
Global Report

항만 사이버 보안 및 위협: 예방 및 정책 개발을 위한 구조 모델

1. 개요
2. 태국의 Laem Chabang 항만의 가치
3. 태국과 LCP의 사이버 보안 및 위협
4. 연구방법론 및 설문조사
5. 설문측정 모델에 대한 결과
6. 검토 및 결론

1. 개요

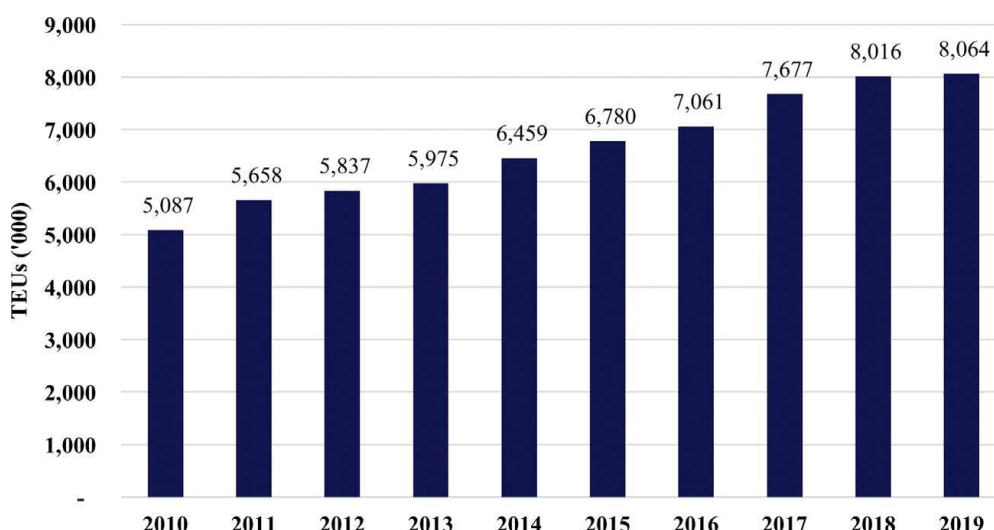
지난 수십 년 동안 대부분의 해상운송 사업자는 디지털 기술을 도입함으로써 자신의 비즈니스 모델을 수정하고 프로세스 효율성을 업그레이드하여 고객을 위한 가치를 창출해왔으며, 아울러 법적 요구사항을 준수하면서 경쟁우위를 유지해왔다[1][2]. 해당 사항의 명백한 증거자료들은 운송부문에서 확인이 가능한데 다음과 같은 사례들이 있다.

- 전 세계 상선(merchant fleet)의 90% 이상이 디지털 시스템을 사용하여 ECDIS, GNSS, AIS, VDR 및 레이더와 같은 디지털 내비게이션 네트워크를 이용하고 있다.
- 해상운송의 효율적인 관리 및 운영을 위해 다양한 운송 관련 리스트(선박, 화주 및 항구 간 물리적 보안, 선박 관리, 승무원의 복지, 화물의 적재목록 등)를 작성하여 디지털 시스템으로 관리하고 있다.
- 선박의 추진 및 조향을 모니터링 및 제어하기 위한 온보드 기계(onboard machinery)의 수동시스템을 디지털 기술로 교체하고 있다.

이처럼 물류센터와 해운선과의 연계가 디지털화됨에 따라 컨테이너 항만은 다양한 항만 활동((공정 설계, 화물 취급 및 내비게이션, 환경오염 방지, 위험 관리, 항만 안전 및 보안 등))에 사이버 기술 적용이 의무화되었다. 이 연구에서는 태국의 Laem Chabang 항만에 대한 사례연구를 통해 항만의 사이버 보안 위협의 핵심 요소와 5개 사이버 위협 그룹과의 관계를 보여주는 새로운 모델을 제시한다.

2. 태국의 Laem Chabang 항만의 가치

태국 동부 해안에 위치한 가장 큰 컨테이너 항구인 Laem Chabang 항만(LCP : Leam Chabang Port)은 태국을 넘어 아세안 지역의 경제성장을 이끄는 데 중요한 역할을 해왔다. 그 결과, LCP는 141개 이상의 세계적인 항만과 연결하여 글로벌 해상운송 산업을 주도하고 있다. LCP는 11개의 터미널(A0~A5, B1~B5)로 구성된 LCP 1항만과, 7개의 터미널(C0~C3, D1~D3)로 구성된 LCP 2항만이 있다. 컨테이너선, 일반 화물선, roll-on/roll-off 선박, 벌크 캐리어, 여객선 및 일반 보트에 항구 서비스를 제공하고 있다. 최근 10년 동안(2010~2019) LCP의 컨테이너 처리량 증가추이를 보면 2010년 5,087TUE, 2016년 7,061 TUE에서 2019년에는 8,064 TUE로 지속적으로 증가하고 있다[6][7][8]. (그림 1 참조)



* 자료 : Chalermpong Senarak, "Port cyber security and threat: A structural model for prevention and policy development", The Asian Journal of Shipping and Logistics xxx (2020) xxx-xxx, p.3.

