Journal of the KNST

2025; Vol.8, No.1; pp.81-87

ISSN: 2635-4926 https://doi.org/10.31818/JKNST.2025.3.8.1.81

Check for updates

Received: 2025/02/07
Revised: 2025/02/14
Accepted: 2025/03/06
Published: 2025/03/31

*Corresponding Author:
Seunghoon Jung
E-mail: seunghoon.jung@hanwha.com

Abstract

본 연구에서는 해군 함정을 중심으로 한국군 운용 전술데이터링크에 대한 K-RMF 적용 방안을 제시하였다. 국외 도입 전술데이터링크의 경우 미측 RMF와의 연관성 및 중복성을 고려하여 하드웨어 장비 중심의 해당국 RMF 절차 준수와 국내 개발 구간에 대한 K-RMF 절차 준수를 제안하였다. 국내 개발 전술데이터링크의 경우 다양한 획득 경로의 HW/SW에 대한 개별 검증 및 통합 검증 절차를 제시하고, 함정 체계 통합 관점에서의 K-RMF 적용 시 고려사항을 제시하였다. 본 연구는 한국군 전술데이터링크에 대한 K-RMF 적용 방안 연구에 기여할 수 있을 것으로 기대된다. 향후 국외 도입 및 국내 개발 전술데이터링크에 대한 상세한 K-RMF 통제 항목 선정 및 가이드라인 설정 연구가 필요하며, 실제 적용 사례 데이터베이스 구축을 통해 K-RMF의 실질적인 활용 단계로 나아갈 수 있을 것이다.

This study proposes a K-RMF application plan for the ROK's tactical data links operated by the Navy, focusing on naval vessels. For foreign tactical data links, I propose compliance with the relevant national's RMF procedures centered on hardware equipment, considering the relevance and redundancy with the US RMF, and compliance with K-RMF procedures for nationally developed sections. For national tactical data links, I present individual verification and integrated verification procedures for HW/SW of various acquisition paths, and present considerations for K-RMF application from the perspective of ship system integration. This study is expected to contribute to the research on K-RMF application plans for ROK's tactical data links. Future research is needed to select detailed K-RMF control items and establish guidelines for foreign and national tactical data links, and to advance to the practical use stage of K-RMF by building a database of actual application cases.

Keywords

전술데이터링크(Tactical Data Link), 사이버보안 위험관리제도(Risk Management Framework), 국방 사이버보안 위험관리 (K-RMF), 함정전투체계(Combat Management System), 체계통합(System Integration)

Acknowledgement

이 논문은 2024년도 한국해군과학기술학회 동계학술대회 발표 논문임.

한국군 운용 전술데이터링크에 대한 국방 사이버보안 위험관리 적용방안 연구

A Study on the Military Cybersecurity Risk Management Framework(K-RMF) to ROK's Tactical Data Link

정승훈*

한화시스템 C4I연구소 수석연구원

Seunghoon Jung*

Chief engineer, C4I Research Institute, Hanwha Systems

1. 서론

사람들에게 관심이 잊혀질 만하면 언론을 통해 북한의 사이버해킹 뉴스가 이슈화되는 모습을 볼 수 있다. 2024년 9,600억원에 달하는 암호화폐를 해킹으로 탈취한 뉴스[1]나, 그렇게 탈취한 암호화폐를 활용해서 현역 장교 등을 포섭하여 군사기밀을 유출하는 행위[2]에 이르기까지 다양한 뉴스를 접할 수 있다. 이처럼 전방위적인 북한의 해킹과 관련된 사이버안보 중요성은 대다수 인원이 인식하고 있는 수준으로 지속적으로 자주 제기되는 사안이다. 북한은 해킹목적 달성을 위한 높은 수준의 기술력을 보유하고 있으며, 대부분의 해킹사건은 사건이 발생한 이후 세부 분석을 실시하면서 그 경과가 밝혀지고 결과가 공개되는 경우가 많다.

