Journal of the Korean Society of Marine Environment & Safety
Research Paper
Vol. 26, No. 7, pp. 830-837, December 31, 2020, ISSN 1229-3431(Print) / ISSN 2287-3341(Online) https://doi.org/10.7837/kosomes.2020.26.7.830

선박 사이버보안 책임자를 위한 교육과정 개발에 관한 연구

이은수* · 안영중**† · 박성호***
* 한국해양수산연수원 교관, ** 한국해양수산연수원 교수, *** 한국해양대학교 교수

A Study on the Development of a Training Course for Ship Cyber Security Officers

Eunsu Lee* · Young-Joong Ahn**† · Sung-ho Park***
* Instructor, Korea Institute of Maritime & Fisheries Technology, 367 Haeyang-ro, Yeongdo-gu, Busan 49111, Korea
** Professor, Korea Institute of Maritime & Fisheries Technology, 367 Haeyang-ro, Yeongdo-gu, Busan 49111, Korea
*** Professor, Korea Maritime & Ocean University, 727 Taejong-ro, Yeongdo-gu, Busan 49112, Korea

요 약 : 정보통신기술의 발전에 따라 선박과 육상 간의 정보교환은 더욱 빠르고 편리해졌으나 선박정보에 대한 접근이 용이해져 사이버보안 공격에 대한 우려도 커지고 있다. 선박이 사이버 공격의 피해를 입게 되면 복구하는데 막대한 비용과 시간 손해가 발생하며, 해사산업계는 선박 사이버보안 책임자를 지정하여 보안관리 업무를 담당할 것을 요구하고 있다. 공격의 피해를 줄이고 효과적인 대응을 위하여 선박 사이버보안 책임자를 위한 전문적 교육과정이 필요하다. 이 연구의 목적은 선박 사이버보안 책임자 교육과정과 법제정비 필요성 제시에 있으며, 이를 위해 국내외 동향 및 사고사례, 주요 사이버보안 교육과정을 조사하였다. 조사결과를 바탕으로 선박 사이버보안 책임자에게 필요한 표준교육과정을 개발하였고 관련 법제정비의 방향성을 제시하였다. 연구의 결과는 향후 선박 사이버보안 책임자 교육과정을 개설하는데 기초자료로 활용될 수 있다.

핵심용어 : 선박 사이버보안, 선박 사이버보안 책임자, 보안사건, 교육과정, 법제정비

Abstract : *With the rapid development of information and communication technology, information exchange between ships and shore has become faster and more convenient, However, accessing ship information has also become easier and concerns about cyber security attacks are growing. When a ship suffers a cyber-attack, it may cause considerable damage and incurs enormous costs and time to repair. In response to this threat, the maritime industry now demands that a cyber security officer be assigned to each ship to take charge of cyber security management onboard. In order to reduce the damage cause by an attack and to respond effectively, a specialized training course for the ship's cyber security officer is required. The purpose of this study was to present a training course for the position of the ship's cyber security officer, and to highlight the necessity of amending current legislation, To this end, domestic and foreign trends, ship cyber security incident cases, and cyber security training courses were investigated, and based on the results a standard training course for a ship's cyber security officer was developed. Additionally, recommendations on the related amendments to legislation ware established. The results of the study can be used as basic data to establish future training courses for cyber security officers.*

Key Words : *Ship cyber security, Ship cyber security officer, Ship cyber security incident, Training course, Amendment of legislation*

1. 서 론

정보통신기술(Information and Communications Technologies, 이하 'ICT'라 함)의 발전에 따라 선박과 육상 간의 정보교환은 더욱 빠르고 편리해졌다. 위성통신을 이용하는 선박대상의 사이버보안 위협과 공격 사례가 급증하고 있으며 이로 인해 해사산업계의 사이버보안강화 필요성이 제기되고 있다. 특히, 2017년 발생한 머스크사의 사이버보안사건은 약 3000억의 피해 손실을 입히며 국제적으로 사이버보안 강화의 필요성을 인식하는 계기가 되었다(KMI, 2019).

일부 해사산업계에서는 이러한 사이버보안 공격에 대응하기 위해 Oil Major Inspection과 CDI Inspection 및 Rightship Inspection의 점검항목에 사이버보안 항목을 포함하여 이행여

* First Author : lmrds4@seaman.or.kr, 051-620-5877
† Corresponding Author : yjahn@seaman.or.kr, 051-620-5795

부를 확인하고 있다(Jo and Cha, 2019). 그러나 선박 사이버보안 관리를 요구하는 검사들은 일부 선종에 한해 시행되고 있어, 해당되지 않는 선종에 대한 사이버보안 관리의 필요성 인식은 상대적으로 미비하다. 선박 사이버보안 관리 계획이 수립되어 있지 않거나 취약하다면, 선박 감항능력 담보의 문제로도 발전할 여지가 있다(Lee and Kwon, 2020).

