Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.765

무기체계의 사이버보안 시험평가체계 구축방안 연구*

이 지 섭,† 차 성 용, 백 승 수, 김 승 주‡
고려대학교 정보보호대학원

Research for Construction Cybersecurity Test and Evaluation of Weapon System*

Ji-seop Lee,† Sung-yong Cha, Seung-soo Baek, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

IT 기술이 발전함에 따라 군의 정보시스템은 효율적인 작전 수행 및 신속한 통신을 위해 현 IT 환경에 맞추어 발전하고 있으며, 이에 따라 네트워크 기술을 사용하는 첨단무기체계에 대한 사이버 공격 위협도 동시에 증가하고 있다. 이러한 문제를 예방 및 완화하기 위해 미국은 무기체계 개발 초기부터 전반에 걸쳐 사이버보안 시험평가체계를 적용하고 있다. 그러나 국내의 경우 사이버보안 시험평가 프로세스가 미약하여 사이버 공격에 따른 피해가 우려된다. 이에 본 논문에서는 미국과 국내 무기체계의 사이버보안 시험평가 현황을 분석하여 국내 무기체계 시험평가에 대한 문제점을 제기하고, 사이버보안 시험평가체계를 도입하는 방안을 제안한다.

ABSTRACT

As the IT technology develops, the military information system develops to the current IT environment for efficient operation and rapid communication, and the threat of cyber attack against the advanced weapon system using network technology is increasing simultaneously. In order to prevent and mitigate these problems, the United States has applied the cybersecurity test evaluation system from the beginning to the beginning of weapon system development. However, in Korea, the evaluation process of cyber security test is weak, and there is concern about the damage due to cyber attack. In this paper, we analyze cybersecurity test evaluation status of U.S. and domestic weapon systems and propose a solution to the problem of cybersecurity test evaluation system.

Keywords: Cybersecurity, Test and Evaluation, Weapon Systems

I. 서 론

항시 전쟁 승리를 위해 군 정보시스템은 효율적인 작전 수행 및 신속한 정보통신 기술과 발맞추어 발전하고 있다. 이에 따라 군 무기체계 또한 네트워크 기술을 포함한 다양한 IT 기술이 도입되어 사이버영역 내에서 체계 간 원활한 통신이 가능해졌다. 그러나 군 무기체계는 네트워크 기술을 통해 외부와의 정보 교류가 이루어지므로 사이버 공격으로 인한 정보 유출 및 데이터 위·변조가 발생할 수 있으며, 이로 인한 피해가 우려된다.

사이버보안을 위협하는 사이버 공격은 지능형 지속 위협(APT, Advanced Persistent Threat), 악성코드, DDoS 공격과 같은 기술을 종합적으로

Received(05. 02. 2018), Modified(06. 08. 2018), Accepted(06. 12. 2018)
* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2018-2015-0-00403)
† 주저자, gsleegs4@naver.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

사용하며, 지속적으로 군을 위협하고 있다[1]. 예를 들어 지난 2014년 북한의 공격으로 추정되는 국방과학연구소의 3천여 대 컴퓨터 해킹 사건[2]을 비롯하여, 2015년에는 군 간부 스마트폰 해킹 사건[3], 2016년에는 국방통합데이터센터(DIDC, Defense Integrated Data Center) 해킹[4] 등 각종 기밀정보가 유출되어 군의 보안 체계를 위협하였다. 또한, 최근에는 사이버 공격이 군 관련 정보 시스템 뿐 아니라 무기체계를 무력화하는 방향으로 변화하고 있다. 2015년, 미국 MDAA(Missle Defense Advocacy Alliance)에 의해 'Left of Launch'라 불리는 전략이 공개되었다[5]. 이 전략은 사이버 공격을 통해 네트워크와 연결된 무기체계 시스템 내에 침입하여 미사일이 발사되기 전 준비단계에서 이를 무력화하는 것이다. 이러한 사이버 공격으로부터 무기체계의 사이버보안을 보장하기 위해 미군은 무기체계 초기부터 사이버보안 시험평가를 체계적으로 수행하고 있다[6].