해킹의 방식 및 수단은 특정한 목적 달성을 위해 방향성을 가지고 지속적으로 시행되는 경우가 많은데, 북한의 경우 미사일 정보 수집 및 자금 확보를 위해 암호화폐, 방산 및 항공우주 업체 대상으로 해킹이 활발히 이루어지고 있다[3]. 방사청 등 주요 국가기관뿐만 아니라 방산업체의 경우에도 안심할 수 없는 상황[4]으로, 방산사업을 수행하는 기간 중 보안에 유의하는 것뿐만 아니라 그 이후 자체 보관 중인 설계도 등의 자료관리가 보안 차원에서 중요한 부분을 차지한다. 물리적으로 분리되어 운영되는 내부망의 경우에도 호주에서 발생한 국방부 내부망 공격사례[5]를 보면 안심할 수 없음을 알 수 있다.

이처럼 최근에는 전통적인 사이버보안 시스템 구축 이외의 공급망 관리, 외주업체 인원 관리 등 관리적인 요소의 중요성이 함께 부각되고 있다. 이에 더하여 국방에 적용되는 암호장비 등 특수성에 따라 독점, 고착화, 신기술 접목의 둔화가 우려된다. 예를 들어 OS 버전 업데이트 적용 지연, SW형 암호코드 방식 적용으로의 전환 등 보안상 기존에 예상하지 못한 제한사항이 발생할 가능성이 높은 실정이다.

또한, 다양한 위협요소를 전부 고려해서 사전에 차단하기란 불가능에 가깝고, 사전 차단을 가정하여도 다양한 체계의 복잡성 때문에 예상치 못한 취약요소가 식별될 수 있으므로, 이러한 위험요소를 전반적으로 관리하는 방식으로 사이버보안의 패러다임이 변화하고 있다. 미국에서 실시하고 있는 사이버보안 위험관리 제도를 참고하여 우리나라도 2024년부터 국방부에서 자체적으로 국방 사이버보안 위험관리 제도를 공식 운용하고 있다. 하지만 실제 적용하는 수준, 범위, 방향에 대한 연구 및 자료가 부족한 실정으로 앞으로 실체계 적용 등을 통해 발전시켜 나가야 한다. 특히, 전술데이터링크(tactical data link)와 같이 군사작전에 핵심이 되는 특정한 체계들을 대상으로 실질적 적용방안에 대한 우선적인 연구가 필요하다. 따라서, 본 논문에서는 한국군에서 운용하고 있는 전술데이터링크에 대해 국방 사이버보안 위험관리를 어떻게 적용할 수 있는지에 대해 해상전력 중심으로 연구하였다.

2. 관련 연구

2.1 국방 사이버보안 위험관리 지시

국방부 정보통신기반정책담당관실에서는 2024년 4월 12일 국방부장관 지시 '국방 사이버보안 위험관리 지시(국방부기타 제15호)'를 제정·공개하였다[6]. 제1조(목적)을 보면 '무기체계 및 전력지원체계의 사이버보안 위험을 수명주기 관점에서 관리하기 위해 국방 사이버보안 위험관리(이하 K-RMF)의 추진, 운영, 관리 등에 필요한 사항을 규정'하는 것으로 표현되어 있다. 해당 목적에 따라 향후 우리나라에서 사용되는 모든 무기체계 및 전력 지원체계는 K-RMF를 따라야 할 것으로 예상된다. 물론 제49조(적용 특례)에 따라 단계적 확대 적용에 대한 내용을 언급하면서 현 시점에서 급하게 모든 체계를 동시에 적용하는 것은 제한적이란 점을 고려하고 있다. 해당 조항에 '이 지시에 따라 보안계획서 검토 및 보안평가를 받은 경우 (기존의) 보안대책 검토와 보안측정을 받은 것으로 본다'라는 문구를 보면 향후 적극적으로 K-RMF를 적용하는 사업들은 중장기적 관점에서 선제적으로 대응할 수 있을 것으로 보인다.

K-RMF 지시 중 제4장에는 무기체계 위험관리, 제5장에는 전력지원체계 위험관리의 단계가 설명되어 있다. 한국군 운용 전술데이터링크의 경우 무기체계에 해당하므로 제4장을 따라야 한다. 무기체계 위험관리를 위해 소요 단계(시스템 보안분류), 획득 단계(보안통제항목 선정, 보안계획서 작성, 보안통제항목 구현, 무기체계 보안평가, 보안평가 후속조치, 인가), 운용 단계(모니터링, 운영 중 평가 및 재인가, 폐기)로 구분하여 각 기관별 역할이 정의되어 있다. 큰 틀에서의 기준은 정의되어 있으나 새롭게 시작되는 제도인 만큼 참고할 만한 자료는 부족한 실정이다.

