박사학위논문

무기체계 사이버 보안 강화를 위한 보안정책 및 정보보호 관리체계

Security Policy and ISMS for Strengthening Cyber Security of Weapon Systems

제주대학교 대학원

융합정보보안학협동과정

정 성 욱

2022년 8월

무기체계 사이버 보안 강화를 위한 보안정책 및 정보보호 관리체계

지도교수 박 남 제

정 성 욱

이 논문을 융합정보보안학협동과정 박사학위 논문으로 제출함

2022년 6월

정성욱의 융합정보보안학협동과정 박사학위 논문을 인준함

심사위원장 김종우 ㊞

위원 김철 ㊞

위원 주연수 ㊞

위원 박남제 ㊞

위원 변영철 ㊞

제주대학교 대학원

2022년 6월

Security Policy and ISMS for Strengthening Cyber Security of Weapon Systems

Sung-wook Jung
(Supervised by professor Namje Park)

A thesis submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in Convergence Information Security

2022. 6.

This thesis has been examined and approved.

Namje Park

Chong Deo Kim

Chul Kim,

Yeon Soo, Jeong

Yung-chul Byun

2022. 6.

Department of Convergence Information Security
GRADUATE SCHOOL
JEJU NATIONAL UNIVERSITY

목 차

표 목 차

그 림 목 차

요 약

기술발전에 따라 무기체계의 소프트웨어 비중이 증가하고 있으며, 첨단 과학기술이 무기체계에 적용됨으로 인해 무기체계의 사이버 보안 문제는 갈수록 중요해지고 있다. 또한, 무기체계를 무력화하기 위한 적대적 세력에 의한 다양한 시도가 발생하고 있으나 이를 선제적으로 발견, 예방, 대책 수립 및 조치할 수 있는 제도적 장치가 미흡하다. 그리고 북한과 대치하고 있는 안보 상황에서 軍 국방망 및 전장망에 대한 해킹 위협은 실존하고 있다.

미국 회계검사원(GAO)에서 2018년 미국 국방부가 개발 중인 차세대 무기체계 전산망이 허술한 전산망 암호관리와 암호화 통신 미사용 등으로 인해 탐지되지 않은 敵에 의해 쉽게 해킹되고 있다는 사실을 국방부가 인식하지 못하고 있다고 공개하였다.

본 논문에서는 국방 분야의 무기체계 분류기준 등 우리 軍의 사이버 보안 실태에 대해 분석 후, 무기체계 사이버 보안과 무기체계 공격 사례 및 관련 연구 동향에 대해 제시하였다. 그리고 무기체계 사이버 보안 수행체계 및 한계점을 분석하였다. 현재의 폐쇄적인 軍의 무기체계 환경에서 보안성을 강화하기 위해 무기체계 보안취약점 식별 및 관리방안, 방산업체 보안관리 강화 방안, 무기체계 전문인력 양성, 무기체계 악성코드 대응방안, 무기체계 사이버 보안 강화를 위한 기존제도 융합 방안으로 무기체계 정보보호 관리체계 제안 등 총 5개 항목으로 구분하여 무기체계 사이버 보안 정책을 제안하였다.

무기체계 보안취약점 식별 방안으로 무기체계 보안 관련 지침 및 제도 정비, 국방 버그바운티 제도 도입 등을 제시했고, 방산업체 보안관리 방안으로 방산업체 보안관리 개선 및 공급망 보안 관리체계 수립을 제안했다. 그리고 무기체계 보안전문 인력 양성 방안, 무기체계 악성코드 대응 방안 및 무기체계에 특화된 정보보호 관리체계를 제안하였다.

국내에서는 아직까지 무기체계 사이버 보안 정책이 걸음마 단계에 있다. 미국처럼 무기체계 보안 강화를 위한 아낌없는 예산 지원과 국가적 차원의 법적 제

도 지원이 필요하다. 본 논문에서 제시한 보안정책을 적용하고, 민간 분야와 적극적인 교류와 협력 등을 통해 무기체계 사이버 보안을 강화해야 한다.

무기체계 사이버 보안을 강화하기 위해서는 지속적인 연구가 필요하다. 특히 무기체계 개발 시 무기체계에 특화된 소스코드 검증방안이 수립되어야 하며, 무기체계 운용 간 가용성을 보장하면서 효과적인 무기체계 보안취약점을 진단 할 수 있는 방법과 도구가 개발되어야 한다. 그리고 해외 구매 무기체계의 경우 계약 단계에서 우리 軍에 필요한 보안요구 사항에 대해 명확히 정의되고 반영하고, 운용 단계에서 보안 요구사항 준수 여부를 확인할 수 있는 절차에 대해 지속적인 연구가 필요하다.

주제어 : 무기체계, 무기체계 운용 보안, 사이버 공격, 해킹, 사이버 보안

Ⅰ. 서 론

1.1. 무기체계 개요

무기시스템의 사이버 보안 이슈는 일반적인 정보시스템과 매우 다르다. 시스템의 다양성에도 불구하고 다음과 같은 일반적인 용어로 설명할 수 있다.

사이버 취약성은 액세스 권한을 얻거나 시스템의 기밀성, 무결성 및 가용성에 영향을 줄 수 있는 시스템의 약점이다. 사이버 보안 위협은 의도적으로 또는 우발적으로 시스템을 손상시킬 수 있는 모든 것이다. 사이버 보안위험은 위협(의도 및 능력), 취약성(일관성 또는 도입) 및 결과(수정 가능 또는 치명적)의 함수이다[1].

무기체계 사이버보안 강화를 위한 방안 연구에 앞서 무기체계에 대한 명확한 정의에 대해 이해하는 것이 중요하다. 단순히 무기체계를 흔히 이야기하는 미사일, 전차 및 전투기 등으로 생각해서는 안 된다. 무기체계에 대한 명확한 정의는 방위사업법, 방위사업법 시행령 및 시행규칙, 국방전력발전업무훈령 등에 명시되어 있다.

무기체계는 유도무기·함정·전투기 등 전장에서 전투력을 발휘하기 위한 무기와 이를 운용하는데 필요한 장비·부품·시설·소프트웨어 등 제반요소를 통합한 것이다[2]. 대표적으로 통신망 등 지휘통제·통신 무기체계, 레이다 등 감시·정찰 무기체계, 전투함 등 함정무기체계, 위성 등 우주무기체계 등이 있다[3]. 세부적인 주요 무기체계는 [표 Ⅰ-1]과 같이 분류하고 있다[4].

구 분	분 류
지휘 통제·통신 무기체계	연합지휘통제체계(AKJCCS), 합동지휘통제체계(KJCCS), 군사정보통합처리체계(MIMS), 지상전술C4I체계(ATCIS), 해군전술C4I체계(KNCCS), 공군중앙방공통제체계(MCRC), 전술정보통신체계(TICN), 합동전술데이터링크체계(JTDLS), 군위성통신체계(ANASIS) 등
기동 무기체계	전차, 장갑차, 전투차량, 기동 및 대기동 지원장비, 개인전투체계 등
함정 무기체계	구축함, 호위함, 초계함, 대형수송함, 상륙함, 군수지원함, 잠수함, 수상함 전투체계, 잠수함 전투체계, 함정사격통제장비, 함정 피아식별장비 등
항공 무기체계	전투임무기, 공중기동기, 감시통제기, 해상초계기, 공격헬기, 항공전투지원장비 등
화력 무기체계	개인화기, 대전차화기, 화포, 화력지원장비, 탄약, 유도무기, 특수무기 등
방호 무기체계	대공포, 대공유도무기, 방공레이더, 화생방 보호장비 등

구 분	분 류
사이버 무기체계	사이버전장관리체계, 사이버 무력화체계, 사이버훈련체계, 사이버 전투실험 분석체계 등
우주 무기체계	우주물체감시체계, 우주기상감시체계, 위성조기경보 및 정찰체계, 위성항법체계 등
그 밖의 무기체계 (국방M&S체계)	워게임 모델 - 연습·훈련용 : 태극 JOS모의모델, 창조21모델, 천자봉모델 등 - 분석용 : 합동작전 분석모델, C4ISR 분석모델, 해군 교전급 분석모델 등 - 획득용 : 함대공 교전효과도 분석 모델, 잠수함 작전효과도 분석 모델 등 전술훈련모의장비

[표 I-1] 무기체계 분류

특이하게도 무기체계 종류 중 그 밖의 무기체계에 국방M&S체계가 포함되어 있다. 국방 M&S는 모델링(Modeling)과 시뮬레이션(Simulation)의 합성어로써 기존의 워게임 영역을 대폭 확대하여 국방기획 관리상의 소요제기, 획득관리 및 분석·평가는 물론, 軍의 훈련까지 과학적으로 지원하는 도구 및 수단을 총칭하는 개념으로 전쟁 또는 전투요소들의 영향을 연구하기 위해 실전과 유사한 가상 전투상황을 조성해 주고, 전쟁 또는 전투요소들의 효과를 측정 및 평가해 주는 도구이다. 이러한 국방 M&S는 사용 용도에 따라 워게임 모델과 전술훈련 모의장비로 구분되며, 워게임 모델은 적용 분야에 따라 훈련용, 분석용, 획득용으로 구분된다[5]. 국방 M&S체계는 워게임을 모의하는 연습·훈련, 분석, 획득, 합동·전투실험 4개 분야로 분류하고 이러한 분야의 워게임 운영 및 체계관리에 필요한 기반환경을 총칭하는 체계를 말한다[6].

전력지원체계는 무기체계 외의 장비·부품·시설·소프트웨어 그 밖의 물품 등 제반요소를 의미한다[2]. 획득 절차가 상이하기 때문에 국방부에서 군수품을 무기체계나 전력지원체계로 구분하는 기준을 [표 I-2]와 같이 수립하였으며 구분이 불명확한 경우 국방부 전력자원관리실장이 종합적으로 판단하여 결정한다[7].

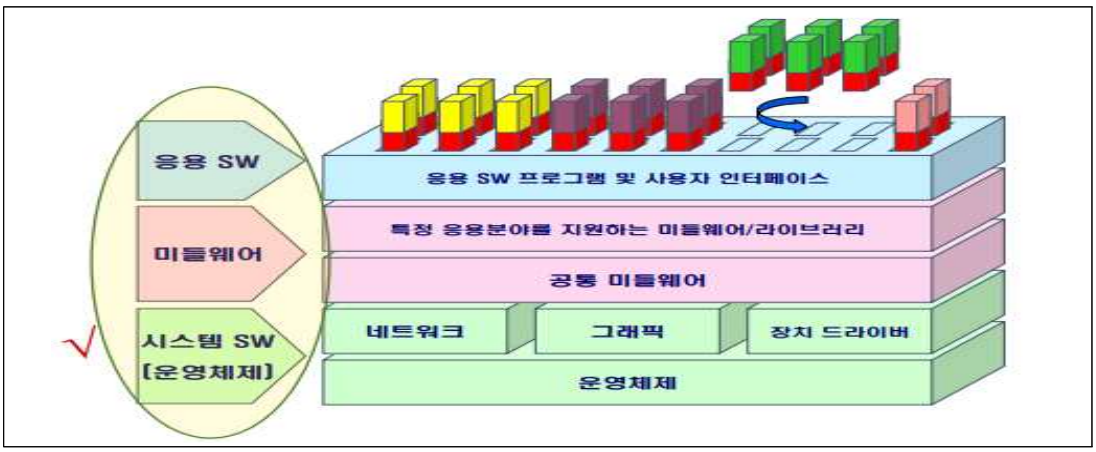
무기체계 선정 기준
o 군사작전에 직접 운용되거나 전투력 발휘에 직접 영향을 미치는 장비·물자 o 무기체계의 전투력 발휘에 영향을 미치는 장비·물자 o 전투력 발휘에 영향을 미치는 주요 전술 훈련장비 및 소프트웨어, 관련시설 o 국방M&S체계 중 전투력 운용과 능력배양에 직접 관련이 되는 모델, 전투력 운용과 전력증강 타당성 분석을 위한 모델, 무기체계 획득과 직접 연계되는 모델 o 기존장비나 주장비와 달리 별개의 무기체계로 본다. - 무기체계 성능 개량으로 운영 개념이 현저하게 변경되거나 중대한 작전 운용성능 변경 시 - 무기체계의 구성장비로 독립된 기능을 발휘하고 타 무기체계에 탑재, 연결, 결합하여 사용하고 있거나 사용될 수 있는 경우 - 그 밖에 별개의 무기체계로 결정된 경우

[표 I-2] 무기체계 선정 기준

무기체계 內 포함된 정보시스템은 각종 정보를 교환할 수 있는 기능을 수행하는 것으로 다양한 체계가 있으며 그중에서도 전장관리체계는 정보를 수집, 가공, 전달 등의 기능을 수행하는 컴퓨터, SW, 데이터, 통신수단이 통합되어 그 기능을 발휘하는 SW 중심의 체계로서 범용컴퓨터를 활용하는 체계를 의미한다[8]. [그림 Ⅰ-1][9]과 같이 분류된다.

[그림 Ⅰ-1] 무기체계SW 분류

탑재 형태별로 구분하면 무기체계 내장형 SW와 정보시스템으로 구분된다. 무기체계 내장형 SW는 전차, 전투기, 함정, 유도무기 등 무기체계에 탑재되어 해당 기능을 수행하는 것이며 이러한 무기체계 SW의 일반적인 구성은 응용SW, 미들웨어, 시스템 SW로 구분된다.



[그림 Ⅰ-2] 무기체계SW 일반적 구성요소

이렇게 우리가 일반적으로 생각하는 무기체계와 법적인 기준에 의한 무기체계 분류 기준은 무척 다르다. 하지만 이러한 혼동은 軍에서 전력지원체계로 관리하고 있는 국방정보시스템에서도 동일하게 나타난다. 전력지원체계 세부분류기준[10]에 의하면 국방정보시스템 하위 분류에 국방M&S체계가 포함되어 있으며 전시 자원소요산정모델, 전투근무지원 분석모델 등으로 [표 I-3]과 같이 선정되어 있다.

중분류	소분류	대상 장비
자원관리 정보체계	기획・재정 정보체계	조직정원관리체계, 국방통합재정정보체계, 국방정보자원관리체계 등
	인사・동원 정보체계	국방통합인사정보체계, 국방동원정보체계, 국방의료정보체계 등
	군수・시설 정보체계	군수통합정보체계, 육·해·공군 장비정비정보체계, 국방탄약정보체계, 국방수송정보체계 등
	전자・행정 정보체계	홈페이지 및 포탈시스템, 지식관리시스템, 국방통합전자도서관체계 등
국방 M&S체계	분석용	전시자원소요산정모델, 전투근무지원분석모델 등
기반운영 환경	정보통신망	무기체계를 제외한 정보통신망
	컴퓨터체계	서버 장비(서버), 개인장비(PC), 저장장비, 입력장비, 기타 부수장비, 회의장비, 기본 소프트웨어
	사이버 방호체계	공통/기반보호체계, 네트워크보호체계, IT플랫폼보호체계, 응용체계보호체계, 보호관리체계
	상호 운용성 체계	공통운용환경체계, 데이터공유환경체계, 상호운용성평가체계, 정보기술표준체계, 정보기술아키텍처체계, 국방M&S표준자료체계

[표 I-3] 전력지원체계 세부분류 기준 中 국방정보시스템 분야

하지만, 앞서 설명한 무기체계 기준에 비해 '국방정보화 기반조성 및 국방정보자원관리에 관한 법률(약칭 : 국방정보화법)'에 근거한 국방정보화업무훈령의 기준과 매우 상이하다. 국방정보화업무훈령에서는 국방정보시스템의 정의를 '국방 정보의 수집・가공・저장・검색・송신・수신 및 그 활용과 관련되는 기기 등 응용소프트웨어와 기반운영환경의 조직화된 체계를 말하며, 정보시스템 장비운영 및 관리를 위해 분류한다'고 명시되어 있다[11]. 또한 정보시스템의 응용소프트웨어로 전장관리정보체계(지휘통제, 전투지휘, 군사정보체계), 자원관리정보체계(기획・재정, 인사・동원, 군수・시설, 전자행정, 군사정보지원, 상호운용성), 국방M&S 체계(연습・훈련용, 분석용, 획득용)로 구분하고 있다. 그리고 정보시스템의 기반 운영환경은 주장비, 통신망, 단말기, 주변장치, 시설, 정보보호체계, 상호운용성 관리에 필요한 시스템

및 그 밖의 시스템 소프트웨어로 정의하고 있다. 국방정보화업무훈령에서 국방정보시스템의 세부적인 분류 기준은 [표 1-4]와 같다[12]. 이와 같은 분류 기준에도 불구하고, 여기에서도 무기 체계와 유사하게 국방정보시스템의 구분이 불명확 할 경우 국방정보화책임관 실무협의회의 심의를 거쳐 결정하고 있다.

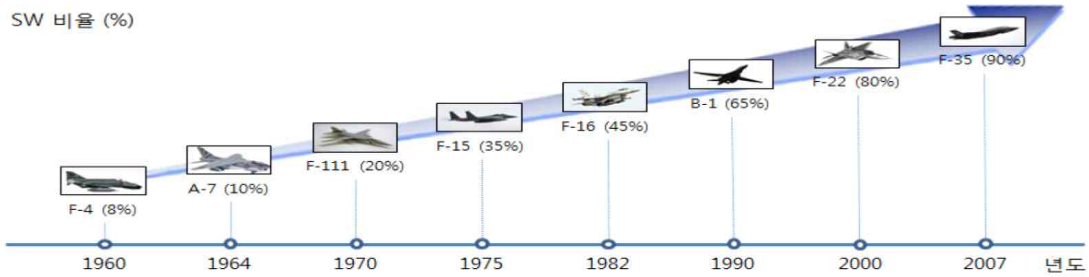
구 분	주요 해당 시스템
전장관리정보 체계	연합지휘통제체계(AKJCCS), 합동지휘통제체계(KJCCS), 군사정보통합처리체계(MIMS), 지상전술C4I체계(ATCIS), 해군전술C4I체계(KNCCS), 공군자동화방공체계(MCRC) 등
자원관리정보 체계	조직정원관리시스템, 국방통합재정정보체계, 국방정보자원관리시스템(DRIMS), 국방 통합인사정보체계, 국방탄약정보체계, 한미영상정보공유체계, 군사정보전파체계 등
국방M&S 체계	- 연습·훈련용 : 태극JOS모의모델, 창조21모델, 천자봉모델 등 - 분석용 : 합동작전 분석모델, C4ISR분석모델, 전구급 해상전 분석모델 등 - 획득용 : 함대공 교전효과도 분석 모델, 잠수함 작전효과도 분석모델 등
기반운영환경	정보통신망 : 전술정보통신체계(TICN), 전투무선망, 군위성통신체계(ANASIS), 해상작전 위성통신체계(MOSCOS), 합동전술데이터링크체계(JTDLS) 등 컴퓨터체계 : 서버장비, PC, 기본SW 정보보호체계 : 네트워크 보호체계, 서버·단말 보호체계, 사이버대응체계, 보안관리체계, 암호체계 상호운용성체계 : 국방정보화 표준체계, 상호운영성 평가체계, 국방M&S 표준자료 체계, 연동관리체계

[표 I-4] 국방정보화업무훈령에 따른 국방정보시스템 분류 기준

이러한 규정은 무기체계 보안 관리에 혼란을 유발하고 있다. 국방정보시스템 분류 기준에 포함된 주요 시스템이 무기체계 분류기준과 중복되는 부분이 많이 발생한다. 대표적으로 무기체계의 지휘통제·통신무기체계의 대상 장비가 국방정보화업무훈령의 국방정보시스템 분류 기준의 전장관리정보체계 및 기반운영환경 정보통신망과 대부분 일치한다. 또한 국방M&S체계의 경우도 무기체계 분류기준과 대부분 일치하며, 국방정보화업무훈령 별표2 국방정보시스템 분류기준 말미에 '각군 및 기관의 정보시스템도 동일한 분류기준을 적용하며 국방정보시스템을 제외한 무기·전력지원체계 분류는 국방전력발전업무훈령을 적용함'이라고 마지막 줄에 명시하고 있다.

이와 같이 軍에서는 무기체계에 대한 정의를 내림에 있어 상당히 혼란스러워 하고 있는 것을 알 수 있다. 이러한 혼란으로 인해 무기체계를 관리 중인 실무자들은 정보체계로 관리해야 할지, 아니면 무기체계로 관리하게 될지 어려움을 겪게 된다. 이러한 원인은 기존에는 무기체계가 컴퓨터 기반이더라도 단순하고 비중이 작았으나 기술이 발전함에 따라 소프트웨어 비중이 많아지게 됨에 따라 발

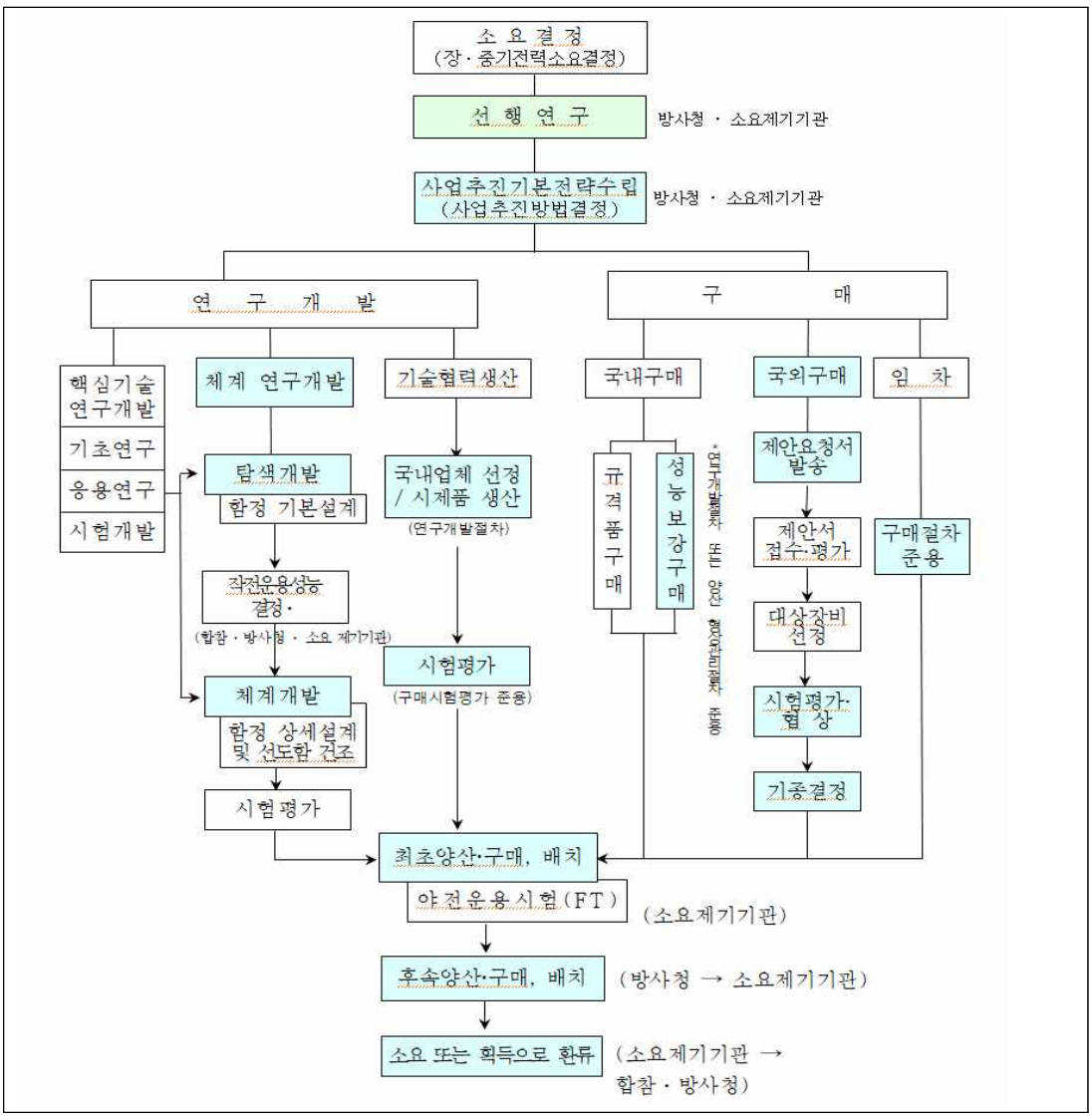
생한 자연스러운 결과로 판단된다. 실례로 무기체계 SW 발전 추세는 단거리·저고도 무기에서 장거리·고고도 정밀 무기로 발전하고 있으며, 첨단화·정밀화·복잡화로 인해 SW 개발비용의 급격한 증대가 나타나고 있다. 또한 신기술 출현 및 기술변화에 따라 지속적인 무기체계 성능개량이 필요하며, 미래전 양상에 대비한 무기체계의 무인·로봇체계로 진화하고 있으며 이러한 발전에 따라 무기체계 기능 구현에 필요한 SW 비중이 [그림 Ⅰ-3]과 같이 지속적으로 증가하고 있다[13].



[그림 Ⅰ-3] 무기체계 발전에 따른 SW 비율

1.2. 우리 軍의 무기체계 사이버 보안

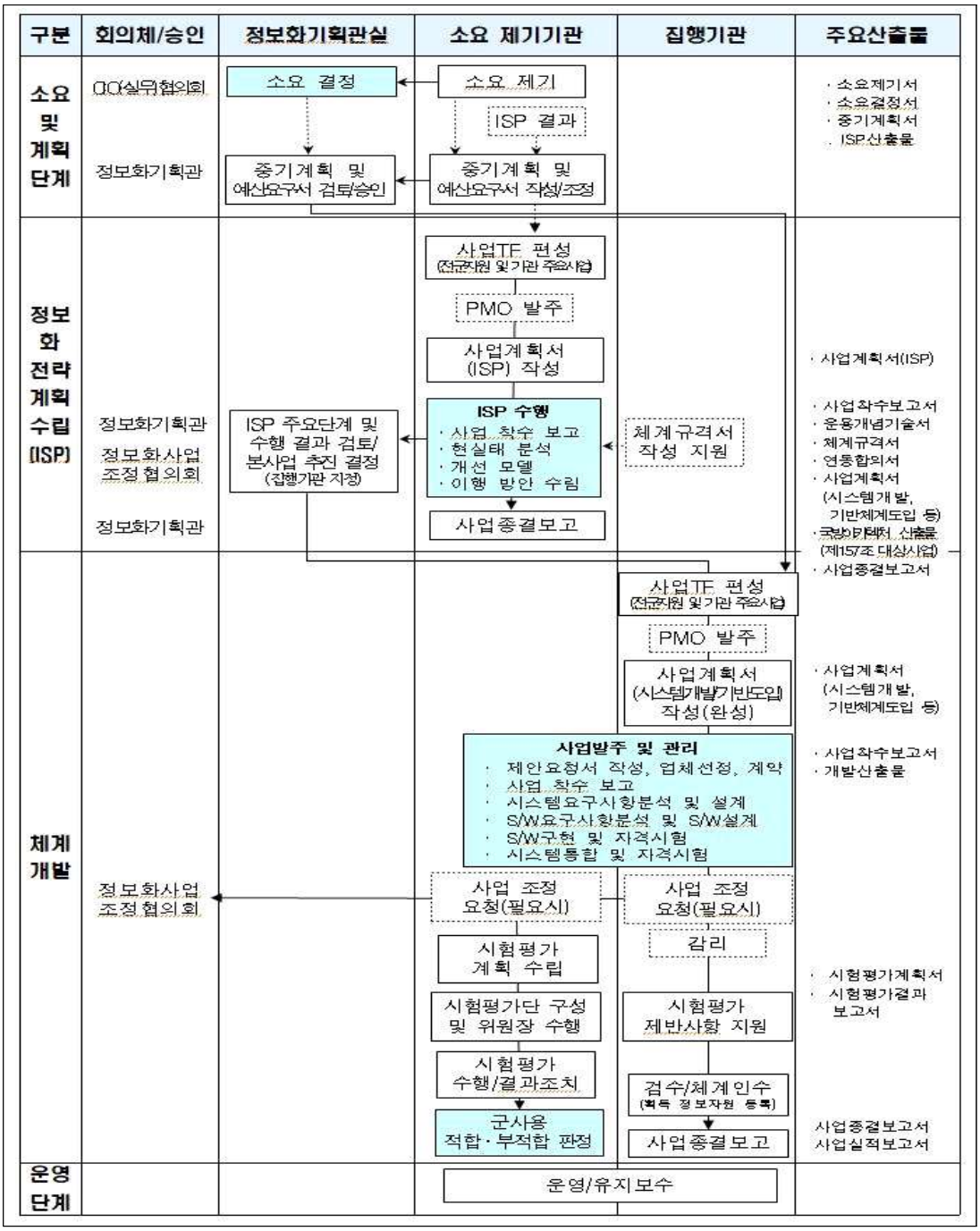
무기체계의 획득 절차는 [그림 Ⅰ-4][14]과 같다. 무기체계 획득 절차에 대한 부분은 본 논문의 연구 주제와 상이하므로 무기체계 획득 절차는 간략히 확인하고 무기체계 보안과 관련된 부분에 대해 집중적으로 살펴보겠다.



[그림 Ⅰ-4] 무기체계 획득 절차

軍에서는 국방전력발전업무훈령 6조에 의해서 국방정보시스템의 분류 및 국방정보시스템의 연구개발 및 구매는 국방정보화업무훈령을 따른다고 명시하고 있

다. 그리고 국방정보화업무훈령 제9조에서는 무기체계로 분류된 정보시스템의 기획관리절차는 국방전력발전업무훈령을 따르고, 사업관리 절차는 방위사업관리절차를 따르고 있지만 상호운용성과 아키텍처에 관한 사항은 본 훈령을 따라야 한다고 명시하고 있다. 국방정보화사업 업무 절차는 [표 Ⅰ-5][15]과 같다.



[표 Ⅰ-5] 국방정보화사업 업무 흐름도

무기체계와 국방정보시스템의 구분이 모호하고 무기체계와 정보시스템이 혼재되어 있어 무기체계 도입간 절차상의 혼란을 야기할 수 있다. 무기체계 보안과 관련된 부분은 국방전력발전업무훈령 제6조에 의해서 국방전력발전업무와 관련된 보안대책은 국방보안업무훈령을 따르고 있다. 국방전력발전업무훈령 제17조에 의해서 소요제기기관에서 소요제기서 작성시 무기체계의 사이버방호에 요구되는 능력을 기술하고 정보통신분야 보안대책 검토결과를 포함하도록 되어 있다.

국방정보화업무훈령 제9조에 의하면 정보시스템의 보호관리 및 사이버보안에 관한 업무는 국방사이버안보훈령을 따르도록 하고 있다. 국방정보화업무훈령에서 정보시스템의 응용소프트웨어 중 전장관리정보체계와 국방M&S체계는 전력발전업무훈령의 무기체계 대상과 거의 동일하다. 무기체계이면서 국방정보시스템의 응용체계인 것이다. 일반적인 무기체계의 경우 보안대책은 국방보안업무를 따르지만 무기체계 중 국방정보시스템은 국방사이버안보훈령을 따르게 되는 것이다.

