Journal of the KNST

2026; Vol.9, No.2; pp.531-539

ISSN: 2635-4926 https://doi.org/10.31818/JKNST.2026.6.9.2.531

Check for updates

Received: 2026/05/28
Revised: 2026/06/09
Accepted: 2026/06/27
Published: 2026/06/30

*Corresponding Author.
Jung-Sik Lee
Tel: +82-2-3400-2687
Fax: +82-2-403-3512
E-mail: godsider@add.re.kr

Abstract

본 논문에서는 미래 함정 통합 사이버방호체계 설계 방안을 제안한다. 미래 함정 환경은 무인화·자동화로 네트워크는 통합되고 사이버 담당 인력은 줄어드는 등 사이버 대응환경이 악화되는 것을 고려하여 통합 사이버 방호 및 계층적 사이버 대응을 위한 설계를 수행하였다. 향후 미래 함정의 사이버 방호체계를 계획할때 참고로 활용할 수 있다.

This paper proposes a design framework for an integrated cyber defense system intended for future naval vessels. Considering the deteriorating cyber environment—characterized by integrated networks resulting from unmanned automation and a simultaneous decrease in dedicated cybersecurity personnel—this study implements a design for integrated cyber protection and hierarchical cyber response. This research can serve as a key reference for planning cyber defense architectures for future naval ships.

Keywords

사이버방호체계(Cyber Defense System),
거대언어모델(Large Language Model),
REST 아키텍처 기반 API(RESTFul API),
개방형 지휘통제(Open C2),
대응방책(Course of Action)

Acknowledgement

이 논문은 2023년 정부의 재원으로 수행된 연구 결과임

미래 함정 환경을 고려한 함정 통합 사이버방호체계 설계 방안 연구

A Study on the Design of an Integrated Cyber Defense System for Future Naval Vessel Environments

이정식[1*], 옥지원[2], 구성모[3], 한인성[3]

[1]국방과학연구소 제3기술연구원 수석연구원
[2]국방과학연구소 제3기술연구원 연구원
[3]국방과학연구소 제3기술연구원 책임연구원

Jung-Sik Lee[1*], Ji-Won Ock[2], Sung-Mo Koo[3], In-Sung Han[3]

[1]Senior principal researcher, 3rd R&D Institute, Agency for Defense Development
[2]Researcher, 3rd R&D Institute, Agency for Defense Development
[3]Principal researcher, 3rd R&D Institute, Agency for Defense Development

1. 서론

미래 함정 환경은 초연결 네트워크를 기반으로 하는 '시스템의 시스템(system of systems)'이며 유/무인 복합체계로 진화는 필연적이다. 이러한 환경은 사이버 공간에서의 취약점을 증대시키고 있다. 또한 인공지능(AI) 기반 공격 도구가 보편화됨에 따라 함정 개별 수준의 보안 대응체계만으로는 지능형 지속 위협(advanced persistent threat, APT)과 다각적인 사이버 공격을 차단하는 데 한계가 있다. 특히 함정 내부의 사이버 보안 인력 부족은 가장 시급한 문제 중 하나이다.

이를 극복하기 위해 본 연구는 함정 내부에서 모든 의사결정을 내리는 전통적인 방식에서 벗어나, 상위 부대인 함대 지휘통신대와 해군본부 사이버 작전센터가 유기적으로 협력하는 계층적 방호체계를 제안한다. 이 구조는 함정이 수집한 로우 데이터를 함대 수준에서 전문적으로 판단 및 대응하고, 표준화된 Open C2을 통해 대응을 함대에서 수행 가능하게 하는 것을 목표로 한다. 본 연구의 목적은 함정 내부의 보안 장비와 상위 지휘 계통 간의 원활한 연결을 위해 RESTful API와 전용 프록시 기술을 도입하여, 인력 부족에

도 사이버 대응의 정확성과 작전 지속성을 동시에 확보하는 방안을 모색하는 데 있다.

2. 관련 연구

본 장에서는 선진국의 사이버 방호체계에 대한 조사 결과를 설명한다.

2.1 미 해군 CASA(Common Architecture System Assurance)

미 해군의 CASA는 NSWCDD(Naval Surface Center Dahlgren Division)에서 2013년도에 개발한 함정용 정보보호체계로 함정 내부의 시스템, 네트워크를 포함한 다양한 센서로부터 사이버 이벤트를 수집하고 중앙 저장소에서 상관관계를 분석하는 고도의 보안 정보 및 이벤트 관리(security information and event management, SIEM) 플랫폼으로 볼 수 있다.