2.2 미 사이버보안 위험관리제도(RMF) 및 한국군 사이버보안 위험관리제도(K-RMF)

미 국방부(Department of Defense, DoD)는 무기체계 및 정보체계 획득 시 지속적으로 발생하는 사이버위협으로부터 자신들의 체계를 보호하기 위한 별도의 평가 기준을 제정하여 운영하고 있다. 1985년 TCSEC(Trusted Computer System Evaluation Criteria)으로부터 시작된 평가 기준은 최근엔 RMF A&A(Risk Management Framework Assessment & Authorization)까지 발전되었다[7].

미 연방 및 DoD에서 적용하는 RMF는 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)의 NIST 800-37[8]를 따른다. 800-37은 위험관리 프로세스를 단계별로 안내하며, 각 단계에서 필요한 보안통제항목을 선택하고 적용하도록 한다. 보안통제항목은 해당 문서가 아닌 NIST 800-53[9]에 명시되어 있다. 800-53도 가이드 성격이 강하여 실제 미군에서 적용되는 보안통제항목에 대한 세부 정보는 미공개되어 있다. 하지만 큰 틀에서 800-53을 통해 미군에서 사용하는 보안통제항목을 연구해 볼 수 있을 것이다. 800-53에 정의된 20개의 분류는 Table 1과 같다.

Table 1. US RMF security & privacy control families[9]

ID	Family
AC	Access control(접근통제)
AT	Awareness and training(보안 교육 및 훈련)
AU	Audit and accountability(감사 및 책임)
CA	Assessment, authorization and monitoring (자산, 권한, 모니터링)
CM	Configuration management(형상관리)
CP	Contingency planning(비상계획)
IA	Identification and authentication(식별 및 인증)
IR	Incident response(침해사고대응)
MA	Maintenance(유지보수)
MP	Media protection(매체보호)
PE	Physical and environmental protection (시설 및 운용환경 보호)
PL	Planning(계획수립)
PM	Program management(프로그램 관리)
PS	Personnel security(인원 보안)
PT	PII processing and transparency (PII 처리 및 투명성)
RA	Risk assessment(위험평가)
SA	System and service acquisition (시스템 및 서비스 획득)
SC	System and communication protection (시스템 및 통신 보호)
SI	System and information integrity (시스템 및 정보 무결성)
SR	Supply chain risk management(공급망 위험 관리)

방첩사령부에서는 각 보안통제항목의 정의와 의미에 대해 참고자료를 작성하여 배포하였다. K-RMF 제도 보안통제항목 목록서[10]에는 보안통제 항목 17개의 분류와 명칭, 해당 분류별 작성되어야 할 항목, 기준선 등이 설명되어 있다. 비공개로 관리 중인 미군과 다르게 통제항목을 공개한 것은 미국의 경우에도 연방 차원에서 NIST 800-53 등을 통해 공개된 정보가 다수 있고, K-RMF 제도의 국내 조기 정착을 위해 공개 가능한 수준/범위를 고려한 조치로 생각된다. 해당 목록도 기존의 민간에서 적용되던 정보보호 종류와 범주에 속하는 사항이 대부분으로, 기존에 분산되어 개별적으로 이뤄졌던 정보보호를 체계 중심의 생명주기를 가지고 큰 틀에서 관리하는 측면이 더 강하다. K-RMF의 분류는 Table 2와 같다.

Table 2. ROK K-RMF security control families[10]

ID	Family
AC	Access control(접근통제)
AT	Awareness and training(보안인식 교육·훈련)
AU	Audit and accountability(감사 및 책임)
CM	Configuration management(형상관리)
CP	Contingency planning(비상계획)
CR	Cryptography management(암호관리)
IA	Identification and authentication(식별 및 인증)
IR	Incident response(사고대응)
MA	Maintenance(유지보수)
MP	Media protection(매체보호)
PA	Security planning and assessment (보안 계획 및 평가)
PE	Physical and environmental protection (시설 및 운용환경 보호)
PS	Personnel security(인원 보안)
SA	System and service acquisition (시스템 및 서비스 획득)
SC	System and communication protection (시스템 및 통신 보호)
SI	System and information integrity (시스템 및 정보 무결성)
SM	Supply chain management(공급망 관리)

