과 해운물류 경쟁력을 강화하기 위한 R&D 투자를 확대하고 있고, 중국도 '중국 제조 2025' 전략을 통해 10대 산업 주요 발전계획으로 스마트 자율운항선박 관련 기술의 확보에 대한 발전전략을 제시한 바 있다(정보통신산업진흥원, 2013). ····· (중략) ·····.

2. 해양산업의 전통적인 위협과 디지털 전환에 따른 사이버보안 위협

2.1 해양산업의 전통적인 위협

해양산업은 전 세계 교역량의 90% 이상을 운송하는 국가 기간 산업이기 때문에, 국제선박 및 항만시설에는 전통적으로 선박안전 확보, 해상테러 방지 및 해양환경 보호를 위해 IMO의 ISPS(International Ship and Port facility Security) 코드를 적용받고 있다. 특히 항만은 육상과 해상의 접점으로 생산, 물류, 정보교류의 필수적인 플랫폼을 제공하는 해상 비즈니스의 핵심이기 때문에 항만의 기능이 훼손되거나 상실될 경우 국가적 혼란을 초래할 수 있는 특징이 있다.(한국해양수산개발원, 2019) ····· (중략) ·····..

2.2 해양산업의 디지털 전환에 따른 사이버 위협 동향

최근 해양산업은 자율운항선박, 스마트 항만, 스마트 조선소 등 디지털 전환(DX)을 통해 상호 연결성 기술이 급격하게 발전하고 있지만, 해상 사이버보안에 대한 관심은 비례적으로 증가하지 않았다. 해양산업에 대한 사이버 보안위협의 증가 추세는 미국 내무부(Department of Homeland security)와 해안경비대(USCG, United States Coast Guard)에서 발간하는 간행물에서 확인할 수 있다. 2022년 해양 정보시스템을 겨냥한 사이버 공격 시도는 작년 대비 400% 이상 증가하였으며, 이러한 추세는 지속될 것으로 보인다. (Atlantic Council, 2021)

Table 1 해양산업 사이버 위협 동향

시기	대상	시스템	공격유형
2017	컨테이너선	선박 항해 시스템	-
2017	머스크	터미널 IT 시스템	랜섬웨어
2017	클락슨	회사 이메일	내부자
2018	해운선사	IT 시스템	스피어 피싱
2018	COSCO	항만 IT 시스템	랜섬웨어
2018	바르셀로나 항만	항만 IT 시스템	랜섬웨어
2018	샌디에고 항만	항만 IT 시스템	랜섬웨어
2019	자동차 운반선	선박 IT 시스템	랜섬웨어
2019	국내 H선사	선박 IT 시스템	랜섬웨어
2020	CMA CGM	회사 IT 시스템	랜섬웨어
2021	트랜스넷 SOC	항만 IT 시스템	랜섬웨어

…… (중략) …….

3. 해상 사이버보안 국내·외 교육훈련 동향

3.1 국제동향

국제해사기구(IMO)는 1978년 선원의 훈련·자격증명 및 당직 근무의 기준에 관한 국제협약(STCW)을 채택하고, 선원의 교육훈련과 자격증명에 대한 요구를 엄격히 관리하고 있다. IMO 해사안전위원회(MSC)는 2017년 MSC 98차 회의에서 해사 사이버 리스크 관리에 관한 가이드라인(MSC-FAL.1/Circ.3)을 발표하고, 동 회의에서 2021년1월 전에 선주와 선박관리자에게 사이버리스크를 선박 안전관리시스템(SMS)에서 관리하도록 촉구하는 결의서(Resolution MSC.428(98))을 채택하였다.

…… (중략) …….