Port Authority of Thailand, based on data from performance reports 2010–2019.

[그림 1] LCP의 컨테이너 처리량 증가추이

이처럼 태국 내 및 지역 컨테이너 운송수요가 지속적으로 증가함에 따라 LCP-3 프로젝트는 태국 EEC(Eastern Economic Corridor) 개발계획에서 가장 중요한 메가 프로젝트 중 하나가 되었다. LCP 3항만은 공공-민간 파트너십으로 형성된 1,558만3,400만THB(태국바트)의 거대예산을 투자하여 최상의 컨테이너항 가치를 갖춘 터미널 E1, E2, F1 및 F2를 설립하여 연간 770만TUE에서 1,810만 TUE의 컨테이너 처리용량을 늘리는 것을 목표로 하고 있다. LCP 3항만에 대한 투자는 UN의 지속가능한 개발 목표를 지원하기 위해 자동화 기술, 녹색 장비 및 전자시스템 등에 중점을 두고 있다[6][7][8].

3. 태국과 LCP의 사이버 보안 및 위협

2018년 글로벌 사이버보안 지수는 태국 정부가 데이터 보호법(ITU, 2018)의 관점에서 사이버 역량을 개선하기 위해 많은 노력을 기울였다고 평가하였다[9]. 특히 태국은 아시아-태평양 지역에서 사이버 공격에 대비한 상위 10개국에 속하지만 매년 엄청난 사이버공격을 경험하고 있는 국가 중 하나이기도 하다. 2011~2019년까지 태국의 공공 및 민간 부문에서 사이버 사건(보고서 수)을 <표 1>에 나타낸다 [9].

<표 1> 태국의 공공 및 민간 부문에서 사이버 사건(보고서 수)

연간 사고유형	2011	2012	2013	2014	2015	2016	2017	2018	2019	계
사기	309	534	694	1007	1141	1002	841	929	912	7,369
악성코드	63	82	73	1738	1546	1020	271	127	436	5,356
침입 시도	94	75	316	504	664	706	939	1102	467	4,867
침입	0	13	631	709	1005	1020	570	335	218	4,501
가용성	6	2	10	8	6	29	540	0	79	680
정보보안	0	2	0	4	1	20	68	18	165	278
정보 수집	93	62	8	29	0	0	8	0	60	260
가학적인 콘텐츠	77	3	13	8	8	0	0	1	124	234
기타	4	19	0	0	0	0	0	8	9	40
계	646	792	1745	4007	4371	3797	3237	2520	2470	2,620.56 (Ave.)

* 자료 : Chalermpong Senarak, “Port cyber security and threat: A structural model for prevention and policy development”, The Asian Journal of Shipping and Logistics xxx (2020) xxx-xxx, p.4.

2011~2019년까지 다양한 사고유형 중 사기와 관련된 사고건수가 7,369건으로 1위, 악성코드가 5,356건으로 2위, 침입 시도가 4,867건으로 3위를 기록하였다. 특히 2019년의 경우, 전체 사고유형(사기/악성코드/침입 시도/침입/가용성/정보보안/정보 수집/가학적인 콘텐츠/기타) 건수는 2470건으로 2015년 4371건, 2014년 4007건, 2016년 3797건, 2017년 3237건, 2018년 2520건에 이어 6위를 기록하면서 2013년 이후부터 전년 대비 2배 이상 증가하고 있는 것으로 나타났다.

4. 연구방법론 및 설문조사

태국과 Laem Chabang 항만의 사이버 보안 및 위협요인을 보다 더 구체적으로 파악하기 위해 두 그룹을 기반으로 설문조사를 시행하였다. 설문항목은 다음과 같이 두 그룹으로 나누어 시행하였다.

- 첫 번째 그룹은 5가지 사이버위협(4대 hacktivism, 8대 사이버범죄, 7대 사이버 스파이, 4대 사이버 테러, 2대 사이버 전쟁)과 관련된 25개 항목으로 구성하였다.
- 두 번째 그룹은 사이버 보안위협의 3요소(6대 인적 요인, 27대 인프라 인자, 10대 절차 계수)를 나타내는 43가지 항목으로 구성하였다.

설문지는 다음과 같이 세 부분으로 설계하였다.