한편 사이버보안의 취약점 개선을 위해 국제해사기구(International Maritime Organization, 이하 'IMO'라 함)는 해사안전위원회(Maritime Safety Committee, 이하 'MSC'라 함) 98차 회의에서 사이버리스크관리 항목을 선박안전관리시스템에 포함하도록 권고 하였다. 또한 발틱국제해사협의회(The Baltic and International Maritime Council, 이하 'BIMCO'라 함)는 'The Guidelines on Cyber Security Onboard Ships'를 개발하였고, ABS, LR, KR 등의 선급에서도 선박 사이버보안 강화를 위한 지침서를 제공하고 있다.

사이버보안 강화는 육상의 항만 및 해운회사 뿐 아니라 선박에도 중요하다. 해상에서 선박이 사이버보안 피해를 입게 되면 사이버보안 전문가의 지원이 쉽지 않아 본선 자력으로 신속하게 대응하기 어려운 측면이 있다. 선박 사이버보안 강화를 위한 지침서들은 선박 사이버보안 책임자(Ship Cyber Security Officer, 이하 'CySO'라 함)의 지정과 교육 필요성을 언급하고 있으며(IET, 2017), Oil Major Inspection, CDI Inspection의 검사항목에는 선박 승선자에게 선박 사이버보안에 대한 교육 제공을 요구하고 있다. 그러나 CySO에 대한 역할과 임무 뿐 아니라 필수로 이수하여야 할 교육에 대한 국제규정과 국내 법적 근거는 부재한 상황이다. 이로 인해 해사산업계의 지침서가 요구하고 있는 수준에 맞는 선박 사이버보안 교육을 제공하기 어려운 문제가 있다. 따라서 표준화 된 CySO 교육과정 개발을 위해 교육시간, 교육방법, 교육내용 등의 교육과정의 세부사항 제시와 함께 관련 법제정비의 필요성이 제기된다.

이 연구에서는 CySO 교육과정 개발과 관련된 법제정비의 필요성 제시를 목적으로 선박 사이버보안에 대한 국내외 동향과 대응현황을 조사하였다. 그리고 CySO 관련 교육을 시행하고 있는 교육과정을 비교분석하여 시사점을 도출하였고, CySO 교육의 필요성을 확인하였다. 조사 분석결과를 기반으로 CySO 교육과정안과 CySO 교육과정의 효과적인 이행을 위한 관련 법제정비 필요성을 제시하고자 한다.

2. 선박 사이버보안의 국내외 동향 및 위협사례

2.1 선박 사이버보안의 국내외 동향

MSC 제94차 회의에서 미국과 캐나다는 해사산업에 위협이 되고 있는 사이버 공격 대응을 위한 가이드라인 개발의 필요성을 제기하였고(IMO, 2014), 제95차 회의에서 선박 사이버보안 지침 개발로 범위를 한정하였다(IMO, 2015). 제96차 회의에서는 해상 사이버리스크관리에 대한 임시지침서(MSC.1/Circ. 1526)를 승인하였고(IMO, 2016), 제98차 회의에서 IMO Resolution MSC.428(98) 결의서를 채택하여 기국들의 안전관리시스템에 2021년 1월 1일 이후 안전관리적합증서의 첫 번째 도래하는 연차검사까지 사이버리스크관리 항목을 포함하도록 권고하였다(IMO, 2017). 영국 런던의 공학기술협회(The Institution of Engineering and Technology, 이하 'IET'라 함)에서는 2017년 9월 영국 교통부와 국방과학기술연구소의 지원으로 'Code of Practice Cyber Security for Ships'를 발행하였다. 선박 사이버보안의 소개 및 필요성, 선박보안평가와 선박보안계획서 개발, 사이버보안 관리 등의 내용을 담고 있으며, 사이버보안 관리의 7.1 항목에서는 CySO의 역할을 명시하였다. 세부내용으로는 CySO의 위치, 담당분야, 책임, 준수사항, 권한 등이 있다(Shaw and Ayerst, 2017).

국내에서는 한국선급(Korean Register of Shipping, 이하 'KR'이라 함)이 2016년부터 '선박사이버보안 대응 TFT'를 구성·운영해 관련 핵심기술 파악 및 솔루션 제공을 위한 기반을 구축했으며, 각 선박과 해운회사에 사이버보안체계 구축 및 관련 검사에 대응하기 위해 '해상 사이버보안 가이드라인'을 제공하고 있다. 해상 사이버보안에 대한 일반적인 사항, 리스크 평가 및 관리, 사이버보안 사고 대응, 복구 관리 등의 내용을 담고 있다. 리스크 관리 제3절 사이버보안 인식 제고 및 교육에서 교육계획, 교육대상, 교육내용 및 방법, 교육 시행 및 평가를 다루고 있다. 또한 KR은 해사 사이버보안의 이해와 해사 사이버보안 관리실무의 교육과정을 개설하여 선원 및 선사 직원을 대상으로 사이버보안 관련 교육을 시행하고 있다(KR, 2017). 또한 사이버보안에 대한 국제표준(IEC 62443 4-2, IEC 61162-460)을 기반으로 자체 개발한 사이버보안 승인서비스를 제공하고 있으며, 사이버보안 교육을 위한 교육도구를 개발 하였다(KR, 2020a).