CASA의 핵심 가치는 함정 시스템 구축 단계부터 보안 기능을 내재화(secure by design)하여, 개별 장비의 알람이 아닌 전체적인 cyber 영향(네트워크 침투, USB, file 변조, login 시도 등)을 아래 Fig. 1과 같이 지휘관에게 시각화하여 제공한다는 점이다.

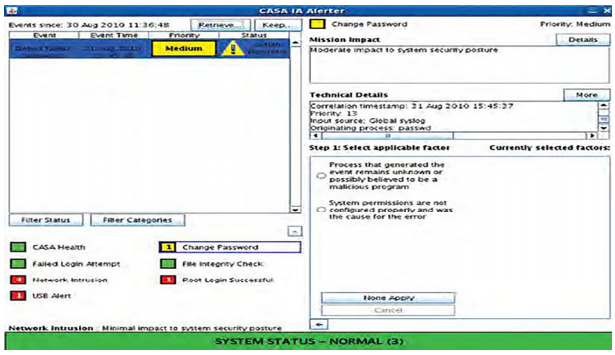

Fig. 1. CASA user interface

2.2 미 해군 CANES(Consolidated Afloat Networks and Enterprise Services)

CANES는 Fig. 2와 같이 해상 정보 시스템에 탑재한 네트워크 통합 솔루션이며, 유연한 개방형 아키텍처를 도입하여 장기적으로 비용을 절감하고 전투함 운용의 민첩성을 제공하여 기존 C4I 네트워크를 통합/강화하려는 시스템이다. 또한 CANES는 미 국방부에서 주관하는 C4ISR 시스템과 연계하는 크로스-도메인 솔루션을 가지며 CANES 시스템은 IT 인프라의 혁명적인 변화를 가져올 것으로 예상된다[1].

미 해군 전함중 최초로 맥캠벨호(DDG85)가 CANES를 2013년 11월에 설치, 운영하고 있다.

Fig. 2. Concept of with CANES and without CANES

2.3 이스라엘 Neptune 및 사이버 돔

이스라엘 IAI ELTA사의 Neptune 체계는 함정용 정보보호체계로, 전함, 프리깃함, 잠수함, 무인함 등 해군 플랫폼을 위한 사이버 모니터링 시스템이다.

Neptune은 방화벽, 안티바이러스, 네트워크 장치, 기타 센서의 이상 상황 이벤트를 취합하여 함정 무기체계 및 부체계의 이상 여부를 계층적으로 보고한다. Neptune은 여러 함정에서 수집된 사이버 이벤트를 종합하는 솔루션을 제공하며, 해군 지휘부는 Neptune을 이용해 통합 플랫폼으로 사이버 뷰 및 함대 사이버 뷰를 제공할 수 있다.

Neptune 시스템은 다음과 같은 3가지 서브시스템으로 구성되어 있다.

- WPCM(warfare platform cyber monitoring): 해군 플랫폼에 내장된 모니터링 및 경고 시스템
- PSOC(platform security operational center): WPCM용 지휘통제 및 사용자 인터페이스
- SOC(security operational center): 경고를 수집해 각 함의 사이버 상태를 나타내는 함대 레벨의 관제

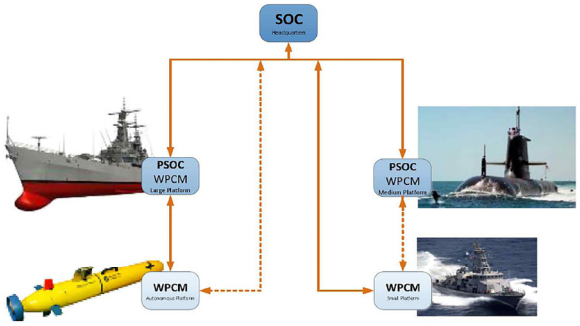

Fig. 3. Neptune SOC architecture

2.3.1 WPCM

WPCM은 보안장비, IT 장비에서 수집된 원시 데이터, 서드파티 센서의 경고, 시스템 기술 모니터 로그, 가공된 센서 등을 통하여 데이터를 수집한다. 이러한 행위는 전투체계, C4I 체계, 항해 체계에 영향을 주지 않는 선에서 수행된다. 수집된 데이터는 머신러닝을 이용하여 이상행위 여부를 판단하는데 활용되며, 이상 행위가 탐지되는 경우에는 경고를 생성하여 PSOC 및 SOC로 전달하는 역할을 수행하게 된다.