Table 1과 Table 2를 비교하면 K-RMF에서는 미 RMF의 20개 항목 중 CA, PL, PM, PT, RA, SR을 빼고, PA, CR, SM을 추가한 17개 분류로 재정리하였음을 알 수 있다. 국내환경에 맞도록 재정립하는 과정에서 당연히 재정리가 필요한 부분으로 생각된다. 한국군 운용 전술데이터링크의 경우 방첩사에서 재정리하여 공개한 17개의 분류를 기준으로 K-RMF 적용이 필요하다.

2.3 한국군 운용 전술데이터링크 사이버보안

국방 무기체계 소요는 정보보호항목을 포함하여 작성해야 한다. 정보보호 수준, 암호장비 적용방안, 사이버위협 대비, SW 취약점 제거 등을 포함한 보호대책을 작성하는데, 해당 무기체계가 장기전력인지 중기전력인지에 따라 작성하는 내용의 깊이가 달라진다. 장기전력이 기본적인 개념 수준으로 작성된다면 중기전력은 네트워크, 응용체계, 서버, 단말기, 관

제, 키 관리 등의 내용을 구체적으로 작성해야 한다. 중기신규전력이 아닌 일반적인 중기전력인 경우 장기소요 결정 이후 실시한 선행연구 결과 등을 반영하여 구체화해야 한다.

무기체계에 해당하는 전술데이터링크의 경우에도 동일한 수준의 정보보호 내용을 소요결정 기간 중 작성하고, 획득 순기에 따라 구체화 및 보완한다. 정보보호체계가 정상적으로 구축되었는지의 여부는 실시스템 구현과 연계하여 개발시험평가 및 운용시험평가를 통해 확인하고, 최종적으로는 보안측정 등을 통해 검증하게 된다. 그런데 이러한 절차를 준수하는 과정 중에서 전술데이터링크가 가지는 구조적인 문제가 떠오르게 된다.

전술데이터링크는 태생적으로 단독으로 운용할 수 없는 체계이다. 각종 센서, 전투체계 등 타 체계와 상호연동 없이는 운용이 불가하여 정보보호 관점에서 타 체계의 정보보호 수준과도 밀접한 관계를 맺게 된다. 또한, 전술데이터링크의 특성상 합동작전, 연합작전을 고려한 체계구성은 전술데이터링크 도입, 구매, 개발 방식이 복잡화·다양화되는 큰 요인 중 하나가 된다. 이러한 상황을 고려하면 전술데이터링크에 적용되어야 할 정보보호 수준 및 체계는 국내외 도입/개발 장비 및 상호 연동되는 체계에서 식별되는 취약점에 따라 기하급수적으로 증가할 가능성이 높다고 생각된다. 여기에 공급망 관리를 포함한 기타 관리적 부분까지 추가된다면 아예 해당 전술데이터링크 체계를 쓰지 않는 것이 낫다고 여겨질 수도 있다. 현재 한국군에서 운용하고 있는 전술데이터링크 종류는 Table 3와 같이 Link-11, Link-16, Link-22(미래), JTDLS, KVMF 등이 있다[11].

Table 3. Past, present and future of ROK TDL[11]

Category	ROK TDL
Past	Link-11/16, ISDL, Link-K
Present	Link-16/22, ISDL-II, Link-K, KVMF
Future	Multi-TDL(ISDL-II, Link-K, KVMF, Link-22), Link-16, etc.

하지만 보안상의 이유로 작전적으로 필수인 전술데이터링크를 운용하지 않는 것은 수많은 작전상의 이점을 스스로 포기하는 것과 같기 때문에 최대한 사이버보안 위험을 낮추고, 기(旣) 식별된 취약점을 관리하여 체계를 운용하는 것이 타당하다. 그래서 최근 이슈화되어 시작된 K-RMF의 한국군 운용 전술데이터링크 적용은 현 시점에서 매우 적절하고 유용한 방법이라고 생각된다.