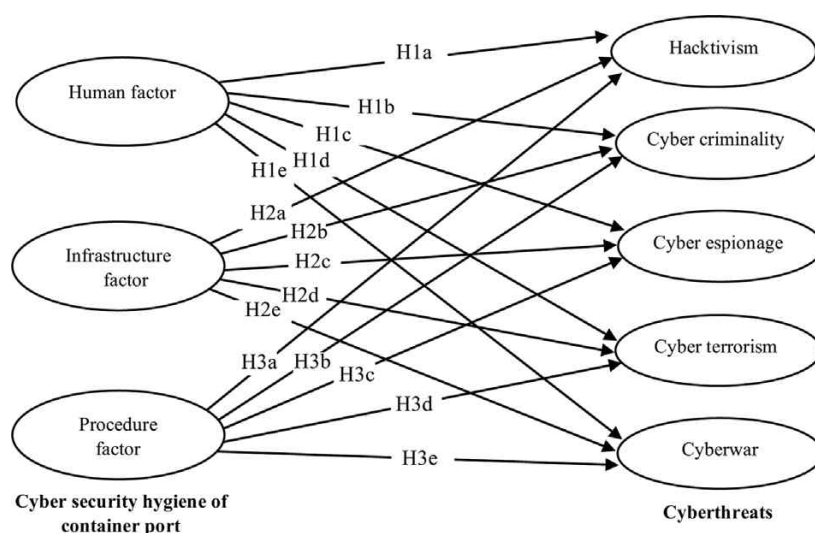
- 첫 번째 설문지는 응답자와 기업에 관한 일반적인 정보를 수집하였다.
- 두 번째 및 세 번째 설문지는 각각 제1 및 제2군에 대해 위에서 언급한 68개 항목에 대해 정보를 수집하였다.

(제1그룹인 5가지 사이버위협 관련 25개 항목 + 제2그룹인 3대 사이버 보안위협을 나타내는 43가지 항목)

모든 설문은 5점 만점(1=절대 동의하지 않음, 2=동의하지 않음, 3=동의 없음, 4=동의함, 5=강하게 동의함)으로 점수를 매겼다. 응답자들은 태국이 다른 나라의 컨테이너 포트의 사이버보안 위협에 비해 위협요인이 많다고 응답하였다. 이를 통해 사이버위협을 방지하기 위한 측정값에 대한 역량을 평가할 수 있었다.

5. 설문측정 모델에 대한 결과

태국과 LCP의 사이버 보안 및 위협요인을 측정하기 위한 설문조사 결과를 토대로 도출한 연구 개념 모델을 [그림 2]에 나타낸다. 이는 8개의 잠정 구조는 기존 문헌(사이버 보안위협을 위한 3개 구조 및 사이버 위협에 대한 5개 구조)을 기반으로 개발되었다.



* 자료 : Chalermpong Senarak, "Port cyber security and threat: A structural model for prevention and policy development", The Asian Journal of Shipping and Logistics xxx (2020) xxx-xxx, p.9.

[그림 2] 연구 개념 모델

IBM의 SPSS 통계 version 22를 사용하여 EFA(Exploratory Factor Analysis : 탐색인자분석)를, IBM의 AMOS version 21을 사용하여 측정 모델을 평가하기 위해 CFA(Confirmatory Factor Analysis : 확인인자분석)를 수행하여 계수 분석을 시행하였다. 사이버 보안위협은 인적, 인프라 및 절차요인으로 구성된

다. 인적 요인을 측정하는 데 6개 항목이 사용되었고, 27개 항목이 인프라 계수를 측정하는 데 사용되었으며, 10개 항목이 절차계수를 측정하는 데 사용되었다. 요인분석을 수행한 결과, 26개 항목에는 수렴유효성을 유지하기 위해 0.6 미만의 로딩 팩터가 있는 것으로 나타났다. 따라서 인명구조에서 하나의 항목을 제거하고, 인프라 인자 구조에서 21개 항목, 계수구조에서 4개의 항목을 제거하였다 이 이유는 특정 구문을 적절히 나타내지 못하고 0.6 이상의 로딩 인자를 가진 항목만 유지 및 추가 분석을 고려했기 때문이다. 이러한 26개의 항목을 제거한 후 나머지 항목은 요소를 분석했으며 결과는 <표 2>와 같다.