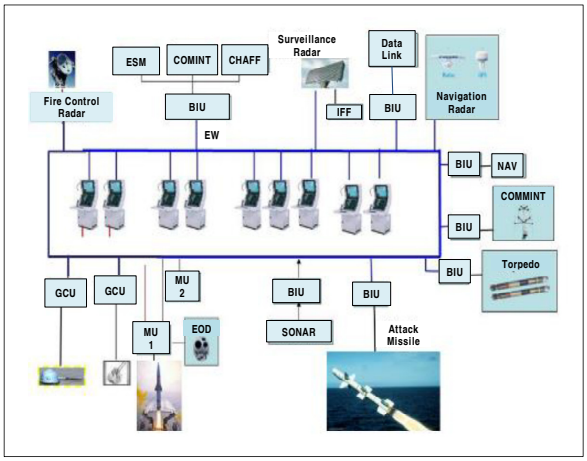

Fig. 4. WPCM architecture

2.3.2 PSOC

PSOC의 주요 기능은 크게 3가지로 나뉜다. 플랫폼의 사이버 상황을 형성하고 가시화하는 기능, WPCM에 인터페이스를 제공하는 기능, 지휘부의 SOC와 통신하는 기능을 제공한다.

Fig. 5. Example of PSOC UI

2.3.3 SOC

SOC는 함대 레벨의 사이버 상황 가시화, 특정 사이버 이벤트 발생사항 전시, PSOC와의 통신 등의 역할을 수행한다. 해군 지휘부는 Neptune의 SOC(Security Operational Center, 보안 작전 센터)를 통해 함대 내 사이버 현황을 모니터링하고 원격으로 관리를 할 수 있다. AI 기반의 이상 징후 탐지 기술과 다중 센서 데이터 퓨전(satellite, AIS, radar)을 결합하여 해상 상황 인식을 극대화한다.

Fig. 6. Example of SOC UI

2.4 일반적인 함정의 사이버방호체계

함정에는 전투체계, 통합함교체계, 통합통신체계, 통합기관제어체계 등 다양한 시스템들이 있으며, 각 시스템의 방호대책에 따라 상용 방호장비(방화벽, IPS, UTM 등)를 운용하여 시스템을 개별적으로 보호하고 있다.

함정의 운용환경이 인터넷 연결이 불가하고 시스템 간에 연동이 제한적이라 사이버 위협은 적은 편이나, 공급망 보안 취약점, 제로데이 공격 및 일부 연동에 의한 위험은 계속 상존하고 있으며 사이버 문제점이 발생하기 전까지는 함정 내부 및 함정 상위 부대에서 판단은 불가한 환경이다[2].

3. 제안하는 지능형 함정 통합 사이버방호체계 구축 방안

본 연구에서 제안하는 지능형 방호체계는 미래 함정 환경의 인력 한계, 전술 통신망 한계, 그리고 실제

운용 장비의 물리적 하드웨어 규격을 종합적으로 고려하여 설계된 지능형 함정 통합 사이버방호체계이다. 이를 위해 본 장에서는 소프트웨어 수준의 동작 메커니즘을 정의하는 3.1절 논리 아키텍처 및 소프트웨어 협업 메커니즘과 이를 하드웨어 인프라에 안착시키는 3.2절 하드웨어 구축 방안 설계로 나누어 제안한다.

본 연구가 제안하는 논리 아키텍처는 부대 구조와 연계된 3개 계층(tier)으로 구성되며, 각 계층은 고유의 임무와 기술적 역할을 수행한다.

3.1 계층별 논리 아키텍처 및 소프트웨어 협업 메커니즘

제안하는 논리 아키텍처는 '함정-함대-해군본부'로 연계되는 긴밀한 다계층 상호 연동을 중심으로 설계된다.

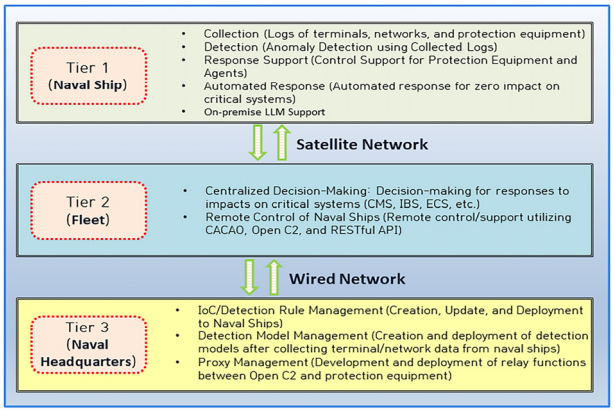

Fig. 7. Concept of an intelligent integrated cyber defense system for naval ship

3.1.1 함정 계층(Tier 1): 로그 수집, 실시간 탐지, 자동 대응, 함대 대응 명령 수행 및 AI 보조

함정은 최일선에서 사이버 위협 데이터가 발생하는 지점이며, 함정 내부의 정보자산(무기체계, 전투체계, 제어장비, 지원장비)에 영향이 없이 함께 운영되어야 한다.