현재 軍에서는 국방정보시스템의 중요도와 위험 판단에 따라 해당 시스템의 보호요구수준 설정 후 보호 통제항목과 보호 요구사항을 기준으로 보호대책서를 작성하여 안보지원사로 검토를 의뢰하면, 안보지원사에서 보호대책의 적절성과 충분성을 검토 후 검토 결과를 통보하면 미흡점을 보완하도록 하고 있다[8].

운용단계에서는 국방정보체계 취약점 분석·평가 실무지침서를 이용하여 국방정보시스템 중요도를 고려하여 취약점에 대한 분석·평가를 수행한다[16]. 하지만 무기체계 평가를 위한 점검기준으로 판단하기 부적절한 부분이 존재한다.

2018년 12월 국방사이버안보 훈령이 개정됨에 따라 국방정보시스템과 내장형 소프트웨어를 가지고 있는 무기체계 및 전력지원체계로 정의하면서 수명주기와 연계한 보안활동으로 그 업무를 명시하고 있다[17].

무기 체계도 보호대책서를 작성하게 되는데 시험평가기본계획서와 연계 없이 별도 프로세스로 관리되고 있어 무기체계 획득 프로세스를 고려하여야 하며, 사이버 보안 강화를 위한 구체적인 항목이 반영되어야 한다[18].

1.3. 연구 배경

무기체계 보안 분야는 그 동안 국내에서 큰 관심을 갖지 않았던 분야이다. 특히 운용중인 무기체계에 대한 연구 현황은 미미한 실적이다. 물론 무기체계에 대한 접근이 제한되고 공개된 내용이 부족한 연구 현실이 원인일 수 있다. 하지만 무기체계는 국가안보에 중요한 요소이며, 무기체계가 공격을 받게 된다면 사회적 혼란과 피해는 상당할 것이다. 무기체계 보안의 중요성을 인식하고 연구를 시작하는 단계에서 큰 혼란을 겪게 되었다. 무기체계보안 관련 무기체계 SW의 개발단계에서의 보안에 대한 연구가 대부분으로 실제 운용단계에서 보안취약점에 대한 검증 방법 및 안전성 확보에 대한 내용은 거의 찾아 볼 수가 없었다.

무기체계 운용간 사이버 보안 향상을 위해 어떤 방법으로 접근하고 어떻게 발전시켜야 할지 세부적인 방향을 알려주는 논문을 찾지 못했다. 그나마 찾은 관련 국내 논문들은 대부분 무기체계 소프트웨어 개발 단계에서 보안 수준을 향상시키는 것에 집중되어 있었다. 일부 논문에서 RMF, 국방 사이버 보안, 국방 보안 정책 등의 연구 산출물이 있었으나 실제 운용 중에 있는 무기체계의 보안수준을 향상 시킬 수 있는 내용은 거의 없다.

국방 무기체계의 사이버 보안은 누구나 공감하듯이 중요하다. 생각하기 싫지만 무기체계가 해커의 공격에 의해 오작동 된다면 상상하기 힘든 끔찍한 비극이 일어날 수 있을 정도로 중요한 문제이다. 하지만 현실은 무기체계 사이버 보안을 강화하기 보다는 무기체계 획득 소요결정에 의한 작전운용 성능에 부합되는 무기체계 연구개발 또는 성능 검증에 집중되어 있고 사이버 보안은 우선순위가 매우 낮다.

현재 국가적 차원의 사이버 공격 및 전문 해커 집단에 의한 은밀한 공격이 지속적으로 자행되고 있다. 인터넷 공간과 분리된 내부망에 은밀히 침투하여 핵심 정보를 탈취하기 위해 지속하고 있다.[19].

1) 북한의 軍 내부망 사이버 공격 사례

이러한 무기체계 사이버 보안 위협을 이해하기 위해서는 우리 軍에 대한 북한

의 사이버 보안 위협에 대해 살펴볼 필요가 있다. 현재까지 북한 해킹의 주요 타겟은 국방정보체계를 대상으로 한다.

대표적인 사례로 2016. 9월에 발생한 국방망 해킹 사건은 북한 해커 조직 소행으로 추정되며 軍 전산망 관제를 책임지고 있는 국군사이버사령부의 미흡한 대응 조치로 국방망 PC 700대, 인터넷 PC 2,500대 등 3,200대가 악성코드에 감염되어 다수의 군사자료가 유출되는 피해를 입었다[20].

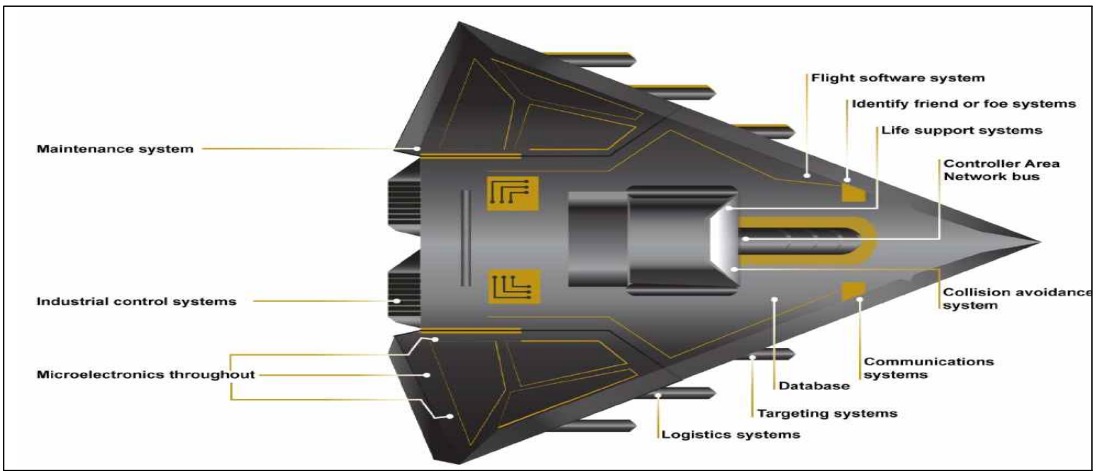
첨단 무기체계는 인터넷이 연결되어 있지 않지만 장비 제조단계에서 악성코드를 심어놓을 수 있고 소프트웨어 업데이트 과정에서 얼마든지 우회 침투가 가능하다[21].

2) 美 회계검사원(GAO)의 美軍 무기체계 진단 사례 소개

우리나라에서 운용중인 대부분의 무기체계는 직접 개발한 체계보다 미국에서 수입하여 운용중인 무기체계가 많다. 도입된 무기체계가 미국에서 생산되었기 때문에 안전하게 운용할 수 있을 것으로 생각 할 수 있지만 현실은 미국 국방부(U.S. Department of Defense, 이하 DoD)에서 개발 중인 차세대 무기체계 조차도 해킹에 취약한 실정이다.

미국 회계검사원(U.S. Government Accountability Office, 이하 GAO)이 2018. 10. 9. DoD가 개발 중인 차세대 무기체계 전산망이 해킹에 취약하다고 발표했다[1]. GAO가 공개한 보고서에는 국방부의 허술한 전산망 암호관리와 비암호화 통신 사용 등을 문제 삼아 “탐지되지 않은 적(敵)이 중앙컴퓨터와 무기체계에 접근해 내부에서 작업을 하는 게 얼마나 쉬운 지 국방부는 인식하지 못하고 있다”고 지적했다.

이 보고서에서 소개하고 있는 미국의 무기체계 운용 사례에 대해 살펴보겠다. DoD는 무기시스템 획득에서 사이버 보안을 우선시하지 않았으며 부분적으로 네트워크의 사이버 보안에 초점을 맞추었지만 무기 시스템 자체에는 초점을 맞추지 않았기 때문에 사이버 보안을 무기 시스템에 적용하는 방법을 이해하려는 초기 단계에 있다고 설명한다. 또한 DoD의 무기 시스템 소프트웨어의 비중이 기하급수적으로 증가하고 있으며 다양한 하드웨어와 IT 구성요소를 포함하는 기술적으로 복잡한 수많은 하위 시스템이 [그림 Ⅰ-5]과 같이 내장되어 있다.



[그림 Ⅰ-5] GAO에 명시된 무기체계 하위 시스템

과거 무기시스템 개발 시 사이버 보안을 고려하지 않고 설계 및 구축되었기 때문에 개발 주기 후반이나 시스템이 배포된 이후 사이버 보안을 강화하는 것은 처음부터 설계하는 것보다 더 어렵고 비용이 많이 소요된다. 이러한 시스템은 해당 임무의 보안이 위험할 뿐만 아니라 구형 시스템은 최신 시스템을 위험에 빠뜨릴 수 있다. 무기시스템과 기존 IT 시스템 간에는 유사점이 있지만 DoD의 보안 통제가 무기 시스템이 아닌 IT 시스템을 염두에 두고 개발되었기 때문에 보안 통제 방법이 달라져야 한다.

많은 무기시스템은 산업제어 시스템을 사용하여 장비를 모니터링하고 제어하며, 컴퓨터와 마찬가지로 소프트웨어를 포함한다. 예를 들어 선박은 엔진 및 화재 진압 시스템을 제어하기 위해 산업용 제어 시스템을 사용할 수 있다. 미국 국립표준기술연구소(National Institute of Standards and Technology, 이하 NIST)에 따르면 산업제어시스템은 원래 신뢰할 수 있는 환경에서 사용하도록 설계되었으므로 많은 경우 보안 제어가 통합되지 않았다. 미국 정부 및 미국 산업보고서에 따르면 이러한 시스템에 대한 공격이 증가하고 있다. 그러나 DoD 차원에서 현재 사용중인 무기에 어떤 산업제어 시스템이 내장되어 있는지 또는 그것을 사용하는 것이 보안에 어떤 영향을 미치는지 모르고 있다.

무기 시스템은 상호 의존성이 많은 매우 크고 복잡한 시스템일 수 있으므로 시스템의 한 구성요소를 업데이트하면 다른 구성 요소에 영향을 줄 수 있다. 일

반적인 시스템 패치와 달리 무기체계의 경우 시스템의 복잡성으로 인해 안정적으로 운영하는데 몇 달 또는 오랜 시간이 소요될 수 있다. 무기 시스템 패치를 연기하거나 포기하는데에는 타당한 이유가 있지만, 이는 일부 무기시스템이 알려진 취약점으로 장기간 작동할 수 있음을 의미한다.

미국에서 2012년부터 2017년 사이에 운영 테스트를 거친 거의 모든 주요 무기체계에서 공격자가 손상시킬 수 있는 치명적인 사이버 취약점이 발견되었다. GAO 모의 해킹팀은 손쉽게 무기체계 전산망 해킹에 성공했으며, 하루만에 관리자 권한을 탈취했다. GAO는 “국방부 전산망에 접속할 수 있는 접속 포인트가 계속 늘어나면서 관리자들의 통제에 한계가 있다”면서 “전산망에 연결되지 않은 컴퓨터는 보안 취약성이 매우 심각한 수준”이라고 진단했다. 공격팀이 상대적으로 간단한 도구와 기술을 사용하여 짧은 시간에 무단 액세스 권한을 얻고 공격 대상 무기 시스템을 완전히 또는 부분적으로 제어할 수 있었다. 어떤 경우 단순히 시스템을 스캔하는 것만으로도 시스템 일부가 종료되었고, 여러 무기 시스템은 상용 또는 오픈 소스 소프트웨어를 사용했지만 소프트웨어가 설치될 때 기본 암호를 변경하지 않아 테스트팀이 쉽게 액세스 할 수 있었다. 또한 일부 무기체계의 경우 내부통신을 암호화 하지 않아 일반사용자가 관리자의 계정명과 비밀번호를 얻어 더 많은 시스템에 접근 할 수 있었다.

그리고 기존 무기체계 개발간 취약점을 식별하였으나 무슨 이유에선지 취약점 자체를 해결하지 않고 방치한 사례도 다수 식별되었으며, 충격적인 것은 테스트팀이 몇 주 동안 해킹을 시도하였으나 전혀 감지되지 않았다. 침입탐지 공격이 식별되었지만 오인탐지로 오인하거나 일부에서는 시스템 로그에 대해 전혀 검토하지 않았다.

무기체계 사이버 보안평가의 경우 해당 시스템의 모든 취약점을 식별하지 못한다. 이는 부분적으로 사이버 보안평가가 무기 시스템이 작동 중에 직면할 수 있는 위협의 전체 범위를 반영하지 않기 때문이다. 대부분 사이버 보안평가가 며칠에서 몇주에 걸쳐 수행되지만 이와 대조적으로 공격자들은 몇 달 혹은 몇 년에 걸쳐 공격을 수행하고 있다. 테스트팀이 공격을 할 수 없는 계약자의 기업 네트워크를 활용하거나 보안 문제로 인해 테스트팀이 기밀 네트워크를 사용하여 무기 시스템을 공격하는 것이 허용되지 않았다. 또 다른 테스트는 실험실 환경에

서 수행되었으므로 테스트 팀은 외부 통신을 시뮬레이션해야 했다. 이는 사이버 보안 테스트의 한계로 인해 DoD가 인지하고 있는 취약점의 일부일 가능성이 있다.

GAO는 “컴퓨터 의존형 무기의 설계·조달에도 사이버 보안기술을 적용하지 않고 있었다”며 “무기 개발자들 스스로 사이버보안 문제에 대한 이해도가 낮은 경우도 있었다”고 밝혔다. GAO는 공개한 보고서에 ‘보안상 이유’로 취약성이 확인된 무기체계 전산망을 구체적으로 명시하지 않았다[1].

3) 첨단 기술의 무기체계 적용에 따른 위협

무기체계 발전에 따라 민간의 새로운 기술을 필요로 한다. 한국국방기술진흥연구소는 2022. 2월 AI 기술을 미래전장의 게임체인저로 활용하기 위한 전략으로서 ‘미래국방 2030 기술전략 : 국방 AI 기술로드맵’ 책자를 발간하였다. AI 기술이 적용될 것으로 예상되는 무기체계 핵심기술의 예시로 앞으로 10년~15년 이내에 적 무기체계 취약점 분석에 기반한 무력화 코드 자동 생성 기술을 제시했다[19].

국방부에서는 2022. 3.18. 민간분야의 첨단 기술 신속 도입을 위해 무기체계에 대해 신속획득사업을 실시할 수 있도록 국방전력발전업무훈령을 개정했다. 첨단기술 분야 무기체계에 신속획득사업이 적용될 경우, 민간이 가지고 있는 첨단 기술을 적용한 제품을 군이 1~3년 이내에 신속히 사용해 보고 도입 필요성을 판단해 볼 수 있다[20].

앞서 살펴본 봐와 같이 북한의 위협은 실존하고 있다. 북한에서 가장 공격하고 싶은 분야는 우리 軍의 무기체계일 것이다. 꼭 필요한 순간에 우리군의 핵심 무기체계가 해커의 공격에 의해 불능 상태가 된다거나 공격 타겟 목표를 임의로 변경해 버리는 일이 불가능한 일이 아닐 것이다. 미국에서도 첨단 무기체계의 취약점에 대해 인식하고 무기체계에 대한 보안을 강화하고 있다. 軍에서 신속하게 무기체계를 도입하게 될 것이며 무기체계 보안 프로세스를 소홀하게 취급한다면 추후에 발생할 수 있는 문제는 상상을 초월 할 것이다.

1.4. 연구의 필요성과 목적

무기체계에 대한 보안위협은 실존하고 있다. 그런데 실존하는 보안위협을 어떻게 확인할 수 있는지 구체적인 방안이 제시되어야 할 것이다. 하지만 딜레마가 존재한다. 무기체계의 보안위협은 '이것'이라고 구체적인 대상 장비와 제원, 세부적인 보안취약점에 대해 언급하게 된다면 이것은 적을 이롭게 하는 행위가 될 것이다. 국방 분야의 특성상 군사기밀로 분류된 사항에 대해서는 접근할 수 없는 것은 당연하다. 하지만 이러한 특성에 기인해 무기체계의 위협에 대한 연구를 소홀히 한다면 무기체계 보안 분야의 발전은 힘들 것이다.

이번 연구에서 수많은 무기체계에 대한 보안 취약점에 대해 직접 확인하는 것은 당연히 불가능하다. 이런 거시적인 차원의 확인은 국방부, 정부, 또는 국회 차원에서 수많은 예산과 전문가를 투입해야 가능할 것이다.

대부분의 논문들이 무기체계 관련 소프트웨어 개발 단계에서의 보안취약점 개선에 집중하고 있다. 하지만 정작 중요한 것은 실제 운용중에 있는 무기체계의 보안 취약점을 어떻게 확인하고 개선 시킬 수 있는지에 대한 거시적인 차원에서의 연구가 필요하다. 선진국에서는 어떤 방법으로 무기체계 취약점에 대한 문제점을 식별하고 조치하고 있는지에 대한 연구를 통해 이를 벤치마킹하면 한국군에 적용 할 수 있는 혜안을 찾을 수 있을 것이다. 이번 연구에서는 특히 미국의 사례에 집중하여 연구할 것이다. 왜냐하면 한국군에서 운용되고 있는 주요 무기체계들은 대부분 미국에서 구매하여 배치·운용하고 있기 때문이다.

무기체계 개발단계와 무기체계 SW의 자체 취약점을 개선시키는 것도 중요하다. 하지만 앞선 軍의 해킹 사례에서 보는 것과 같이 아무리 좋은 바이러스 탐지체계라 할지라도 설치 시 오류가 발생하고 운용단계에서 제대로 조치하지 않는다면 문제가 발생할 수밖에 없는 것이다.

무기체계 운용 단계에서 어떻게 하면 사이버 보안을 강화할 수 있는지 표준모델을 수립하는 것이 중요하다. 또한 이를 위해 정책적으로 필요한 사안, 관리적으로 보완해야 할 사항, 기술적인 조치 방안에 대해 제시하고자 한다. 이를 통해 국방분야 무기체계 운용간 해킹 취약점을 식별하거나 향후 문제점을 개선할

수 있는 마중물의 역할을 하고자 한다. 물론 무기체계 접근에 대한 정보 제한으로 인해 세부적인 사항에 대한 연구는 불가할 것이다. 하지만 선진국과 미국의 사례 연구 및 공개된 자료를 연구한다면 충분히 핸디캡을 극복할 수 있을 것이다.

최근 軍에 대한 사이버 해킹 공격 시도가 급증하고 있다. 軍에서 운용 중인 정보체계의 취약점을 이용하여 내부망으로 침투 후 공격하는 사이버전이 발생하고 있다. 앞서 살펴본 것처럼 2016년 북한 해커에 의해 국방전산망에 대한 정보유출 사고가 발생하였고, 국방통합데이터센터에서 내·외부망 혼용에 의해 백신중계 서버에 악성코드가 감염되어 장기간 동안 피해를 유발한 사례이다[23]. 하지만 국방 분야에서 보안 취약점 완화를 위한 보호대책이 미흡하여 지속적으로 보안 위협이 증가되고 있다.

미국에서는 2015년 'Left of Launch' 전략이 공개되었는데 주요 내용은 주요 미사일 발사 전 사이버 공격으로 무기체계에 침입 후 발사하기 전단계에서 무력화 시키는 것이다. 앞서 미군의 무기체계의 취약점 발견을 언급했지만 미군은 무기체계 안전성 보장을 위해 개발 초기 단계에서부터 사이버보안 시험평가를 체계적으로 수행하고 있다.

반면, 우리 軍의 무기체계 사이버 공격 대응체계는 미흡하다. 국내 무기체계 사이버보안 관련 규정은 국방전력발전업무훈령과 국방사이버안보훈령에 일부 포함되어 있지만 무기체계에 적합한 세부 사이버 보안 지침 적용이 미흡하며, 훈령 간 연계성이 부족하다[18].

현대 무기체계들은 정보체계와의 결합, 전자화, 복합화, 융합화, 복잡화 되어가고 있으며, 소프트웨어의 성능이 무기체계 성능에 많은 영향을 주고 있다. 소프트웨어에 대한 의존도가 증가하고 있는 경향을 보이고 있고, 이로 인한 개발 리스크도 증가하고 있다. 다양한 사이버 위협들이 정보체계 또는 소프트웨어에 대해서 발생하고 있는데, 무기체계는 분리된 자체 통신망을 사용하여 사이버 위협의 가능성이 낮다는 인식이 많았다.

그러나 실제로 사이버 위협에서 안전하지 못하며, 다양한 사이버 위협에 노출되어 있는 것으로 확인되었다. 무기체계 내장형 소프트웨어는 이름은 내장형 소프트웨어이지만 대용량의 소프트웨어로 정보체계의 성격을 가지는 경우들이 많

으며, 사이버 위협에 대한 기술적, 제도적 다양한 대응이 필요하다. 그러나, 무기체계 내장형 소프트웨어의 사이버 위협에 대한 대응이나 연구는 미흡하여, 일부 연구자에 의해서만 연구가 진행되어 왔는데, 무기체계 내장형 소프트웨어의 사이버 위협 대응과 관련한 기존 연구들은 소프트웨어 개발보안의 적용을 통한 개발단계 시큐어 코딩의 적용 기법 개발에 초점을 맞추었다[24].

이렇게 다양한 사이버 위협과 관련해서 중요한 부분은 위험관리일 것이다. 반면 국방분야의 위험관리의 절차에 대한 우선순위 식별분야에 대한 구체적인 근거를 기반으로 한 연구가 필요하다. Matrix 기반 위험 우선순위 식별(Risk Matrix) 방법은 IT 사이버보안 분야에서 가장 많이 사용되는 위험 우선순위식별방법이다. DoD RMF에서도 Matrix 기반 위험 우선순위식별방법을 채택하고 있다[25]. 이제는 한국군에 적합한 위험관리 연구도 필요하다.

1.5. 연구의 범위와 방법

본 연구는 무기체계 운용간 사이버보안 강화를 위한 관리적·기술적 방안을 제시하기 위해 아래와 같이 범위를 선정하였다.

□ 무기체계 사이버 보안을 위한 기존 업무수행 체계를 확인한다.
- 한국군과 미군의 수행 체계에 대해 구체적으로 비교 및 분석한다.

□ 무기체계 해킹 사례 및 관련 연구 동향을 조사한다
- 무기체계 해킹 사례 및 연구 동향 분석을 통해 발전 방향을 확인한다.

□ 무기체계 사이버 보안 강화 방안에 대해 구체적으로 제시한다.
- 정책 및 제도분야, 기술적 분야에 대해 사례로 방안을 제시한다.

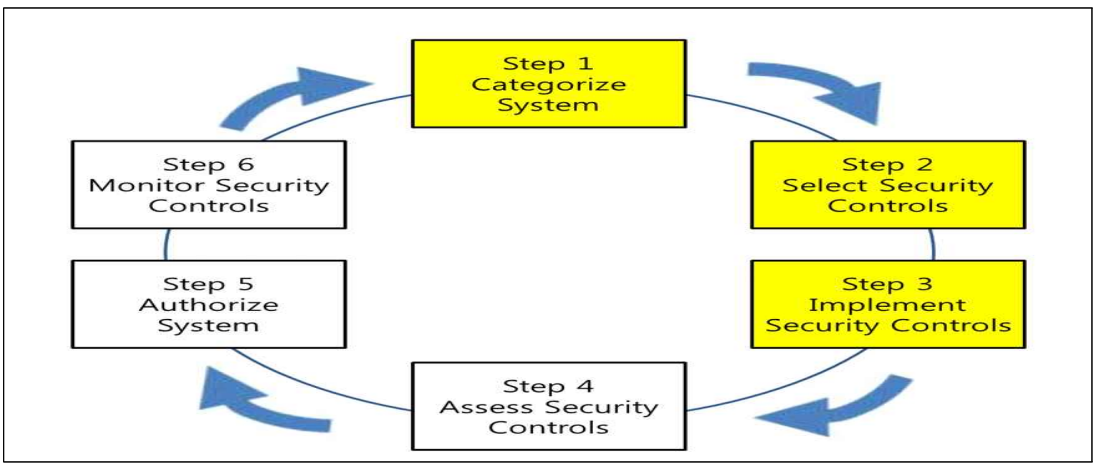
본 논문은 공개 자료, 학술자료 및 해외 인터넷 자료 등 공개된 자료만 대상으로 하여 연구한다. 무기체계와 관련된 제한된 자료 접근으로 인해 세부적인 내용 확인이 제한 될 수 있으나 면밀한 분석과 정책적 차원의 무기체계 발전과 관련된 대안 제시를 통해 국방 무기체계 사이버보안 강화에 기여할 것이다.

Ⅱ. 배경 지식 및 관련 연구

2.1. 미군의 무기체계 사이버 보안

미군은 RMF(Risk Management Framework, 이하 RMF)를 2013년 만들어 현재까지 적용되고 있다. 미군의 지침인 DoDI 8510.01은 RMF로 불리며 무기체계의 의무 준수사항이 되었다.

RMF는 무기체계를 개발하는 단계부터 평가와 유지관리하는 전 생명주기에 걸쳐 보안보증 활동을 고려한 모델이다. RMF 수행 절차는 NIST SP 800-37을 따르며 [그림 Ⅱ-1]의 6단계 절차[26]로 진행되는데 국방분야 관련 각 단계의 세부적인 내용은 비공개로 되어 있다. 한국군에서도 2019년 전반기 연례 한-미 국방부 지휘통제 상호운용성위원회에서 RMF를 적용하기 위한 MOU를 체결하고 RMF를 공동으로 작성하였다. 미국은 이에 따라 사이버보안 검증을 수행할 것을 우리나라에 명시적으로 요청하였다[27].



[그림 Ⅱ-1] RMF 6단계

Step 1 단계는 시스템 분류(Categorize System)이다. 사이버보안 요구사항을 확인하기 위해 체계에 영향을 주고 있는 연동되고 있는 정보들의 영향도를 평가하여 중요도에 따른 시스템 분류를 한다.

Step 2단계에서는 보안통제 수단설정(Select Security Controls)을 통해 1단계에서

확인된 사항을 보안통제항목으로 변환한다. 조직의 역할, 업무 요구 사항 및 운용 환경을 고려한 보안 통제 기준에 대한 선택적 적용에 대한 가이드라인을 제공한다.

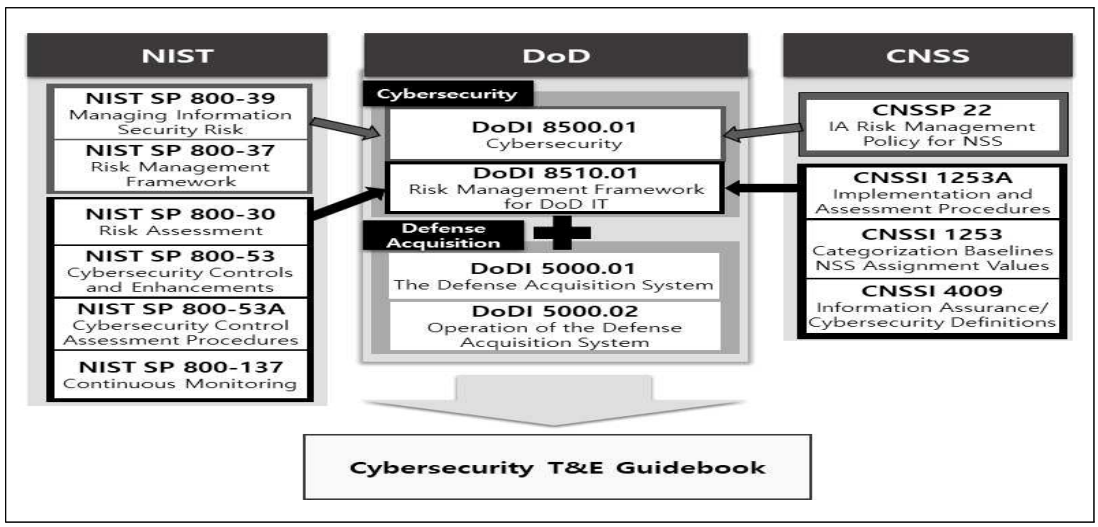
3단계는 보안통제 구현(Implement Security Control)으로 보안통제항목을 시스템 기능을 중심으로 할당하여 구현한다. 사업관리자는 보안 통제항목별 지식 서비스 구현지침 참조 하 구현한다.

4단계는 보안통제항목 평가(Assess Security Controls)로서 3단계에서 구현한 보안통제항목에 대해 목적에 맞게 작동되는지 확인한다. 포괄적인 절차와 보안평가 계획 수립을 위해 기본절차를 명시하고 있다.

5단계 시스템 인가(Authorize System)는 4단계 평가 이후 보완사항 확인 후 시스템 위험을 판단한다. 시스템 위험이 용납되는 수준이면, DATO(Denial of Authorization to Test)로 승인 결정을 내린다.

6단계는 모니터링(Monitor Security Controls) 단계로 시스템 인가 이후 대상 체계의 현황을 지속적으로 모니터링한다. 최대한 신속하게 문제점을 식별하고 대응하기 위해 종합적인 가이드를 제공하는 최종 단계이다[27].

미국의 사이버보안 시험평가는 NIST SP 800 분야 문서와 CNSS(Committee on National Security Systems)를 통합하여 사이버 시험평가 효과를 최적화시켰다. [그림 Ⅱ-2]는 관련 지침의 관계를 나타내고 있으며 지침별 세부 내용은 [표 Ⅱ-1]와 같다[18].



[그림 Ⅱ-2] 미국 국방부 사이버 시험평가 지침

구 분	제 목	내 용
DoDI 5000.02	Operation of the Defense Acquisition System	All the information systems planning to purchase or develop by DoD must be confirmed if information assurance strategy related to standard and structure are in agreement with DoD's policy
DoDI 8510.01	Risk Management Framework for DoD Information technology	Guidelines are provided for RMF for DoD IT and related cyber security policy establishment
DoDI 8500.01	Cybersecurity	General Guidelines are provided for protechtion and defense of DoD IT

[표 Ⅱ-1] 미국 사이버 보안 지침 관련 세부 내용

미군에서는 사이버보안 시험평가 프로세스를 통해 무기체계의 전반적인 사이버 보안을 확인하고 있다. 소요 분석에서부터 생산, 배치 등 전 수명 사이클에 거쳐 지속적으로 수행되며 RMF에 통합되어 수행된다.

DoD에서는 2015. 7. 1. 사이버 보안 테스트 및 평가 가이드북(Cybersecurity Test and Evaluation Guidebook)을 제정한 이후 2020. 2.10. 2.0 버전으로 업데이트 했다[28]. 중요한 변경사항으로 사이버 보안표준, 운영 탄력성 및 시스템 사이버 생존가능성 요구사항에 대한 테스트 고려 사항이 문서 전체에 추가되었다. 이 지침은 모든 DoD 획득 프로그램이나 시스템(국가안보시스템, 무기시스템, 산업제어시스템 등 포함) 또는 언급되지 않는 한 획득수명주기의 단계에 관계없이 독립 실행형 영역이 아니라 전체 프로그램의 Cybersecurity Test and Evaluation(이하 T&E) 전략의 일부로 적용된다. 핵심전략으로 방지, 완화, 복구인데 정의는 아래와 같다.