4. 해양산업 사이버보안 전문인력 양성 필요성

해양산업에 대한 사이버 보안 위협이 증가함에 따라 해양산업 종사자에 대한 사이버보안 교육훈련과 사이버보안 전문인력 양성이 필요하다. 사이버 범죄자들은 가장 취약한 링크를 식별하고 악용한다. 해상 사이버 공격에 대한 수많은 언론 보도에도 불구하고, 범 국가 차원의 대책 마련이 부족한 것이 현실이다. 가장 이상적인 대책은 선박과 항만의 시스템 설계단계부터 사이버보안을 고려하는 것이지만, 이는 엄청난 투자가 필요로 한다. 따라서, 사이버 범죄자들도 집중하는 영역 중 하나인 “사이버보안 교육을 받지 못한 인력”과, “숙련되지 않은 운영인력이 저지르는 실수”를 예방할 수 있는 사이버보안 전문인력 양성이 가장 효율적으로 해양산업 디지털 전환에 따른 사이버 복원력을 유지하는데 효율적인 방법이 될 수 있다.

…… (중략) …….

5. 해양산업 사이버보안 인력양성 방안

5.1 목표

앞에서 해양산업의 디지털 전환에 따른 사이버보안 위협과 국내·외 동향을 통해 해양산업의 사이버보안 전문인력 양성 필요성을 소개하였다. 본 절에서는 해양산업의 특징과 디지털 전환에 따른 인력양성 방안을 제시하고자 한다. 다음은 해양산업 사이버보안 인력양성 시스템 개발 목표이다.[1]

· 국제규제 기반 해양산업 사이버보안 훈련모델 개발
· 해양산업 위협의 특성 기반 사이버보안 훈련모델 개발
· AR/VR 및 메타버스를 활용한 사이버보안 훈련 효과 향상

5.2 해양산업 사이버보안 전문인력 양성시스템 개발

해양산업에서 선박의 인적요소는 IMO의 STCW 협약을 기반으로 교육훈련이 필요하고, 선박과 항만에 특화된 OT 시스템 특성을 반영하여 해양산업에 특화된 사이버보안 교육훈련 모델개발이 필요하다. 따라서, 해양산업 모든 종사자를 대상으로 하는 공통 사이버보안 교육훈련 모델과 해양산업에 특화된 사이버보안 전문인력 양성 시스템 개발을 제안한다.

Table 2 해양산업 사이버보안 인력양성 목표

구 분	인력양성 목표	교육훈련 대상
공통 과정	사이버보안 관리체계 OT 시스템 보안운영	ALL
스마트 선박 사이버 보안	선박 사이버리스크 관리	선원
	IMO 사이버 리스크 관리체계 운영	선사 관리자
	선박 사이버 침해사고 대응훈련	선원/선사 관리자. IT 담당자
	스마트 선박 사이버 보안 설계	조선소 설계 엔지니어
	스마트 선박 기자재 사이버보안 개발	선박 기자재 개발자
스마트 항만 사이버 보안	스마트 항만 시스템 개발	항만 시스템 개발자
	스마트항만 운용	항만 운용/관리자
	스마트항만 시스템 유지보수	항만 시스템 유지보수자

…… (중략) …….

스마트 선박 또는 자율운항선박에 특화된 교육훈련 모델은 IMO의 사이버 리스크 관리체계 프레임워크를 운영·관리 하고, 선박 및 기자재 설계보안, 사이버보안 시스템 운영, 침해사고 대응, 시스템 보안성 평가 전문가 양성을 위한 교육훈련 시스템 개발의 프레임워크를 설계하였다. 또한, 스마트 항만에 특화된 교육훈련 모델은 항만 시스템 개발, 항만 시스템 운용, 항만 시스템 유지보수 엔지니어의 사이버보안 전문인력 양성을 위한 커리큘럼과 교육훈련 시스템 프레임워크를 설계하였다.

…… (중략) …….