함정 계층은 경량형 구조로서 기존 시스템에 영향이 미치지 않는 최소 연산 자원 사용과 무인 자동 대응을 목적으로 한다. 1계층의 주요기능은 정보수집, 실시간 탐지, 비전문 인력 지원용 대화형 AI(폐쇄망 LLM), 기존체계 가용성 보장 기반 자동 대응으로 구성되며, 상세한 설명은 아래와 같다.

3.1.1.1 분산 정보 수집 및 실시간 탐지

함정 내부에 구축된 방화벽(FW), 침입차단시스템(IPS), 통합위협관리(UTM), 네트워크 접근제어(NAC) 장비와 단말 에이전트 및 네트워크 수집기를 통해 모든 로그 및 보안 이벤트를 수집한다.

- 단말 에이전트(endpoint agent): CMS 운영 OS 및 무기체계 통제 단말에 최소한의 CPU 점유율(5% 이하)을 갖는 데몬(Daemon)으로 상주하며 프로세스 생성, 파일 무결성 훼손, 비인가 계정 접근 등 호스트 로그를 수집한다.
- 네트워크 수집기(network collector): 패킷 미러링 스위치와 연결되어 송/수신 데이터의 페이로드를 스캔하고 변동 정보를 실시간으로 수집한다.
- 온보드 이상행위 탐지: 중앙 통제 없이 agent와 수집기로부터 수집한 데이터 특징값들을 입력받아 함정 내 에지 서버에 적재된 사이버 이상행위 탐지 추론기를 통해 정상 범주 이탈 여부(anomaly score > θ)를 판단하여 이상행위 여부를 결정한다.

3.1.1.2 체계 영향 제로(Zero-Impact) 가용성 보장형 자동 대응

함정 내부에서의 방호체계 오작동이나 무분별한 네트워크 포트 격리는 함정의 전투 가용성에 치명적인 손실을 발생시킬 수 있다. 따라서 본 사이버 방호체계는 위협 등급과 자산의 물리적 위험도에 근거하여 엄밀한 '가용성 보장 세이프가드 필터'를 적용한다.

- 자산 등급별 대응 통제 방식 차별화:
  - 등급 A(핵심 전투/기동/항해 체계 - CMS, IBS, IBS): 해당 계통에서 위협 신호가 식별되더라도 네트워크 인터페이스를 강제로 끊거나 제어 노드를 임의로 정지시키지 않는다. 대신 트래픽 유입률을 정밀하게 완화하는 미세 쉐이핑(rate limiting 등)을 적용하고, 실시간 로그를 기록하며 폐쇄망 LLM을 통해 운용 요원에게 상황 판단 정보를 제공하고, 함대 사이버 전문 요원에게 대응을 요청한다.
  - 등급 B(일반 행정 지원망, CCTV 등 보조 체계):

보안 침투가 전파되는 즉시, 타 계통으로의 횡적 이동(lateral movement)을 저지하기 위해 내부 방호장비의 방화벽 테이블을 업데이트하여, 네트워크 단을 에지 수준에서 즉각 자동 격리한다.

- 안전성 판단의 수학적 평가지표:
  · 방호 대응 액션 a가 특정 체계 c의 전술적 정상 구동 시간 보장도 Tc에 미치는 영향성 함수 S(a, c)를 정의하여 제어 가능 여부를 수학적으로 판정한다.

$$S(a,c) = \begin{cases} 1 \text{ if } \Delta\, Tc(a) < \epsilon \text{ (체계 가용성 영향 없음)} \\ 0 \text{ if } \Delta\, Tc(a) \geq \epsilon \text{ (체계 가용성 영향 있음)} \end{cases}$$

세이프가드 필터는 S(a, c) = 1을 충족하는 자동화 규칙만 자동 대응을 자율 권한으로 부여하고, S(a, c) = 0에 해당하는 조치는 즉각적인 차단이 아닌 실시간 위협 완화 처리를 유도하고 함대 사이버 전문 요원에게 대응을 요청한다.

3.1.1.3 함대 대응 명령 수행(대응 지원)

함정에서 자동대응하지 못하고 함대에 대응요청한 위협에 대해서 함대의 대응방책 선정에 따른 함대 대응 명령을 수행하는 proxy 기능이다. 함정 proxy는 함대에서 받은 Open C2 명령을 proxy를 통해 RESTful API로 변경하며, RESTful API 명령을 통해 함정의 방호장비(IPS, FW, UTM, NAC)로 전송되어 즉각적인 포트 차단이나 IP 블랙리스팅 등을 수행한다.

3.1.1.4 비전문 인력 지원용 폐쇄망 LLM 지원

미래 함정에는 사이버 전담 요원이 탑재하지 않는 무인화가 심화되기 때문에, 탐지된 위협 상황을 전술지휘관 및 일반 요원이 인지하고 대처할 수 있도록 폐쇄망 LLM 기반의 AI 지원 체계 구축이 필요하다[3].