BIMCO는 사이버보안 관련하여 2016년부터 국제건화물선주협회, 국제해운회의소, 국제유조선선주협회, 국제정유사해운포럼, 국제크루즈선사협회, 국제해상보험연맹과 함께 'The Guidelines on Cyber Security Onboard Ships'를 개발하였고, 2018년 Ver.3으로 개정하여 발표하였다(BIMCO, 2018a).

국제유조선선주협회는 탱커선운영사안전관리평가(Tanker Management and Self Assessment, 이하 'TMSA'라 함)에 사이버보안 항목을 추가하여 2017년에 TMSA3을 개발 하였으며, 광탄선 화주검사에서도 검사항목에 사이버보안을 포함하였다(RIGHTSHIP, 2017). 포함된 검사항목에는 사이버보안 리스크 평가, 대응계획 유무, 대응절차 및 관리사항, 보안 교육 및 훈련, 보안 인증 등이 있다(OCIMF, 2017).

2.2 선박 사이버보안 위협 및 사건 사례

1) 선박 사이버보안 위협

미국표준기술연구소(National Institute of Standards and Technology)에 따르면 사이버보안 위협이란 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 접근, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건으로 정의하고 있다(NIST, 2019).

BIMCO는 선박에서 발생 가능한 사이버보안 위협을 비표적공격 유형과 표적공격 유형으로 구분하였다. 비표적공격은 회사나 선박 시스템과 데이터는 많은 잠재적 표적의 하나로 보고 공격하는 방식이며 Malware, Phishing, Water holing 등이 있다. 표적공격은 회사나 선박의 시스템 및 데이터가 의도된 대상으로 보고 공격하는 방식이며 Social engineering, Brute force, DDoS, Spear-phishing, Subverting the supply chain이 있다. 사이버보안 위협 유형의 세부내용은 Table 1과 같다 (BIMCO, 2018b).

Table 1. Type of cyber security threats

Type	Content
Malware	Malicious software which is designed to access or damage a computer without the knowledge of the owner.
Phishing	Sending e-mails to a large number of potential targets asking for particular pieces of sensitive or confidential information
Water holing	Establishing a fake website or compromising a genuine website to exploit visitors
Social engineering	A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media
Brute force	An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found
Deploying a botnet	To deliver a DDOS (Distributed Denial of service) attack
Spear -Phishing	Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software
Subverting the supply chain	Attacking a company or ship by compromising equipment, software of supporting services being deliverd to the company or ship

Source: BIMCO, The Guidelines on Cyber Security Onboard Ships, 2018a

2) 선박 사이버보안사건 사례

선박 사이버보안 위협과 관련된 주요사건으로 2016년 3월 북한이 GPS신호를 교란시킨 사례가 있다. 당시 GPS신호를 교란시켜 어선 등 280여척의 한국선박이 GPS시스템이 무력화 되었고, 공격을 당한 선박은 항구로 회항하였다. 두 번째 사례는 해적에 의한 선박의 선적화물 관리시스템 해킹 사건이다. 해적들은 2016년 3월 글로벌 해운사의 선적화물 관리 시스템과 선하증권 관리 시스템에 악성코드를 삽입하고, 시스템에서 선박, 항로, 화물 및 배송 기간 정보 목록을 확보하였다. 이후 싱가포르를 지나 인도로 가는 도중 공해 상에서 해당 선박을 납치하고 특정 고부가가치 화물이 적재된 컨테이너만을 강탈하였다. 세 번째는 선박의 운항시스템이 직접 해킹된 사례이다. 2017년 2월 8250TEU의 독일의 컨테이너선이 키프로스 항에서 지부티 항으로 가는 도중 10시간 동안 해커에 의해 선박의 항해시스템을 장악당하여 예정된 항로를 벗어나 해적들이 출몰하는 해역으로 항해 하였다. 결국 이 선박은 운항을 중단시키고 전문가가 승선하여 복구를 한 뒤에야 정상운항을 재개 할 수 있었다. 네 번째는 항만운영 소프트웨어의 랜섬웨어 감염이다. 랜섬웨어는 석방금(Ransom)과 소프트웨어(Software)의 합성어이다. 시스템 소프트웨어의 취약점을 이용하여 침입한 뒤, 해당 장비의 시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 한 다음 사용자에게 돈이나 금품 등을 요구하는 수법이다. 2017년 6월 머스크 해운회사는 랜섬웨어 공격을 받았다. 우크라이나 지점에서 감염된 Notpetya 랜섬웨어는 전 세계 지점과 항만 등에 전이되었다. 피해를 중단하기 위해 전체 IT시스템을 3개월가량 강제 다운시켰으며, 이로 인한 피해는 약 3천억으로 집계되었다(Jo and Kang, 2018).