3. 한국군 전술데이터링크 대상 사이버보안 위험관리 적용 방안: 함정 중심으로

3.1 함정 체계통합 요구능력(안)에 따른 고려사항

함정에 적용되는 체계는 매우 복잡한 형태로 구성되어 있다. 함정의 핵심인 전투체계의 복잡도는 다른 어떤 체계에도 비교할 수 없을 정도라고 봐도 과언이 아니다. 함정의 특성에 따라 적용되는 전투체계는 각자 다르지만, 전반적으로 Fig. 1과 같이 데이터버스를 기반으로 각기 다른 개별체계의 데이터를 활용하는 형태[12]로 구성되어 있다.

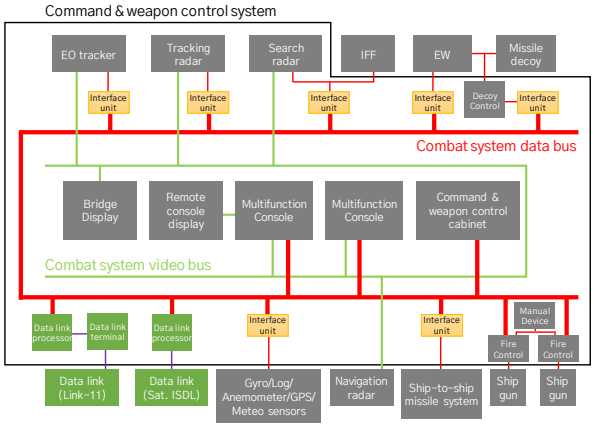

Fig. 1. Example of naval ship combat system[12]

함정 전투체계 요구능력(안) 연구[13]에 따르면 향후 함정 전투체계에는 통합함정컴퓨팅(total ship computing environment, TSCE) 개념이 적용되고, 통합전투기능, 항해/조함기능, 통신기능, 기관/손상통제기능을 각각 통합하는 형태로 발전될 가능성이 높다. 이에 더하여 함정 전 구역 체계운용을 고려한 최신기술이 적용될 것이다.

이러한 향후 미래 함정 전체에 K-RMF가 적용된다고 가정하였을 때 데이터, 네트워크, 물리적/관리적 보호에 대한 고민이 필요할 것이다. 이에 대한 고려사항을 정리하면 Table 4와 같다. 해당 고려사항에

Table 4. Considered factors for system integration in naval ships

Requirements (draft)	K-RMF view	Considered factors
TSCE concept	Data protection	Level/information definition
Integrated combat, navigation/ship handling, communication and engine/damage control systems	Network protection	Network separation and integration
System operation for all ship areas, latest technology	Protection of all areas	Authorizer by each system

따라 전술데이터링크의 K-RMF 적용은 개별 단위체계의 정보보호 수준뿐만 아니라 함 전체에 영향을 미치는 부분으로 접근해야 한다.

3.2 국외 도입 전술데이터링크 적용 방안

국외 도입 전술데이터링크(예: Link-16)의 경우 기본적으로는 미(美) 측(또는 판매하는 국가의 사이버보안 제도) RMF를 그대로 따라야 한다. 미 측에서 제공하는 연합암호장비 등을 활용해야 하므로 미 RMF를 따르지 않으면 해당 체계 사용이 매우 제한될 것이다. 타 연구[14]에서 언급된 바와 같이 F-35처럼 해당 플랫폼 일체를 구매하면서 해당 플랫폼에 전술데이터링크를 같이 탑재하여 도입되는 경우는 전술데이터링크만 단독으로 RMF를 적용하는 것이 아닌, 해당 플랫폼 및 플랫폼을 운용하는 시스템 일체에 대해 RMF가 적용되므로 미 RMF를 그대로 수용하여 적용할 수밖에 없다.

공군과는 다소 차이가 있는 한국 해군에 설치되는 국외 도입 전술데이터링크의 경우 RMF의 적용 대상 및 범위에 대한 고민이 필요하다. 예를 들어 해상작전헬기에 탑재[15]되는 국외 도입 전술데이터링크는 플랫폼은 유럽인데 탑재링크는 미국이고, 함정에 탑재되는 국외도입 전술데이터링크[16]는 미국의 데이터링크가 국내 개발 전투체계와 연동되는 상황이므로 K-RMF 및 미 RMF의 상호 연관 및 중복성에 대한 정리가 필요하다.