- 오프라인 격리형 구동: 위성망 대역폭 등에 영향받지 않도록 함정 서버에서 완벽히 오프라인 형태로 연산되는 3B~7B 매개변수 규모의 경량 언어 모델을 운용한다.
- 자연어 질의응답 기반 대응 보조: 함정 내 장비 및 해군 보안 규정에 대한 RAG와 파인 튜닝을 수행하여 비 전문 인력이 적절히 지원받을 수 있도록 한다. 이를 통해 탐지 상황, IP 변동, 호스트 훼손 등 난해한 원격 분석 로그를 자연어 형태로 변환하여 표출한다. 예를 들어, 승조원이 “3번 CMS 서버에서 발생한 경보의 원인과 즉각 조치 방안은 무엇인가?”와 같은 자연어 질문을 입력하면, LLM은 발생 원인을 상세히 풀어서 설명하고 단계별 매뉴얼을 답변으로 출력한다.

이러한 구조는 함정 내부에 폐쇄망 LLM의 구축으로 외부로 프롬프트 전달 및 정보 전달이 이루어지지 않아 함정 보안 안전성을 확보할 수 있다.

3.1.2 함대 계층(Tier 2): 대응방책 결정 및 Open C2 지원

함대 소속 하위 다수 함정의 위협 가시성을 원격으로 유지하고 전문 판단에 의거하여 대응 프로세스를 실현하는 지휘통신대이다.

함대 수준에서는 다수 함정에서 올라온 정보를 바탕으로 구체적인 방어 전략을 수립한다.

3.1.2.1 중앙 집중식 대응방책 결정

각 함정에서 발생한 위협 경보들을 단일 화면에 대시보드로 시각화한다.

함대는 대응방책별로 ‘start-action-end’ 구조의 플레이북을 미리 작성하여 보유하고, 사이버 위협 상황 발생 시 즉각적으로 적절한 대응방책을 선정한다. 필요시 수동 대응방책으로 신규 작성이 가능하다.

함대 지휘통신대의 사이버 전문 요원은 함정에서의 자동 대응 현황과 함정의 현재 군사 작전 등급을 종합 매핑하여 최선의 대응 방책(course of action, COA)을 선정하고 이를 표준화된 포맷인 CACAO 보안 플레이북(collaborative automated course of action operations , CACAO)으로 작성한다.

3.1.2.2 Open C2 기반 함정 원격 제어

선정된 대응방책의 플레이북 워크플로우 절차는 Open C2의 표준화된 명령으로 변환하여 함정에 전달된다. 전달된 명령들은 함정의 proxy에 의해서 방호장비를 제어할 수 있는 RESTful API로 변경되어 함정의 방호장비에 적절한 대응을 수행하게 한다.

또한 방호장비에서 수행한 결과는 Open C2 명령

을 변환하여 함대로 전달되며, 함대에서는 결과를 확인하여 대응방책의 성공 여부를 확인할 수 있다.

3.1.3 해군본부 계층(Tier 3): 탐지 모델 개발/배포, proxy 개발/배포 및 전역 정책 수립

해군본부는 전체 작전 영역에 대한 사이버 우세를 확보하는 컨트롤 타워 역할을 수행한다.

3.1.3.1 함정 정비 시 오프라인 데이터 수집

임무 수행을 마친 함정이 정박하면, 네트워크 대역폭 한계로 원격 전송이 불가하였던 함정 내 수집 로그 파일(네트워크 패킷 원본, 단말 에이전트 수집 로그 등 수십 TB 상당)을 정비 인터페이스를 통해 물리적 연결로 추출하여 해군본부 내 데이터센터에 보관한다.

3.1.3.2 탐지 모델 생성/배포 및 IoC 관리

해군본부 사이버 작전센터의 데이터 센터(GPU 인프라) 서버 내 함정 데이터들을 결합, 레이블링 및 최적화 연산을 수행하여 신규 공격 유형까지 학습시킨 함정 이상행위 탐지 모델을 생성/배포하고 폐쇄망 LLM 미세 조정(fine-tuning) 가중치 데이터셋(weight metric)을 고도화 빌드하여 함정에 배포한다. 또한 최신의 글로벌 사이버 위협 지표(indicator of compromise, IoC) 목록을 생성 및 통합 패키징하여, 함정 재출항 전 또는 저대역 전술망을 활용해 경량 패치 파일 형태로 각 개별 함정에 배포 및 관리한다.