위에서 언급한 주요 사건사례를 살펴보면 선박과 관련된 ICT의 취약점을 이용하여 사이버보안 공격을 가한 사실이 확인되었다. 이러한 공격에 대응하려면 선박 사이버보안 강화를 위한 CySO의 지정과 관련교육이 필요하다. CySO 역할의 중요성에 대한 인식개선이 필요하며, CySO 역량을 강화시킬 수 있는 방안이 요구된다.

3. 국내외 선박 사이버보안 책임자를 위한 사이버보안 교육 현황 및 필요성

3.1 국외 사이버보안 교육 현황

선박 사이버보안 책임자에 대한 교육필요성과 교육내용 및 방법 등을 참조하기 위해 국외 교육 현황을 조사하였다. 사이버보안에 대한 교육은 다양한 분야에서 이루어지고 있기에 선박을 대상으로 하는 교육만을 조사하였으며, 교육명칭과 개발기관 및 조직, 교육내용과 기간 등은 Table 2와 같다.

Table 2. Comparison of characteristics of cyber security training Personnel edited by the author

Institute	Name of training	Target Audience	Contents	Length of Training	Training Method
Aboamare	Maritime Cyber Security Introduction Course	IT security service specialists and experienced master mariners	-IMO's regulations and guidelines on cyber risk management onboard ships -Familiar with threats -Threat actors and their objectives know how to identify potential cybersecurity incidents -Management of cyber security strategies -Actions within an organization or onboard a ship	1 day	Lectures (On-site or virtual classroom)
DNV GL	Maritime Cyber Security Awareness	Shore-based and vessel personnel	-Role as a user in cyber security -Common threats & traps -Good practices towards cyber security	3 hours	e-learning only
LR	Maritime Cyber Security Awareness	Not defined	-Current and forthcoming regulatory requirements -Sources of potential cyber security threats and vulnerabilities -Conducting a cyber security risk assessment -Identifying risk mitigation strategies and control options -Utilising third-party specialist support when necessary -Implementing an effective cyber security risk management plan -Achieving continual improvement.	1 day	Lectures, Presentation, Group discussions, Case studies
MITAGS	Maritime Cyber Security Course	Not defined	-Quantitative risk analysis -Considerations in bridge communications, operations, navigation -Involvement in cargo operations and network sensors -Connection to engine room operations, shipboard IT networks -Association with port operations and vessel interface -Relationship to passenger ships, network IT and passenger data -The human factors of credentialing, regulations -Shaping the future of maritime industry through autonomous	5 days	Lectures, Discussions, Student-led presentations
SEANET	Cyber and Ship Security Training	Not defined	-Important knowledge and familiarization on all of topics including cyber-security, general security, stowaways, and anti-piracy measures	2 hours	DVD
Videotel	Cyber Security At Sea Training Course	Masters, officers, ratings and shore management	-Cyber security threats -IMO now requires companies to include a cyber risk management plan in the Safety Management System (SMS) -How to assess the risks to the ship's IT and OT -How the risks can be reduced -How to respond to a cyber security breach or attack -Necessitation constant vigilance and reviews of the cyber risk management plan	2-3 hours	CBT Video, Reference workbook, Tutorial and Course test
VTC	Cyber Security Awareness for Seafarers	Vessel personnel	-Information & operational technology, IT/OT systems onboard -Common threats and vulnerabilities -Best Practices and basic cyber-hygiene -Cyber security and safety management system (SMS) -Real-world examples of successful Cyber Attacks	5 hours	e-learning only

노르웨이-독일 선급(Det Norske Veritas Germanischer Lloyd, 이하 'DNV-GL'이라 함)은 TMSA를 준수하고, Oil Major Inspection을 수검 하는 유조선 관리회사들을 위해 'Maritime Cyber Security Awareness' 교육과정을 개발하였다. 사이버보안에 대한 역할, 일반적인 사이버보안위협과 공격방식, 사이버보안 강화를 위한 모범사례에 대한 교육모듈을 구성하여 'Seagull CBT distributor'를 통해 이러닝 형태로 선박 근무자들에게 교육을 제공하고 있다. 영국선급(Lloyd's Register, 이하 'LR'이라 함)은 DNV-GL와 동일한 교육과정 명칭으로 'Maritime Cyber Security Awareness' 교육과정을 개발하였으나, 교육대상을 특정하고 있지 않으며, 프레젠테이션 및 그룹토의와 사례 학습방식의 1일 교육을 운영하고 있다.

SEANET은 DVD를 이용한 사이버보안 및 선박 보안교육을 2시간으로 구성하여 이와 관련된 근무자들이 LMS나 Server 기반의 교육 시스템에서 이용하도록 교육과정을 개발하였다.