<표 2> 사이버 보안위협 및 사이버 위협요인 분석

구분	위협요인지수		
사이버 보안위협	인적 지수	인프라 지수	생산자 지수
인력 교육	.751		
인력에 대한 보안인식	.904		
임원 교육	.734		
경영진의 보안인식	.909		
ICT 보안 직원 및 대응팀	.638		
화물 컨테이너 추적 및 교통관제시스템	.709		
인터넷 제어시스템		.676	
외부 협업 네트워크		.785	
정보보안		.661	
통신 및 공동작업 보안		.666	
인터넷 및 네트워크 보안		.686	
위협 관리			.844
항만 리스크 거버넌스			.621
정보공유			.800
위협 및 취약점 관리			.823
사이버 및 프로그램 관리			.776
복원력 측정 및 시스템 중복성			.778
복합 신뢰성	0.849	0.807	0.877
추출된 평균 분산	0.533	0.511	0.545

* 자료 : Chalermpong Senarak, “Port cyber security and threat: A structural model for prevention and policy development”, The Asian Journal of Shipping and Logistics xxx (2020) xxx-xxx, p.11.

6. 검토 및 결론

설문조사 결과를 토대로 도출한 연구 개념 모델을 이용하여 태국과 LCP의 사이버 보안 및 위협요인을 조사한 결과, 세 가지 요인(인간, 인프라 및 절차)이 항만 사이버 보안위협을 구성하고 있으며, 이들은 상호 의존하는 것으로 나타났다. 즉, 한 요인의 실패는 다른 요인을 약화시킬 수 있다는 것이다. 이러한 결과는 세 가지 요인 간 상호의존성을 강조한 기존의 이론과 일치하는 것을 확인하였다. 가장 효과적으로 사이버 보안위협에 대응하기 위해서는 항만의 디지털 자산, 기술 및 시설(인프라 요소)을 사이버위협에 대비하여 예방적 조치(절차 요소)를 구현하고, 숙련된 인력(인적 요인)을 양성할 필요가 있다.

- 인적 요인의 경우, 특히 항만의 정보기술 및 네트워크 관리, 사이버보안 관리 및 정책개발에 직접적인 책임이 있는 사람들로 하여금 항만근로자에 대한 교육을 제공할 필요가 있다.

- 인프라 요인의 경우, 컨테이너 포트가 사이버 보안위험을 강화하기 위해서는 항만 인프라 및 시설에 대한 투자가 필수적으로 요구된다.
- 절차 요인의 경우, 컨테이너 포트에서 발생할 수 있는 보안위험요인에 대한 예방적 조치 및 보안 절차를 엄격하게 구현할 필요가 있다.

사이버 기술을 항만운영에 통합하여 항만을 통한 운송 산업의 경쟁력을 높이고 있다. 이 연구에서는 항만의 사이버 보안위험요인(인간/인프라/절차요인)을 개념화하여 항만의 사이버 위험요인(해킹비즈니스/사이버 범죄/사이버 스파이/사이버 테러/사이버 전쟁 등)과의 관계를 조사하였다. 이 연구결과는 국내 컨테이너항의 사이버 위험을 해소할 수 있는 정책에 벤치마킹 자료로 활용할 수 있을 것이다.

[참고문헌]

- [1] Shepherd, J. (2004). What is the digital era? Social and Economic Transformation in the Digital Era, 18.
- [2] Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management*, 11(4), 519-540.
- [3] International Chamber of Shipping. (2018). The Guidelines on Cyber Security Onboard Ships. <<https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20>>
- [4] Tsai, M.-C. (2006). Constructing a logistics tracking system for preventing smuggling risk of transit containers. *Transportation Research Part A: Policy and Practice*, 40(6), 526-536.
- [5] Yeo, G.-T., Pak, J.-Y., & Yang, Z. (2013). Analysis of dynamic effects on seaports adopting port security policy. *Transportation Research Part A: Policy and Practice*, 49, 285-301.
- [6] Laem Chabang Port. (2019a). Laem Chabang Port phase 3 - Project scope. <<http://www.laemchabangportphase3.com/files/MarketSounding2/Documentation2.pdf>>
- [7] Laem Chabang Port. (2019b). Statistics 2016-2019. <<http://lcp.port.co.th/cs/Satellite?blobcol=urldata&blobheadname1=Content-Disposition&blobheadname2=filename&blobheadvalue1=inline%3B+filename%3D%22st2562.pdf%22&blobheadvalue2=filename%3D%22st2562.pdf%22&blobkey=id&blobnocache=false&blobtable=Mung>>
- [8] Laem Chabang Port. (2019, January 25). Translation of the invitation to tender. Chonburi, Thailand. <<http://www.laemchabangportnew.com/attachments/article/1959/LCP%20Ph3%20Invitation%20toTenderEN%2020190125.pdf>>
- [9] International Telecommunication Union (ITU). (2018). Global Cyber security Index 2018. <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>
- [9] Thailand Computer Emergency Response Team. (2019). Statistics. <<https://www.thaicert.or.th/statistics/statistics-en.html>>

<원문제목> Port cybersecurity and threat: A structural model for prevention and policy development

<원문출처> The Asian Journal of Shipping and Logistics xxx (2020) xxx-xxx