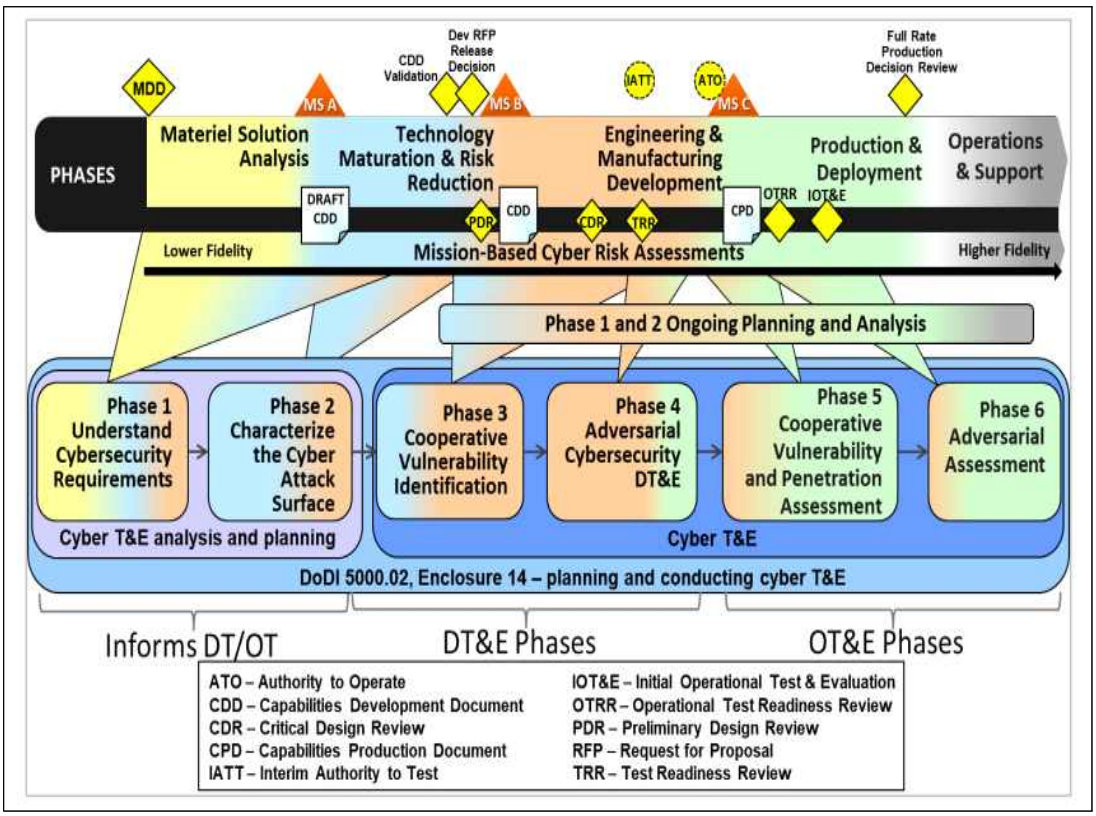
- o 방지(Prevent) : 사이버 위협으로부터 중요한 임무 기능을 보호하는 능력
- o 완화(Mitigate) : 사이버 공격을 감지 및 대응하고 공격에서 생존하고 중요한 임무 및 작업을 완료하기 위한 복원력(Resilience)을 평가하는 능력
- o 복구(Recover) : 사이버 공격으로부터 회복하고 다음 전투를 위한 임무 시스템을 준비하는 회복력(Resilience)

NIST SP 800-37에 정의된 RMF는 DoDI 8510.01에 의해 DoD에 위임되었다. 8510.01에서 RMF 활동을 개발 및 운영 테스트 활동과 통합하며 중복 테스트, 평가, 문서화 및 관련 비용을 줄이기 위해 테스트에 대한 특정 개념과 규칙을 정의

하도록 하고 있다.

효과적인 사이버 보안 T&E의 핵심 기능은 개발 계약자, 개발 테스터 및 운영 테스터가 테스트 분석 및 계획에 조기에 참여하는 것이다. 각 사이버 보안 T&E 단계는 반복적이며 후속단계에 대한 1단계 및 2단계 지속적인 계획 및 분석 활동을 포함한다. 예를 들어 5단계 전에 계약업체와 정부 테스트팀은 1단계와 2단계를 반복하여 요구 사항이 명확하고 간결하고 공격 표면에 대한 업데이트를 이해해야 한다.

[그림 Ⅱ-3]은 DoDI 5000.02 획득 수명 주기에 맞춰 정렬된 사이버보안 T&E 단계를 보여준다.



[그림 Ⅱ-3] Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle

□ 1단계 : 사이버보안 요구사항 이해(Understand Cybersecurity Requirements)

- 계약자 및 정부 사이버 보안 T&E를 수행하기 위한 초기 및 후속 접근 방식과 계획을 개발하기 위한 시스템의 사이버 보안, 시스템 생존 가능성 및 운영 탄력성 요구사항을 조사

□ 2단계 : 사이버 공격표면 식별(Characterize the Cyber Attack Surface)

- 정부 및 계약자 테스트팀은 공격자가 시스템을 악용하는데 사용할 수 있는 취약점과 공격 경로를 식별하고 임무에 대한 영향을 평가하기 위한 계획을 개발

□ 3단계 : 협업을 통한 취약점 식별(Cooperative Vulnerability Identification)

- 목적은 조기에 테스트를 시작하여 사이버 보안 및 운영 탄력성을 확인하고 취약성을 식별하고 필요한 완화 구현을 알리는 것임.

□ 4단계 : 적대적 사이버 보안 개발시험평가(Adversarial Cybersecurity Developmental Test and Evaluation)

- 통합 계약자 및 정부 적대 테스트팀은 중요한 기능을 테스트한다. 사이버 보안 및 운영 탄력성 테스트는 미션 컨텍스트를 사용하여 시스템 개발중에 수행되며 4단계는 계약자 시스템 개발중에 반복된다.

□ 5단계 : 합동 취약점 평가 및 침투 평가(Cooperative Vulnerability and Penetration Assessment)

- 협력 사이버보안 테스트 이벤트의 데이터를 사용하여 운영 컨텍스트에서 시스템의 사이버 보안 및 복원력을 특성화하고 AA(Adverasrial Assessment)를 지원하는 시스템의 정찰을 제공한다. 이 단계는 이전 테스트의 모든 테스트 데이터를 평가하는 것을 포함하며 단일 단계가 아니다.

□ 6단계 : 적대적 평가(Adversarial Assessment)

- 미 사이버사를 통해 인증된 NSA 인증레드팀을 사용하여 DoDIN(국방부 정보망)에 연결된 시스템에 대한 테스트를 수행한다. 이 외에도 중요한 임무기능을 보호하기 위해 시스템, 계층방어 및 방어자의 능력을 평가한다.

2.2. 무기체계 공격 사례 및 관련 연구 동향

2.2.1. 무기체계 보안취약점

무기체계는 국방과 직결되는 분야로, 공개적인 연구에 많은 어려움이 수반되는 분야이기에 보안 취약점에 대한 관련 연구 분야가 많지 않다. 또한 연구가 존재하는 경우, 무기체계의 실질적인 보안취약점에 대한 연구가 아닌, 무기체계에 적용되는 일반적인 구조론적 관점에서 발생하는 보안 취약점에 대한 논의, 무기체계에 대한 사이버 공격에 의해 발생할 수 있는 현실적인 위험성에 대한 연구가 중점적으로 진행되고 있다. 따라서 본 절에서는 무기체계가 가지는 근본적인 보안 취약점을 분석하고, 사이버 공격에서 요구되는 기술을 통해 발생할 수 있는 보안 취약점을 소개한다.[29]

1) 무기체계 보안 취약점 분석

(1) 개발 및 운용 환경상의 문제와 대책

개발 및 운용 환경상의 문제는 대상 무기체계의 개발 및 운용 환경에서 사용하는 운영체제의 보안 취약점으로 인해 해당 무기체계에서 사용하는 소프트웨어가 보안에 취약해지는 경우이다. Windows/Linux, RTOS 등 운영체제 버전 및 커널의 버전에 따른 공개된 취약점 항목이 존재하며, 취약점이 존재하는 버전의 커널 및 운영체제를 사용할 시 취약점을 이용하여 버퍼 오버플로우, 관리자 권한 획득, 원격코드 실행 등의 해당 무기체계 소프트웨어에 치명적인 공격이 가능하다. 따라서 개발 및 운용 환경에 구성된 무기체계 소프트웨어 운영체제와 커널의 공개된 취약점, 익스플루잇, 제로데이 취약점에 대해 지속적으로 확인하여야 하고, 취약점이 발표된 운영체제는 해당 취약점이 해결된 버전으로 업데이트가 반드시 필요하다. 운영체제 취약점이 발표되어 해결된 버전으로의 업데이트가 필요한 경우, 현재 개발중인 무기체계 소프트웨어는 개발 환경과 테스트 베드의 운영체제를 최신 버전으로 업데이트하여야 하고, 개발 완료되어 현재 야전에서 운영중인 무기체계 소프트웨어는 사용중인 운영체제의 버전을 확인하고 취약점이 해

결된 최신 버전으로 운영체제를 업데이트 해야 한다.

소스코드 컴파일러 취약점은 개발 당시 사용한 컴파일러의 취약점이 발견되어 해당 컴파일러를 사용한 바이너리가 문제가 되는 경우이다. 메모리의 중요 정보를 사용 후 초기화하였지만, 컴파일러 최적화 옵션으로 인해 초기화가 되지 않는 경우(CWE-14 Compiler Removal of Code to Clear Buffers), 언어나 OS에서 정의된 특별한 이름을 사용할 경우(CWE-733 Compiler Optimization Removal or Modification of Security-critical Code), Visual Studio의 스택 기반 버퍼 오버런 탐지 기능 추가 등 컴파일러 자체 취약점이 각 버전별로 공개되어 있고, 취약점을 해결한 상위 버전의 컴파일러가 각 프로그램 언어별로 존재한다.

무기체계 소프트웨어 개발자는 개발 시에 가능한 최신 버전의 컴파일러를 사용하여 구 버전에 존재하는 컴파일러 취약점을 최소화하도록 개발하여야 하며, 컴파일러 보안 취약점 발표 시 개발 및 전력화된 무기체계의 소스코드를 컴파일한 컴파일러가 포함되는지 확인하고, 적용 가능한 컴파일러 패치 및 핫픽스를 적용한다. 이미 전력화된 무기체계 소프트웨어에 취약점이 존재하는 구 버전의 컴파일러로 컴파일된 바이너리 운용 시, 취약점이 제거된 최신 버전의 컴파일러로 재컴파일한 패치를 무기체계에 신속히 배포하여 최단 시간에 취약점을 제거하여야 한다. 라이브러리 관련 취약점은 무기체계 소프트웨어 개발 간 사용하는 오픈소스 라이브러리 등 개발에 필요한 라이브러리에 취약점이 포함되어 있는 경우이다.

(2) 취약 함수 및 취약한 버전 API 사용

무기체계 개발 간 개발자가 통상적으로 사용하는 함수에서 취약점이 다수 발생할 수 있다. 특히 strcpy() 등과 같은 메모리 경계를 체크하지 않는 함수로 인해 Heap Overflow/Stack Overflow 등의 문제가 발생 가능하고, User After Free와 같은 메모리를 할당하고 해지한 후 동일한 사이즈의 메모리를 다시 할당할 경우 이전에 할당된 영역을 재사용시 원하지 않는 값을 참조할 수 있으며, Double Free 등의 다양한 문제가 발생될 수 있다. 이러한 개발 간의 문제를 예방하기 위해 메모리 內 데이터를 복사하는 함수는 항상 경계를 체크하는 개선된 함수를 사용하여 코딩하도록 하며, 선언된 변수 사용이나 메모리 할당 등 메모리

를 사용할 경우 반드시 초기화 후에 사용하여야 한다. 위의 취약 함수 사용을 예방 및 수정하기 위해서는 내부적으로 사내 표준 코딩 규칙에 취약 함수 사용 금지 관련 사항을 포함하거나 코드 리뷰시 취약 함수 사용 부분 확인 등 개발 간 개발자가 항상 준수할 수 있는 강제성이 있는 시큐어 코딩 방안을 제시하여야 한다. 또한 시큐어 코딩 취약점 검사 제품 및 개발 후 시니어 개발자 코드 검토 등을 이용하여 무기체계 소프트웨어에 작성된 코드를 검사하여, 취약한 함수 사용 여부 및 버퍼 오버플로우, 힙 참조 등의 문제가 발생할 수 있는 잘못된 코드 작성 여부를 반드시 확인하여야 한다.

(3) 운영체제 명령어 삽입 취약점

운영체제 명령어 삽입은 사용자 입력값이 검증 절차 없이 운영체제 명령어로 실행되어 의도하지 않은 명령어 실행으로 인해 발생할 수 있는 보안 취약점이다. 운영체제 명령어 삽입 취약점을 이용하여 공격자가 악의적인 명령어를 입력함으로써 부적절하게 권한이 변경되거나 시스템 동작에 악영향을 미칠 수 있다. 일례로 내장형 시스템의 경우 CGI 등을 통한 관리자 페이지로 다수의 기기를 통제하는 경우가 있다.이 때 시스템을 관리하기 위해 사용자 입력을 받아 운영체제 명령어의 인자로 주는 경우가 있는데, 시스템 명령어 실행 인수로 외부 입력값을 사용할 경우 공격자가 원하는 명령어를 실행할 수 있다. 외부 입력이 시스템 명령어 실행 인수로 사용될 경우, 미리 적절한 후보 명령어 리스트를 만들고 그 중에서 선택하게 하거나, 예외처리 후 사용해야 하며 명령어 실행에 사용되는 특수문자를 필터링 처리하도록 한다.

(4) 중요 정보 하드 코딩

중요한 정보의 하드 코딩으로 인한 정보 노출은 개발자가 작성한 코드 내부에 중요정보(계정, 비밀번호, 암복호화 키 등)가 하드 코딩되어 있는 경우, 프로그램 소스가 노출되었을 때 핵심정보도 동시에 노출되는 취약점을 가진다. 또한 실행 파일 역공학(Reverse Engineering)을 통해 해당 정보를 추출하면 공격자가 추출 데이터 복호화 등의 공격 시도가 가능하다. 따라서 중요 정보는 소스 코드 내 하드코딩 하지 않아야 하며, 외부에 저장할 때는 암호화하여 저장하여야 한다.

또한 중요 정보를 저장하는 파일은 정보가 포함된 파일임을 파일의 이름만으로 쉽게 유추할 수 없도록 사용하여야 한다.

(5) 중요 데이터 평문 통신

중요한 데이터의 평문 통신은 보안 관련 민감한 데이터를 평문 통신 채널을 통해 송수신할 경우, 공격자가 통신 채널 중간에서 오고가는 데이터 패킷을 스니핑하고 분석하여 민감한 데이터를 획득할 수 있는 사항이다. 보안에 민감한 중요 정보는 전송 전 반드시 암호화하는 코드를 삽입하여야 하며, 통신 채널에서 민감한 정보를 전송하는 코드 작성시에는 OpenSSL 등의 오픈소스 라이브러리 등을 활용하여 반드시 통신 채널을 암호화하여 전송하여야 한다. 웹 시스템은 HTTP 대신 HTTPS와 같은 보안 채널을 사용해야 하며, 브라우저 쿠키에 중요 데이터를 저장하는 경우 쿠키 객체에 보안 속성을 설정하여 중요 정보 노출을 방지하여야 한다.

2.2.2. 무기체계 관련 연구 동향

1) 국내 무기체계 관련 연구 동향

무기체계 사이버 보안과 관련하여 국내 논문이 많지 않다. '첨단 무기체계 획득 운용 시 사이버보안 강화방안 연구(2019. 6. 7, 차성용, 고려대 박사학위논문)'에서는 무기체계 구매시 사이버보안 평가 프로세스와 무기체계 운용유지 단계 사이버 보안강화 방안을 제안하였다. 무기체계 구매시 위협식별, 보안통제항목 선택, 국제표준 항목으로 전환, RFP 평가기준 정립, 제안서 평가, 기능요구사항 검증, 위험평가 및 운용시험평가를 거쳐 선정하는 방안을 제안하였다. 또한 무기체계 운용유지 단계에서 공급망 위협을 해소하고 주요 부품의 추적성 향상을 위해 블록체인 적용 방안을 제안하였다.

'안전한 무기체계 소프트웨어를 위한 취약점 분석 기법에 관한 연구(2018.12월, 김종복, 배재대 박사학위논문)'에서는 방사청 지침인 '무기체계 소프트웨어 개발 및 관리 매뉴얼'에 있는 개발 절차, 방법론 및 개발 단계별 산출물 위주로 작성된 보안약점 진단 기준이 명확하지 않아 이러한 문제를 해결하기 위해 어플리케이션의 위험도 평가를 반영하여 안전한 개발과 관리를 할 수 있는 취약점 탐지기법이 제한되었다.

'항공무기체계 소프트웨어 사이버공격에 대한 작전영향성평가 방안(2021. 2월, 홍병진, 아주대 박사학위논문)'에서는 항공무기체계 소프트웨어 사이버공격에 대한 작전영향성을 평가하는 방안을 제안하였다. 작전영향성평가는 항공무기체계 소프트웨어에 대한 사이버공격을 무결성 검증과 실행코드 분석을 통하여 탐지하고, 세부적인 공격코드의 기능과 영향을 받는 시스템을 분석하여 항공작전에 미치는 영향을 평가하는 것이다. 임무영향도 판단, 사이버 공격에 대한 지휘결심체계 지원과정, 작전영향성평가 방안 적용 효과 및 사이버전 전투평가를 포함한 통합작전수행체계에 대해 제안하였다.

'사이버전 대비차원의 국방정보보호관리체계 연구(2012. 6월, 최광복, 수원대 박사학위논문)'에서는 국방정보보호관리체계 수립을 위한 접근 방법과 구축 방안에 대해 제안하였다. ISMS에 대한 국방분야 적용 가능성, 구축 기본개념과 현행 부대 보안활동과 정보보호관리체계 비교, 위험관리 및 적용 결과에 대해 제시하였다.

적용 결과 기존의 보안 점검방법으로 알 수 없었던 부대의 현재 보안수준을 정량적으로 측정할 수 있으며 부대의 정보보호관리를 보다 효과적이고 체계적으로 수행 할 수 있어 도입이 필요하다고 제안하였다.

2) 해외 무기체계 관련 연구 동향

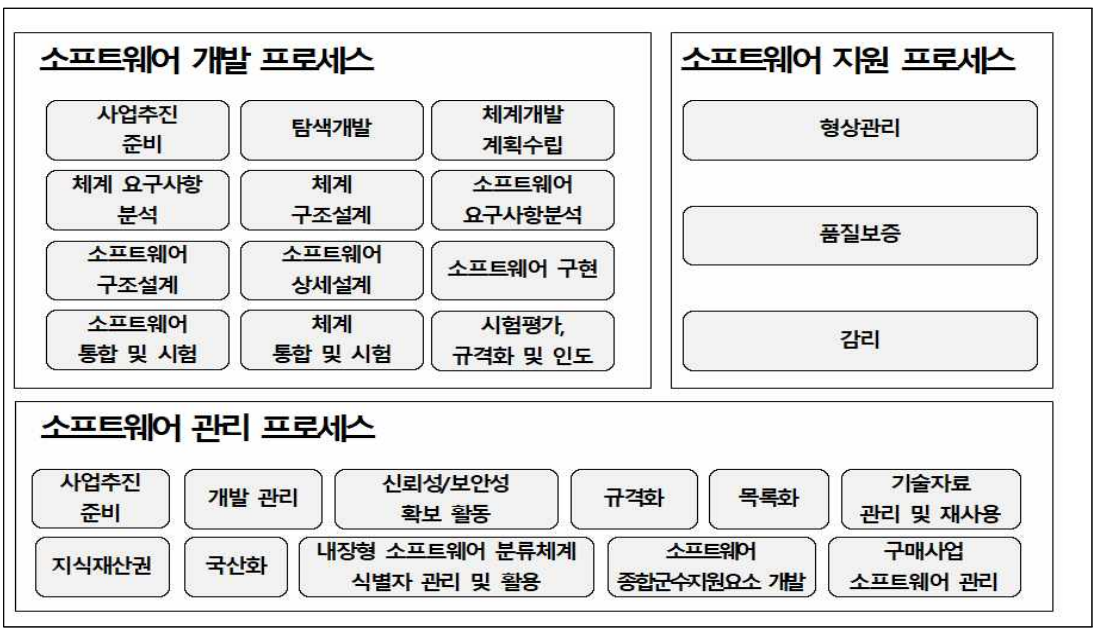
해외 무기체계 논문도 거의 찾을 수가 없다. 미공군의 AIR UNIVERSITY에서 S.ANDREW BAILEY 소령이 작성한 'Beyond the Barrier: Cyber Defense for C2ISR Weapon systems' 석사학위 논문에서는 미국의 무기체계가 사이버위협에 노출되어 있으며 조종사, 유지보수 인원 등이 무기체계의 취약성을 인식해야 하며, 특히 이러한 무기체계 취약점에 대해 비행훈련 과정에 포함하여 사이버 위협 훈련을 제공해야 한다고 제안한다. 또한 무기체계 시스템 방어를 위해 Mission Defence Teams(MDT) 구성 시 통합 계약과 훈련의 표준화가 필요하며 이미 배치된 자산에 대한 소프트 업그레이드와 이를 사용할 수 있는 MDT 툴킷이 배포되어야 한다고 제안한다. 또한 침임탐지시스템을 설치하고 시스템내에 존재하는 취약성을 억제하기 위한 격리방안을 제시하였다.

Ⅲ. 무기체계 사이버 보안 실태

3.1. 무기체계 사이버 보안 수행체계

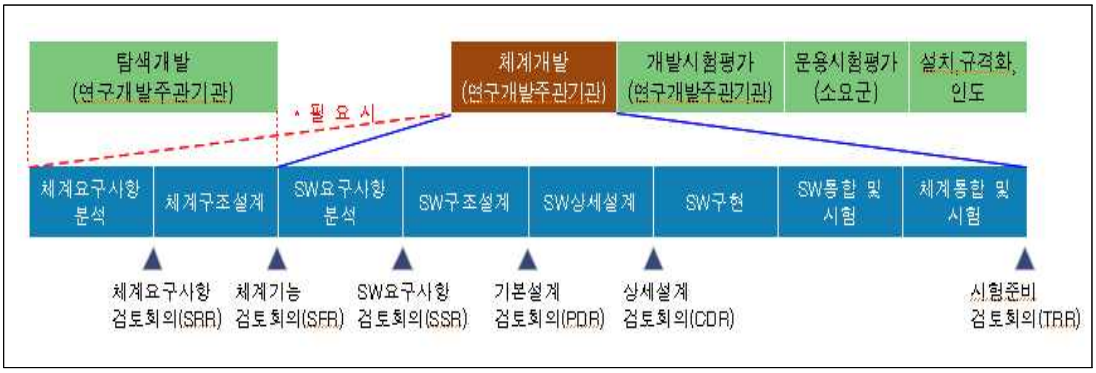
방사청에서는 방위력개선사업 획득하는 소프트웨어에 대해 체계적 개발과 관리를 위해 프로세스 및 산출물 작성표준 등에 대해서는 '무기체계 소프트웨어 개발 및 관리매뉴얼(2020. 2.13)'을 적용하고 있다. 국방아키텍처 프레임워크(MND-AF)에 의해 적용 대상은 전장관리체계 및 전장관리체계와 상호 연동요소가 있는 부분을 적용하고 있다.

무기체계 소프트웨어의 획득 절차는 실제 활용하기 위한 소프트웨어를 정의하고, 요구사항에 따라 실제 구현 및 평가를 통해 현장에서 활용할 수 있는 소프트웨어를 개발하는 소프트웨어 개발 프로세스, 개발한 소프트웨어에 대한 형상관리 및 품질을 보증하고 전반적인 관리감독을 수행하는 소프트웨어 지원 프로세스, 개발된 소프트웨어에 대한 유지보수 및 운영에 대한 전반적 관리 및 문서적 정리, 활용에 대한 업무를 수행하는 소프트웨어 관리 프로세스로, 아래의 [그림 Ⅲ-1]과 같이 세 가지 절차로 구성된다.



[그림 Ⅲ-1] 국방분야 소프트웨어 관리 프로세스

무기체계 소프트웨어 개발 절차는 체계요구사항 사업추진 준비→탐색개발→체계개발 계획 수립→분석→체계구조 설계→SW요구사항 분석→SW구조설계→SW상세설계→SW구현→SW통합 및 시험 단계를 거치며 세부 내용은 [그림 Ⅲ-2]와 같으며, 각 프로세스에 대한 상세한 진행 절차 및 산출 결과는 [표 Ⅲ-1]과 같이 나열할 수 있다.



[그림 Ⅲ-2] 무기체계 소프트웨어 획득 프로세스

프로세스		세부 프로세스	산출물
개발 준비		개발계획 작성	• 탐색/체계개발실행계획서
체계 개발	체계 요구사항분석	체계/요구사항 정의 (소요군 운용요구에 의거)	• 체계요구사항명세서 • 소프트웨어개발계획서
		체계/요구사항 검토	
	체계 구조설계	체계 구조설계	• 체계설계기술서
		체계 구조설계 검토	
	소프트웨어 요구사항 분석	소프트웨어 요구사항 정의	• 소프트웨어요구사항명세서
		소프트웨어 요구사항 검토	
	소프트웨어 구조설계	소프트웨어 구조 정의 및 설계	• (개략)소프트웨어설계기술서 • (개략)인터페이스설계기술서 ((개략)소프트웨어설계기술서에 포함 가능) • (개략)데이터베이스설계기술서 ((개략)소프트웨어설계기술서에 포함 가능)
		인터페이스 설계	
		데이터베이스 설계	
		소프트웨어 구조설계 검토	
	소프트웨어 상세설계	소프트웨어 구성요소 상세설계	• (상세)소프트웨어설계기술서 • (상세)인터페이스설계기술서 ((상세)소프트웨어설계기술서에 포함 가능) • (상세)데이터베이스설계기술서 ((상세)소프트웨어설계기술서에 포함 가능) • 인터페이스통제문서 • 소프트웨어단위시험계획 • 소프트웨어통합시험계획서(초안)
		인터페이스 상세설계	
		데이터베이스 상세설계	
		소프트웨어 상세설계 검토	
		소프트웨어 통합시험 계획 수립	

프로세스		세부 프로세스	산출물
	소프트웨어 구현	단위 소프트웨어 구현 및 데이터베이스 개발	• 소스코드/실행 프로그램 코드(라이브러리/오브젝트코드 포함) • 소프트웨어단위시험결과 • 소프트웨어통합시험계획서 • 소프트웨어통합시험절차서
		단위 소프트웨어 및 데이터베이스 시험 준비	
		단위 소프트웨어 시험	
		소프트웨어 코드 및 단위시험 결과 검토	
		소프트웨어 통합시험계획서 갱신 및 시험절차서 개발	
	소프트웨어 통합 및 시험	소프트웨어 통합 및 시험	• 소프트웨어통합시험결과서 • 사용자/관리자 문서(초안) - 사용자지침서 - 체계운영자지침서 - 소프트웨어버전기술서 (소프트웨어산출물명세서에 포함 가능) - 소프트웨어산출물명세서 • 체계통합시험계획서 • 체계통합시험절차서
		소프트웨어 통합결과 검토	
		사용자/관리자 문서 개발	
		체계통합시험계획서 및 시험절차서 개발	
	체계통합 및 시험	체계 통합 및 시험	• 체계통합시험결과서 • 소프트웨어설치계획서 • 소프트웨어전이계획서 • 소프트웨어설치절차서 (소프트웨어산출물명세서에 포함 가능) • 소프트웨어목록명세서 • 개발시험평가계획서(안) • 개발시험평가절차서
		체계 통합결과 검토	
		소프트웨어 설치계획 작성	
		개발시험평가계획서(안) 및 시험절차 개발	
시험평가, 규격화 및 인도	개발시험평가	개발시험평가 환경 구성 및 시험평가	• 개발시험평가결과보고서 • 운용시험평가지원계획서 • 사용자/관리자 문서
		개발시험평가 결과 검토	
		운용시험평가지원 계획 작성	
	운용시험평가	운용시험평가 지원	• 운용시험평가지원결과서
	소프트웨어설치	소프트웨어 설치 수행	• 소프트웨어설치결과서
	규격화	소프트웨어 국방규격화	• 규격화 기술자료
	인도	소프트웨어 산출물 인도 및 발주자 지원	

[표 Ⅲ-1] 무기체계 소프트웨어 개발 상세 프로세스

국방부 주관 2013년부터 보안성 검증 일부에 대한 신뢰성 시험이 실시되기 전까지 무기체계 보안은 무시되었다. 하지만 2017년 6월 기무사에서 무기체계 SW 보안성검증 필요성을 제안하여 국방부에서 국방전력발전업무훈령에 반영되어 방사청에서 소프트웨어 신뢰성 및 보안성 시험을 시행하고 있다[30].

소프트웨어 신뢰성 시험은 SW가 동작할 수 있는 다양한 경우의 수를 확인함으로써 SW가 일으킬 수 있는 결함을 식별(사전 제거)하는 시험을 의미하며, 연구개발, 핵심기술(시험개발), 핵심SW(시험개발), ACTD, 부품국산화(핵심부품)를 대상으

로 진행한다. 소프트웨어 신뢰성 시험은 정적 시험과 동적 시험으로 다시 한번 구분한다. 정적시험은 코딩규칙(MISRA-C, MISRA-C++, JSF++, Java, C# 등), 취약점(CWE-658, 659, 660), 소스코드 메트릭 등과 같이 SW를 실행하지 않은 상태에서 잠재적인 결함을 검출하는 시험을 의미한다. 동적 시험은 위험도 등급 선정 후, Statement Coverage, Branch Coverage, MC/DC Coverage 측정과 같이 SW를 실제 하드웨어(Target)에 탑재한 상태에서 SW통합시험절차서에 기술된 시험절차에 따라 요구사항 기반으로 SW 코드 실행률을 점검하는 시험을 의미한다. 소프트웨어 보안성 시험은 해킹 등 사이버공격의 원인인 보안약점을 개발단계에서 사전 제거, 행안부의 'SW개발보안 가이드'에 따른 설계단계 및 구현단계에서의 보안 설계 및 취약점 제거 기준에 따른 개발여부 확인을 수행한다.