상기 사항을 고려한 국외 도입 전술데이터링크의 K-RMF 적용 방안은 다음과 같다.

우선 함정에 설치되는 국외 도입 전술데이터링크에 한정하여 하드웨어 장비 기준으로 해당국 RMF 절차 준수가 필요하다. 적용 범위는 Link-16 기준으로 데이터링크처리기, 암호장비, 통신기, 안테나까지가 적절할 것으로 보인다. Link-16은 별도의 단독 안테나를 설치하므로 미 RMF에 해당하는 항목을 구분하여 적용 가능하다. 나머지 데이터링크처리기에서부터 연동단, 전투체계까지의 연결구간은 K-RMF 절차를 준수한다면 각 구간별 책임 범위와 사이버보안 대책 수립이 용이할 것이다.

물론 Link-16 표준 최신화 등 SW 개조소요 발생 시 미 RMF 및 K-RMF 모두 재승인 절차가 진행되어야 하므로, 연동구간 확인 및 승인과 관련해서는 한미 간 사전 절차를 만들어 관리하여야 할 것이다. 하지만 최종 조정 및 승인 권한은 함 전체를 총괄하는 한국 측에서 가져야 할 것으로 생각된다.

3.3 국내 개발 전술데이터링크 적용 방안

전술데이터링크 장비 일체를 국내에서 개발하고 일반 상용품을 구매하여 설치하는 경우에는 K-RMF를 적용하는 데 큰 무리가 없을 것이다. 하지만 연합해상전술데이터링크인 Link-22는 매우 특수한 경우이므로 K-RMF를 적용하기 위해서는 여러 사항을 고려하여야 한다.

Link-22에 적용될 사이버보안은 미 RMF, NATO의 사이버보안정책(정식 명칭이 없어 본 연구에서는 편의상 이하 'NATO RMF'로 칭함), K-RMF의 혼합형태라고 볼 수 있다. 예컨대 NILE PMO에서 제공하는 Link-22 SW[17]의 경우 NATO RMF, 연합암호장비는 미 RMF, 국내에서 개발하는 SW 및 일반상용장비는 K-RMF를 따라야 한다. 이 중에서도 해외에서 구매하는 일반상용장비는 해당 국가에서 RMF가 검증되었다고 볼 수 없으므로 도입 후 K-RMF를 적용해야 한다. 뿐만 아니라 국내에서 개발되더라도 관급으로 제공되는 SW의 경우 K-RMF 적용 간 식별되는 취약점 해소를 위해 다른 통제항목을 강화해서 적용해야 하는 등 추가 고민이 필요한 실정이다.

이처럼 국내 개발 전술데이터링크라고 할지라도

HW 및 SW 획득 방식에 따라 해외 상용 구매, 해외 FMS 구매, 국내 자체 개발, 국내 상용 구매, 관급 제공 등이 혼재되어 있다면 전술데이터링크 체계 전체적인 관점에서 신호전달 방식과 메시지 처리방식을 중점으로 사이버보안대책 수립이 필요하다.

상기 사항을 고려한 국내 개발 전술데이터링크의 K-RMF 적용 방안은 다음과 같다.

개별 단위체계 측면에서 해외 상용 구매품은 해당 국가에서 정보보호 검증이 완료된 결과제시가 가능한 경우 해당 결과를 참조하고, 별도 검증결과가 없는 경우 국내에서 가능한 수준에서 단위 검증을 실시한다. 해외 구매품(연합암호장비 등)은 정보보호 검증 결과를 확인하여 참조한다. 국내 자체 개발 HW 및 SW는 사전 지정된 보안통제항목에 따라 개발하여 검증하고, 국내 상용 구매 HW는 적합성 검증 등 타 제도에서 이미 검증된 장비의 경우 해당 결과를 참조하고, 그렇지 않은 경우 사전 지정된 보안통제항목에 따라 조치하고 검증한다. 관급제공 SW의 경우 사전 지정된 보안통제항목에 따라 검증하는데, 이때 식별된 취약점은 체계특성을 고려하여 타 보안통제항목을 강화 적용하는 등의 조치를 통해 보완한다.