3.1.3.3 Proxy 개발 및 배포

RESTful API는 방호장비 종류 및 밴더마다 다르며, 함정별로 다양한 방호장비(FW, IPS, UTM, NAC 등)와 밴더(안랩, BlueMax, 지니언스 등)를 운용하고 있어, proxy의 Open C2와 방호장비 RESTful API 간의 맵핑은 다양할 수 있다. 따라서 Open C2 시스템과 함정 방호장비 RESTful API를 안정적으로 관리하기 위해 함정별 맞춤형 proxy를 해군본부에서 개발 및 배포하여야 한다. 또한 해군본부에서 최신 보안 정책이 반영된 proxy를 각 함정에 정기적으로 배포함으로써 최신 방호 성능을 유지할 수 있다.

3.2 제안 아키텍처의 하드웨어 구축 방안

본 절에서는 지능형 통합 사이버방호체계가 실제 함정, 함대, 해군본부라는 물리적 하드웨어 제약 요건(공간, 전력, 발열, 통신 속도 등) 하에 구축될 수 있도록 하드웨어 인프라 설계를 제안한다.

3.2.1 함정(Tier 1): NPU 기반 추론 플랫폼

미래 함정은 열악한 환경 조건(협소한 장소, 지속적인 진동, 염분, 밀폐 공간으로 인한 방열 한계 및 제한된 전력)을 갖는다. 따라서 일반적인 x86 고성능 GPU를 탑재하는 것은 물리적 설계 제약(size, weight, and power) 때문에 적절하지 않다.

- NPU 하드웨어의 필요성: 본 방호체계는 함정에 물리적 탑재가 용이하도록 저소비 전력, 쉬운 냉각 기술, 충격 하우징 처리가 가능한 NPU 시스템 도입이 필요하다. NPU는 GPU 대비 낮은 소비 전력으로도 딥러닝 고성능 행렬 연산을 수행할 수 있어 함정의 비상 전원(UPS) 가동 시에도 안정적인 동작을 보장한다.
- NPU 기반 경량 추론 프로세스
  - 이상행위 탐지: NPU의 신경망 연산 코어에 탐지 모델을 이식함으로써, 수십 ms 이하의 사이버 이상행위 탐지를 보장한다.
  - 폐쇄망 LLM 모델 탑재: 3B~7B 매개변수 규모의 LLM을 4비트 또는 8비트 정수형 양자화(INT-4/INT-8) 기법을 적용하여 NPU 전용 메모리에 상주시키고, 초당 20 tokens 이상의 속도로 비전문가 대응을 지원할 수 있다.

3.2.2 함대(Tier 2): 대응방책 서버 인프라

함대에서는 수십 척에 달하는 하위 함정들의 실시간 경보를 실시간 수용하고, 관제 요원에게 실시간 상황 판단을 제공해야 한다.

- 다중 동시 추론 연산 하드웨어 구성: 인텔 제온(Xeon) 고성능 엔터프라이즈 프로세서와 GPU 가속장치를 탑재한다.
- 대응방책 SW 구동: 관제 요원이 수십 척의 함정 상태를 신속히 평가할 수 있도록 컨테이너 가상화(Docker/Kubernetes) 클러스터를 적용한다.

대응방책 서버에서는 수집된 개별 함정의 위협을 병렬 분석하여 위협 우선순위를 자동으로 수립하고, 대응방책을 제안하고 선정된 대응방책은 Open C2를 이용한 함정 통제 페이로드를 만들어 위성망을 통해 함정에 전파한다.

3.2.3 해군본부(Tier 3): GPU 데이터센터 인프라

해군본부(사이버 작전센터)는 정박 함정을 통해 수집된 수십 테라바이트(TB) 분량의 원시 패킷과 호스트 감사 데이터를 학습하여 이상행위 탐지 모델을 생성하는 중앙 데이터 센터 역할을 맡는다.

- 대규모 GPU 클러스터 설계: 다중 멀티 GPU 노드(예: 대규모 H100 또는 A100 GPU 장비 다수 및 초고속 NVLink 스위칭 인터페이스 패브릭) 및 100 Gbps급 네트워크 인터페이스를 결합한 AI 학습 시스템을 구축한다.
- 함정 물리적 연동 연계: 함정 정비를 수행하는 군항에 기가비트급 광학 가선 인터페이스 시스템을 배치하여, 해군본부의 대용량 스토리지로 함정 데이터를 전송한다.
- 학습 및 모델 압축 컴파일러(compiler) 인프라: 수집된 대규모 데이터를 기반으로 함정 이상탐지 모델 및 폐쇄망 LLM 미세조정 연산을 수행한다. 완성된 이상행위 탐지 모델 및 폐쇄망 LLM은 함정에 배치된 NPU 아키텍처에 부합되도록 모델 컴파일러 기법을 사용해 경량 형태로 빌드하여 함정에 배포한다.