미국의 해양기술고등교육원(The Maritime Institute of Technology and Graduate Studies, 이하 'MITAGS'라 함)는 항해 장비부터 기관실, 화물에 관련된 센서들까지 선박의 특수한 네트워크 구조에 대하여 강의와 토론 및 학습자 주도의 발표과정을 포함하는 Maritime Cyber Security Course를 운영 중이다. MITAGS의 교육기간은 5일로 가장 길고 IT 시스템에서 생성, 처리 및 저장하는 데이터의 기밀성, 무결성 및 가용성을 보장하는 방법들과 사이버보안위협의 법적, 도덕적, 윤리적 파급효과와 보호에 관한 모범 사례 및 대응책까지 다루고 있다.

영국의 VTC(Virtual Training Centre)는 이러닝 형태로 'Cyber Security Strategy for Vessels' 교육과정을 개발하였다. 교육대상을 선원으로 명시하고 있으며, 동 기관에서는 육상과 선박의 관리 수준 이상 사용자들을 위한 'Cyber Security Strategy for Vessels'의 과정도 이러닝 형태로 교육을 제공하고 있다. Videotel은 CBT 기반의 영상과 워크북을 이용한 'Cyber Security At Sea Training Course' 교육과정을 제공 중이다. 선박의 선장과 사관 및 부원 뿐 아니라 육상 직원들까지 교육대상으로 하며, ISM code(MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems)와 ISO의 Information Security Management(ISO/IEC 27001, 2013)을 근거로 교육을 개발하였다. 선박 사이버보안 강화의 동일한 목적으로 개발된 교육과정들이지만, 교육명과 교육시간, 교육내용들이 상이했고, CySO를 대상으로 개발된 과정은 부재하다. 일반적으로 선박 사이버보안에 관련된 근무자들에게 도움이 된다거나 특정하지 않은 경우가 많았고, 특정된 경우도 선박의 선장 또는 책임자로 명시하고 있다. 교육의 방법도 이러닝 콘텐츠를 이용하거나, 토론 및 참여형 학습기법을 혼합한 강의, 학습자 주제발표 등 다양하게 개발되어 제공되고 있다. 국외의 사이버보안 교육과정 이행은 관련 법제를 기초로 하고 있다. 국외 법제를 비교·검토한 자료는 국내 관련 법제정비에 참고 될 수 있으며, 이를 위한 심도 깊은 관련 후속 연구가 필요하다.

3.2 국내 사이버보안 교육 현황

선박에 대한 사이버보안 교육을 제공하고 있는 국내기관은 KR이 유일하다. 선사 사이버보안 담당자(안전관리책임자, 보안책임자), CySO, 선장 또는 보안관리 업무에 지정된 자를 대상으로 '해사 사이버보안 관리 실무' 교육과정을 운영 중이다. '해사 사이버보안 관리 실무' 교육과정은 Table 3과 같이 2일(16시간)의 교육시간으로 구성되어 있다(KR, 2020b). KR의 교육과정은 CySO 대상의 교육내용과 교육방법을 제시하고 있으나, 선사 사이버보안 담당자에게 필요한 교육내용도 일부 포함되어 있다. 해당 교육은 연간 교육 횟수와 인원이 제한적이고, 선박 근무자들의 교육 참여가 어려운 문제점이 있어, KR은 '해사 사이버보안의 이해', '해사 사이버보안 관리 실무' 교육 동영상과 실무에 적용 가능한 샘플문서를 담은 'KR-CS++'를 USB 형태로 개발한 바 있다(KR, 2020c).

Table 3. Maritime cyber security management practice course of KR

Subjects	Contents
Understanding maritime cyber security	-Maritime Cyber security Overview -Cyber security organization -Cyber asset management -Cyber threat -Personal security -Physical security
Maritime cyber security IT	-Understanding the network -Network attack techniques & security solutions -Overview of diagnosis of technical weaknesses
Maritime cyber security IT Practice	-Account and permission management practice -User (PC) security practice
Understanding Maritime Cyber Security Risk Assessment	-Understanding ship cybersecurity and risk assessment -Understanding of risk assessment procedures and methods -Understanding of network diagram, risk acceptance criteria, cyber threat list
Maritime Cyber Security Risk Assessment Workshop	-Comprehensive chart of shipping company & ship network -Asset list creation and evaluation practice -Shipping/ship cyber security risk assessment practice -Control item cost/effectiveness evaluation
Physical security	-Purpose and method of physical security -KR Computer Room Physical Security -Risk assessment physical security
Technology security	-Technical Security: Network Security Solution -Technical vulnerability diagnosis overview -PC security vulnerability diagnosis tool