이렇게 개별단위품으로 확인한 다음 체계 전체 연결 및 설치 후 전투체계, 연동단을 거쳐 DLP에서부터 안테나단까지 보안통제항목 충족 여부를 확인한다. 이때 승인은 앞서 언급한 국외도입 전술데이터링크의 최종 승인권자와 마찬가지로 함 전체를 총괄하는 인원이 담당하는 것이 타당하다. 국외 도입 및 국내 개발 전술데이터링크는 그 역할 및 운용방식이 유사하므로 함 운용을 총괄하는 입장에서 승인에 대한 판단이 필요하다. 승인권자는 전술데이터링크가 단독 운영되지 않고 전투체계를 포함한 타 체계에 미치는 영향이 큰 점을 고려하여 함정 체계통합 관점에서 적용되는 K-RMF 범위에 대한 사전 조율 및 검토를 선행조치하여야 할 것이다.

4. 결론

전반적으로 전술데이터링크의 정보보호는 단위장비 수준의 정보보호 관점을 따르는 K-RMF와 체계 전체 통합관점의 K-RMF가 상존하고 있다. 이에 더하여 무기체계 특성상 연합작전을 위한 해외도입 무기체계는 해당 국가의 RMF를 따라야 하는 경우도 있다. K-RMF의 정착과 해당 목표를 감안하여 zero-base에 해당하는 최초 기획, 계획, 검토 단계부터 시작한다면 좋겠지만 기존 무기체계를 포함한 전반적인 국방사업의 특성/시기 등을 고려하면 그렇게 하기는 매우 제한적인 상황이다. 따라서 적용 범위를 특정체계로 한정짓거나 여러 체계에 일부만 적용하는 등의 방식으로 단언할 것이 아니라 병렬적 방식으로 접근이 필요하다. 승인 수준과 내용을 고려하여 최상위 승인권자에 의한 적절한 권한 이양과 배분이 필요하다. 물론 이 때 해당 체계를 최종적으로 승인하는 승인권자의 부담감이 매우 클 것으로 생각된다. 따라서 이러한 부담감을 덜어주고 체계의 사이버보안 안정성을 확보하여 K-RMF 제도를 안착시키려면 기존의 정보보호를 담당하는 여러 기관들의 많은 노력이 있어야 할 것이다.

이러한 점을 고려하여 본 논문에서는 한국군 전술데이터링크를 대상으로 K-RMF 적용 방안에 대해 연구하였다. 한국군에 적용되는 전술데이터링크는 여러 종류가 있지만 그 중 해군함정에 적용되는 주요 전술데이터링크 중 국외 도입 전술데이터링크와 국내 개발 전술데이터링크로 구분하여 K-RMF를 적용하는 방안을 모색하였다.

본 논문에서 제시하고 있는 주요 방식을 요약하면 우선 단위체계(HW 및 SW)별 도입 방식에 따라 개별 인증 및 인가를 받고, 국외 도입 또는 국내 개발 전술데이터링크 단위체계에 대한 인증 및 인가를 거쳐 2개 이상의 전술데이터링크 다중체계의 인증 및 인가단계로 발전하는 부분을 언급하였다. 최종적으로 함정 플랫폼 전체의 인증 및 인가 시 해당 결과를 참조하는 형태로 적용될 것이다. 실제 함정에 설치되는 체계의 형태 및 구성이 매우 복잡하므로 본 논문에서는 전반적인 적용 방안에 대해 연구하였다. 향후 국외 도입 및 국내 개발 전술데이터링크에 대한 상세한 K-RMF 통제항목을 선정하고 각 케이스 별로 활용 가능한 가이드라인을 설정할 필요가 있다.

최근 국정원에서 추진 중인 국가 네트워크 보안 프레임워크(National Network Security Framework, N^2SF)[18]를 고려한 정보보호 수준에 대한 단계별 적용은 K-RMF에도 시사하는 바가 크다고 생각된다. 군사비밀, 비밀에 준하는 데이터, 일반 데이터 등을 구분하여 K-RMF 적용에 대한 가이드가 구성된다면 사용자들이 좀 더 쉽게 적용할 수 있을 것이다. 해당

가이드와 병행해서 방첩사에서 실시한 기존 보안측정 사례들을 K-RMF 문서 형태로 변환하고 데이터베이스화한다면 전술데이터링크와 같은 특정한 분야에서도 K-RMF가 막연한 개념이 아닌 실질적 활용이 가능한 단계로 나아갈 수 있을 것이다.