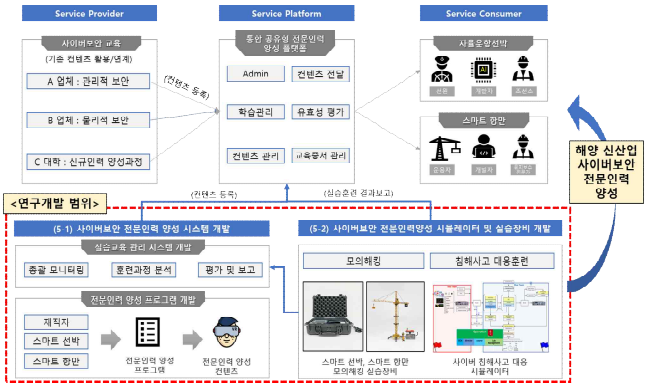

Fig. 2 해양산업 사이버보안 인력양성 시스템 개발 개요

5.3 해양산업 사이버 침해사고 대응훈련 시스템 개발

5.1에서 해양산업 사이버보안 인력양성 목표와 5.2에서 전문인력 양성 시스템 개발 프레임워크를 소개하였다. 여기서는 해양산업에 특화된 침해사고 대응훈련 시스템 개발 방안을 제안한다. 선박은 IT시스템과 OT시스템이 융합된 환경이기 때문에 국내 타산업에서 시행하고 있는 IT시스템 보안교육은 선원이나 항만 종사자들에게 적합하지 않다. 따라서, IT시스템과 OT시스템이 융합된 해양산업 사이버 침해사고 대응훈련 시스템을 개발하고, 가상환경에서 침해사고 대응훈련을 할 수 있는 시스템 개발 프레임워크를 제시한다.

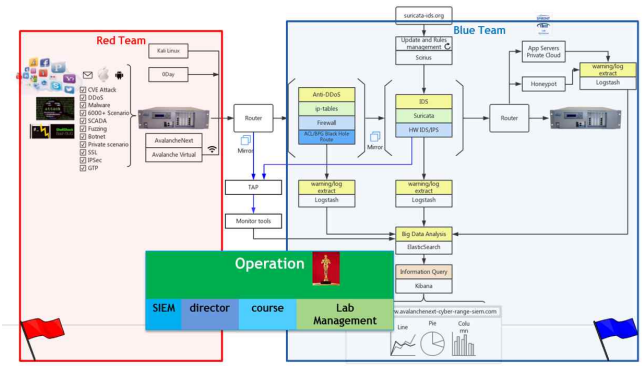

Fig. 3 사이버 침해사고 대응훈련 시스템 예시

5. 결 론

본 연구에서는 해양산업의 디지털 전환에 따른 사이버보안 전문인력 양성의 필요성과 해양산업에 특화된 사이버보안 인력양성 방안을 분석해 보았다. 해양산업은 전통적으로 해상테러 위협에 대한 대응정책은 잘 마련이 되어 있으나, 디지털 전환에 따른 사이버 위협을 대응하기 위한 정책은 아직까지 뚜렷한 방안이 수립되어 있지 않다. 해상 사이버 리스크 관리 체계수립에 있어 가장 취약한 요소인 인적요소를 잘 훈련하면 사이버 공격으로부터 “인간 방화벽”의 역할을 수행하여 최악의 사이버 침해사고를 막을 수 있을 것으로 추론하였다.

…… (중략) …….

참 고 문 헌

[1] 정보통신산업진흥원, EU Horizon 2020 정책 분석, 2013

Bendovschi, A. (2015). Cyber-attacks - trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

[2] 한국선급(2022), 해양신산업(친환경, 스마트선박, 항만) 서비스 전문인력양상 사업 기획보고서

[3] Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of information security and applications, 42, 36-45.

[4] Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybersecurity Ventures.

[5] Jeric Bacasdoon(2021), A multiple case study of METI cybersecurity education and training: a basis for the development of a guiding framework for educational approaches

[6] 임정규·손금준(2020), 해상 사이버 보안 동향 및 선박 사이버 안전체계 구축방안, 기술정책제언연구집

[7] 해양수산부(2022), 국제해사기구(IMO) 제8차 인적요인, 훈련 및 당직(HTW) 전문위원회 결과보고서

[8] 김경호(2019), 제어시스템 사이버 보안 교육훈련 방안 연구, 정보보호학회논문지 VOL.29, No.3, pp. 645-656

[9] 한국선급(2022a), KR Cyber Safety News and Report Vol.50

[10] 한국해양수산개발원(2019), 해상 사이버 보안체계 강화방안 연구

[11] Atlantic Council(2021), Signaling for Cooperation on Maritime Cybersecurity

[12] 해양수산부(2020), “해사(선박안전) 사이버보안 대책마련” 연구용역 과업지시서

[13] 한국선급(2021b), KR 사이버인증 Brochure