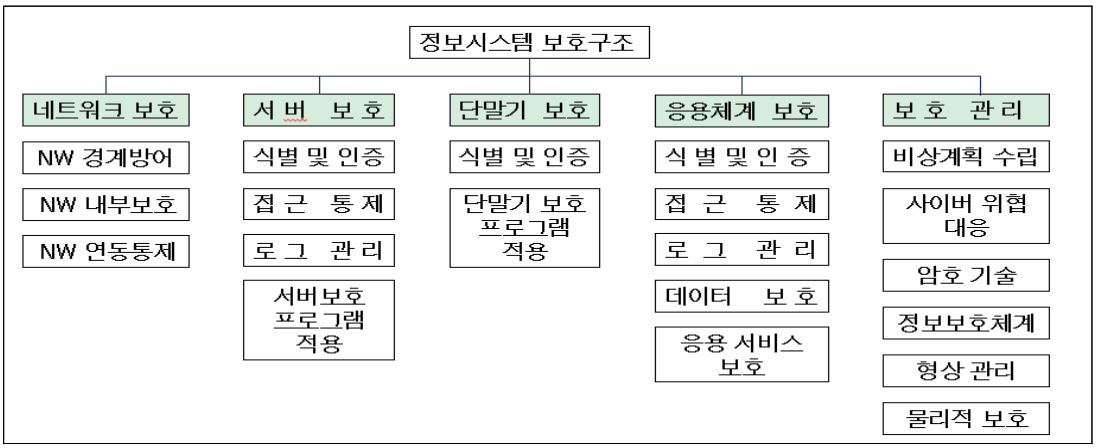
3.2. 기존 사이버보안 수행체계의 한계와 문제점

미군에서는 무기체계 초기단계에서 체계적으로 사이버 보안 시험평가를 진행하고 있지만 한국군은 국내에서는 무기체계 획득 절차에 따른 사이버 보안 절차의 연계성이 부족하여 무기체계 사이버보안 적용이 미흡하다.

우리나라의 무기체계 보안보증 정책의 시작은 2016년 개정된 무기체계 개발 및 관리매뉴얼이다. 전장관리체계가 대상이며 행정안전부 시큐어코딩 가이드를 준수하고 있다. 전체 개발 단계가 아니라 소스 코드의 구현단계로 제한되어 있기 때문에 개발 단계에서 발생 할 수 있는 보안 취약점을 발견할 수 없는 구조이다.

한국에서는 뒤늦게 2017년부터 국방전력발전업무훈령 內 국방사이버안보훈령을 준수하도록 포함시켰다. 국방사이버안보훈령에 따라 무기체계의 기능에 적합한 보안통제항목을 선정하고, 보안통제항목을 국방정보시스템 보호대책서에 반영하도록 규정하고 있다[26].

국방사이버안보훈령은 국방정보시스템 보호구조는 [그림 Ⅲ-3]과 같이 네트워크 보호, 서버 보호, 단말 보호, 응용체계 보호, 보호관리 등 5개 분야로 구성되어 있으며 모두 분야에 대해 요구 수준을 충족해야 한다.[23].



[그림 Ⅲ-3] 국방정보시스템 보호구조

軍의 무기체계 소프트웨어의 경우 방위사업청에서 방위력개선사업으로 획득되는 소프트웨어의 체계적인 개발 및 관리를 위해 방위사업청 '무기체계 소프트웨어 개발 및 관리 매뉴얼' 및 방위사업청 '무기체계 소프트웨어 개발 지원에 관한

규정'에 등에 명시되어 있다[31]. 무기체계 소프트웨어 개발 지원에 관한 규정에 의하면 SW기술지원기관 부서장은 기술지원 요청을 받는 경우 개발된 소프트웨어의 신뢰성 시험결과를 확인하며 전장정보관리체계의 경우에는 추가로 보안성 시험 결과를 확인한다. 신뢰성·보안성 시험을 하지만 보안 요구사항을 충족 여부 확인에 대한 구체적인 방법이 없으며, 행정안전부의 '소프트웨어 개발보안 가이드'를 준수하는 것은 전장관리정보체계만 적용하고 있다.

방사청 '무기체계 내장형 소프트웨어 획득 및 관리 지침'의 경우 2008. 1.24 제정된 이후 현재까지 개정되지 않고 있다. 품질보증에 대한 내용은 포함되어 있으나 보안성 시험과 관련된 부분은 없는 상태이다. 또한 각 기관별 업무분장에서도 방위사업청, 국과연, 기품원만 명시되어 있다. 무기체계 내장형 SW에 대해 조정 및 확인 감독하는 기관에 대해 세부적으로 포함할 필요가 있으며, 국방사이버안보훈령과 같이 내장형 무기체계에 적합한 보호기준 및 보호 요구사항이 수립되어야 할 것이다. 또한 주기적으로 지침에 대한 최신화가 필요하다.

무기체계 획득업무가 2006년에 방사청 이관 이후 방사청에서는 획득정책/제도 위주로 무기체계 소프트웨어 발전 전략을 추진했다. 부작용으로 무기체계 수명주기에 다른 단계별 종합적인 무기체계 소프트웨어 관리정책/제도가 정착되지 못하고 전력화 전·후를 구분하게 되어 컨트롤타워 모호하다. 이에 따라 앞서 지적한 무기체계 수명주기에 따른 무기체계 소프트웨어 보안업무는 고려 대상이 되지 못했고, 각 기관별 무기체계 보안 관리정책이 미흡하게 되었다.

무기체계 전력화 이후 소요군에서 소프트웨어 관리업무를 인계받게 되어 체계적인 관리가 미흡하다. 무기체계는 하드웨어 위주의 종합군수지원를 지원하고 있어 소프트웨어에 대한 정비개념이 미흡하다. 특히, 소프트웨어 보안성 결함에 대해 운용단계에서 점검하거나 업데이트 개념이 전혀 없다. 소프트웨어 결함시 품질보증 절차로 하자보증 처리를 통해 보완중에 있으나, 전력화 이후 변경된 소프트웨어에 대한 보안성 재검증 절차가 없기 때문에 도입 이후 추가된 소프트웨어 보안성 결함에 대한 확인은 제한된다[17].

무기체계 소프트웨어는 일반적으로 구매하는 정보화 영역의 소프트웨어가 아니기 때문에 관리 부서가 다르고 일반적인 도입 소프트웨어와 구별되어 관리된다. 무기체계 소프트웨어 전력화 이전 및 이후로 나누어 주관 기관이 다르며 전

력화 이후 지속적인 관리가 어려운 실정이다.

무기체계 소프트웨어 결함 및 취약점 제거를 위해 신뢰성과 보안성 시험을 거치게 된다. 신뢰성 시험 중에서 취약점 점검 시험 항목은 C, C++, Java로 개발된 소프트웨어에서 결함 유발 가능한 취약점 목록을 정의한 CWE 658, CEW 659, CWE 660의 취약점을 점검하는 것이다.

보안성 시험은 행정안전부 소프트웨어 개발보안 가이드를 준수하여 내재되어 있는 소프트웨어 보안 약점을 제거하는 것이다. 소프트웨어 보안성 시험은 국정원 CC 인증을 받은 도구로 상기 가이드라인에 대한 준수 여부를 점검 후 판단하게 된다.

하지만 행정안전부 소프트웨어 개발보안 가이드는 개발 배경이 전자정부 소프트웨어에 해당하는 웹 어플리케이션을 대상으로 하고 있다. 무기체계 소프트웨어의 특성을 미반영하고 있어 무기체계 소프트웨어 분야에 적용하는 것은 부적절하다. 무기체계에 따라 보안 취약점이 다르기 때문에 무기체계 소프트웨어 특성에 부합되는 보안 취약점 목록을 사전에 선정 후 탐지하는 것이 필요하다. 또한 무기체계 소프트웨어 취약점 제거를 위해 개발 단계에서부터 시큐어 코딩 적용이 필요하지만 현재 무기체계 소프트웨어는 의무화 적용이 되지 않고 있다[24].

도입 예정인 무기체계 소프트웨어 통합 및 시험 단계에서 소프트웨어 개발 언어 사용간 논리적 오류 문제 및 설계 구현간 개발자 실수에 의한 소프트웨어 보안 약점을 줄이기 위한 활동이 바로 시큐어 코딩이다.

무기체계 소프트웨어 보안성 시험 및 검증제도는 한계가 있다. 방사청은 소프트웨어 신뢰성 시험 및 보안성 시험 제도가 있으나 시행 시기인 2011년 이후 전력화된 무기체계에 적용중에 있고, 소프트웨어 보안성 시험 대상은 전장관리정보만 해당된다. 특히 개발시험 이후 소프트웨어 변경사항은 연구개발 주관기관 자체 시험 실시 후 결과만 확인하고 있어 실질적인 보안성 검증이 불가하다. 특히 '국방정보보안시스템 업무훈령'을 근거로 무기체계 소프트웨어 안정성 검증 시행을 의무화 하였지만 보안시스템이 설치되고 국방망과 비밀을 소통하는 무기체계 소프트웨어로 한정하고 있으며, 안전성 검증은 각급 부대의 장이 신청하지만, 실제 신청한 경우는 거의 없다[32].

Ⅳ. 무기체계 사이버 보안 강화 방안

4.1. 무기체계 사이버 보안 강화방안 요약

무기체계는 사이버 공격에 노출되는 경우, 사상자가 발생할 수 있다는 점에서 매우 민감한 영역이며 나아가 국가의 국방에 큰 영향을 끼칠 수 있는 분야이다. 따라서 무기체계는 최우선적으로 항상 원하는 상황에 바로 사용할 수 있어야 한다는 가용성이 가장 높은 우선순위를 가진다. 문제는 가용성을 확보하기 위해 무결성과 기밀성에 대한 가치가 상대적으로 낮게 평가될 수밖에 없다는 점이다. 무기체계의 무결성은 시스템이 무기 활용에 대해 원래의 목적에 따른 작동이 진행될 수 있음을 의미하며, 기밀성은 무기가 인가된 사용자에 의해 활용되고 있음을 의미하기에 두 요소 모두 중요하다. 하지만 軍의 무기체계는 그 중요성에 의해 외부와 차단된 환경에서 운용되며, 제한된 사이버 보안 전문인력에 의한 무기체계 보안 업무가 수행될 수 밖에 없다.

이와 같은 문제는 軍 내부적 측면에서의 방안 도출만이 아닌 국가적, 방위산업적 측면에서의 방안이 요구된다. 현재 무기체계는 보안취약점과 같이 무기체계에 문제를 발생시킬 수 있는 요소의 제거 및 관리까지 일반적으로 軍에 의해 관리되고 있다. 하지만 軍이라는 한정된 영역에서 사이버보안 전문인력은 제한되어 있으며, 사이버공격을 시도하는 공격자에 비해 절대적으로 인원 수가 적을 수밖에 없다. 이는 무기체계에 대한 신뢰성을 떨어뜨릴 뿐만 아니라 무기체계의 가용성을 훼손하여 본래의 목적을 수행하지 못하도록 하는 최악의 가능성으로 이어질 수 있다.

국방력으로 자신의 위치를 공고히 자리잡고 있는 미국의 경우, 무기체계에서 발생하는 보안 취약점에 대해 기밀을 제외한 일부을 외부에 공개함으로서 외부 전문가의 자문을 받아 제거하거나, 軍의 내부환경 일부를 모방하여 재현할 수 있는 사이버 훈련모델을 민간업체와 협력하여 진행함으로써 인재를 양성하는데 있어 개방적인 행보를 보이고 있다. 이는 무기체계 관련 잘못된 유출에 따라 피해가 발생할 수 있다는 단점이 존재하나, 동시에 현재 가지고 있는 보안 취약점에

대해 적극적으로 대처함으로써 사이버 공격에 따른 피해 가능성을 최대한 낮추는 방안으로 무기체계 보안산업이라는 영역을 육성하여 보다 강력한 무기체계 사이버 보안영역을 구축하는데 이바지하고 있다.

본 논문에서는 현재의 폐쇄적인 軍의 무기체계 환경에서 보안성을 강화하기 위해 무기체계 보안취약점 식별 및 관리방안, 방산업체 보안관리 강화 방안, 무기체계 전문인력 양성, 무기체계 악성코드 대응방안 및 ISMS-W 제안 등 총 5개 항목으로 구분하여 무기체계 사이버 보안 정책을 제안한다.

1. 무기체계 보안취약점 식별 방안
• 무기체계 보안 관련 지침 및 제도 정비 • 무기체계 보안 전담기관 지정 운용 • 국방 버그바운티 제도 도입 • 무기체계 보안취약점 통합 데이터베이스 구축 및 운용 • 국제적 차원의 무기체계 보안취약점 관리 및 공유
2. 방산업체 보안관리 강화 방안
• 방산업체 보안관리 개선 • 공급망 보안관리체계 수립
3. 무기체계 전문인력 양성
• 무기체계 보안 전문 인력 양성 • 무기체계 보안 교육기관 지정 및 운용
4. 무기체계 악성코드 대응 방안
• 무기체계 전용 바이러스 백신 운용 • 무기체계 사이버 보안 테스트베드 구축 및 운용
5. 무기체계 사이버 보안 강화를 위한 기존 제도 융합 방안
• 기반시설 취약점 분석평가 기준 및 ISMS-P를 적용한 무기체계에 특화된 (Weapon system) 제안

[표 Ⅳ-1] 무기체계 사이버 보안정책 제안

본 논문에서 설계한 무기체계 보안영역의 상세한 내용은 아래와 같이 정리할 수 있다.

1) 무기체계 보안취약점 식별 및 관리 방안

무기체계 운용간 발생될 수 있는 무기체계 관련 지침을 재정비하여 무기체계 보안 강화하고, 무기체계 장비 도입 시 단계별 보안정책을 수립한다. 또한 무기체계만 전담기관 지정을 통해 무기체계 사이버 인증 제도 시행 및 신뢰성 강화한다. 그리고 사이버보안에 취약한 무기체계에 버그바운티 제도 적용을 통해 보안취약점을 선재적으로 해소할 수 있다. 또한 민간영역의 우수 전문인력에 의한 무기체계 취약점 점검을 통해 잠재적 무기취약점을 제거하며 향후 해커들에게 금전적 지원을 통해 국방 사이버 인력으로 양성화 할 수 있을 것이다.

무기체계 보안취약점 통합 데이터베이스 구축 및 운용을 통해 무기체계 정비 및 도입부서에서 독립적으로 관리중인 무기체계에 대해 통합 관리함으로써 무기체계별 효과적인 보안취약점 제거가 가능하며 보안이력 관리를 통해 체계적인 취약점 관리가 가능 할 것이다.

또한 통합데이터베이스를 내부 전용 온라인으로 구축하여 무기체계 운용 인력에 의해 최신 보안취약점 확인 및 업데이트를 통해 보안약점 해소가 가능하다. 단, 모든 인원들에게 무기체계 보안 취약점 공유 시 해킹에 악용될 우려가 있어 통합데이터 베이스 접근은 체계별 실무자와 접속 가능하며, 전체적인 현황에 대해서는 사이버사 및 군사안보지원사령부 등 보안전문기관에서 확인 및 통제 필요하다.

마지막으로 국제적 차원의 무기체계 보안취약점 관리 및 공유를 통해 해외 무기체계 도입시 계약 단계에서부터 무기체계 보안취약점 발생시 즉각 공유 및 유지보수 우선 수행을 통해 구매 후 무기체계 보안 업데이트를 실시하지 않아 보안취약한 상태에서 운용되지 않도록 선제적으로 조치가 가능할 것이다.

무기체계 보안 관제에 대해 개별적으로 실시하는 것이 아니라 사이버사 등 통합 관제체계 구축이 필요하며, 외국군 CERT와 교류 협력을 통해 북한 등 국가를 배후로 하는 해커집단에 의한 무기체계 해킹 관련 기술 공유 및 협력체계 구축을 통해 무기체계 보안 강화가 요구된다.

2) 방산업체 보안관리 강화 방안

방산업체에 대한 보안관리 기준을 수립하여 무기체계 정비 및 유지보수 단계에서 발생할 수 있는 무기체계 위협 요인 제거하며, 업체 출입인원에 의한 무기체계 접근에 대한 보안 통제 강화한다.

그리고 미군처럼 방산업체 공급망 인증 제도 수립을 통해 공급망 단계에서 유입될 수 있는 보안취약점을 선제적으로 수립하고, 軍의 보안정책에 적합한 무기체계가 납품될 수 있도록 유도하며 무기체계에 안전한 제품 납품 여부에 대한 절차 수립 및 강구한다.

3) 무기체계 전문인력 양성

무기체계의 보안취약점을 진단할 수 있는 사이버 보안 전문 인력 양성한다. 또한 무기체계 보안 교육기관 지정 및 운용을 해야 한다.

4) 무기체계 악성코드 대응 방안

무기체계에 적합한 전용 바이러스 백신을 구축하여 무기운용간 가용성 보장하며, 무기체계에 적합한 백신 유포체계 구축 및 다양한 바이러스 백신에 의한 무기체계 점검으로 보안위협 제거한다.

무기체계의 가용성 보장을 위한 테스트베드 구축을 통해 운용단계 무기체계 보안위협 선제적 확인 가능하며 실전적 무기체계 보안 테스트가 가능해 레드팀에 의한 보안위협 확인 여건 보장할 것이다.

5) 무기체계 사이버보안 강화를 위한 기존제도 융합방안

무기체계에 적합한 사이버 취약점 분석 및 평가 기준을 정립하여 무기체계에 특화된 점검 기준 및 자동화 점검툴 배포하며, 소프트웨어가 내장된 무기체계에 대한 점검 기준 정립한다.

무기체계별 ISMS 인증 방법을 적용하여 체계별 보안점검 기준에 의해 모든 장비에 대한 보안취약점 점검 후 안정성과 보안성에 대해 인증하는 무기체계 ISMS(가칭 ISMS-W) 시행을 제안한다.

4.2. 무기체계 보안취약점 식별 및 관리 방안

4.2.1. 무기체계 보안 관련 지침 및 제도 정비

1) 무기체계 보안 관련 지침 및 제도 정비 필요성

무기체계 보안 관련 지침 및 제도 개선이 필요하다. 무기체계 중에서 대표적으로 함정용 전투체계를 사례로 설명하겠다. 함정용 전투체계는 당연히 해상이라는 제한된 통신 환경에서 운용된다. 일반적인 무기체계와 동일하게 소프트웨어 업데이트가 제한되며 인터넷 연결이 불가하다는 이유로 외부 침입과 사이버 공격에 안전하다는 인식이 존재했다. 이로인해 과거에는 네트워크 보안장비 및 네트워크 모니터링 시스템의 필요성이 낮았으며, 소프트웨어 업데이트 등 보안에 관련된 다양한 사이버 위험에 노출되어도 크게 문제가 없었기 때문이다.

함정용 전투체계는 체계 간 또는 네트워크 간에서 사이버보안 대책이 부족한 것으로 판단된다. 서버 및 네트워크 장비는 일반적인 무기체계에서와 같이 전투체계에서도 동일하게 사용되며 보호 방안에서도 큰 차이가 없다. 전투체계 특성상 직접적인 외부 사이버 공격보다는 USB 등 저장매체를 통한 악성코드 감염, 내부자에 의한 악의적 공격, 각종 보안 패치를 적기에 하지 못할 때 해킹 공격에 표적이 될 수 있다.

단말은 대부분 사용자가 장비의 운용과 조작을 위해 사용하는 장비로 보안 취약점이 가장 많이 노출되는 장비이다. USB, CD/DVD 저장매체를 장비에 연결하기 용이하며, 프로그램 설치 및 장비 교체 등이 서버에서 보다는 자유롭다. 이러한 단말들은 서버 및 데이터베이스 접속이 가능하기 때문에 해킹 공격을 받게 되면 서버 및 타 장비도 공격을 받을 수 있다. 단말의 기본적인 정보보호는 사용자의 계정 및 비밀번호에 대한 관리이다. 전투체계 및 함정에서는 승선인원이 정해져 있고 특정 인원만 단말을 사용하기 때문에 기본 계정만을 사용하거나 패스워드를 공유해서 사용하는 경우가 많다. 하지만 이런 경우 단말장비의 감염 및 단말장비 간의 악성코드 전파, 내부 인원에 의한 의도적 공격에 쉽게 노출 될 뿐만 아니라 공격을 받은 후 로그 등을 통한 원인 분석에 어려움을 초래한다.

또한 단말은 windows와 같이 사용자가 많이 사용하는 범용 OS를 쓰는 경우가 많은데 전투체계 특성상 실시간 업데이트를 하기 어렵기 때문에 보안 취약성에 쉽게 노출된다[57]. 따라서 폐쇄망 환경에서 보안패치 및 백신 업데이트 방안을 고려해야 한다. 또한 단말이 사용하는 네트워크와 서버에서 사용하는 네트워크 분리, 운용에 필요하지 않은 프로그램 및 파일 자동 삭제 프로그램 설치운용 등의 엄격한 보안 정책이 필요하다.

그리고 내부로부터 발생하는 보안 위험은 조직구성원에 의해 발생하는 보안사고가 대부분으로 이는 사람에 의해 발생하는 특성으로, 보안사고 발생 자체에 대한 감지가 어려운 문제점이 있다. 내부로부터 발생하는 보안 위험은 조직구성원에 의해 발생하는 보안사고가 대부분으로 이는 사람에 의해 발생하는 특성으로, 내부에서 발생하는 융·복합적 보안 위험에 대비하기 위해서는 다차원적인 보안 활동이 필요하다.

軍 내부자에 의한 정보유출 경로는 본인이 직접 유출하는 것이 대부분이기 때문에 기존의 내부정보 유출방지 시스템이 갖고 있는 보안 취약점을 보완할 필요가 있다. 그래서 탐지대상을 유출 대상인 군사기밀이 아닌 유출 당사자인 군 내부자로 변경하고 탐지기법도 시스템에서의 행위기반이나 규칙기반이 아닌 내부자의 감정변화를 기반으로 한 탐지방안이 보다 효율적일 것이다. 이렇게 다양한 경로를 통해 무기체계 보안은 위협을 받고 있다.

2) 무기체계 사이버 보안에 심층 방어전략 도입

무기체계 보안을 위해 심층 방어전략을 적용하는 것이 필요하다. 심층방어의 개념은 침입자가 목표를 달성하는 것을 방해하기 위한 장벽을 제공하면서 그들의 진행 상황을 감시하고 그들을 격퇴하기 위해 사건에 대한 대응을 개발하고 실행하기 위한 군사 전략에서 유래되었다. 사이버보안 패러다임에서 심층 방어는 사이버 침입자의 진행을 방해하도록 설계된 보호 조치와 관련이 있으며, 조직은 침해의 피해를 줄이고 완화하기 위한 목적으로 침입을 탐지하고 대응할 수 있도록 한다.

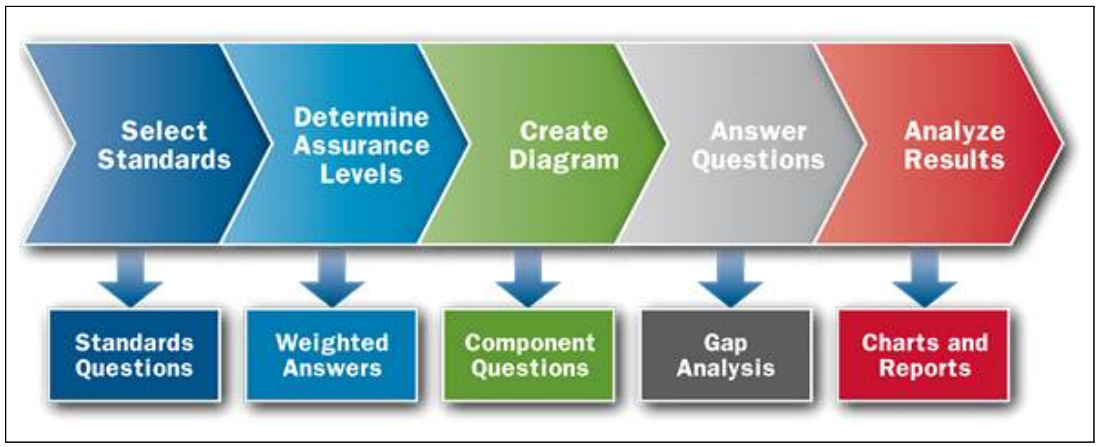
심층방어는 조직이 동등한 위험에 대응하기 위해 특정한 기술을 배치하는 일대일 연습이 아니다. 심층방어는 모든 자산을 보호하기 위해 전체적인 접근 방식

을 사용하면서 상호 연결 및 종속성을 고려하고 조직의 가용 자원을 사용하여 비즈니스의 사이버보안 위험에 대한 노출에 기반한 효과적인 감시 및 보호계층을 제공한다.

미국 산업제어시스템 사이버비상대응팀이 2016년 9월 작성한 보고서에 따르면 산업제어시스템(이하 ICS) 아키텍처의 복잡성으로 인해 아래와 같은 방법으로 시스템내에 오랫동안 탐지되지 않는 지능형 지속위협(APT)이 발생할 수 있다고 소개했다[33].

- o 인터넷에서 인터넷에 연결된 ICS 장치에 직접 공격
- o 인증된 ICS사용자 도용 또는 도용된 원격접속 자격증명을 사용하여 공격
- o 외부 비즈니스 웹 인터페이스에 대해 공격
- o 감염된 모바일 미디어를 시스템 구성요소에 삽입하여 공격
- o 위협 행위자는 피싱 전자메일을 사용하여 기업 사용자 PC 존재

미국 국토안보부 산업제어시스템 사이버 비상대응팀은 보안 상태 개선에 도움을 주는 주제별 전문 지식, 도구 및 서비스를 제공한다. 대표적으로 무료로 운용기관에서 사용할 수 있는 사이버보안 평가 도구(CSET, 이하 CSET)를 제공한다[34]. [그림 Ⅳ-1]은 CSET 평가프로세스를 보여준다.



[그림 Ⅳ-1] CSET 평가 프로세스

이 도구는 통합 네트워크 맵을 사용하여 시스템의 현재 보안 상태를 시각적으로 표시하고 평가를 위한 구성요소 대상을 식별하며 조직에 가장 큰 가치를 제

공하기 위해 사이버보안 보호 매커니즘을 배치할 위치에 대한 지침을 제공한다.

무기체계 사이버 보안 강화를 위해 심층방어 개념을 정립하고 무기체계별 CSET과 같이 정형화된 자체 평가프로세스를 개발하여 심층 방어가 지속 가능하도록 보장해야 한다.

3) 한국군 RMF 적용 방안

RMF는 사이버보안 위험평가 개념에 익숙하지 않은 한국군 특성상 위험우선순위 식별 과정에서 주관적 판단에 따른 모호성과 중복성의 문제 해결을 위해 큰 어려움이 예상된다[32].

한국 국방부는 우리의 보안수준 향상과 한미 연동체계 전반에 대한 RMF 적용 요구에 대비하여 대응계획을 수립하고 있다. 미 전투사령부는 작전능력 향상을 위해 파트너 국가와 함께 상호 연결된 네트워크의 보안을 보장하고 미 국방부는 연결을 승인한다. 우리나라 국방 사이버공간은 악의적 사이버 위협에 대해 더욱 강력한 조치가 필요한 시점으로 파트너 국가와의 연동정책 전반에 대한 평가 및 안전성을 담보할 수 있는가에 대한 평가가 불가피한 상황이다.

현재 한국군과 미군에서 적용되는 국방획득체계 프로세스는 매우 유사하다. 이는 한국이 국방획득체계 프로세스를 구축할 시 미군의 체계를 표준으로 삼아 도입하였기 때문이다. 미군의 RMF는 기존의 국방획득체계 프로세스를 크게 변경하지 않고 RMF 세부 활동을 추가하여 구축한 것으로 평가된다[27]. 그러므로 한국에서 RMF를 적용할 때도 미국 국방획득체계에 적용된 RMF를 우리나라 상황에 맞게 적용하는 것을 고려해 볼 수 있으며 아래와 같은 사항들이 필요하다.

한국군이 미군의 RMF를 효율적으로 수행하기 위해서는 모든 RMF 수행자에게 동일한 관점과 지식, 절차를 공유하도록 해주어야 한다. 이를 위해서는 우선적으로 국방 RMF MKS(Military Knowledge Service) 체계를 구축해야 한다. 국방 RMF MKS는 국방부의 RMF 정책과 지침을 제공하기 위한 각종 지식을 전달하는 수단이다. 이는 국방부의 ICT를 보호하기 위한 가장 적절한 방법, 표준, 절차를 제시하고 지금까지 관행적으로 적용되고 있던 절차에 대한 효과성을 확립하고 체계화시키는데 기여할 것이다. 국방 RMF MKS의 구현 지침은 진화하는 보안목적 및 위험조건에 관한 가장 최신의 국방부 의도를 반영 해야 한다. 국방

RMF MKS가 설치되면 다음과 같은 이점을 제공할 것이다.

A. 한국군에게 RMF를 구현하고 실행하기 위한 지침과 도구를 제공한다.
B. 권위 있는 RMF 지침의 출처와 국방부 RMF정책의 출처 역할을 수행한다.
C. ICT 위험관리 책임이 있는 모든 사람에게 일관성 있는 정보를 제공한다.
D. 보안통제 기준, 개별 보안통제 및 보안통제 구현 지침과 평가 절차에 대한 접근이 편리하다.
E. RMF의 자동 및 비자동 구현을 지원한다.

국방 RMF MKS는 도구, 도표, 절차 도표, 문서 등의 라이브러리를 호스팅 하여 RMF의 실행을 지원해야 한다. 또한 RMF 사용자 커뮤니티는 습득한 교훈, 모범사례, 사이버보안 뉴스 및 이벤트, 기타 사이버보안 관련 정보 리소스를 개발, 공유 및 게시할 수 있는 공동작업 공간이 될 것이다. 향후 한국의 RMF 조직 내에도 구성될 RMF TAG는 국방 RMF MKS의 기능 구성 및 콘텐츠 관리를 담당하며 MKS 콘텐츠의 엔터프라이즈 부분에 대한 자세한 분석 및 제작을 지원하게 될 것이다.

RMF는 무기체계 개발 후 안전을 담보하는 것이 아니다. 무기체계 개발 시부터 최초 요구사항 분석과 설계단계에서의 보안성을 고려하여 개발해야 한다. 또 보안수준은 체계가 수행해야 할 임무의 중요도에 의해서 결정되어야 한다.