참고문헌

[1] 이민석, "한미일 '북, 작년 9,600억원 암호화폐 탈취…위협 공동대응,'" 조선일보, 2025. 1. 14, https://www.chosun.com/politics/diplomacy-defense/2025/01/14/ONRFXH5MSVBG3LC5EO54KLU54Q (검색일: 2025. 1. 18)

[2] 노선웅, "북 공작원에 7억 암호화폐 받고 군사 기밀 유출…1심 징역 4년," 뉴스1, 2025. 1. 17, https://www.news1.kr/society/court-prosecution/5664277 (검색일: 2025. 1. 18)

[3] 김지은, "MS, '북, 올해 방산·암호화폐 대상 해킹 시도 활발,'" 뉴시스, 2022. 11. 9, https://www.newsis.com/view/?id=NISX20221109_0002078706&cID=10301&pID=10300 (검색일: 2024. 11. 23)

[4] 김태훈, "KF-21 기밀 노렸다…북, 독일 방산업체 해킹," SBS, 2024. 10. 5. https://news.sbs.co.kr/news/endPage.do?news_id=N1007823301&plink=ORI&cooper=NAVER (검색일: 2024. 11. 23)

[5] 박의래, "해킹에 몸살 앓는 호주, 이번엔 국방부 내부망 공격당해," 연합뉴스, 2022. 10. 31, https://www.yna.co.kr/view/AKR20221031100100104?input=1195m (검색일: 2024. 11. 24)

[6] 국방부, "국방 사이버보안 위험관리 지시(국방부기타 제15호)," 2024. 4. 12.

[7] 안정근, 조광수, 정한진, 정지훈, 김승주, "무기체계 개발을 위한 한국형 국방 RMF 구축 방안 연구," 정보보호학회 논문지, Vol. 33, No. 5, pp. 827-846, 2023. 10.

[8] NIST, "Risk Management Framework for Information Systems and Organizations," NIST SP 800-37 Rev. 2, 2018.

[9] NIST, "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53 Rev. 5, 2020.

[10] 국군방첩사령부, "K-RMF 제도 보안통제항목 목록서," 2024. 6, https://www.dcc.mil.kr (검색일: 2024. 11. 28)

[11] 정승훈, 이정언, "국내 개발 전술데이터링크 표준 발전방향 연구," Journal of the KNST, Vol. 7, No. 3, pp. 378-383, 2024. 9.

[12] 김수한, "군, 해군함정 브레인 '전투체계' 논의," 헤럴드경제, 2016. 6. 9, https://mbiz.heraldcorp.com/article/983258 (검색일: 2024. 12. 14)

[13] 정승훈, 지해근, 최삼욱, 정남식, 임진국, "함정 체계통합 발전방향," 대한조선학회지, Vol. 57, No. 1, pp. 15-20, 2020. 3.

[14] 김경애, "무기체계 사이버보안 제도 K-RMF, 풀어야할 과제는," 보안뉴스, 2024.10.25. https://www.boannews.com/media/view.asp?idx=133791 (검색일: 2024. 12. 17)

[15] 이운안, "해군, AW-159 신형 해상작전헬기 영해수호 임무 투입," 국제뉴스, 2017. 2. 1, https://www.gukjenews.com/news/articleView.html?idxno=642563 (검색일: 2024. 12. 17)

[16] 이종윤, "해군, 광개토대왕급 구축함에 '링크-16' 탑재 "현존전력 극대화" 노린다," 파이낸셜뉴스, 2024. 1. 13, https://www.fnnews.com/news/202401132140078962 (검색일: 2024. 12. 17.)

[17] NILE PMO, "Customer Information Guide(CIG)," LINK 22 Official Webpage, 2020. 11. 3, http://www.link22.org/uploads/7/9/3/2/7932022/20201001_nile_cig_v2.3.pdf (검색일: 2024. 12. 21)

[18] 조재학, "망분리 개선 정책, 'MLS'서 'N^{2}SF'로 간판 바꿨다," 전자신문, 2024. 12. 12, https://www.fnnews.com/news/202401132140078962 (검색일: 2024. 12. 21)