3.3 기대 효과 및 이점

- 현장 전문 인력 부족 문제 해결: 함정 승조원이 고도의 보안 분석을 직접 수행하지 않아도, 상위 계층의 전문가들이 선정한 대응방책에 의해 방어가 가능하다.
- 이기종 장비 간 상호 운용성 확보: RESTful API와 Open C2 프록시를 도입함으로써 서로 다른 제조사의 보안 장비(FW, IPS 등)가 통합되어 작동할 수 있다.
- 대응 시간의 획기적 단축: 수작업 대응 절차를 표준화된 포맷으로 전환함으로써 탐지에서 차단까지의 '사이버 킬체인' 시간을 최소화할 수 있다.
- 구축비용 감소: 함정에 고가/고전력 GPU 설치 없이 저가/저전력 NPU로 구축함으로써 구축 비용 및 운용성이 향상될 수 있다.

4. 계층적 대응구조 구축 실험

본 논문에서 제안하는 계층적 대응구조는 해군본부-함대-함정의 구조이며, 이중 계층 구조의 핵심 요소는 함정의 방호장비(IPS, FW, NAC, UTM)를 함대의 대응방책에서 제어하는 기능이다. 이를 실험실에서 구축하여 가능성을 검증하였다.

4.1 계층적 대응 구조 구축 방안

함정에는 방호장비로 FW, IPS, UTM, NAC을 구성하고, 방호장비에서 수집된 로그로 이상행위를 탐지하는 이상행위 탐지기/통합위협분석기 그리고 함대에서 오는 Open C2 명령을 RESTful API(방호장비 제어명령)로 바꾸어주는 proxy로 구성하였다.

함대에는 대응방책 서버를 두고 함정에서 오는 위협에 대한 대응방책 선정, 플레이북 승인, 대응지원 정책과 Open C2 맵핑 기능이 구성된다. 이러한 함정-함대 구성의 동작구조는 Fig. 8과 같다.

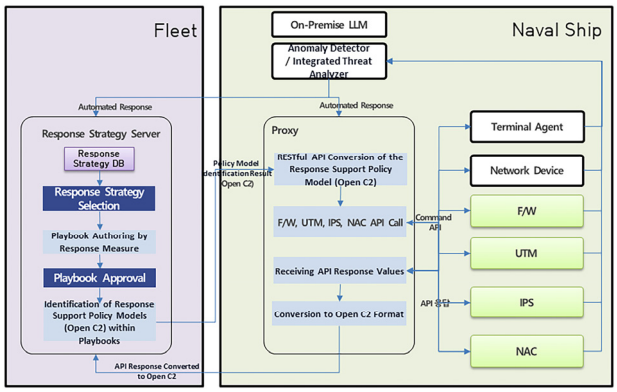

Fig. 8. Operational architecture between fleet and naval ship hierarchies

4.2 계층적 대응 시스템 구축 실험

해군 함대 대응방책 서버는 Nvidia L40 GPU가 탑재된 환경에서 구축하였으며, 대응방책 서버 기능은 파이썬 언어로 개발하였다.

함정의 C2와 Restful API를 맵핑하기 위한 방호장

비별 RESTful API 등록 화면은 Fig. 9과 같다.

Fig. 9. Registration of naval ship RESTful APIs

대응방책에서 RESTful API를 통한 방호장비(방화벽)의 객체(IP) 추가 결과 및 drop 결과 화면 예시는 Fig. 10 및 Fig. 11과 같다.