Source: Website, http://champ.krs.co.kr/applyView.do

3.3 선박 사이버보안책임자 교육 개발 필요성

국내외 다양한 기관과 조직에서 실시하고 있는 사이버 보안 교육을 조사한 결과, CySO만을 대상으로 개발된 과정은 부재하였으며, 교육명칭부터 교육내용, 교육기간까지 다양하게 실시되고 있다. 그러나 IMO의 ISM code에 대한 MSC.428(98) 결의안에 따라 선박의 사이버보안에 대한 요구가 더욱 강화될 전망이고, Oil Major Inspection, CDI Inspection, Rightship Inspection의 영향으로 선내 보안관리를 책임지는 CySO에 대한 교육수요가 증가할 것이다. 이에 따라 국제적인 가이드라인과 IMO와 ISO의 요건, TMSA에 만족하는 CySO 대상의 교육이 요구되지만, 현재의 국내외 교육들은 교육근거가 개발한 조직이나 기관에 따라 상이하므로 상기 요건들을 모두 만족할 수 있도록 CySO 업무와 국제적 가이드 라인에 따른 교육내용 구성이 제시되어야 한다. 그리고 랜섬웨어와 같은 형태를 통한 피해가 발생하고 있으므로 이러한 피해를 대비할 수 있는 교육내용도 필요하다.

선박 사이버보안 강화를 위해 CySO는 역할에 대한 명확한 인식 뿐 아니라 선박의 통신 시스템에 대한 이해도 요구된다. 선박 통신환경은 IT(Information Technology)와 OT(Operational Technology)의 범위가 명확히 구분되지 않고 정렬되지 않은 네트워크 형태로 인해 사이버보안 위협에 취약하다(KR, 2020a). 선박 통신 시스템과 IT 및 OT에 대한 교육은 필수적인 학습내용이며, CySO의 역할과 직무중심의 교육내용 구성 및 적절한 교육기간과 방법에 대한 개발이 필요하다.

4. 선박 사이버보안 책임자 교육과정(안)

4.1 선박 사이버보안 책임자 교육과정(안)

선박 사이버보안의 필요성과 국내외 사이버보안 관련 교육기관의 교육과정을 비교 분석하여 도출된 내용을 근거로 표준화된 CySO 교육과정안을 Table 4와 같이 제시하였다.

Table 4. Concept of Standard of CySO Training Course

Day	Content	Outline	Time	Training Mathod
1 Day	· Introduction & Familiar with threats	· Course introduction · Maritime Cyber security Overview · Role and responsibility as a ship cyber security officer	1 hour	Lectures, Presentations,
	· Recent ship cyber security incidents, domestic and international trends related to ship cyber security	· Common threats and vulnerabilities · Ship cyber security attack cases · Trends in maritime cyber security · Good practices towards cyber security	3 hour	Group discussions, Case studies
	· Punishment regulations and legal responsibility for violations of ship cyber security regulations	· IMO's regulations and guidelines on cyber risk management onboard ships · Current and forthcoming regulatory requirements · Reviews TMSA3 and RIGHTSHIP checklist for cyber security · Maritime Cyber Security Act	4 hour	Lectures, Presentations,
2 Day	· CSA/CSP development, understanding of periodic review procedures, and CSP implementation and execution ability	· Reviews CSP and CSA · Constant vigilance and reviews of the cyber risk management plan · CSA/CSP development	3 hour	Group discussions, Case studies
	· Prevention, detection and response, analysis, and recovery technology for ship cyber security incidents	· Detect and isolate equipment under ship cyber attacks and actions to be taken · How to respond to a cyber security breach or attack · Quantitative risk analysis · How to assess the risks to the ship's IT and OT · Utilising third-party specialist support when necessary	3 hour	Group discussions, Case studies
	· Understanding the procedures and methods of establishing a ship cyber security management system	· Ship cyber security measures · Cyber security and safety management system (SMS) · Implementing an effective cyber security risk management plan · Achieving continual improvement	2 hour	Lectures, Presentations,

교육기간은 2일이며 하루 8시간씩 총 16시간의 과정으로 구성하였다. 교육내용은 교육과정소개와 선박 사이버보안 위협의 친숙화 과정을 시작으로 최근 선박 사이버보안 사고 사례 및 선박 사이버보안 관련 국내외 동향과 선박 사이버보안 관련규정, 위반 시 처벌규정, 법적 책임사항을 포함하였다. 그리고 사이버보안평가(Cyber Security Assessment, 이하 'CSA'라 함)와 사이버보안계획서(Cyber Security Plan, 이하 'CSP'라 함)의 개발과 주기적 검토 절차의 이해와 CSP 구현 및 실행 능력을 갖추도록 하였고, 선박 사이버보안 사고 관련 예방, 탐지, 대응, 분석, 복구 등의 기술을 익히도록 하였다. 마지막으로 선박 사이버보안 관리시스템구축 절차 및 방법으로 구성하였다.

책임자급 대상으로 교육내용들은 공통적으로 사이버보안의 위협과 위험관리, IMO 규정 및 지침의 교육내용을 담고 있으며, IET 지침서에서도 CySO의 역할과 책임, 충분한 지식과 대응능력을 강조하고 있다. 그래서 선박 사이버보안의 개념, 위협, 동향, 관련 규정은 CySO에게 필요한 기본적인 교육내용으로 1일차 교육내용에 포함하였다. 2일차에는 위험관리기술 향상의 목적으로 심화된 내용을 다루며 실제적인 교육효과를 얻기 위해 선박 사이버보안 실무에 해당되는 내용을 포함하였다.