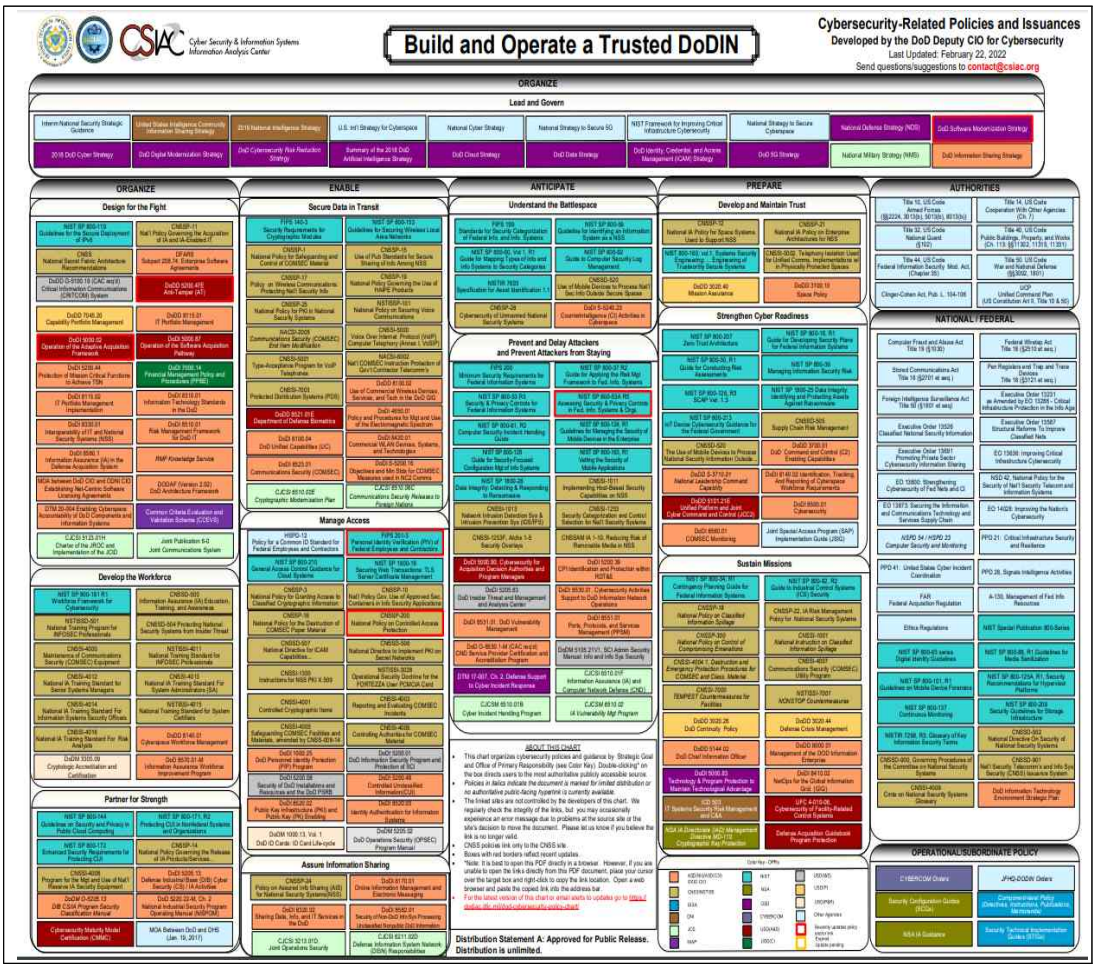
또한 RMF는 절차에 따라 미국 측과 체계 안전성 검증과 통합을 위한 기술적 조치들을 수행할 능력을 확보한 조직으로 구성해야 한다. 해당 실행 조직에 요구되는 인적구성은 수준 높은 컴퓨터 기술 인력으로 미국 측과 연동해야 하기 때문에 언어능력을 갖추는 것이 유리할 것이다. 이러한 인력은 미국 측의 경우처럼 기술 요원으로서 기업과 군을 기술적으로 잘 융합시켜주는 Contractor를 채용하는 것이 바람직할 것이다.

RMF를 원활히 수행하기 위해서는 체계와 보안에 대한 전문가가 필요하다. 해당 전문가는 체계개발의 요구사항 분석단계, Design 및 설계단계, 구현을 위한 SW의 Coding 단계, 운용단계까지를 체계개발 시점부터 판단 예측하여 위협요소를 사전에 제거할 수 있는 능력을 갖춰야 한다.

즉, 체계개발도 하면서 Secure Testing도 해낼 수 있는 고급 SW개발자가 필요한 것이다. 향후 RMF의 원활한 수행을 위해서는 이상의 분야에 대한 지식을 습득하고 현장을 경험한 인원이 필수적으로 확보되어야 할 것이다

4) 무기체계 사이버 보안 영역에 세부 지침 수립

미국 사이버보안 정보시스템 정보분석센터는 DoD의 사이버보안 및 정보기술 관련 정보를 수집 및 분석하여 보급하는 활동을 수행한다[35]. CSIAC 홈페이지에 신뢰할 수 있는 美 국방부 정보 네트워크 구축 및 운영 지침 차트가 [그림 Ⅳ-2]와 같이 게시되어 있다. 일목요연하게 분야별 보안정책이 수립되어 있는데 이와 같이 우리나라에서도 기관별 및 사이버 보안영역별 세부 지침을 수립 및 보완해야 한다.



[그림 Ⅳ-2] 신뢰할 수 있는 美 국방부 정보 네트워크 구축 및 운영 지침

4.2.2. 무기체계 보안 전담기관 지정 운용

무기체계 보안을 강화하기 위해서는 국방부 차원에서 종합적인 컨트롤 타워 설립이 필요하다. 무기체계 도입을 위한 소요 계획단계에서부터 폐기단계에 이르기까지 체계적인 보안관리 절차를 마련이 시급하다. 무기체계 보안전단 기관 부재에 따른 대표적인 문제는 아래와 같다.

1) 무기체계 SW 운용단계 보안관리 부실

무기체계가 전력화된 이후 소프트웨어 관리는 소요를 제기한 각군에서 관리를 하고 있다. 문제는 운용 단계에서는 하드웨어에 대한 정비 및 유지차원에서 관리되고 있기 때문에 SW 보안취약점에 대해 정기 및 수시 점검하는 개념이 없다. 소프트웨어 품질보증 절차에 따라 하자발생 시 문제를 처리하고 있으나, 전력화 이후 업그레이드 되거나 신규 도입된 소프트웨어에 대한 보안성 검증 절차가 없기 때문에 보안 취약점 확인은 제한된다.

무기체계 수명주기에 맞도록 소프트웨어도 관리되어야 한다. 해외 구매장비 및 국내 개발 장비로 구분하여 운용단계에서도 지속적으로 소프트웨어에 대한 보안검증 및 취약점을 확인 할 수 있도록 제도적 절차와 전담기관을 마련하고 확인하는 체계를 구축해야 한다.[17]

2) 방산분야 기술유출

방위산업 기술유출의 유형은 방위사업청에서 국내외 기술유출 사고사례를 바탕으로 '방위산업기술 유출·침해사고 대응 매뉴얼(2020)'을 통해 분류하였다.

구 분	내 용
인력에 의한 기술유출	· 핵심 기술인력이 해외로 이직 또는 해외 창업 · 퇴사자가 경쟁업체에 기술유출 · 외국인 직원이 기술유출
정보통신시스템 사용 부주의에 의한 기술유출	· 이메일, 팩스 무선공유기, P2P 등의 사용 부주의로 기술유출 · 노트북, USB 등을 외부에서 분실
불법 수출에 의한 기술유출	· 국가의 수출 승인 없이 방산물자 및 방위산업기술을 수출
기업합병, 기술이전 시 기술유출	· 정부 승인 또는 허가 없이 합병 또는 기술이전 · 계약 협상 단계에서 기술자료를 공유했으나 계약이 파기되어 기술유출
보안성 검토 미흡에 의한 기술유출	· 외부로 공개되는 자료의 보안성 검토가 미흡하여 기술 공개 · 저장장치, 운용장비 정비 시 보안성 검토가 미흡하여 기술자료 유출
기 타	· 군 기관 등 사칭하여 기술자료 요청 · 도청을 통한 기술유출 · 부도, 폐업 시 기술유출

[표 IV-2] 방위산업 기술유출 유형

방산기술유출의 유형은 [표 Ⅳ-2][36]과 같이 인력에 의한 기술유출, 정보시스템 해킹에 의한 기술유출, 정보시스템 사용 부주의에 의한 기술유출 등이 있다.

3) 무기체계 보안전담 기관 설립

무기체계 도입 관련 軍 내부의 조직이 있고 방산업체 등 외부의 조직이 존재한다. 무기체계 사이버 보안을 위해서는 軍에서의 보안만 강조한다고 해서 지켜질 수 없다. 연구기관, 방산업체 등 통합적인 무기체계 보안대책이 수립 및 이행되어야 할 것이다.

북한의 사이버공격에 대한 대응을 위해 범정부 차원의 무기체계를 위한 보안 컨트롤타워가 설립되어야 한다. 또한 컨트롤타워를 뒷받침할 조직이 있어야 하며 이를 통해 무기체계 보안을 근본적으로 강화할 수 있을 것이다.

4.2.3. 국방 버그바운티 제도 도입

1) 버그 바운티의 개념

버그 바운티는 버그바운티를 운용하는 주체가 보안 취약점을 보고한 인원에게 금전적으로 보상해 주는 것이다. 버그바운티 플랫폼 종류에 따라 [표 Ⅳ-3][37]과 같이 정의 할 수 있다.

종류		정의	사례
자가 소유 플랫폼 사용 버그 바운티 (self-owned bounty program)		버그 바운티 프로그램을 통해 취약점을 파악하고 이를 개선하려는 주체가 직접 버그 바운티 프로그램을 운영하는 플랫폼을 가지고 있는 것	Google Vulnerability Reward Program(VRP), Microsoft Bug Bounty Program
별도 플랫폼 사용 버그 바운티 (bug bounty of third-party owned platform)	one-sided bug bounty platform	보상금의 자본이 플랫폼으로부터 비롯된 것으로, 버그 바운티 운영주체와 참여자는 각각 플랫폼과의 관계만 가지고 있을 뿐인 버그 바운티	Zerodium, SW 취약점 신고포상제(KISA)
	two-sided bug bounty platform	보상금으로 주어지는 자본이 버그 바운티 운영주체에서 비롯되어, 플랫폼은 버그 바운티 운영주체와 참여자 사이의 중개기관으로서의 역할만을 가지는 버그 바운티	Hackerone, Bugcrowd, Safehats, Synack

[표 Ⅳ-3] 플랫폼에 따른 버그 바운티의 종류

2) 미국 DARPA의 Cyber Grand Challenge 사례

미국 DARPA(방위고등연구계획국)에서는 오늘날 버그, 해킹 및 기타 사이버 감염 벡터를 찾고 대응하는 프로세스가 전문 버그 헌터 및 보안 전문가에 의해 수작업으로 수백만 줄의 코드를 검색하여 숨은 의도를 가진 사용자가 이용할 수 있는 취약점을 찾고 수정하며 엄청난 시간을 일하는 문제를 극복하기 위해 결함에 대해 추론하고 패치를 공식화하고 실시간으로 네트워크에 배포할 수 있는 자동 방어 시스템을 만들기 위한 경쟁인 Cyber Grand Challenge(이하 CGC)를 세계 최초로 2016년 8월 4일 개최했다.

세계 최고의 보안 연구원과 해커로 구성된 100개 이상의 팀으로 시작하여 DARPA는 최종 이벤트에서 7개 팀이 서로 경쟁했다. 대회 기간 동안 각 팀의 CRS(Cyber Reasoning System)는 소프트웨어 결함을 자동으로 식별하고 특수 제작된 에어갭 네트워크를 스캔하여 영향을 받는 호스트를 식별했다. 거의 12시간 동안 팀은 시스템이 호스트를 얼마나 효과적으로 보호하고, 네트워크에서 취약점을 검색하고, 소프트웨어의 올바른 기능을 유지했는지에 따라 점수가 매겨졌다. 200만

달러, 100만 달러, 75만 달러의 상금이 상위 3명에게 수여되었다.

CGC는 지금까지 개발된 가장 정교한 자동화 버그 헌팅 시스템 간의 첫 번째 일대일 경쟁이었다. 이 기계는 이전에 분석된 적이 없는 맞춤형 소프트웨어에 숨겨진 일련의 버그가 포함된 특별히 제작된 컴퓨터 테스트베드에서 Capture Flag의 고전적인 사이버 보안 연습을 수행했다. 시스템은 해킹에 취약한 결함이 있는 코드를 평소 몇 개월이 아닌 몇 초 안에 찾아 패치해야 했으며, 상대방이 방어하기 전에 약점을 찾아내야 했다[38].

사람의 개입 없이 취약점을 찾아 수정하는 1세대 자율 컴퓨터 보안 봇 중 하나인 카네기멜런대의 Mayhem은 2016년 8월 DARPA 사이버 그랜드 챌린지에서 우승했다. DARPA의 사이버 그랜드 챌린지(CGC)는 사이버 보안의 최전선에서 새로운 기술인 사이버 추론 시스템(Cyber Reasoning System, 이하 CRS)을 탐구했다. CRS는 일련의 소프트웨어 서비스를 방어하는 완전한 책임을 지는 완전 자율 시스템이다.

사이버 그랜드 챌린지에서 경쟁하는 CRS는 공격 트래픽을 차단하는 방화벽 규칙 자동 개발, 공격자보다 먼저 버그를 찾기 위한 프로그램 분석, 소스 코드에 대한 액세스 없이 컴파일된 프로그램의 취약점 패치를 포함하여 모든 핵심 사이버 보안 영역에서 기술을 시연했습니다. 인간 분석가가 개발하고 테스트하는 데 수 많은 시간이 걸릴 수 있는 소프트웨어 방어를 수십 초 정도의 기계 속도로 배포되었다.

Mayhem은 인간 개발자나 보안 분석가와 다르게 소프트웨어 결함을 확인하고 패치한다. 서비스를 분석할 때 Mayhem은 서비스를 충돌시키거나 잠재적으로 악용할 수 있는 동작을 나타내는 테스트 사례가 있는 경우에만 소프트웨어 결함을 확인한다[39].

ForAllSecure 회사에서 개발한 Mayhem은 2020. 5.11. DoD와 4,500만 달러의 계약을 체결하고 배포되고 있으며 여러 DoD 기관에서 사용 예정이다. 무기 시스템 사이버 보안 결함 탐지를 위해 응용프로그램을 확인하는 Mayhem은 자동으로 테스트 제품군을 구축하고, 고급 퍼징의 결합된 기술을 사용하여 코드 테스트에서 자동화의 강력한 이점을 보여주고 있다[40].

이렇게 미군에서는 국방 영역에서 버그바운티 제도를 통해 기술적으로 확인된

제품을 발굴하고, 세계 최고 수준의 자동화된 무기시스템 보안 취약점 자동진단 툴을 도입하여 잠재되어 있는 지능형 사이버 공격에 대비하고 있다.

3) 무기체계 적용 방안

국방 무기체계에 대한 버그바운티에 대한 거부감은 상당할 것으로 판단된다. 하지만 DoD의 사례처럼 이제는 변화를 두려워 해서는 안된다. 부작용 또한 당연히 있겠지만 이제는 기술의 고도화 발전 추세에 부합되도록 무기체계 분야의 보안 취약점 해소를 위해 버그바운티 제도를 도입해야 할 것이다. 이를 위해서 기밀성이 낮은 체계를 우선적으로 고려해 볼 수 있을 것이다.

DoD에서는 배경조사를 거쳐 검증된 해커들에게만 참가 자격을 부여했다. 발견된 취약점으로 인해 중요한 업무가 마비될 것을 우려해 주요 핵심 시스템과 분리된 시스템을 대상으로 진행되었다. 이를 벤치마킹하여 우리 軍에서도 공개 가능한 무기체계를 선정하여 점검해야 할 것이다. 대표적으로 전장망의 경우 정보시스템 기반으로 구축되어 있으며 실제 운용 데이터가 아닌 가상의 데이터를 사용하도록 한다면 실질적인 점검이 가능할 것이다.

효과적인 무기체계 보안을 위해서는 앞서 미국 GAO의 사례에서처럼 무기체계 진단이 가능하도록 전문인력과 예산을 투입하여 공식적으로 대한민국 무기체계에 대한 사이버 보안 취약점을 전면적으로 진단하고 국회 차원에서 확인 및 조치할 수 있도록 예산을 지원하고 각군의 무기체계에 대해 지속적인 확인과 감독을 통해 선진 무기체계 보안 생태계를 구축해야 할 것이다. 이를 위한 별도의 외부 전문기관의 설립이 필요하다.

또한 일회성 버그바운티 행사를 하는 것이 아니라 매년 지속적으로 시행하여 軍 내부에서 확인하기 어려운 잠재적인 보안취약점을 식별하여 선제적으로 조치하는 것이 필요하다.

4.2.4. 무기체계 보안취약점 통합 데이터베이스 구축 및 운용

1) 국방정보시스템의 보안취약점 관리

국방정보화 사업 예산으로 취득한 IT 자산은 국방정보자원관리시스템을 이용하고 관리 중에 있다. 국방정보자원관리시스템은 위험관리 측면에서는 취약점을 가진 자산을 식별하기에는 입력 내용이 불충분하다. 그래서 위험관리를 지원하기 위한 시스템인 취약점 관리시스템에서 국방정보자원관리시스템의 자산DB를 사용하지 않고 별도의 자산DB를 구축하였다. 이에 따라 자산관리 내용 중복에 따른 자산 불일치 및 자산관리를 위한 추가 자원이 중복 투입되고 있다.

무기체계 취약점은 잘 알려져 있는 일반적인 보안취약점에 해당되는 운영체제 패치 미실시, 구형 소프트웨어 프로그램 및 애플리케이션, 서버와 네트워크 장비 펌웨어 업데이트 미실시 등 최신 업데이트를 하지 않아 보안 취약점이 될 수 있다. 이런 취약점 제거를 위해 軍에서는 SW개발 보안 적용 및 각종 보안 인증 획득 제품을 도입하고 있다. 시스템 운영간 발생한 신규 취약점이나 개발 과정에서 미식별된 취약점은 유지 보수단계에서 조치하고 있다. 軍에서 시행 중인 취약점 관리는 계획된 취약점 관리와 긴급 취약점 관리로 구분 시행되고 있다. 국방정보체계 취약점 분석 및 평가 실무지침서를 기준으로 매년 점검 계획 수립 후 점검하고 있다[41].

사이버 대응을 위해 軍에서는 국방정보자원관리시스템 DRIMS(Defense IT Resource Information Management System)를 사용 국방정보화 사업 예산으로 획득하여 운영 및 유지하고 있는 IT 자산과 軍에서 자체적으로 개발한 응용SW를 관리하고 있다. 軍에서는 국방정보체계에 대해 매년 국방정보체계 취약점 분석 및 평가 실무지침서를 기준으로 취약점을 점검하여 보안취약점 제거를 위해 노력하고 있다. 軍정보화 자산 취약점 정보 관리 절차는 [그림 Ⅳ-3][42]과 같은 절차를 수행하고 있다.

[그림 IV-3] 軍 취약점 정보 관리 절차

위협정보공유 확인한 취약점에 대한 정보가 침해대응시스템을 통해 상황실에 전파되면 첫 번째 단계에서 취약점을 접수하고, 전자결재시스템 메모보고 형식으로 전 부대의 정보보호부서와 정보체계의 운영부서에 전파된다. 두 번째 단계를 통해 전파받은 해당 부대 정보보호부서에서 정보체계 운영부서 협조 후 취약점을 보유한 장비에 대해 후속조치를 한다. 마지막 단계에서 조치결과에 대해 최초 전파된 메모보고에 의견을 적어 보고하는 절차로 수행한다. 그러나 취약점 식별 및 제거 절차 관련 취약점을 관리하는 데이터베이스가 없어 취약점 이력관리가 되지 않고 있다. 또한 취약점을 지닌 정보화 자산 식별은 해당 정보화 자산관리자와 개발자만 확인 가능하기 때문에 신속한 자산 식별이 제한된다. 마지막으로 취약점 조치 관련 후속조치 방안 수립 및 시행을 위한 주체에 대한 선정이 신속하지 못하다. 결국 이러한 문제점로 취약점 제거에 많은 시간이 소요되며 장기간 보안 취약점에 노출될 수밖에 없게 된다.

소프트웨어를 보호하기 위해서는 운영단계에서 취약점으로 발현 가능성이 높은 보안약점을 개발 단계에서 제거할 필요가 있다. 이러한 활동을 지원하기 위해 중요 보안약점 목록과 같은 정보를 체계적으로 구축할 필요가 있다. 중요 보안약점 목록은 특정 시점의 해킹 트렌드 또는 소프트웨어 개발 트렌드에 따라 달라질 수 있으므로 지속적으로 갱신할 필요가 있으며 적용 도메인의 소프트웨어 운용 방식 및 소프트웨어 개발 특징에 따라 달라질 수 있으므로 적용 도메인별로 중요 보안약점 목록을 식별할 필요가 있다.

2) 국내・외 소프트웨어 보안취약점 관리

현재 국내・외 기관에서 필요에 의해 다양한 약점 목록을 구축관리하고 있다. 대표적으로 자동차 업계의 HIS, HICPP, MISRA-C 등과 항공 업계의 JPL, BSSC C/C++, JSF Air Vehicle C++ 등이 있다. 이 외에도 MITRE에서 관리하는 CWE, OWASP(the Open Web Application Security Project)에서 4년 주기로 발표하는 Top 10 보안약점 목록, 마이크로소프트와 시만텍 등의 주요 업체 뿐만 아니라 미 국방부와 국가안보국의 정보안전부 등이 참여하고 SANS 와 MITRE가 주관하고 있는 CWE/SANS Top 25가 있다. 상용 보안약점 진단도구는 위에서 제시한 다양한 약점 목록에 대한 진단 기능을 제공하고 있지만 이들 목록은 CWE처럼 너무 포괄적이거나 MISRA-C, JPL처럼 특정 도메인 위주로 관리되고 있으므로 이들과는 다른 특징을 가지는 무기체계 내장형 소프트웨어에 그대로 적용하기에는 무리가 있다. 이와 같은 이유로 무기체계 내장형 소프트웨어에 적합한 보안약점목록을 정의할 필요가 있다. 무기체계 소프트웨어의 공통 특성을 기반으로 무기체계 별로 중요 보안약점 도출 시 기본 자료로 활용할 수 있는 보안약점 목록을 우선 선정할 필요가 있는 것이다.

3) 무기체계 보안취약점 통합DB 운용 방안

무기체계 소프트웨어의 주요 라이브러리명을 확보하면 미국 NIST에서 관리하는 NVD(NataionalVulnerability Database)에서 해당 라이브러리에서 발견된 보안 취약점(CVE) 정보를 획득할 수 있다. 또한 해당 CVE와 관련된 보안약점(CWE) 정보도 확보할 수 있다.

무기체계 소프트웨어 개발 단계에서 보안약점의 사전 제거 여부는 무기체계의 안전한 운용에 크게 영향을 미칠 것으로 예상된다. 이와 같은 이유로 무기체계 내장형 소프트웨어에 적합한 보안약점 목록을 정의할 필요가 있다. 보안약점 목록은 소프트웨어가 사용되는 환경 및 운용 방식, 유행하는 해킹의 형태, 소프트웨어 개발 유형이 시간에 따라 달라질 수 있으므로 지속적인 갱신이 필수적이다[42].

무기체계 통합DB를 신규 구축할 수 있지만 중요한 부분은 오히려 이를 악용하여 무기체계를 공격하는 수단으로 활용되면 안된다. 철저하게 무기체계별 보안

관리자 및 운용자에 한해 해당 무기체계 취약점 정보만 접속할 수 있도록 열람 권한을 차등 부여해야 한다. 또한 무기체계의 특성상 운용상의 안정성 보장을 위해 즉각적인 보안패치 적용은 제한될 것이다. 또한 장기간의 시간이 소요될 수 있는 바, 무기체계별 통합DB에 대한 입력 정보를 확인하고 적시적인 교체 여부에 대해 감독이 필요할 것이다.

무엇보다 중요한 것은 무기체계별 체계적인 보안 취약점에 대한 이력 관리를 통해 해소 여부를 알 수 있을 것이다. 또한 장기적으로 해외 도입 및 국내 개발 무기체계의 신규 발생된 취약점에 대해 체계적으로 관리할 수 있는 효과적인 도구로 사용될 수 있을 것이다.

4.2.5. 국제적 차원의 무기체계 보안취약점 관리 및 공유

1) 각국의 사이버 보안 관련 협력 현황

세계는 우방국간의 정보보안 정책, 제도, 요구사항, 인증 등 정보보안 협력을 강화해 나가고 있다. 미국 NIST의 사이버보안 프레임워크는 일본의 NTT 등 주요 기업과 정부가 적용하여 모범사례로 공유되며, 2018년 NIST 컨퍼런스에서 일본에서의 사이버인증 프레임워크 적용 사례가 별도 세션으로 진행 되었다. 미국과 일본은 2017년부터 ICS 합동 교육을 진행하며, 2018년에는 ASEAN 회원국으로 확대했으며, 미국과 일본의 사이버 보안 강화를 위한 파트너 관계를 강화시키고 있다.

EU의회는 2019년 3월 사이버 보안법(Cybersecurity Act, 이하 EU 사이버보안법)을 시행됐다. 주요 내용은 ENISA의 권한 강화와 EU의 사이버인증 프레임워크의 개발이다. 사이버인증 프레임워크는 EU 국가 간 인증, 요구사항을 재정립하여 통합된 제도를 만들어서 EU 단일시장으로 EU의 경쟁력을 강화하기 위한 제도이다. 사물인터넷 기기, ICT 제품, 네트워크 설비 등 공통 적용이 가능한 인증 제도를 ENISA가 각국 정부와 협업하여 개발을 주도한다. 한국도 국제 협력을 위해 지속적으로 활동하고 있다. 주요 전략국가의 우호 네트워크 구축 및 협력과제 발굴을 위한 '글로벌 사이버보안 협력네트워크 구축(CAMP)', 경제개발협력기구(OECD), IDB(미주개발은행)의 중남미ICT 교육센터 설립·운영하고 있다. 아시아태평양 CERT간 협력을 위해 AP-CERT와 글로벌 사고대응 보안팀 포럼인 FIRST에서 보안협업을 진행하고 있다. 2018년에는 FIRST, WEF, ENISA, GFCE 등 기반시설 보호방안 및 모범사례를 논의하는 메리디안(MERIDIAN) 컨퍼런스가 개최됐다. 유럽-아시아 지역 간 보안협력 논의를 위해 2019년 제2차 한-OSCE 컨퍼런스를 개최하였다. 4차 산업혁명 흐름 속에서 각국이 당면하고 있는 사이버 공간의 위협요소와 대응전략을 논의하기 위해 국제 사이버범죄 대응 심포지엄을 매년 개최하고 있으며, 2018년에는 인터폴, 유럽평의회, 미국, 영국, 독일, 일본을 비롯해 총 58개국에서 1,133명이 참석하였다[43].

2) 무기체계 보안취약점 국제 공유 및 관리 방안

국방부는 2009년 7.7 DDoS 공격을 계기로 국방 사이버전 기획, 계획, 시행, 연구개발 및 관련 부대 훈련 등을 관장하는 국군사이버사령부를 2010년에 창설하였다. 사이버 위협정보 공유와 관련하여 국군사이버사령부는 국방 사이버전 유관기관 간 정보공유 및 협조체계를 구축하도록 되어있다[44].

무기체계 보안취약점 공유를 위해서는 사이버사의 노력으로는 부족하다. 국내개발 무기체계와 구매한 무기체계의 관리 역시 다를 수밖에 없을 것이다. 무기체계 보안취약점 국제 공유방안은 먼저 구매한 무기체계의 경우 계약 단계에서 무기체계 보안취약점에 대한 지속적인 보완 및 조치가 필요하다. 이를 통해 개발 및 시험평가 단계에서 식별되지 못한 무기체계 보안 취약점을 운용단계에서 제거할 수 있는 기반을 마련 할 수 있을 것이다. 앞서 살펴본 봐와 같이 미국에서 구매한 무기체계의 경우 GAO가 식별하거나 또는 운용간 식별되어 미군에서 보안취약점을 제거하는 작업을 할 경우 이런 무기체계 취약점을 제조사 또는 미군과 협력하여 국내 도입된 무기체계에 대해서도 동일한 조치를 할 수 있도록 정부 차원의 관심과 지원이 필요하며, 무기체계 소요를 제거하는 각군에서도 이를 유념하여 계약단계에서부터 이러한 보안요소를 반영해야 할 것이다.

국제 사이버협력 네트워크를 확대하는 것이 필요하다. 이를 위해서 국제 사이버정보 공유체계를 구축하고, 주도적으로 사이버안보 국제 규범화 및 국제 거버넌스에 참여할 필요가 있다[45]. 다만 국제규범 및 국제 거버넌스에의 참여는 상이한 관점과 국가이익의 충돌이 존재하므로 각기 사안별로 별개의 차원에서 접근할 필요가 있다. 무기체계 취약점 관리를 위해 북한 등 악의적 해커그룹에 의한 무기체계 공격이 있을 경우 이를 공유하고 해소하기 위한 노력이 필요하다. 또한 해킹기법 및 대책에 대한 공유를 통해 우리 무기체계를 대상으로 하는 적의 공격기법을 사전에 식별하여 예방적 대책을 강구할 수 있을 것이다. 일반적인 사이버 보안 협력 및 위협정보 공유만 하는 것이 아니라 무기체계까지 협력 분야를 확대하여 국가간 이익을 침해하지 않는 범위에서 충분히 무기체계 위협에 대한 정보 공유가 가능할 것이다.

4.3. 방산업체 보안관리 강화 방안

4.3.1. 방산업체 보안관리 개선

방산업체 보안사고 방지를 위해 망분리 의무 구축 및 정보보호체계 운용 등의 방산업체 보안관리를 강화하고 있으나 대기업 대비 중소 하도급 업체를 통한 보안사고가 지속 발생하고 있다. 또한 방산업체의 망분리 시스템에서 외부반출한 방산기술 자료 관리상 문제점이 식별[46]되는 등 방산업체 보안관리 개선을 위한 대책이 필요하다. 방산업체 보안관리 개선을 위한 미국 사례에 대해 살펴보겠다.

1) 미국의 사이버보안 성숙도 인증체계(CMMC)

미국은 방위산업의 특수성으로 인해 DoD에서 관리 감독하고 있고 국토안보부와 공조하고 있다. 중점은 대기업보다는 사이버 보안에 취약한 중소 방산업체에 대한 지원분야에 중점을 두고 있으며, 자연재해・화재・테러 등 물리적 보안에 대한 피해 대응도 포함하고 있다[47].

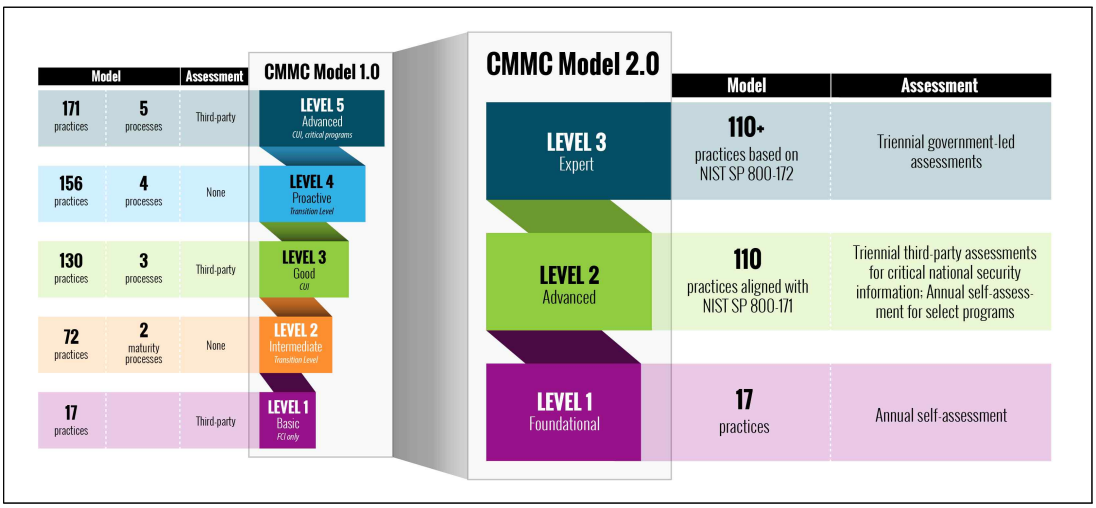
최근에 미국 국방사업에서 주목할 만한 변화로, DoD는 2020년 후반기부터 국방사업 입찰참가 주 계약 및 하도급 계약 업체에 외부인증 평가기관 C3PAO(CMMC Third-Party Assessment Organization)을 통한 Cybersecurity Maturity Model Certification(이하 CMMC)라는 인증절차를 수행해야 함을 공지하였다. 이를 위해 인증관리조직 CMMC-AB(CMMC Accreditation Body)를 출범시켜 인증평가기관에 대한 교육훈련 및 등록관리를 수행하게 하고 인증평가 지원시스템 CMMC EMASS(CMMC Enterprise Mission Assurance Support Service)를 구축하고 있다. CMMC는 소프트웨어 개발 역량의 성숙도 평가 기준인 Capability Maturity Model Integration(이하 CMMI)에 상응하는 사이버보안 성숙도 인증체계로, 조직의 사이버보안 절차(Processes) 표준화의 기준과 방향을 제시하면서 실무(Practices) 보안역량의 수준을 측정하는 평가 지표로도 활용할 수 있는 미국 국방부의 새로운 보안인증 프레임워크이다.