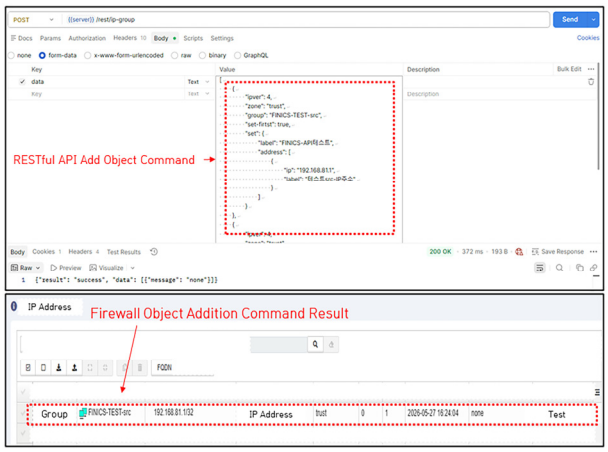

Fig. 10. Example of adding IP to firewall

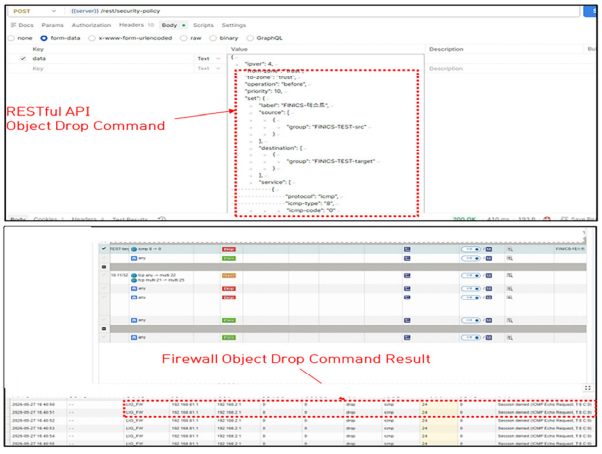

Fig. 11. Example of IP drop in firewall

5. 함대- 함정 간 운용 시나리오

데이터 흐름으로 본 전술적 시나리오 예시는 다음과 같다. 동해상(1함대 소속) 작전 중인 A 함정에서 사이버 공격이 발생됨을 가정으로 한 유기적인 데이터 흐름은 아래와 같다. 이때 독립망 운용에 동해상 작전으로 통신망 침입은 실제 일어날 수 없지만 운용 시나리오의 이해를 위해 간단한 시나리오를 선정하였다.

[함정 탐지]: 함정에 탑재된 AI 모델이 내부 네트워크에서 유해 트래픽을 유발하는 호스트(IP: 192.168.81.1)를 이상행위로 탐지하고 함대로 위협 탐지 상황을 보고.

[함대 분석 및 CoA 선정]: 1함대 대응방책 서버는 위협을 MITRE ATT&CK TTP와 매핑하고, 미리 준비된 CACAO 플레이북을 이용하여 대응방책을 선정한다.

[함대 명령 하달]: 함대 대응방책 서버는 CACAO 절차에 따라 “A 함정 내 방화벽 장비를 통해 해당 호스트를 객체 등록하고 격리하라”는 OpenC2 표준 명령인 객체 추가(Action: Set, Target: 192.168.81.1)와 격리(Action: Drop, Target: 192.168.81.1)을 생성해 위성 통신으로 함정에 송신.

[함정 수행 및 보고]: 함정의 proxy가 이 표준 명령을 수신, 방호장비(방화벽)에 맞는 RESTful API로 즉시 실시간 통역하고 방화벽에 전송하여 해당 IP를 물리적으로 차단한다. 또한 차단 결과를 Open C2 메시지로 함대 대응방책 서버에 전달하여 정상 수행되었음을 알려서 위협에 대한 대응을 완료한다.

6. 결론

본 논문에서는 미래 함정 환경에 대비한 해군의 인력 부족 문제와 전술적 대역폭 제약 사항을 현실성 있게 돌파하기 위해, ‘함정-함대-해군본부 계층적 지능형 통합 사이버방호체계’를 설계하고 그 구현 성능을 검증하였다. 함정 내 단말/네트워크 수집기와 결합한 에지 탐지 및 무장 가용성을 저해하지 않는 가용성 보장 세이프가드는 실시간 침투 위협의 최소 단위 자율 방어를 보장하며, 비전문가도 직관적으로 사용 가능한 폐쇄망 LLM 인터페이스는 방호 작전 요원의 상주 한계를 명확하게 해결한다. 또한 함대 레벨의 RESTful API 제어, 정박 시 대용량 로그 오프라인 재학습 기법

을 활용한 순환 최적화 모델 구조는 무인체계 증가에 따르는 전사적 관제 및 모델 유지 비용 부담을 혁신적으로 절감시킨다.

향후 연구로는 함정에 탑재될 무인 수상정(USV) 등 저사양 임베디드 체계에 탐지 모델을 전이하기 위해 인공신경망의 양자화(quantization) 및 전이학습 최적화를 심화 연구하며, 전군 차원의 사이버 전장관리 체계와의 연동에 의한 최상위 부대(국방부/합참)에서 edge 체계(USV 등) 까지의 사이버 공격과 방어에 대한 연구를 이어 나갈 예정이다.

참고문헌

[1] Harry J. Thie, Consolidated Afloat Networks and Enterprise Services (CANES), RAND Corporation, 2009.
[2] 옥지원·이정식·한인성, '오픈소스 기반 OSINT 자동화의 신뢰성 확보 방안: 함정 전투체계 운용 환경 적용,' 2025년 한국인터넷정보학회 추계학술발표대회, VOL. 26, NO. 2, 2025, pp. 327-328.
[3] Jiwon Ock, Jungsik Lee, & Insung Han, 'Design and Operational Scenarios of LLM Systems for Closed-Network Naval Platforms,' Journal of KNST, VOL. 8, NO. 3, 2025, pp. 474-480.