교육내용 구성을 기반으로 관련한 학습요소들을 검토하여 선박 사이버보안의 기초과정 8시간을 구성하였고 기초과정을 바탕으로 실무에 적용할 수 있도록 8시간의 심화과정을 구성하였다. 선박 사이버보안에 대한 이해도를 높이고 선박 사이버보안 실무역량을 향상시키는 CySO 교육과정은 CySO에게 실효성이 높은 교육결과를 가져올 것으로 예상된다.

국내외 사이버보안 교육기관에서는 이러닝, 집체교육, 사례 연구, DVD, CBT 등 다양한 교육방법을 사용하고 있었다. 사이버보안 기초 지식 전달은 온라인 교육 방식이 사용되었으며 책임자급 교육과정에서는 강의 방식과 케이스 스터디 방식이 사용 되었다. 또한 일부에서는 CBT Video 방식을 이용한 경우도 확인할 수 있었다. 여러 가지 사이버보안 교육의 방법을 비교하였을 때, 선박 사이버보안의 중요 실무 역할을 담당하는 CySO의 교육은 기본 이론을 바탕으로 그룹토론 및 케이스 스터디 등의 교육방법을 이용하는 것이 교육성과를 높일 수 있을 것으로 사료된다.

4.2 교육을 효과적으로 실시하기 위한 국내외 법제 정비의 필요성

1) 국제법제 정비의 필요성

선원의 훈련·자격증명 및 당직근무 기준에 관한 국제협약(International Convention on Standards of training, Certification and Watchkeeping for Seafarers 1978, 이하 'STCW'라 함)의 보안교육은 선박보안책임자 교육에 추가하여, 2010년 선박보안업무를 수행하는 담당자와 모든 선원에 대한 승선 전 교육요건 규정을 의무화 하였다. 선박보안책임자 증명서 발급 강제적 최저요건(STCW Table A-VI/5), 보안인식에 관한 해기능력의 최저기준 명세(STCW Table A-VI/6-1), 보안업무에 지정된 선원을 위한 해기능력 최저기준 명세(STCW Table A-VI/6-2)가 규정 되어 있다. 선박보안책임자의 규정은 명시하고 있으나, CySO의 자격기준에 대한 규정은 부재하여 관련 규정 마련이 요구된다.

IMO Model Course는 1978년 STCW 협약에 따라 여러 IMO 회원국의 제안으로 개발된 모델 훈련 과정 프로그램이다. IMO Model Course의 항목 중 '3.19 Ship Security Officer', '3.26 Security Training for Seafarers with Designated Security Duties', '3.27 Security Awareness Training For All Seafarers'에서 선박보안책임자 및 담당자와 전 선원들을 대상으로 하는 교육과정 프로그램이 규정되어 있다. 그러나 CySO에 대한 교육과정은 부재한 상태이며, 관련 교육과정 개발이 필요하다.

2) 국내법제 정비의 필요성

선원법은 선원의 직무, 복무, 근로조건의 기준, 직업안정, 복지 및 교육훈련에 관한 사항 등을 정하고 있다(NLIC, 2020). CySO 교육훈련에 관한 내용은 현재 부재하며 관련 항목을 제정하여 CySO교육의 기본 근거마련이 필요하다.

선박직원법은 선박직원으로서 선박에 승무할 사람의 자격을 정함으로써 선박 항행의 안전을 도모함을 목적으로 하고 있다. 선박안전법 제16조에는 해기사의 보수교육을 규정하고 있으며 CySO에 대한 부분은 부재하고 있는바 CySO가 자격을 갖추기 위해서는 관련 법령 제정이 요구된다.

국제항해선박 및 항만시설의 보안에 관한 법률(이하 국제선박항만보안법)은 국제항해에 이용되는 선박과 그 선박이 이용하는 항만시설의 보안에 관한 사항을 정함으로써 국제항해와 관련한 보안상의 위협을 효과적으로 방지하여 국민의 생명과 재산을 보호하는데 이바지함을 목적으로 하고 있다. 국제선박항만보안법 제8조에는 선박보안책임자에 대해 규정하고 있으나 CySO에 대한 규정은 부재한 상태이다. 선박보안책임자와 같이 CySO의 역할 정의가 필요하다.

국가사이버안전관리규정은 대통령 훈령이며 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다. 선박 사이버보안 사고는 선박을 이용하여 항만 등 국가중요시설을 파괴할 수 있는 가능성을 내재하고 있다. 따라서 CySO 및 선박 사이버보안 강화 관련 규정을 제정하여 해상에서의 사이버 공격에 대응 할

수 있는 법적 근거가 마련되어야 할 것이다.