CMMC 인증체계에서 사이버보안 성숙도를 평가하는 단계는 CMMI 모델과 유사하게 보안수준에 따라 5단계 레벨(Level)로 구성된다. 모든 국방사업 입찰참

가 업체는 기본적으로 연방계약정보 FCI(Federal Contract Information) 보호 기준인 레벨 1(Basic Cyber Hygiene) 인증을 취득해야 하고, 사업 기간에 통제평문정보를 취급하게 되는 계약업체는 레벨 3(Good Cyber Hygiene) 이상의 인증이 요구된다. 이는 미국 방산업계의 사이버보안 위협을 감소시키고 방산업체의 시스템과 네트워크를 통해 유통되는 중요한 사업정보를 보안요구 수준에 따라 표준화하여 관리하는 데 목적이 있다.

이르면 2020년 말부터 DoD 입찰제안요청서 RFP(Request For Proposal)에 계약자의 CMMC 인증 요건(레벨 1~5)이 기술되기 시작할 것으로 예상하고, 관련 솔루션 제조사들은 국방사업 입찰참가 준비 업체를 대상으로 인증 관련 제품과 서비스를 준비하고 있다. DoD는 2026년까지 모든 국방사업에 CMMC 인증체계를 통합하고 사업의 입찰참가, 공급망, 솔루션제공, 시스템통합 등에 관련된 30만 개 이상의 사업체들이 CMMC 인증을 수행할 것으로 예측하고 있다. 또한 연구개발 조직의 역량수준을 평가하는 국제표준으로서 자리를 잡은 CMMI 인증 모델과 같이 향후 미국 연방기관들과 외국의 기관들까지도 지식재산권 보호를 위해 CMMC 또는 유사한 인증체계를 표준적으로 채택할 것이라 기대한다[48].

미 국방부는 2020. 11. 4. 방위산업 및 정부 등 이해 관계자 의견을 수렴하여 'CMMC 2.0'을 발표했다. 주요 변경사항 [그림 Ⅳ-4][49]와 같으며 세부 내용은 아래와 같다.



[그림 Ⅳ-4] CMMC 모델 1.0과 2.0 비교

특징은 기존 5개 등급의 모델을 3개로 간소화했으며 NIST 사이버보안 표준을 사용했다. 평가비용 절감을 위해 1등급과 일부 2등급 기업은 자체 평가를 가능하게 하였고, 외부 평가자에 의한 감독을 강화하였다.

CMMC 인증은 미국에 방산물자 수출을 할 경우 외국의 경우에도 동일하게 적용되기 때문에 미국의 CMMC 인증을 중심으로 국방분야 글로벌 공급망이 구축될 것으로 예상된다.

일본과 이스라엘 등에서는 CMMC 인증에 위해 방산업체를 대상으로 미국 CMMC 수준을 준용하여 구축하고 있고, 특히 자체 인증 제도를 미국으로부터 상호 인정받기 위해 노력하고 있다.

2) 한국형 CMMC 제도 도입

우리나라의 방산분야 사이버안보 주권을 위해 2025년 CMMC 전면 시행 전 한국형 CMMC를 구축하고, 상호인정을 위해 노력해야 한다.

이를 통해 방산분야의 사이버보안 수준이 국제적 기준에 부합하게 될 것이고, 방산업체 사이버 보안 수준 향상에 따라 국가안보 및 방산수출에 큰 도움이 될 것으로 기대된다.

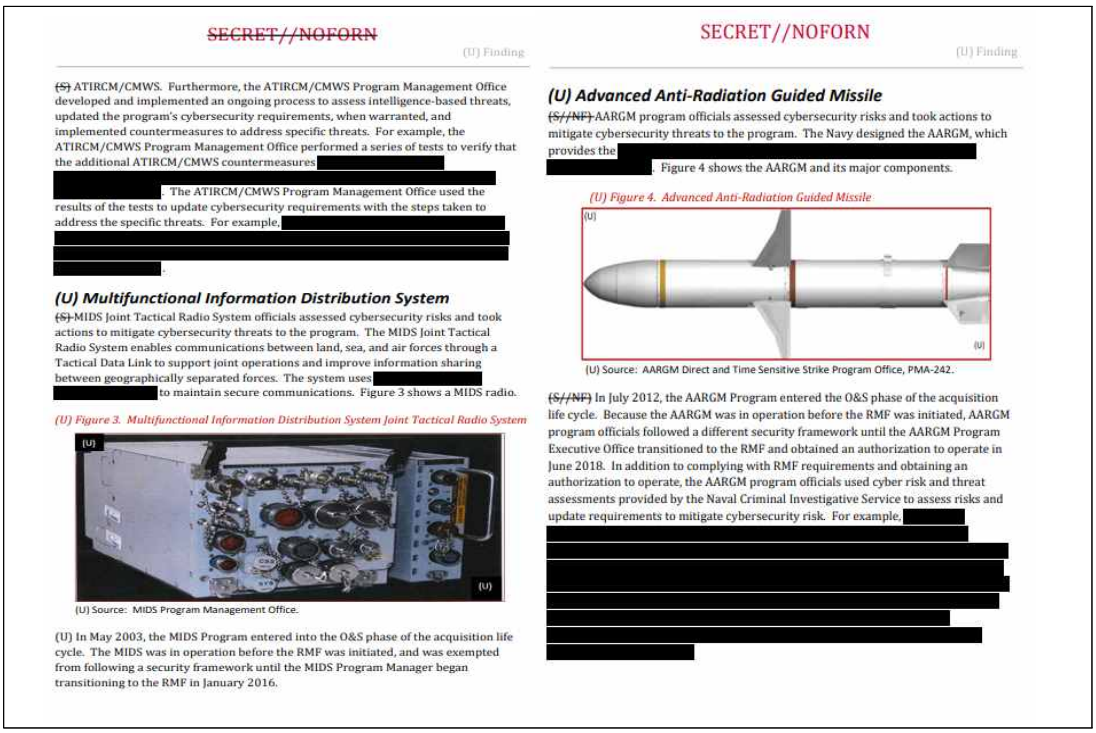
한국형 CMMC 제도를 통해 무기체계의 근본적인 보안 취약점을 개선 할 수 있도록 미국 체계를 모방하는 것이 아니라 우리나라 상황에 부합하도록 발전적으로 적용할 것이다. 범정부 차원에서 방산업체, 軍, 학계가 함께 제도를 개발해야 한다.

3) 무기체계 보안 산업 육성

보안 분야는 대다수의 기업에서 활용되는 정보시스템에 대한 외부 유출 및 사고를 방지하기 위해 필수적으로 도입되어야 하는 분야로, 사이버 기술이 발전함에 따라 그 중요성이 강조되는 분야이기도 하다. 보안 산업의 목표는 시스템이나 시스템에 대한 비정상적인 동작을 예방하거나 차단함에 있다. 따라서 보안 시스템은 대상 시스템의 보안 취약점을 탐지하고, 해당 취약점에 의한 사건을 방지할 수 있도록 하는 시스템을 구축한다.

하지만 국방과 관련된 무기체계는 일반적으로 기밀로 취급되며, 외부 인사에 의한 접근이 일체 차단되는 폐쇄적 구조를 가진다. 국방 자료는 국가의 안위에 직결되는 문제이며, 무기체계의 접근이 외부 인사에 의해 이뤄질 경우 유출의 경로가 증가할 뿐 아니라 무기체계로 접근할 수 있는 악의적 공격자의 접근 경로가 발생할 수 있기 때문이다. 따라서 무기체계의 보안성 강화는 전문 지식을 가진 軍 내부 전문가에 의해 이뤄져야만 한다. 하지만 한정된 인력과 예산 내에서 보안업무를 수행하여야 하기 때문에 국방 보안 체계의 발전에 많은 제약이 수반된다.

이와 같은 문제에 대하여 미국의 경우, 내부적 보안 강화를 수행하기 위하여 민간업체 및 민간 전문가를 통한 업무 수행에 많은 비용을 지출하고 있다. 국방 강화를 위해 무기체계에 대한 비밀문서 중 일부 취약점을 평문으로 재분류하여 외부에 공개[50]함으로써 해당 문제의 해결을 위한 민간 전문가 도입에 적극적인 시도를 진행하고 있을 뿐 아니라, 미군의 네트워크와 같은 사이버 환경에 대해서 발생할 수 있는 사이버전에 대한 평가나 교육을 위해 민간업체를 통해 무기체계에 특화된 보안 산업의 육성을 진행하고 있다.



~~SECRET//NOFORN~~

(U) Finding

~~(S)~~ ATIRCM/CMWS. Furthermore, the ATIRCM/CMWS Program Management Office developed and implemented an ongoing process to assess intelligence-based threats, updated the program's cybersecurity requirements, when warranted, and implemented countermeasures to address specific threats. For example, the ATIRCM/CMWS Program Management Office performed a series of tests to verify that the additional ATIRCM/CMWS countermeasures [redacted]. The ATIRCM/CMWS Program Management Office used the results of the tests to update cybersecurity requirements with the steps taken to address the specific threats. For example, [redacted].

(U) Multifunctional Information Distribution System

~~(S)~~ MIDS Joint Tactical Radio System officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. The MIDS Joint Tactical Radio System enables communications between land, sea, and air forces through a Tactical Data Link to support joint operations and improve information sharing between geographically separated forces. The system uses [redacted] to maintain secure communications. Figure 3 shows a MIDS radio.

(U) Figure 3. Multifunctional Information Distribution System Joint Tactical Radio System

(U) Source: MIDS Program Management Office.

(U) In May 2003, the MIDS Program entered into the O&S phase of the acquisition life cycle. The MIDS was in operation before the RMF was initiated, and was exempted from following a security framework until the MIDS Program Manager began transitioning to the RMF in January 2016.

SECRET//NOFORN

(U) Finding

(U) Advanced Anti-Radiation Guided Missile

~~(S//NF)~~ AARGM program officials assessed cybersecurity risks and took actions to mitigate cybersecurity threats to the program. The Navy designed the AARGM, which provides the [redacted]. Figure 4 shows the AARGM and its major components.

(U) Figure 4. Advanced Anti-Radiation Guided Missile

(U) Source: AARGM Direct and Time Sensitive Strike Program Office, PMA-242.

~~(S//NF)~~ In July 2012, the AARGM Program entered the O&S phase of the acquisition life cycle. Because the AARGM was in operation before the RMF was initiated, AARGM program officials followed a different security framework until the AARGM Program Executive Office transitioned to the RMF and obtained an authorization to operate in June 2018. In addition to complying with RMF requirements and obtaining an authorization to operate, the AARGM program officials used cyber risk and threat assessments provided by the Naval Criminal Investigative Service to assess risks and update requirements to mitigate cybersecurity risk. For example, [redacted]

[그림 IV-5] 미국 비밀 해제 후 공개한 무기체계 취약점 문건

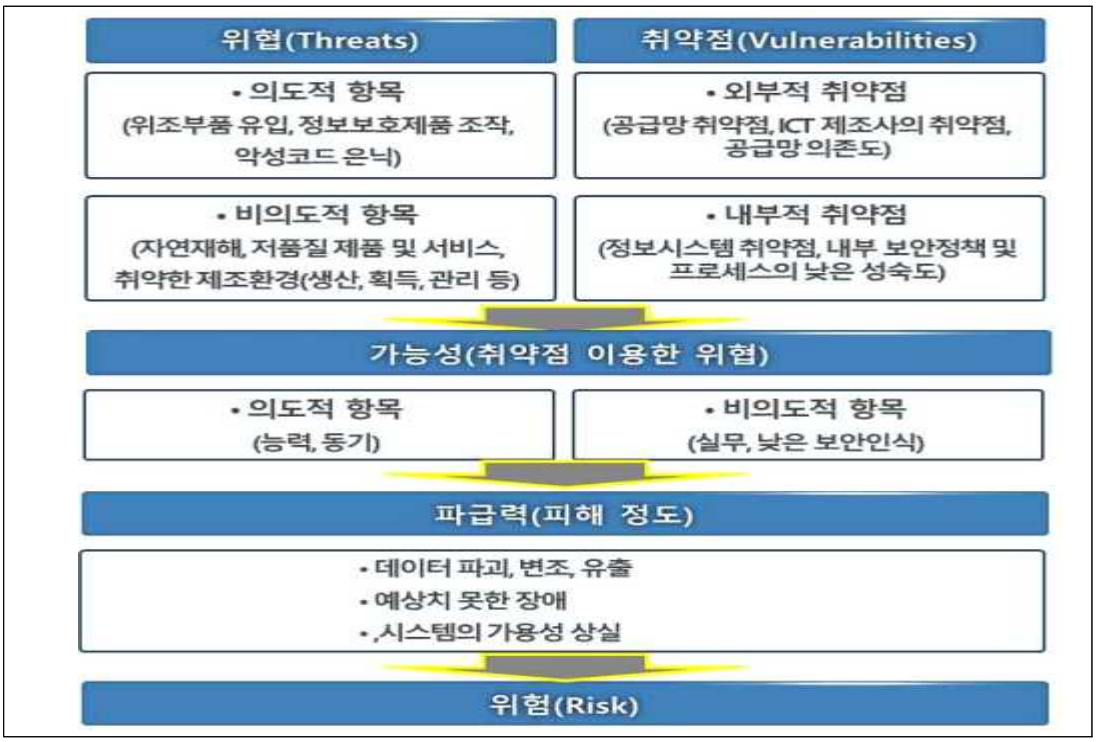
미군은 사이버 작전의 시험이나 평가, 훈련을 위해 SimTEX, CAAJED, SAST, StealthNet과 같은 시스템이나 도구를 민간과 협업하여 개발하고 있으며, 이는 무기체계에 특화된 보안 인력을 통해 보다 강력한 보안 시스템을 구축할 수 있는 산업 육성을 유도하고 있다.

이처럼 일부 환경에 대해 회색 지역으로서 접근을 허가하는 것은 특정 분야에 특화된 전문가에 의한 업무 수행을 가능하게 할 뿐 아니라, 무기체계라는 제한된 분야에 특화된 보안 전문 산업을 육성할 수 있도록 한다. 무기체계에 특화된 보안 전문 산업 육성은 軍의 한정된 사이버 보안 전문인력을 해소함과 동시에 기술의 전문성을 향상시키고, 국내의 보안 수준을 높일 수 있는 방안이 될 수 있다.

4.3.2. 공급망 보안관리 체계 수립

1) 공급망 보안 위협

공급망 위협과 취약점으로 인해 공급망 위험이 발생한다. NIST에서는 SP 800-161 문건에서 공급망 위협에 대해 [그림 Ⅳ-6]과 공급망 위험에 대해 설명하였다[51].



[그림 Ⅳ-6] 공급망 위험

2) 공급망 보안관리 실태

사이버 공격은 정부기관 및 방산업체까지 확대되고 있다. 정부기관 대비 방산업체의 경우 업체별 규모가 상이하고 사이버 보안 수준의 편차가 심해 사이버공격에 취약하다. 특히 코로나 확산에 따른 재택근무 증가 및 업무환경 변화는 새로운 위험을 야기하고 있다.

한국인터넷진흥원과 유사한 방산업체에 특화된 사이버 보안 전문기관 부재로 효과적 대응이 제한된다. 일부 방산업체에서 자료 공유시 보안에 취약한 상용메일도 사용 중으로 효과적 대비를 위해 방산업체 전용 자료교환체계 구축이 필요

하다.[52] 방산기술 보호를 위해 관련부처 간의 긴밀한 협력 필요하며, 기술 유출 방지를 위한 대책이 필요하다.

3) 제품 수명주기별 위험요소 제거 방안

공급망 수명주기에 따른 잠재적 보안 위험은 [표 Ⅳ-4][51]과 같다.

단계	생산	도입	운용	폐기
위험 요소	• 위조부품 사용 • 불법부품 은닉 • 잠재된 취약점 • 악성코드 은닉	• 부실한 제품 검수 • 제품위조 / 변경 • 제품정보 변조 • 악성코드 / 부품 삽입	• 재생 / 위조 부품 사용 • 악성코드 / 부품 교체 • 외주인원 통제 소홀 • 보안 취약점 미조치	• 내용연수 초과 사용 • 임의 재사용 • 잔존 정보유출

[표 Ⅳ-4] 공급망 단계별 보안위험

생산단계 고려 사항은 신뢰 가능한 공급기업을 선정하고 위·변조 제품 도입 방지 및 불법적 기능 은닉을 최소화 해야 한다. 생산기업에 의한 자체검사를 하거나 공식적인 검사기관에 의한 위·변조 검사를 시행한다.

도입단계의 경우 제품에 설치될 수 있는 도·감청장치를 탐지해야 되는데 불법 기능이 포함 될 경우 전력 소비량이 많은 특성을 이용하여 탐지할 수 있다. 또한 제품 도입 시 검수 절차를 강화해야 한다.

운영단계는 하드웨어 및 소프트웨어 보안패치, 업데이트 및 부품 교체 등 유지보수 과정에서 발생할 수 있는 보안위험 예방이 필요하다.

무기체계 도입 시 검수, CC 인증 및 보안적합성 검증 제도를 통해 보안을 강화한다.하고, 운용단계에서 시스템 유지보수를 위해 교체되는 하드웨어 제품과 부품에 대해서는 도입 단계와 비교하여 검수가 소홀한 경우가 있다. 하드웨어 제품 장애 또는 기능개선을 위해 도입된 제품에 대해서도 도입단계와 동일한 수준으로 검사를 강화해야 한다. 시스템 관리자는 장애 발생으로 제품이나 부품을 교체하는 경우 제품에 대한 인증번호와 일련번호를 검증하고 제조사 정품 공급 여부를 검수해야 한다. 유지보수기업은 제품교체 시 시스템관리자에게 사전 승인을 반드시 받아야 하며 도입된 제품과 동일한 제품과 버전으로 교체해야 한다.

폐기 단계의 경우 사업 종료 시 사업자료 및 저장자료의 외부 유출 차단을 위해 외주 인원 보안통제 절차가 필요하다.

4) 공급망 보안관리 강화 방안

공급망 보안관리를 위해서는 공급망 위험에 대한 정확한 식별이 필요하다. 네트워크 장비의 보안 이슈가 발생할 경우 일회성 점검을 하는 것이 아니라 체계적이고 장기적인 계획에 의해 보안관리를 강화해야 한다. 이를 위해 공급망 보안에 특화된 전문보안 기관 설립이 필요하다. 체계적으로 공급망에 의해 발생할 수 있는 보안위협에 대해 제공하고 적시적인 점검 지원과 보안관리를 통해 근본적인 공급망 위험을 감소시켜야 한다.

軍 내부로 도입되는 무기체계 관련 제품에 대한 공급망 차원의 위협을 식별할 수 있는 제도를 마련해야 한다. 예를 들어 공급망 차원에서 스마트TV에 도청 기능이 은밀히 내장시켰는데 軍의 통제구역 또는 무기체계 구성요소로 반입된다면 심각한 피해를 야기할 수 있다. 이를 방지하기 위해 무기체계 도입시 도청 탐지 활동이 병행 되어야 하며, 불시적인 점검 또한 필요하다.

안전한 무기체계 공급을 위해 방사청 차원의 공급망 업체 대상 위협 완화를 할 수 있는 프로세스를 마련해야 한다. 방산업체 및 유관기관 간 MOU 체결을 통해 공유 방법 및 범위 설정을 해야 한다. 자발적 참여 유도를 위해 위협 정보 제공 업체만 정보 공유를 실시하며, 정보제공 업체 동의가 없이 임의 공개행위를 금지해야 한다. 또한 방산업체 보안사고 또는 공급한 제품에서 중대한 보안취약점을 식별한 경우 신속하게 납품한 기관 고지 의무화 및 협력업체 공유를 강화해야 한다.[47]

무기체계에 포함된 저장매체의 경우 정비 시 외부 반출을 금지하고 필요시 적절한 보안대책을 강구할 수 있도록 제도적으로 보안을 강화해야 한다. 또한 폐기 시에도 물리적으로 완전한 폐기가 될 수 있도록 엄격히 통제하여야 할 것이다.

4.4. 무기체계 전문인력 양성

4.4.1. 무기체계 보안 전문인력 양성

1) 해외 사이버 보안 전문인력 양성 사례

지속적으로 사이버보안의 중요성을 강조해오고 있는 미국 정부는 2010년 사이버 보안 수준 강화를 위해 '사이버보안 교육 계획(National Initiative for Cybersecurity Education, 이하 NICE)'을 발표하면서, 국가 차원의 사이버 보안 인력 양성에 나서고 있다. 국토안보부(Department of Homeland Security, 이하 DHS), 국방부, 국가안보국(National Security Agency, 이하 NSA) 등 20여 개 정부 부처가 참여하고 있는 NICE 계획은 사이버 보안 및 정보보호 업무 종사자나 전공자뿐만 아니라 초·중·고등학생부터 일반인에 이르기까지 전 국민을 대상으로 사이버 보안 및 정보보호 기술과 의식 수준의 향상을 목표로 하고 있다[53].

이와 함께 미국은 사이버 인재를 조기 발굴하기 위한 목적으로 국가 기관에서 Cyber Patriot, Digital Forensics Challenges와 같은 해킹 대회를 주관 하거나 음지에서 활동하는 해커와의 개별적인 접촉을 통해 해커를 고용하고, 사이버 안보 분야에 월등히 뛰어난 학생들을 대상으로 장학금을 지원하면서 졸업 후 정부기관에서 일정 기간 동안 일할 수 있는 SFS, CAE/ID 등의 교육프로그램 등을 통해 사이버 안보를 담당할 인재풀에 대해서 인적자원 관리를 체계적으로 운영하고 있다. 즉, 미국은 해커를 국방 사이버 위협에 대응 가능한 자원으로 인식하고 국가 사이버 위협에 대응을 위해 음지에서 활동하는 해커를 고용하거나 우수 정보보호 교육 기관에 장학금 지급 및 정부 기관에서 고용하는 방법을 활용하고 있다. 즉, 미국 정부는 화이트 해커 양성을 통해 블랙 해커를 막고 사이버 국방 위협에 대처하고 있는 것이다.

NICE의 정책 방향 중 연방 사이버 보안 인력 구조 구축 분야는 2011년 국립표준기술연구소가 발표한 사이버 보안 인력 프레임워크(Cyber security Workforce Framework)로 더욱 체계화 되었다. 사이버 보안 인력 프레임워크는 사이버 보안에 필요한 역량을 자세히 명시함으로써 국가 차원에서 일괄적으로 화이트 해커 등

사이버 보안 인력을 세분해서 관리가 가능토록 하였다. 2012년 NICE 실행을 위한 전략계획 수립 이후 매년 전략계획을 업데이트하여 발표하고 있으며, 이를 통해 사이버 보안 인재 유형 및 경력 과정을 제시하고 2014년에는 44개 학교를 우수 학술기관으로 선정하여 국가안보·사이버 군 장학금 등을 지원하였다. 또한 고교생 및 대학(원)생을 대상으로 여름방학 2개월간 포렌식 챌린지 행사 개최, 해킹방어대회 프로그램 등을 통해 10,000여 명 이상의 사이버 보안 전문가를 육성하기 위해 노력하고 있다. 특히 2016년 2월에는 연방정부 CISO 직위 신설, 사이버군대 창설, 사이버보안 주요 커리큘럼 개발, 국가 사이버보안 센터 강화 등의 내용을 담은 실행계획을 발표하였다.

한편 미국은 2000년 20명의 컴퓨터 해킹·바이러스 전문가로 구성된 사이버전 담당부서를 신설하고 사이버 공격 작전을 수행하는 사이버 작전 계획인 'OPLAN 3600'을 수립한 이래 오래전부터 지속적으로 화이트 해커 등 사이버 전담 요원을 양성해 왔다.

DoD에서는 DCWF(The DoD Cyber Workforce Framework)를 제정하여 미국 사이버 자원을 구축, 보안, 운영, 방어 및 보호하는 모든 인력을 포함하도록 재구성하여 현재와 미래의 사이버 작전을 가능하게 하고 있다.

DCWF는 DODD 8140.01에 정의된 사이버 인력의 전체 수행하는 작업을 설명한다. DCWF는 NICE 사이버보안인력 프레임워크(NCWF)와 DoD 공동 사이버 공간 훈련 및 인증표준(JCT&CS)을 활용한다.

DoD에서는 끊임없이 변화하는 국가안보 환경에서 사이버 임무를 수행하는 국방부의 능력을 강화하기 위해 2017년 8월 DoDI 1400.25 Volume 3001에 의거하여 CES(Cyber Exceptioned Service, 이하 CES)를 도입하여 국방부 전체의 민간 사이버 전문가를 관리하고 있다. 채용인력에 대한 고용 및 배치는 2017년 8월 제정된 DoDI 1400.25 Volume 3005를 따르며 체계적으로 관리하고 있다[54].

이스라엘은 총리실 소속 국가 사이버국에서 대학의 사이버 보안 교육을 지원하고 사이버 국방 프로그램 정책을 추진하고 있다. 사이버 국방 인력 양성을 위해 사이버보안 관련 정부 기관과 연계함으로써 수료 후 취직 기회 등 제공하는 '마그니엄 류미트(Magshimim Leumit)' 프로그램을 도입하여 청소년을 대상으로 전문적인 컴퓨팅 교육 프로그램 제공하고 있으며, 탈피오트, Brakim Excellence

Program, 하바찰롯 등 군대의 인재 양성 프로그램을 통해 화이트 해커를 키우고 있다.

2) 무기체계 전문인력 양성 방안

우리나라에서는 사이버보안 분야에 대해서는 인력 양성 및 관리가 사이버사령부를 중심으로 이루어지고 있다. 하지만 무기체계 전문인력에 대한 관리는 소홀한 실정이다. 미국처럼 사이버보안의 전 영역에 대해 세부적인 인력 기준을 수립하고 체계적인 관리방안이 수립되어야 할 것이다. 특히 민간분야 전문 인력의 군내 유입과 관리를 위해 미국에서 시행중에 있는 CES를 벤치마킹 하여야 하겠다.

민간영역에서 제대군인에 대한 인센티브를 부여하고 있다. 군에서 양성된 우수인력에 대해서는 동일하게 우대하여 선발하는 것이 필요하다.

CES의 경우 최고 등급인 Step 12의 CG-15 등급의 경우 연간 최대 154,283달러를 지급받을 수 있으며 여기에 근무기간 및 지역별 추가요금을 받을 수 있다[55].

인력 전문성 향상을 위해 무기체계에 특화된 전문 교육기관 설립되어야 하며 산학 연계프로그램을 개설하여 우수 자원의 유입이 필요하다. 또한 무기체계 사이버보안 전문가 인증 제도를 신설하여 일정 수준 이상 전문성이 유지될 수 있도록 제도적으로 관리해야 할 것이다.

4.4.2. 무기체계 보안 교육기관 지정 및 운용

1) 기존 사이버보안 관련 교육기관 활용

무기체계 보안을 위해서는 기본적으로 사이버 보안에 대한 교육을 바탕으로 한다. 따라서 군에서 현재 활용하고 있는 정보보호 인력 양성 프로그램을 이수 후 무기체계 사이버 보안에 대한 특화된 교육이 필요하다. 먼저 기본적인 사이버 보안 교육은 기존의 양성체계를 활용하며 이를 발전적으로 적용한다.

각 군의 정보보호 인력은 각 군 교육사령부(정보통신학교)에 의해 기초교육이 이루어지고 있다. 또한 각 군에서는 국방부 예하 교육기관의 교육 프로그램을 통해 전문적인 교육을 받고 있으며 일부 대외 민간기관의 교육을 이용하기도 한다. 하지만 일부 교육은 기관 간 내용이 중복되거나 개인 또는 부대별 직무 수준이 고려되지 않고 있다.

따라서 각 군의 교육사령부는 각 군의 정보시스템 환경과 정보보호체계를 고려한 직무별 기초 교육을 단계적(초급, 중급 등)으로 시행함으로써 최초 보직자가 직무를 수행할 수 있는 여건을 제공하고 각 군 초급 인력이 양성할 수 있어야 한다. 인력 양성을 위한 과목은 공통과목, 필수과목, 전문 과목으로 나누고 단계별로 교육을 이수하도록 해야 하며, 공통 및 필수과목은 일반, 정책, 이론, 기술 과목으로 분류한다. 여기에 필수적으로 무기체계 사이버 보안에 대한 기본적인 과목을 선정하여 포함 시켜야 한다.

전문 과목은 기술 및 정책에 관련된 심화과정으로 인력의 인증 유형에 따라 이수하도록 한다. 또한 2~3년 이상 정보보호 관련 직책을 수행하는 인력에 대해서는 각 군 교육 외에도 대외 민간교육을 활용한 위탁교육, 국방부 예하 교육기관에서 제공하는 중급 이상의 통합교육을 통해 중급 전문인력이 양성될 수 있는 여건을 제공해야 한다.

고급 인력에 대한 교육은 전문학위 위탁교육, 대외기관 양성교육(BoB, K-Shield 등), 상급부대 전문가 교육 등을 활용하여 시행함으로써 각 군의 교육과 연계성과 차별성을 두도록 하는 교육체계와 구체적인 과목의 정립이 필요하다[56].

2) 무기체계 사이버 보안 전문기관 설립

무기체계 사이버 보안 강화를 위해서는 무기체계 소프트웨어 개발보안 교육 및 기술지원 전문기관의 신설이 필요하다. 일반분야의 소프트웨어 개발보안 기술지원 전문기관은 한국인터넷진흥원이다. 한국인터넷진흥원은 기술지원뿐 아니라, 개발보안 가이드를 만들어 배포하고 관련 교육을 실시한다. 이러한 역할을 해줄 수 있는 기관이 국방분야에도 필요하다[31]. 이는 관련된 정책제도에서부터 개발단계의 기술지원과 운영유지 단계의 후속 지원까지 아우를 수 있도록 하여야 하며, 많은 자료와 정보가 비밀로 다루어져야 하는 국방분야의 특수성을 고려하여 국방부 산하의 전문화된 조직이 되어야 할 것이다.

무기체계 사이버 보안 전문기관에서 국방부의 무기체계 보안 관련 정책 수립을 지원하고 각군별 운용중에 있는 무기체계별 전문가 양성을 위한 교육 과정 개설 및 전문인력의 수준 유지를 위한 지속적인 노력이 필요할 것이다.

4.5. 무기체계 악성코드 대응 방안

4.5.1. 무기체계 전용 바이러스 백신 운용

1) 무기체계 악성코드 및 랜섬웨어 위협 사례

러시아가 우크라이나 침공 이후 자국 해커들을 동원해 우크라이나 내 주요 시설·기관에 대해 수십차례 사이버 공격을 한 것으로 드러났다. 2022. 4.27 마이크로소프트(MS)는 정부 지원을 받는 러시아 해커들이 우크라이나의 여러 인프라와 기관을 상대로 사이버공격을 벌여 데이터를 파괴하는 등 정보 혼란의 상황을 만들었다고 밝혔다. 러시아가 단행한 사이버공격의 거의 절반이 우크라이나의 핵심적 인프라를 겨냥한 것이었으며 많은 경우 폭격, 미사일 공격과 동시에 이뤄졌다는 것이다. MS는 우크라이나로의 침공이 시작한 후 이달 8일까지 총 37차례에 걸친 사이버공격이 이뤄졌으며, 해킹으로 인해 우크라이나의 여러 기관의 시스템에서 데이터가 영구적으로 파괴됐다고 밝혔다. 또 러시아군의 정보조직인 총정찰국(GRU)과 연계된 해킹 그룹이 우크라이나 침공 이후 일주일에 2~3회 파괴적인 맬웨어인 '와이퍼'를 이용한 공격을 벌이고 있다고 했다[57]. 와이퍼는 한 번 감염되면 컴퓨터의 하드웨어를 통째로 지워버리는 프로그램으로 잘 알려져있다.

내·외부망에 대한 랜섬위협은 지속적으로 [표 Ⅳ-5][58]과 같다. 대부분의 랜섬웨어 인터넷이 연결된 상태에서 암호화를 진행하기 때문에 인터넷 연결이 차단될 경우 암호화 작업을 수행하지 않지만 일부 랜섬웨어는 인터넷이 차단된 환경에서 암호화가 가능하기 때문에 더 이상 내부망도 랜섬웨어로부터 안전하지 않다.

구 분	랜섬웨어	통신	공격기술
외부망 (인터넷)	온라인 랜섬웨어	○	워터링-홀, 이메일, 크리덴셜 스터핑 등
내부망 (국방망)	오프라인 랜섬웨어	×	Bad USB, 크랙된 SW와 외부망 공격기술

[표 Ⅳ-5] 내·외부망 랜섬웨어 위협

軍에서는 랜섬웨어 대응을 위해 전향적인 대책을 마련해야 하지만, 시그니처 기반 백신 및 악성코드 탐지체계를 이용하고 있다.

북한 해커그룹 내에서 동일한 공격과 기능으로 사용된 멀웨어에 대한 이미지 패턴을 적용[59]하여 군 전용백신을 제작한다면 효율적인 해커의 공격으로부터 사전에 탐지 또는 조치할 수 있을 것이다.

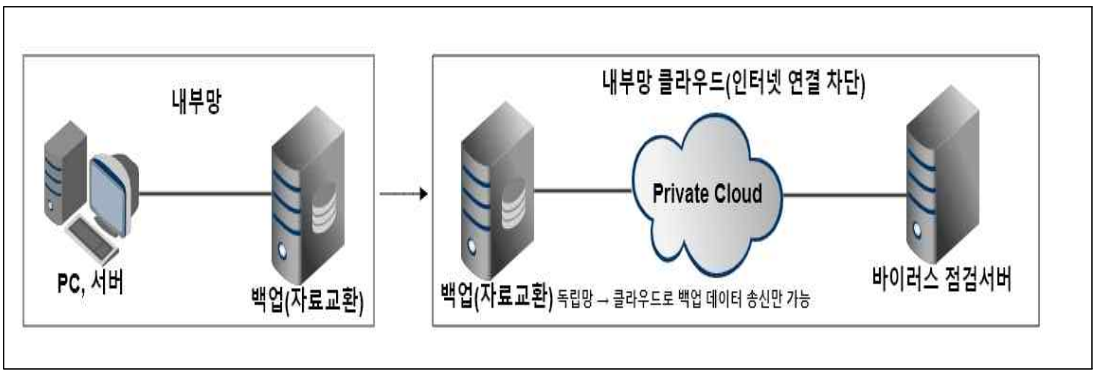
2) 軍 전용 바이러스 백신체계 구축 방안

중요 정보체계임에도 바이러스 방역체계의 특성상 1개의 바이러스 백신만 설치할 수 있기 때문에 탐지하지 못한 악성코드가 존재할 경우 큰 보안위협이 된다. 또한 정상 파일을 악성코드로 오탐하여 시스템 장애를 유발할 수 있으며 지역적으로 점검대상 체계가 장거리 이격될 경우 바이러스 백신 업데이트 후 점검하는 과정에서 인터넷과의 망접점이 발생하여 오히려 악성코드가 유입되는 경로로 악용될 수 있다[60].

내부망 전용 악성코드 점검용 클라우드 구축은 [그림 Ⅳ-7]과 같다. 먼저 운용되는 시스템에 대해 망내 물리적 백업 시스템을 구축한다. 백업된 파일은 자료교환시스템을 이용하여 전송만 가능하도록 구축하여 외부와 연결되지 않은 Private 클라우드로 전송한다. 클라우드와 인터넷 연결은 차단하며 바이러스 점검서버는 DVD 등 읽기전용 매체를 이용하여 업데이트를 실시한다. 바이러스 백신은 최소 2개 이상 설치하며 악성코드 점검 이력관리가 가능한 웹사이트를 구성하여 지속적으로 악성코드 이력관리를 한다. 실제 시스템 운용간 악성코드 점검을 위한 데이터 백업과정에서 개인정보, 기밀자료 등 중요데이터가 포함될 수 있기 때문에 악성코드 점검 후 백업자료는 즉시 삭제하는 보안정책 수립이 우선되어야 한다. 또한 내부자료의 외부 유출 방지를 위해 악성코드 점검을 위한 해당 기관 전용 클라우드 기반 악성코드 방역시스템을 구축해야 한다.

단기적인 관점에서 신속한 점검을 위해 노트북 기반 악성코드 점검기법을 제안한다. 노트북내 라이센스가 있는 바이러스 백신 개수(최소 2개 이상)만큼 가상머신 생성 후 가상머신별 1개의 바이러스 백신을 설치한다. 그리고 하드디스크 복제장비를 이용하여 점검대상 PC 및 서버의 하드디스크 이미지 복사 후 주기적인 바이러스 검사를 실시한다. 바이러스 백신 업데이트 최신화를 통한 주기적 점

검시 내부망내 악성코드의 효과적 탐지 및 제거가 가능할 것이다.



[그림 IV-7] 바이러스 점검용 클라우드 구성 방안

하지만 위의 방법은 전장망 기반의 무기체계에 적용가능한 방식이다. 무기체계에 내장된 임베디드용 바이러스 백신 제작을 위한 국방부 차원의 노력이 절실히 필요하다.

한국군 무기체계를 대상으로 바이러스 백신 운용 실태에 대해 확인 후 전략적인 계획에 의거 무기체계에 특화된 전용 바이러스 백신을 제작하는 것이 필요하다. 또한 가용성을 훼손하지 않도록 무기체계별 특징에 맞도록 통합 관리하는 방안도 검토되어야 할 것이다.

4.5.2. 무기체계 사이버 보안 테스트베드 구축 및 운용

국방 무기체계 소프트웨어에 특화된 사이버 보안 테스트베드가 구축되어야 한다. 무기체계의 경우 IoT/임베디드 시스템과 유사한 소프트웨어 환경을 가지고 있다. 물론 기발표된 IoT/임베디드 시스템에 특화된 시큐어코딩 및 개발 가이드가 존재한다. 그러나 대부분 C/C++ 프로그래밍 언어의 시큐어코딩 가이드 혹은 개발 가이드를 참고하였기에 이는 변별력이 부족하다고 볼 수 있다. 따라서 군 관련 개발자 혹은 기술자들의 의견과 지식을 통해 평가척도 및 가중치를 설계한다면 국방 무기체계 소프트웨어 환경에 특화된 평가체계를 연구 및 개발할 수 있다. 또한, 평가결과를 기반으로 무기체계 소프트웨어 환경에서 우선적으로 조치 및 예방이 필요한 보안약점을 선정하면 각기 다른 진단 범위를 가진 보안약점 진단 도구를 적합하게 활용할 수 있다.

국방 무기체계 소프트웨어 특화 보안약점 진단 도구 개발해야 한다. 최근에는 특정 분야와 AI의 융합 연구가 활발하게 이루어지고 있다. 이는 사이버 공격에 대응하기 위한 보안약점 및 보안취약점과 관련된 진단 기법에도 마찬가지로 적용되고 있다. 현재, 프로그램 자동생성 및 디버깅 기술을 통하여 특정 보안약점의 패턴을 분석하고, 이를 기반으로 탐지 및 제거 과정을 자동화하는 연구가 진행되고 있다. 이와 같은 기술을 활용하여 무기체계 소프트웨어에 특화된 보안약점을 탐지하고 제거하는 지능형 진단 도구를 개발한다면 더욱 효율적으로 보안성이 강화된 무기체계 소프트웨어를 개발할 수 있다[61].

무기체계 사이버보안 테스트베드는 안정적인 무기체계 운용을 위해 매우 중요한 요소이다. 우선순위가 매우 높고 중요한 보안취약점이 식별되더라도 무기체계 전용 사이버보안 테스트베드가 없다면 무기체계에 미치는 영향에 대해 안전하게 테스트하고 해결 방안을 마련하는 것은 불가능할 것이다. 단순히 무기체계의 가용성도 중요하지만 국방부 차원의 무기체계별 테스트베드가 구축되어야 한다.

하지만 국방 예산 등을 고려할 경우 모든 무기체계마다 테스트베드 구축은 제한될 것이다. 따라서 핵심적인 체계는 우선순위를 고려하여 테스트베드를 구축하되 무기체계 규모나 중요성에서 우선 순위가 떨어질 경우 공통적인 사이버 보안

테스트를 할 수 있는 실험환경을 구축해야 한다.

미 랜드연구소의 RAND Project AIR FORCE에서 2016년 9월 미 공군 임무 및 무기시스템에서 사이버 보안 및 사이버 복원력에 대한 연구 결과를 공개했다[62]. 목표는 임무 보증을 위해 수용 가능한 수준의 사이버 보안 및 사이버 복원력을 달성하는 것이며 원하는 결과는 적들이 무기 시스템에 대한 사이버 작전 수행 작업을 어렵게 만들고 작전에 대한 사이버 공격의 영향을 최소화하는 것이다. 이를 위한 사이버 매트릭스 개발을 위한 프레임워크 제시를 통해 무기 시스템이나 임무가 사이버 경쟁 환경에서 얼마나 잘 수행될지 예상되는지 나타낸다. 중요한 것은 사이버 매트릭스의 초점은 방어자가 시도할 수 있는 특정 대응책이 아니라 공격자의 예상 성공 또는 실패에 중점을 두어야 한다.

사이버 보안 테스트베드 구축 및 운용간 Red팀과 Blue팀의 운용은 반드시 필요하다. 효과적인 운용을 위해서는 무기체계 사이버 복원력(Cyber Resiliency)의 명확한 기준을 정의하고 무기체계 사이버 보안 테스트를 진행해야 한다.

4.6. 무기체계 사이버보안 강화를 위한 기존 제도 융합 방안

4.6.1. 기반시설 취약점 분석·평가기준 적용 방안

2001년부터 시행된 정보통신기반보호법은 전자적 침해 행위로부터 주요정보통기반시설의 보호에 관한 대책을 수립하고 시행하기 위해 제정되었다. 기반시설 중에서도 전자적인 해킹, 바이러스, 서비스 거부 등 외부 공격으로 인해 공격을 받았을 때 사회적으로 혼란을 불러올 수 있는 시설에 대해 국가적으로 보호하기 위해 지정한 정보통신 기반시설을 말한다.

2001년 4개 부처의 23개 시설에 대해 주요정보통신기반시설을 최초로 지정하였으며, 매년 주요정보통신기반 시설을 추가로 지정하고, 2021년 국가정보보호백서에 의하면 공공 274개, 민간 148개 등 총 422개를 기반시설로 지정하여 관리하고 있다. 주요정보통신기반시설의 지정 대상은 공공기관과 민간이 운영 및 관리하는 정보통신기반시설을 포함한다. 주요정보통신기반시설 점검 시 '기술적 취약점 분석 및 평가 방법 상세가이드'를 기준으로 관리적·물리적·기술적 취약점 점검 항목을 바탕으로 점검하고 있다.

무기체계의 경우 주요정보통신기반시설의 지정 요건에 포함되지 않지만 무기체계의 파괴력을 감안한다면 무기체계 보호분야도 매우 중요하다. 주요정보통신기반시설과 마찬가지로 법률적으로 무기체계에 대한 의무 확인 사항을 추가하여 무기체계에 특화된 점검 기준과 이를 점검할 수 있는 방법을 강구해야 할 것이다.

4.6.2. ISMS-P 인증 제도를 활용한 무기체계 적용 방안

정보보안관리 시스템(ISMS: Information Security Management System)은 기업이 주요 정보자산을 보호하기 위해 수립·관리·운영하는 정보보호 관리체계가 인증기준에 적합한지 심사하여 인증을 부여하는 제도이다. 정보통신망법에 의해 시행되며 정보보호 위험관리를 통한 비즈니스 안정성 제고, 윤리 및 투명 경영을 위한 정보보호 법적 준거성 확보, 침해 사고 및 집단소송 등에 따른 사회·경제적 피해 최소화, 인증 취득시 정보보호 대외 이미지 및 신뢰도 향상 등이 가능하다[63].

정보통신망 이용 보안분야는 측정할 수 있는 것만 관리할 수 있으므로, 정보시스템의 사이버 보안관리를 위해서는 현재와 미래의 보안성을 측정 및 예측해야만 최적적인 보안관리가 가능하다. 보안성을 측정하는 활동을 사이버 위험평가라 할 수 있고 정보시스템의 개발 및 운영 시 필수적인 활동이다. 위험평가의 결과에 따라서 위험관리가 이루어지며 적정수준으로 정보시스템 내의 보안대책(또는 보안통제, 보안기능)을 수립, 구현 및 운영한다. 특히, 운영 중인 정보시스템의 보안성을 강화하기 위한 활동인 정보보안관리 시스템은 관리적, 물리적 및 기술적 보안대책들을 포함한다. 위험관리와 ISMS는 관점만 다를 뿐 유사한 개념이다[64].

앞서 살펴본 봐와 같이 무기체계에 ISMS와 유사한 인증제도를 구축하는 것도 좋은 방법이다. 무기체계별 공동적인 점검 기준을 수립 후 무기체계 인증심사원에 의해 무기체계의 보안수준이 적합한지 점검하고 매년 단위로 체계적으로 후속조치 이행 여부에 대해 지속적으로 모니터링 및 3년 단위 인증 갱신 제도를 도입한다면 획기적인 무기체계 사이버 보안 강화가 가능할 것이다.

4.6.3. 무기체계에 특화된 정보보호 관리체계

사이버사에서는 국방정보체계 점검을 위해 '주요정보통신기반시설 취약점 분석·평가 기준을 적용하고 있다. 하지만 무기체계 점검을 위한 기준으로 적용하기에는 제한되는 부분이 많다. 따라서 정보통신기반시설의 기준과 ISMS 제도의 인증기준을 참고하여 무기체계에 적합한 공통된 무기체계 전용 사이버 보안 인증체계 신설이 필요하다.

주요정보통신 기반시설 취약점 분석·평가 기준은 과학기술정보통신부고시 제2021-103호('21.12.28. 일부개정)를 적용하고 있다. 취약점 분석 단계에서 점검 항목을 도출하고 항목별 점검 기준 도출하여 취약점 평가를 시행한다. 관리적·물리적·기술적 분야별로 점검 기준이 수립되어 있으며 KISA에서 발간하는 '주요 정보통신기반시설 기술적 취약점 분석 평가 상세 가이드'를 기준으로 점검한다. 무기체계 사이버 보안에 적합하도록 점검 항목 및 방법을 재작성하여 최적화 하는 것이 필요하다.

ISMS 인증제도의 경우 관리체계 기반마련, 위험관리, 관리체계 운영, 관리체계 점검 및 개선 프로세스에 대해 체계적으로 인증을 수행하게 된다. 주요정보통신기반시설 취약점 분석·평가기준은 시스템별 점검 기준에 치중한다면 ISMS 인증은 제도적 관리적 측면에 보다 중점을 두고 있다.

따라서 두 가지 제도의 기준을 적용하여 무기체계에 적합한 통합 방안을 마련하여 법령에 의해 반드시 무기체계 사이버 보안을 평가하고 인증하고 개선하는 제도적 장치 마련이 시급하다. 이를 통해 국방분야에서 운용되고 있는 수많은 무기체계에 대해 전수 조사 차원의 보안 취약점 확인이 가능하고 효과적으로 개선이 가능 할 것이다. 위와 같은 문제들을 해소하기 위해 ISMS-W를 제안한다.

1) ISMS-W(Weapon systems) 개요

ISMS-P와 주요정보통신 기반시설 취약점 분석·평가 기준를 통합하여 무기체계 대상 새로운 인증기준인 ISMS-W를 제안한다. ISMS-P에서 개인정보 분야는 제외하였고 무기체계에 부합되는 인증기준들을 적용하되 무기체계와 적합하

도록 용어 및 일부 항목을 수정하였다. 기반시설 점검기준에서는 대부분의 항목들이 ISMS 점검기준에 포함되어 있기 때문에 상세한 항목까지 포함하지 않았다. 우선순위에 있어 ISMS가 제품의 수명주기 전 영역에 대한 절차적 기준과 점검방법을 제시하지만 기반시설 취약점 분석·평가는 관리적인 부분은 전혀 고려하지 않고 시스템별 취약점에 대한 점검기법만 나열하고 있다. 다만, Web 취약점 점검항목의 경우 ISMS 점검 항목에는 상세히 명시되어 있지 않아 SQL인젝션 등 28개 점검항목은 웹취약점 제거항목(2.6.5)에 전부 포함하였다.

ISMS-W는 무기체계 전용 인증 기준을 제안하는 것으로 체크리스트 기반의 주요 확인사항만 제시하였다. 관련 법규, 세부 설명, 증거자료 및 결함사례를 포함할 경우 보안상 영향을 줄 수 있기 때문에 제안하는 내용을 기반으로 무기체계에 적합한 항목을 軍에서 내부적으로 적용하여 작성해야 할 것이다.

제안하는 항목은 ISMS-P 102개 인증기준 항목[그림 Ⅳ-8][65]에서 개인정보 보호 영역은 제외한 ISMS 80개 영역 중 48개 항목을 적용하였고, 물리적 망분리 등 6개 항목은 신설하였다. 4개의 항목은 항목명을 수정하였으며 접근통제(2.2.1)의 경우 7개 항목을 통합하여 1개로 적용하였다.

인증		구분	인증기준 분야별 개수	
ISMS-P (102)	ISMS (80)	1. 관리체계 수립 및 운영 (16)	1.1 관리체계 기반 마련(6)	1.2 위험관리(4)
			1.3 관리체계 운영(3)	1.4 관리체계 점검 및 개선(3)
		2. 보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3)	2.2 인적보안(6)
			2.3 외부자 보안(4)	2.4 물리보안(7)
			2.5 인증 및 권한 관리(6)	2.6 접근통제(7)
			2.7 암호화 적용(2)	2.8 정보시스템 도입 및 개발 보안(6)
			2.9 시스템 및 서비스 운영관리(7)	2.10 시스템 및 서비스 보안관리(9)
			2.11 사고 예방 및 대응(5)	2.12 재해복구(2)
	-	3. 개인정보 처리단계별 요구사항 (22)	3.1 개인정보 수집 시 보호조치(7)	3.2 개인정보 보유 및 이용 시 보호조치(5)
			3.3 개인정보 제공 시 보호조치(4)	3.4 개인정보 파기 시 보호조치(3)
			3.5 정보주체 권리보호(3)	

[그림 Ⅳ-8] ISMS-P 인증기준 항목

ISMS-W에 대한 인증기준에 대한 변경 사항은 [표 Ⅳ-6]과 같다. ISMS의 **P**lan(계획)-**D**o(실행)-**C**heck(평가)-**A**ct(개선)로 이어지는 PDCA를 기반으로 인증 기준을 새롭게 제시한다.

인증	구 분	인증기준 분야별 개수	
ISMS-W (45)	1. 관리체계 수립(5)	1.1 보안정책(5)	•
	2. 보호대책 구현 (38)	2.1 망분리(1)	2.2 접근통제(1)
		2.3 인증 및 권한관리(4)	2.4 암호화 적용(2)
		2.5 무기체계 운용관리(5)	2.6 무기체계 보안관리(9)
		2.7 사고예방 및 대응(3)	2.8 인원 보안(8)
		2.9 시설 보안(5)	•
	3. 점 검(1)	3.1 무기체계 점검(1)	•
	4. 개 선(1)	4.1 무기체계 개선(1)	•

[표 IV-6] ISMS-W 인증기준 제안

2) ISMS-W 인증 기준

영 역	분 야	항목	ISMS-P
1. 관리 체계 수립	1.1 보안 정책	1.1.1 범위 설정	1.1.4 범위 설정
		1.1.2 자산 식별	1.2.1 정보자산 식별
		1.1.3 운영현황 관리	1.3.3 운영현황 관리
		1.1.4 자산 관리	2.1.3 정보자산 관리
		1.1.5 보호대책 구현	1.3.1 보호대책 구현
2. 보호 대책 구현	2.1 망분리	2.1.1 물리적 망분리	신설 항목
	2.2 접근통제	2.2.1 무기체계 접근통제	2.6.1 네트워크 접근 2.6.2 정보시스템 접근 2.6.3 응용프로그램 접근 2.6.4 데이터베이스 접근 2.6.5 무선 네트워크 접근 2.6.6 원격접근 통제 2.6.7 인터넷 접근 통제
	2.3 인증 및 권한 관리	2.3.1 계정 관리	2.5.1 사용자 계정 관리 2.5.2 사용자 식별
		2.3.2 사용자 인증	2.5.3 사용자 인증
		2.3.3 비밀번호 관리	2.5.4 비밀번호 관리
		2.3.4 관리자 계정 및 권한관리	2.5.5 관리자 계정 및 권한 관리
	2.4 암호화 적용	2.4.1 암호정책 적용	2.7.1 암호정책 적용
		2.4.2 암호키 관리	2.7.2 암호키 관리

영 역	분 야	항목	ISMS-P
2. 보호 대책 구현	2.5 무기체계 운용 관리	2.5.1 변경 관리	2.9.1 변경 관리
		2.5.2 성능 및 장애관리	2.9.2 성능 및 장애관리
		2.5.3 백업 및 복구	2.9.3 백업 및 복구
		2.5.4 로그 관리 및 점검	2.9.4 로그 및 접속기록 관리 2.9.5 로그 및 접속기록 점검
		2.5.5 자산 재활용 및 폐기	2.9.7 자산 재활용 및 폐기
	2.6 무기체계 보안 관리	2.6.1 정보보호 시스템 운영	2.10.1 보안시스템 운영
		2.6.2 무기체계 단말기 보안	2.10.6 업무용 단말기 보안
		2.6.3 취약한 서비스 통제	신설 항목
		2.6.4 비인가SW 통제	신설 항목
		2.6.5 웹 취약점 제거	신설 항목
		2.6.6 공격표면 식별 및 통제	신설 항목 2.10.7 보조저장매체 관리
		2.6.7 바이러스 방역체계	2.10.9 악성코드 통제
		2.6.8 패치 관리	2.10.8 패치 관리
		2.6.9 클린PC 관리	신설 항목
	2.7 사고예방 및 대응	2.7.1 취약점 점검 및 조치	2.11.2 취약점 점검 및 조치
		2.7.2 이상행위 분석 및 모니터링	2.11.3 이상행위 분석 및 모니터링
		2.7.3 피해복구 시험 및 개선	2.12.2 재해복구 시험 및 개선
2. 보호 대책 구현	2.8 인원 보안	2.8.1 주요직무자 지정 및 관리	2.2.1 주요 직무자 지정 및 관리
		2.8.2 인식제고 및 교육훈련	2.2.4 인식제고 및 교육훈련
		2.8.3 전역 및 직무변경 관리	2.2.5 퇴직 및 직무변경 관리
		2.8.4 보안 위반 시 조치	2.2.6 보안 위반 시 조치
		2.8.5 외부자 현황 관리	2.3.1 외부자 현황 관리
		2.8.6 외부자 계약시 보안	2.3.2 외부자 계약시 보안
		2.8.7 외부자 보안이행 관리	2.3.3 외부자 보안이행 관리
		2.8.8 계약변경 및 만료시 보안	2.3.4 계약변경 및 만료시 보안
	2.9 시설 보안	2.9.1 출입통제	2.4.2 출입통제
		2.9.2 정보시스템 물리적 보호	2.4.3 정보시스템 보호
		2.9.3 보호설비 운영	2.4.4 보호설비 운영
		2.9.4 보호구역 내 작업	2.4.5 보호구역 내 작업
		2.9.5 반·출입 기기 통제	2.4.6 반출입 기기 통제
3. 점검	3.1 무기체계 점검	3.1.1 무기관리체계 점검	1.4.2 관리체계 점검
4. 개선	4.1 무기체계 개선	4.1.1 무기관리체계 개선	1.4.3 관리체계 개선

3) ISMS-W 인증 항목별 주요 확인사항

분 야	항목	주요 확인사항
1.1 보안정책	1.1.1 범위 설정	• 무기체계가 누락되지 않고 관리체계 범위에 포함되었는가? • 무기체계 관리 범위에서 제외될 경우 명확한 근거 및 지휘관 승인 등 근거를 기록하여 관리하는가? • 무기체계 관리 범위 설정 관련 관리 대상을 문서로 작성하였는가?
	1.1.2 자산 식별	• 무기체계 관리대상의 모든 범위를 식별 후 누락없이 관리중에 있는가? • 식별된 무기체계에 대해 지휘관 승인 후 적절한 보호등급을 부여하였는가? • 정지적인 자산 확인을 통해 무기체계 현황을 최신화 하고 있는가?
	1.1.3 운영 현황 관리	• 주간, 월간, 분기 단위 또는 수시 수행해야 되는 무기체계 정보보호 활동에 대해 문서로 작성하여 관리중에 있는가? • 지휘관은 무기체계 운영 활동에 대해 주기적으로 확인 및 관리를 하고 있는가?
	1.1.4 자산 관리	• 무기체계의 보호수준에 따른 취급절차(생성·도입, 저장, 이용, 파기)와 보호대책을 정의 후 이행중에 있는가? • 무기체계별 운용실무자와 책임자를 적절히 선정 후 관리하고 있는가?
	1.1.5 보호대책 구현	• 보호대책서에 따른 보호 대책을 구현 후 실시 결과를 지휘관(부서장)에게 보고하고 있는가? • 인증기준에 따른 보호대책 및 운영 현황을 구체적으로 작성였는가?
2.1 망분리	2.1.1 물리적 망분리	• 무기체계를 외부망과 물리적으로 분리 운영하고 있는가? • 외부망(내부망 또는 타 전장망 등)과의 연결접점에 대해 불가피할 경우 일방향 전송을 실시하고 있는가? • 타체계와 연동이 필요할 경우 관련 보안절차를 준수하였는가?
2.2 접근통제	2.2.1 무기체계 접근통제	• 서버, 네트워크, 응용프로그램, DB 등 무기체계에 접근 가능한 모든 경로 식별 후 접근통제 정책을 반영하여 승인된 사용자만 접근 가능하도록 통제하고 있는가? • 네트워크 영역에 대한 물리적 또는 논리적 분리 후 각 영역간의 접근통제 정책을 제대로 적용중에 있는가? • 시스템 접속 후 업무 미처리 시간이 사전 규정된 시간을 초과할 경우 자동으로 접속을 차단하고 있는가? • 원격으로 정보시스템 접속은 금지하되 부득이한 경우 승인권자의 승인 후 특정 단말기에 한해서만 접근을 허용하는가?
2.3 인증 및 권한관리	2.3.1 계정 관리	• 계정과 접근권한에 대한 등록·변경·삭제 시 공식적인 절차를 수립 후 적용중에 있는가? • 운용자 직무에 따른 접근권한 분류 기준에 따라 필요한 최소한의 권한을 부여하고 있는가? • 운용자를 명확히 확인할 수 있는 식별자를 할당하고 추정 가능한 식별자 사용을 제한하는가?

분 야	항목	주요 확인사항
2.3 인증 및 권한관리	2.3.2 사용자 인증	• 무기체계 접근 시 무분별한 로그인 통제, 불법 로그인 경고 등 사용자 인증 절차를 준수하고 있는가? • 외부에서 접속하려는 경우에는 안전한 인증 및 적합한 보안 절차를 준수하고 있는가?
	2.3.3 비밀번호 관리	• 사용자 비밀번호 설정 시 작성규칙을 준수하고 있는가? • 규정에 적합한 비밀번호 작성 정책을 수립 후 이행중에 있는가?
	2.3.4 관리자 계정 및 권한 관리	• 관리자 계정 권한 신청 및 승인 절차를 수립 후 최소 인원에게 권한을 부여하고 있는가? • 관리자 계정 및 권한에 대해 식별하고 통제절차를 준수하는가?
2.4. 암호화 적용	2.4.1 암호정책 적용	• 보호대책에 명시된 무기체계별 암호정책을 준수하고 있는가? • 암호정책을 준수하여 암호화를 수행하고 있는가?
	2.4.2 암호키 관리	• 보호대책에 부합되는 암호키 관리 절차를 수립 후 이행 하는가? • 안전한 장소에 암호키를 보관하고 암호키 사용 시 최소한의 접근 권한을 부여하고 있는가?
2.5 무기체계 운용 관리	2.5.1 변경 관리	• 무기체계의 주요 자산 변경 시 관련 절차 수립 후 적용하고 있는가? • 주요 자산 변경 前 성능 및 보안 영향 분석 후 적절히 적용하고 있는가?
	2.5.2 성능 및 장애 관리	• 무기체계 성능과 용량에 대해 모니터링 체계를 구축하여 가용성을 보장하고 있는가? • 무기체계 성능과 용량 모니터링을 통해 임계치를 초과 할 경우 대응 절차를 준수하고 있는가? • 가용성을 제한하는 무기체계 장애 발생 시 즉각적인 확인 및 대응을 위한 구체적인 절차를 수립하고 이행하고 있는가? • 무기체계 장애 발생 시 보고 절차 준수 및 조치 내역을 기록 후 관리하고 있는가? • 무기체계에 심각한 장애를 초래할 경우 원인분석을 통해 적절한 대책을 수립하였는가?
	2.5.3 백업 및 복구	• 규정에 적합한 백업 및 복구 절차를 수립하여 정상적으로 이행하고 있는가? • 백업 자료에 대해 주기적으로 복구 훈련을 하고 있는가? • 재난에 따른 가용성 보장을 위해 백업 매체를 물리적으로 이격된 장소에 보안성이 담보된 상태로 안전하게 보관하고 있는가?