국가사이버보안에관한법률은 2016년 5월 국회에 발의되었으나 2020년 5월 임기만료폐기 상태이며(NARK, 2020), 법적 근거 부재로 인해 사이버보안 위협 대응에는 한계를 보일 수밖에 없다. 국가의 중요산업인 해운산업을 보호하기 위하여 선박 사이버보안에 관한 규정을 포함하는 국가사이버보안에관한법률의 제정이 시급하다.

5. 결 론

정보통신기술의 발전으로 선박이 디지털화 되면서 선박은 사이버보안 사고에 지속적으로 노출되고 있다. 다가오는 자율운항선박의 시대의 선박 사이버보안 사고는 더 심각한 피해를 가져올 수 있다. 이 연구는 선박 사이버보안 사고의 선제적 대응책으로 CySO에 대한 교육과정안을 제시하였다. 이를 위해 국내외 선박 사이버보안 관련 동향을 검토하고, 전문교육기관에서 시행하고 있는 교육과정을 비교하여 CySO의 표준교육과정안을 도출하였다. 또한 관련된 국내외 법제를 검토한 결과 CySO교육 이행에 대한 근거가 부재하므로 관련법제 정비가 요구된다. 선박의 사이버보안 운영관리에서 CySO 역할은 중요하며 표준화된 교육은 사이버보안 사고예방 및 대응능력 향상에 도움이 될 것이다.

점차 고도화 되어가는 선박 사이버보안 공격에 대비하기 위해 선박에 승선하는 모든 선원 및 해사사업 관련업계 종사자에 대한 사이버보안 교육도 필요할 것으로 예상된다. 따라서 선원 및 해사산업 관련업계 종사자 교육과정 개발에 대한 후속연구도 필요할 것으로 사료된다. 이와 더불어 선박 사이버보안에 대한 노조, 정부, 사측의 지속적인 관심이 필요하며, 선박 사이버보안 위협에 선제적으로 대응하여 피해를 줄이기 위한 상호간의 동의가 필요하다.

References

[1] BIMCO(2018a), The Guidelines on Cyber Security Onboard Ships, Ver. 3, Annex 4 Glossary, pp. 50-52.

[2] BIMCO(2018b), The Guidelines on Cyber Security Onboard Ships, Ver. 3, pp. 10-11.

[3] IET(2017), Code of Practice Cyber Security for ships, The Institution of Engineering and Technology, pp. 27-29.

[4] IMO(2014), MSC 94th session, 17-21 November 2014, Cyber security matters considered.

[5] IMO(2015), MSC 95th session, 3-12 June 2015, Cyber Security matters referred to MSC 96 and FAL 40.

[6] IMO(2016), MSC 96th session, 11-20 May 2016, Cyber Security - interim guidelines approved.

[7] IMO(2017), Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems.

[8] Jo, Y. H. and J. M. Kang(2018), Prospects of cyber security risks of autonomous ships, Institute of Information & Technology Planning & Evaluation, Weekly ICT Trends Vol 1863, 12 Sep 2018, pp. 21-24.

[9] Jo, Y. H. and Y. K. Cha(2019), A Study on Cyber Security Requirements of Ship Using Threat Modeling, Korea Institute of information Security And Cryptology, pp. 661-662.

[10] KMI(2019), A Study on Strengthening to cybersecurity System in the Maritime Sector, p. 39.

[11] KR(2017), Guidelines of Maritime Cybersecurity, Ver 1.0.

[12] KR(2020a), KR Maritime Cyber Security, News from KOREAN REGISTER, Vol 029, pp. 7-11.

[13] KR(2020b), Korean Register Champ, Consortium for HRD Ability Magnified Program, Retrieved from http://champ.krs.co.kr/applyView.do, on Oct 10.

[14] KR(2020c), KR launches a cyber security training tool KR-CS++ 2020', News and Press Releases, Retrieved from http://www.krs.co.kr/, on Oct 10.

[15] Lee, H. K. and O. J. Kwon(2020), The UK Insurance Industry's Response to maritime Cyber Risk and It's Implications, Korean Insurance Law Association, Vol. 14, No 2, pp. 237-238.

[16] NARK(2020), The National Assembly of the Republic of Korea, Bill Information, Retrieved from http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_L1Z6M0L5M3W0U1W4T2M8K4L3S5I0Y2, on Oct 10.

[17] NIST(2019), National Institute of Standards and Technology, NIST SP 800-128, Guide for Security-Focused Configuration Management of Information System, Appendix B GLOSSARY, B-8.

[18] NLIC(2020), The National Law Information Center, Retrieved from http://www.law.go.kr/, on Oct 10.

[19] OCIMF(2017), TMSA3 Fast Facts, p. 2.

[20] RIGHTSHIP(2017), FO D06 Inspection and Assessment Report For Dry Cargo Ships, Rev 11, 11 May 2017, p. 8.

[21] Shaw, N. and C. Ayerst(2017), The UK's Cyber Security Code of Practice for Ships, Reed Smith, Oct 2017, p. 10.

Received : 2020. 10. 12.
Revised : 2020. 11. 25.
Accepted : 2020. 12. 28.