분 야	항목	주요 확인사항
2.5 무기체계 운용 관리	2.5.4 로그 관리 및 점검	• 무기체계 관련 시스템의 로그관리 절차를 준수하여 로그 생성 후 보관하고 있는가? • 별도의 저장매체에 로그를 백업하고 로그기록 접근권한은 최소화 하여 관리하고 있는가? • 규정에 명시된 접속기록 보관 기간을 준수하여 안전하게 보관하는가? • 로그에 대한 적절한 검토와 모니터링을 통해 시스템 오류, 비인가 접속 등 이상 징후에 대해 사전 인지할 수 있도록 임무를 수행하고 있는가? • 로그 및 모니터링 검토 결과를 상급자에게 보고 후 이상 징후에 대한 규정된 절차를 준수하고 있는가?
	2.5.5 자산 재활용 및 폐기	• 무기체계의 재사용 및 폐기 절차를 수립 후 준수하고 있는가? • 무기체계 정보자산과 저장매체의 경우 재사용 및 폐기시 규정된 방법에 의해 안전하게 처리하고 있는가? • 정보자산과 저장매체 폐기 시 적절한 폐기이력을 남기고 관련 자료를 보관하고 있는가? • 외부업체를 통해 정보자산과 저장매체 폐기 시 계약서에 폐기 절차를 명시 후 완전 폐기 여부에 대해 확인하는가? • 무기체계 유지보수 및 정비 시 저장매체에 대한 교체, 복구 소요 발생 시 저장매체 임의 유출 방지 대책을 수립하여 적용하는가?
2.6 무기체계 보안 관리	2.6.1 정보보호 시스템 운영	• 무기체계 정보보호시스템 운영 관련 지침에 적합한 절차를 수립하여 준수하고 있는가? • 정보보호시스템 관리자 인원 최소화 및 비인가자 통제 방안을 수립하여 철저하게 준수하는가? • 정보보호시스템 보안정책 추가, 수정, 삭제 등 설정 변경 시 공식적인 절차에 의해 수행 하는가? • 정보보호시스템 예외정책 등록 시 관련 절차 준수하고 있으며 예외 정책 계정의 권한은 최소한으로 설정하여 관리하는가? • 정보보호시스템에 적용한 보안정책에 대해 주기적으로 검토하여 최신화 하고 있는가?
	2.6.2 무기체계 단말기 보안	• 무기체계 단말기에 기기인증, 접근범위 설정, 보안프로그램 설치 등 보안통제 정책을 적용하고 있는가? • 자료공유 프로그램 사용 금지, 공유 금지, 무선망 사용 통제 등 적합한 보안정책을 준수하고 있는가? • 단말기 분실, 도난 시 중요정보 노출 방지를 위한 보안대책을 적용하고 있는가? • 단말기 접근통제 정책의 적절성을 정기적으로 확인하고 있는가?

분 야	항목	주요 확인사항
2.6 무기체계 보안 관리	2.6.3 취약한 서비스 통제	• 관리자의 원격 접속 허용은 금지되었는가? • 시스템 정보유출 및 DoS공격에 악용될 수 있는 보안 취약 서비스(snmp, echo, daytime 등)를 해제하였는가? • 내부 네트워크를 통해 서버, 네트워크, 정보보호시스템 등을 운영하거나 관리자 웹페이지에 접속하는 경우 지정된 단말기를 통해서만 접근할 수 있도록 통제되어 있는가? • 평문으로 소통하는 원격연결 서비스 사용을 금지하였는가? • 기타 보안에 취약한 서비스 사용 차단 등 적절한 통제를 하고 있으며 관련 근거를 유지하고 있는가?
	2.6.4 비인가 SW 통제	• 인가된 SW만 설치되어 있는가? • SW 반입 절차를 준수하고 있는가? • 무기체계 운용간 검증된 필수 보안프로그램이 설치 · 운용되고 있는가? • 비인가 SW 반입통제를 위해 주기적으로 점검을 하고 있는가? • P2P, 웹하드, 메신저 등 불필요 인터넷 접속SW가 설치되어 있는가?
	2.6.5 웹 취약점 제거	• 주요정보통신기반시설 취약점 가이드에 있는 버퍼 오버플로우, 포맷스트링 등 28개 취약점에 대해 점검 후 조치하였는가? • 웹 서비스별 신규 공개된 취약점에 대해 식별 후 조치하였는가?
	2.6.6 공격표면 식별 및 통제	• 비인가 정보통신장비를 무단 반입하거나 시스템에 접속한 흔적이 있는가? • 사용하지 않는 USB · LAN 포트 등 입출력장치 단자는 물리적으로 봉인조치를 하고 있는가? • 운용중인 시스템에 승인하지 않은 정보통신장치가 설치되어 있는가? • 사용 중인 무기체계의 모든 저장매체에 대해 라이프 사이클에 맞도록 적합한 보안정책을 수립 후 적용하고 있는가? • 무기체계 저장매체 현황 및 관리 실태에 대해 정기적으로 점검하는가? • 저장매체를 통한 악성코드 감염 방지 대책을 준수하고 있는가? • 보조저장매체는 물리적으로 안전한 장소에 잠금장치 후 보관하고 있는가?
	2.6.7 바이러스 방역체계	• 악성코드로부터 무기체계를 안전하게 보호하기 위해 규정된 보호대책을 준수하고 있는가? • 백신 및 보안프로그램 등을 통해 지속적으로 악성코드 검사 및 예방조치를 실시하고 있는가? • 백신 및 보안프로그램은 최신 상태를 유지 할 수 있도록 지속적으로 업데이트를 실시하며 중대한 취약점 발생 시 신속히 보안업데이트를 하는가? • 악성코드 감염 시 규정된 절차에 의해 수행하고 있는가?

분 야	항목	주요 확인사항
2.6 무기체계 보안 관리	2.6.8 패치 관리	• 무기체계 중요도에 따라 운영체제 및 소프트웨어 패치관리를 적절하게 수행하고 있는가? • 무기체계에 설치된 장비별 패치 현황에 대해 최신화하여 관리하는가? • 무기체계 최신 패치 적용 시 가용성 보장대책을 마련하고 있는가? • 최신 패치 적용 제한 시 규정된 절차에 의해 추가 대책을 마련했는가? • 인터넷 직접 접속을 통한 패치를 제한하고 있는가? • 패치관리시스템 활용 시 적절한 보호대책을 강구하였는가?
	2.6.9 클린PC 관리	• 클린PC는 무기체계 전용으로 운용하고, PC보호 및 복구솔루션 등을 이용하여 부팅시마다 초기 PC상태로 복구되도록 설정하였는가? • 불가피하게 USB 등 저장매체를 이용하여 업데이트, 보안패치, 파일 전송 前 클린PC에서 백신 검사를 실시 하는가? • 클린PC 사용시 최신 백신 업데이트 방안이 포함되어 있으며, 국내•외 백신 등 다양한 백신을 설치하였는가? • 클린PC 사용내역을 기록 및 관리하고 있는가?
2.7 사고예방 및 대응	2.7.1 취약점 점검 및 조치	• 정기적으로 무기체계 취약점 점검을 수행하고 있는가? • 취약점 점검간 식별된 보안 취약점은 책임자에게 보고 후 적절한 보안대책을 강구하고 있는가? • 운용 중인 무기체계와 관련된 시스템의 최신 보안 취약점을 주기적으로 확인 및 분석 후 적절하게 조치하고 있는가? • 무기체계 취약점 점검 결과는 이력으로 유지하고 동일한 취약점이 재발생하지 않도록 적절한 대책을 강구하였는가?
	2.7.2 이상행위 분석 및 모니터링	• 무기체계에 대한 침해 행위를 식별할 수 있도록 모니터링 및 이상행위 분석 체계를 구축하고 있는가? • 침해 행위 및 자료 유출 등 이상 행위 판단을 위한 기준과 임계치를 정의하고 주기적인 분석을 통해 적절한 후속 조치를 강구하고 있는가?
	2.7.3 피해복구 시험 및 개선	• 재해 복구 계획에 대한 주기적인 이행을 통해 적절성을 확인하고 있는가? • 정보체계의 환경 변화와 재해복구 실시 결과 등을 분석하여 복구전략 및 대책에 대해 주기적으로 확인하고 있는가?

분 야	항목	주요 확인사항
2.8 인원 보안	2.8.1 주요직무자 지정 및 관리	• 무기체계별 주요 직무 기준에 대해 정확하게 수립하였는가? • 무기체계별 주요 직무자 지정 후 현황을 최신화 하여 관리중에 있는가? • 업무 필요성에 따라 주요 직무자를 최소화 하는 등 관리방안을 수립·이행하고 있는가?
	2.8.2 인식 제고 및 교육 훈련	• 세부적인 연간 정보보호 계획을 수립하고 지휘관의 승인을 받고 있는가? • 연간 교육계획에 의거 연 1회 이상 관리체계에 포함된 내·외부자를 대상으로 정기적인 교육을 시행하고, 법규와 규정의 중대한 변경사항 발생 시 추가적인 교육을 실시하였는가? • 내·외부자에 대해 업무시작 前 정보보호 교육을 시행하였는가? • 무기체계 운용실무자는 정보보호 전문성 향상을 위한 대·내외 교육을 받았는가? • 교육 시행 결과는 근거를 유지하고, 평가 및 분석 사항을 향후 교육 계획에 반영하였는가?
	2.8.3 전역 및 직무 변경 관리	• 전역, 보직 변경 및 퇴사 등 인사 관련 변경사항 발생시 무기체계 운영 부서간 공유하고 있는가? • 내·외부자 직무변경에 따른 정보체계 권한 삭제 등 관련 규정에 따른 절차를 준수하는가?
	2.8.4 보안 위반 시 조치	• 보안 위반 발생 시 내·외부자에 대해 적절한 처벌 규정을 수립하였는가? • 보안위반자에 대해 규정된 절차에 의거 처벌하고 근거를 유지하고 있는가?
	2.8.5 외부자 현황 관리	• 무기체계 관련 외부자 현황을 관리하고 있는가? • 외부자 업무위탁에 따른 위험 요소를 사전에 파악하고, 이와 관련된 적절한 보호대책을 수립하였는가?
	2.8.6 외부자 계약 시 보안	• 외부자 계약 시 정보보호 역량을 반영하였는가? • 외부자 계약에 따른 보안 요구사항을 명확히 식별 후 계약서에 포함하였는가? • 외부자에게 무기체계 개발 시 계약서에 정보보호 요구사항을 포함하였는가?

분 야	항목	주요 확인사항
2.8 인원 보안	2.8.7 외부자 보안이행 관리	• 계약서 및 내부정책에 포함된 외부자 정보보호 요구사항에 대해 수시 확인 및 점검하고 있는가? • 수시 확인 및 점검간 식별된 외부자의 보안 취약점에 대해 적절한 대책을 수립하여 이행하였는가?
	2.8.8 계약 변경 및 만료 시 보안	• 외부자 계약 종료 시 계정 삭제, 서약서 작성 및 정보자산 반납 등의 적절한 대책을 수립하여 확인하였는가? • 외부자 계약 종료에 따라 외부자 보안점검 및 중요정보 회수 및 파기 절차를 수립 후 이행하였는가?
2.9 시설 보안	2.9.1 출입 통제	• 설정된 보호구역의 출입 절차를 준수하여 적절히 통제하고 있는가? • 보호구역 출입 기록은 규정된 기간동안 보유하고, 출입기록과 출입권한에 대해 정기적으로 검토하였는가?
	2.9.2 정보시스템 물리적 보호	• 무기체계 특성 등을 고려하여 설치 장소를 구분하였는가? • 무기체계의 설치 위치를 쉽게 확인할 수 있는가? • 통신 및 전기선의 물리적 손상과 전기적 간섭을 방지하기 위한 대책을 마련 후 적용하고 있는가?
	2.9.3 보호설비 운영	• 자연재해 및 인재로부터 무기체계를 보호하기 위해 보호구역별 규정된 설비를 갖추고 적절하게 운영하는가?
	2.9.4 보호구역내 작업	• 무기체계 설치 및 유지보수 등 보호구역에서 작업 할 경우 공식 작업절차를 수립하여 이행하고 있는가? • 공식적인 작업 절차에 따라 보호구역 작업이 적절히 통제되며, 정기적으로 작업 기록에 대해 검토하였는가?
	2.9.5 반 · 출입 기기통제	• 무기체계와 관련된 작업 시 반출입 장비를 철저히 확인하여 정보유출 및 악성코드에 감염되지 않도록 적절한 통제 절차 수립 후 이행하고 있는가? • 반 · 출입 이력을 철저히 기록하고, 주기적으로 이력에 대한 확인 후 점검하고 있는가?

분 야	항목	주요 확인사항
3.1 무기체계 점검	3.1.1 무기관리 체계점검	• 무기체계에 대한 정보보호 관리체계가 효과적으로 적용되고 있는지 확인할 수 있도록 전 분야에 대한 적절한 점검 계획을 수립하였는가? • 점검 수행 인력은 독립성과 객관성, 전문성을 갖춘 인력으로 편성하여 연 1회 이상 점검 후 식별된 문제점에 대해지휘관에게 보고하였는가?
4.1 무기체계 개선	4.1.1 무기관리 체계개선	• 보안 요구사항 준수 여부 검토 및 관리체계 대상 점검을 통해 식별된 문제점에 대한 근본적인 원인 분석 후 적절한 개선 대책을 적용하고 있는가? • 선정된 개선대책에 대해 정확성과 효과성을 확인 할 수 있는 기준과 절차를 수립하였는가?

4) ISMS-W 적용 방법

ISMS-P의 인증기준은 법적인 구속력과 더불어 실제 정보보호 관리체계 수립에 기여하고 있다. 이를 준용한 인증 기준과 주요 확인사항은 軍에서 사용하는 용어로 일부 수정하였으나, 큰 틀에서의 변경은 없기 때문에 정보보호 관리체계 수립, 운영, 점검 및 개선을 통해 무기체계의 사이버 보안 강화에 기여할 수 있을 것이다. 본 논문에서는 체크리스트 기반의 주요확인 사항에 대해 제시하였으나 이를 효과적으로 구현하기 위해서는 ISMS-W의 제도적 기반이 마련되어야 한다. 무기체계 관련 정책기관, 인증기관, 심사기관이 지정되어야 하며, 무기체계별 인증대상 및 기준이 구분되어야 한다. 또한 심사 절차가 마련되어야 하며, 인증 유지를 위한 최초심사, 사후심사, 갱신심사를 ISMS-P와 같이 3년 주기로 실시하여야 한다. 그리고 인증에 따른 혜택과 벌칙이 있어야 한다. 혜택은 무기체계 관련 보안사고 발생 시 처벌에 대한 감경 조항이 포함되며, 벌칙은 해당 부대에 기관경고 및 우수부대 선발 제외 등 적합한 불이익이 선정되어야 한다. 그리고 시행간 인증기준 및 체크리스트에 대한 지속적인 보완이 필요할 것이다.

Ⅴ. 결 론

본 논문에서는 무기체계 사이버 보안 강화를 위한 다양한 방안을 제시하였다. 무기체계 사이버 보안 강화는 선택이 아닌 필수 사항으로 이를 소홀히 할 경우 예상치 못한 피해 발생이 우려된다. 정밀 유도미사일의 좌표가 적의 공격에 의해 좌표가 변경된다면 외교적 문제를 넘어 국가 존립에 까지 영향을 미칠 수 있는 중대한 사항이다.

국내에서는 아직까지 무기체계 운용간 사이버 보안 강화를 위한 보안정책 수립이 걸음마 단계에 있다. 미국처럼 사이버 보안 분야별 법률적 지원 下 체계적인 보안정책 수립이 필요하다. 국내 무기체계 사이버 보안분야에 대한 연구는 2017년부터 본격적으로 시행되고 있어, 무기체계 도입 초창기부터 사이버 보안 강화를 위해 노력해온 미국의 사례를 교훈 삼아 우리나라 무기체계 사이버 보안 정책의 토대를 마련해야 된다는 것을 알 수 있었다.

무기체계 강화를 위한 제도적 기틀을 수립하고, 민간 분야와 적극적인 교류와 협력을 통해 국방분야는 내부자에 의해서만 발전시켜야 한다는 고정 관념에서 탈피하고 시대 흐름에 부합되도록 민간 영역의 사이버 보안 인재들에 대해 국방부 차원에서 활용하고 적재적소에 배치할 수 있도록 개선해야 한다.

그리고 본 논문에서는 무기체계 사이버 보안 강화를 위한 보안정책과 軍 무기체계 정보보호관리체계에 특화된 ISMS-W를 제안하였다. 각각의 제안들에 대해 보다 구체적이며 세부적으로 발전시켜 나가야 한다. 무기체계 사이버 보안을 강화하기 위해서는 지속적인 연구가 필요하다. 특히 무기체계 개발 시 무기체계에 특화된 소스코드 검증방안이 수립되어야 하며, 무기체계 운용 간 가용성을 보장하면서 효과적인 무기체계 보안취약점을 진단 할 수 있는 방법과 도구가 개발되어야 한다. 그리고 해외 구매 무기체계의 경우 계약 단계에서 우리군에 필요한 보안요구 사항에 대해 명확히 정의되고 반영하고, 운용 단계에서 보안 요구사항 준수 여부를 확인할 수 있는 절차에 대해 지속적인 연구가 필요하다.

참 고 문 헌

[1] GAO 'WEAPON SYSTEMS CYBERSECURITY DOD Just Beginnin to Grapple with Scale of Vulnetabilities'. 2018.10
https://www.gao.gov/products/gao-19-128 (접속일 : 22년 3월 30일)

[2] 방위사업법(시행 2021. 4. 1.) 제3조

[3] 방위사업법 시행령(시행 2022. 2.11.) 제2조

[4] 국방전력발전업무훈령(국방부훈령 제2639호, 2022. 3.18. 일부 개정) 별표4 무기체계 세부분류

[5] 국방전력발전업무훈령(국방부훈령 제2639호, 2022. 3.18. 일부개정) 별표1 용어의 정의 7

[6] 국방전력발전업무훈령(국방부훈령 제2639호, 2022. 3.18. 일부개정) 별표1 용어의 정의 8

[7] 국방전력발전업무훈령(국방부훈령 제2639호, 2022. 3.18. 일부개정) 제8조

[8] 한장근, 이재우. (2016). 자주적 국방역량강화를 위한 무기체계SW 국산화 전략고찰. 정보과학회지, 34(10), 10-11.

[9] 방사청 무기체계 SW 정책 및 제도 소개 자료(2021. 8. 3.) :
https://www.dapa.go.kr/dapa/na/ntt/selectNttInfo.do?bbsId=362&nttSn=39322&menuId=689
(접속일 : 22년 3월 2일)

[10] 국방전력발전업무훈령(국방부훈령 제2639호, 2022. 3.18. 일부개정) 별표5 전력지원체계 세부분류

[11] 국방정보화업무훈령(국방부훈령 제2576호, 2021. 8.12. 일부개정) 제5조 국방정보시스템의 범주 및 분류

[12] 국방정보화업무훈령(국방부훈령 제2576호, 2021. 8.12. 일부개정) 별표2 국방정보시스템 분류

[13] 방사청 무기체계 SW 정책 및 제도(2021. 8. 3.) : https://www.dapa. go.kr/dapa/na/ntt/selectNttInfo.do?bbsId=362&nttSn=39322&menuId=689 (접속일 : 22년 3월 30일)

[14] 국방전력발전업무훈령(국방부훈령 제2639호, 2022. 3.18. 일부개정) 별표3 무기체계 획득 절차도

[15] 국방정보화업무훈령(국방부훈령 제2576호, 2021. 8.12. 일부개정) 별표8 국방정보화사업 업무 흐름도

[16] 김종화, 김용철, 김경민, 강정흥. (2019). 안전한 공급망 관리를 위한 국방사이버보호 파트너십 인증 방안. 융합보안논문지, 19(3), 104.

[17] 정용태, 정현식, 강지원. (2019). 무기체계 수명주기 간 사이버보안 적용 개선 방안. 융합보안논문지, 19(2), 68-73.

[18] 이지섭, 차성용, 백승수, 김승주. (2018). 무기체계의 사이버보안 시험평가체계 구축방안 연구. 정보보호학회논문지, 28(3), 765-774.

[19] 이미화, 윤지원. (2018). 망혼용단말 탐지방법에 대한 연구 및 자동탐지시스템 구현. 정보보호학회논문지 2018. 4, 457-469.

[20] 김두환, 박호정. (2017). 군 보안상 해킹 대응 방안에 관한 연구. 융합보안논문지, 17(5), 133-142.

[21] 윤정환. (2018). 넷리스트의 특성을 이용한 FPGA 하드웨어 악성기능 탐지기법 연구. 연세대 석사학위논문, 8-9.

[22] 박시우, 김법연, 권헌영. (2022). 국방 신속획득제도의 한계와 개선 방안 : 신기술 활용의 통합적 관리 문제를 중심으로. 국방정책연구 135, 163-205.

[23] 안광현, 이한희, 박원형, 강지원. (2020). 국방 네트워크 환경에서 ATT&CK 기반 취약점 완환 체계 구축 방안. 융합보안논문지, 20(4), 136-140.

[24] 최준성, 왕핑, 국광호. (2016). 무기체계 내장형 소프트웨어 침투테스트 환경 특성 분석. 한국통신학회 2016년도 추계종합학술발표회, 204-205.

[25] 주예나, 김범수, 권혁진. (2021). 한국형 RMF 체계구축을 위한 위험우선순위 식별 방법론 제언. 국방정책연구, 37(2), 99-130.

[26] 조현석, 차성용, 김승주. (2019). 국내 무기체계에 대한 RMF 적용 실 사례 연구. 정보보호학회논문지, 29(6), 1463-1475.

[27] 이용석, 최정민. (2020). 한국군에 RMF 적용방안 연구. 한국정보통신학회논문지, 45(12), 2132-2139.

[28] Department of Defense, Cybersecurity Test and Evaluation Guidebook Version 2.0, change 1(2020. 2.10.)

https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/Cybersecurity -Test-and-Evaluation-Guidebook-Version2-change-1.pdf

[29] 유국남, 박규철. (2021). 국방과 기술, 514호, 84-89.

[30] 김소연, 김성표, 밤범준, 정운섭, 추헌우, 윤정, 김진용. (2021). 사이버전 기술 및 발전방향. 한국전자파학회논문지, 32(2), 119-126.

[31] 정연오. (2018). 무기체계 소프트웨어 보안성 확보를 위한 개발 방법론 연구. 한국정보과학회 학술발표논문집, 2018.6, 77-79.

[32] 김종복, 조인준. (2018). 안전한 무기체계 소프트웨어를 위한 취약점 분석 기법에 관한 연구. 한국콘텐츠학회논문지, 18(8), 459-468.

[33] Industrial Control Systems Cyber Emergency Response Team. (2016), Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Pages 4-6, https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508.C.pdf

[34] Cybersecurity & Infrastructure Security Agency 홈페이지 https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_CSET_S508C.pdf

[35] https://csiac.org 홈페이지 (접속일 : 22년 4월 1일)

[36] 오광환, 김권일, 차정훈. (2021). 방산인력 기술유출 방지를 위한 실태분석 및 개선방안. 한국산업보안연구, 11(1), 435-458.

[37] 박혜성, 권헌영. (2019). 한국 버그 바운티 프로그램의 제도적인 문제점과 해결방안. 한국IT서비스학회지, 18(5), 53-70.

[38] DARPA Cyber Grand Challenge(CGC) 홈페이지
https://www.darpa.mil/program/cyber-grand-challenge
(접속일 : 22년 3월 1일)

[39] Thanassis Avgerinos, David Brumley, John Davis, Ryan Goulden, Tyler Nighswander, Alex Rebert, and Ned Williamson. (2018), The Mayhem Cyber Reasoning System. IEEE Security & Privacy Volume 16, Issue 2, Pages 52-60, https://doi.org/10.7249/RR2703

[40] Military & Aerospace Electronics, ForAllSecure to provide cyber security for weapon systems
https://www.militaryaerospace.com/trusted-computing/article/14176650/cyber-security-weapon-systems-test
(접속일 : 22년 3월 29일)

[41] 유진철, 문상우, 김종화. (2020). 국방정보시스템에서의 랜섬웨어 위협 대응 방안:정보보안 위험관리 관점에서. 융합보안논문지, 20(5), 76-78.

[42] 정희진, 김진국, 종승훈, 김희동, 김현숙. (2017). 무기체계 내장형 소프트웨어 보안약점 식별방법론. 한국정보과학회 학술발표논문집, 2017.12, 149-151.

[43] 박태훈, 이성영, 이향진. (2019). 한국과 미국의 사이버안보 전략과 보안 환경 예측. 국방과 보안, 1(2), 58-60.

[44] 김종화, 임재성. (2018). 사이버 위협 대응을 위한 軍 정보화자산관리시스템과 연계한 軍 취약점 관리방안. 융합보안논문지, 18(1), 113.

[45] 채재병. (2019). 국제 사이버공격 전개 양상 및 주요국 대응전략. 국가안보전략연구원 연구보고서 2019-18, 101.

[46] 장경준. (2018). 방위산업기술 자료의 외부 반출 시 보호 방안. 정보보호학회지, 28(6), 50-55.

[47] 박홍순. (2018). 방위산업 사이버 보안을 위한 방산 정보 공유·분석센터(ISAC) 설립 방안. 정보보호학회논문지, 28(6), 60-61.

[48] 이승배. (2020). 사이버보안 강화 측면의 미국 국방 기술 및 사업 보호 정책 변화. 국방과 기술, 502호, 104-111.

[49] https://www.acq.osd.mil/cmmc/about-us.html 홈페이지(접속일 : 22년 4월 1일)

[50] U.S. Department of Defense. (2021). Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle

[51] 이용준. (2020). 국방 ICT 공급에 대한 보안 위협 대응 방안. 융합보안논문지, 20(4), 126-133.

[52] 방사청 2022-2026 “방위산업기술보호 종합계획”(2021.12.)

[53] 홍준호, 유현우. (2017). 화이트 해커 양성 및 활성화 방안에 대한 연구. 한국법학회 법학연구, 17(4), 463-515.

[54] DoD Cyber Excepted Service(CES) : https://public.cyber.mil/cw/dod-cyber-excepted-service-ces/ (접속일 : 22년 5월 3일)

[55] DoD 2022 Department of Defense Cyber Excepted Service Pay Rates : https://dl.dod.cyber.mil/wp-content/uploads/dces/pdf/2022_CES_Pay_Rates.pdf (접속일 : 22년 5월 3일)

[56] 이광호, 김홍택. (2017). 사이버 안보를 위한 軍 정보보호 전문인력 양성방안. 융합보안 논문지, 17(2), 149.

[57] 조선일보, “러, 우크라 주요기관 37차례 사이버공격…그후 미사일로 때렸다”: https://www.chosun.com/international/international_general/2022/04/28/UADIYJBYJFGA5PC4QDDR7CZ6TQ/ (접속일 : 22년 4월 29일)

[58] 이수원, 이재연, 홍석준. (2019). 함정 전투체계 사이버방호에 대한 분야별 보호방안 연구. 한국정보과학회 학술발표논문집, 2019.12, 865-866.

[59] 이광호, 한경용, 이규홍. (2019). 북한 해커그룹 주요 멀웨어의 시각화 구현. 한국정보과학회 학술발표논문집, 2019.12, 45-47.

[60] 정성욱, 박남제. (2020). 인터넷 연결이 불가능한 내부망의 효율적인 악성코드 탐지 방안. 한국멀티미디어학회 추계학술발표대회 논문집, 23(2)

[61] 김경원, 장석민, 손윤식, 임선영. (2021). 무기체계 소프트웨어의 보안성 강화를 위한 보안약점 분석 및 평가체계 연구. 한국군사학논집, 77(1), 426-459.

[62] Don Snyder , Lauren A. Mayer , Guy Weichenberg , Danielle C. Tarraf , Bernard Fox , Myron Hura , Suzanne Genc , Jonathan W. Welburn. (2020), Measuring Cybersecurity and Cyber Resiliency, Pages 1-13, https://doi.org/10.7249/RR2703

[63] 한국인터넷진흥원, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서(2022. 4월)

[64] Gang-Soo Lee, Hyun Mi Jung. (2019). The Integrated Cyber SRM(Security Risk Monitoring) System Based on the Patterns of Cyber Security Charts. Journal of The Korea Society of Computer and Information, 24(11), 100.

[65] 한국인터넷진흥원, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내 리플릿(2020.11월)

ABSTRACT

Security Policy and ISMS for Strengthening CyberSecurity of Weapon Systems

Sung-wook Jung

Convergence Information Security
Graduate School, Jeju National University
Jeju, Korea

(Supervised by professor Namje Park)

With the development of technology, the proportion of software in weapon systems is increasing, and the cybersecurity problem of weapon systems is becoming increasingly important as advanced science and technology are applied to weapon systems. In addition, various attempts have been made by hostile forces to neutralize the weapon system, but there is a lack of institutional mechanisms to preemptively detect, prevent, establish countermeasures, and take action. And in the security situation facing North Korea, the threat of hacking into the military defense network and the battlefield network exists.

The U.S. Office of Accounting and Inspection(GAO) said in 2018 that the U.S. Department of Defense does not recognize that the next-generation weapons system computer network is being easily hacked by undetected 에 due to poor computer network password management and non-used encryption communication.

In this paper, after analyzing the status of cybersecurity in the Korean military, such as the criteria for classifying weapons systems in the defense field, we presented examples of weapons system cybersecurity and weapons system attacks, and related research trends. In addition, the weapon system cybersecurity performance system and limitations were analyzed. In order to strengthen security in the current closed weapon system environment, the weapon system cybersecurity policy was proposed in five categories: identification and management of weapons system security vulnerabilities, security management of defense companies, training of weapons system experts,

response to weapons system malware.

As a way to identify weapons system security vulnerabilities, it proposed to improve the security management of defense companies and establish supply chain security management system as a way to manage defense companies. In addition, a plan to train specialists in weapon system security, a plan to respond to weapon system malicious codes, and an information protection management system specialized in weapon system were proposed.

In Korea, the weapons system cyber security policy is still in its infancy. Like the United States, generous budget support and national legal system support are needed to strengthen the security of weapons systems. The security policy proposed in this paper should be applied, and the cyber security of the weapon system should be strengthened through active exchanges and cooperation with the private sector.

Continuous research is needed to strengthen weapon system cybersecurity. In particular, in the development of weapons systems, a source code verification plan specialized in weapons systems should be established, and methods and tools should be developed to diagnose effective weapon system security vulnerabilities while ensuring availability between weapon systems operations. In addition, in the case of overseas purchasing weapons systems, continuous research is needed on procedures that can clearly define and reflect the security requirements required by our military at the contract stage and check compliance with the security requirements at the operation stage.