하지만, 우리 군의 무기체계에 대한 사이버 공격에 대한 대비는 잘 갖추어지지 않았다. 국내 무기체계의 사이버보안 관련 사항은 '국방전력발전업무훈령'[7]과 '국방사이버안보훈령'[8]에 일부 포함되어있다. 위 문서들은 소요 단계부터 체계개발 단계까지 적용된다. 그러나 무기체계에 사이버 보안을 적용하기에는 너무 형이상학적이고 포괄적이다. 게다가 훈령 이하 사이버 보안관련 세부 지침이 존재하지 않으며, 훈령 간 연계성이 존재하지 않아 무기체계 내 사이버보안의 적용 유무를 알 수 없다.

이에 본 논문에서는 우리 군보다 수십 년 전부터 사이버 보안 시험평가를 적용하고 있는 미국과 우리 군의 현실을 비교하고[9] 현 우리 군의 무기 획득 체계의 문제점을 지적한다. 다음으로 군 무기체계의 사이버 보안을 강화하기 위한 시험평가체계 도입방안을 제안한다.

본 논문은 서론에 이어, 2장에서는 관련 연구를, 3장에서는 국내 무기체계 도입 시 사이버보안성 평가의 문제점을 지적한다. 4장에서는 사이버보안성이 강화된 무기체계 획득 프로세스를 제안하고, 5장에서는 제안하는 프로세스와 국내 프로세스의 비교 평가를, 마지막으로 6장에서는 결론을 맺는다.

II. 관련 연구

2.1 용어 정의

2.1.1 사이버보안

미국의 'National Security Presidential Directive-54/Homeland Security Presidential Directive-23'의 "Cybersecurity Policy"[10]에서는 사이버 보안을 다음과 같이 정의하고 있다. '사이버보안은 컴퓨터, 전자통신 시스템, 전자통신서비스, 유선통신, 전자통신과 그 안에 담긴 정보에 대해 피해를 예방, 보호, 복원하여 기밀성, 무결성, 가용성, 인증, 부인방지를 보장하는 것을 의미한다.'로 정의하고 있다.

국내의 경우 사이버보안을 사이버안전이라는 용어로 사용하고 있으며[11], 이와 관련하여 대통령 훈령인 국가사이버안전관리규정 제2조제3항에서는 '사이버안전이라 함은 사이버 공격으로부터 국가정보 통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.'고 정의하고 있다[12].

이렇듯 국내에서는 사이버보안에 보안 3요소인 기밀성, 무결성, 가용성을 고려하고 있지만 미국은 이를 포함하여 인증, 부인방지까지 보장하고 있어 양 국가에서 사용 중인 용어는 의미상 차이가 있다. 본 논문에서는 사이버보안 용어 사용 시, 한·미 용어가 혼용될 수 있으므로 미국에서 사용하는 용어로 통일하기로 한다.

2.1.2 시험평가

시험평가는 무기체계 개발과정의 한 분야로서 시험(Test)과 평가(Evaluation)의 합성어이다. 시험은 개발 및 운용측면에서 무기체계의 객관적인 성능을 검증하고 평가하는 기초 자료를 획득하는 과정이며, 평가는 시험을 통해 수집된 자료와 기타 수단으로 획득된 자료를 근거로 사전에 설정된 시험 기준과 비교분석함으로써 대상 무기체계가 사용자 요구에 일치하는지를 검증하고 운용목적에 부합하는지의 적합성을 판단하는 과정을 말한다[13]. 즉, 시험평가는 무기체계 개발을 위한 구매 또는 연구개발이나 설계·제작이 요구사항에 일치하는가를 판단하는 의사결정 지원단계이다.

2.2 韓·美 사이버보안 시험평가

2.2.1 美, 군 사이버보안 시험평가 체계

미국은 합리적인 사이버보안 시험평가를 위해서 국가 차원에서 같은 기준을 적용하고 평가 결과들을 공유할 수 있도록 미국표준기술연구소(National Institute of Standard and Technology, 이하 NIST)의 사이버보안과 관련된 NIST SP 800 시리즈 문서[14][15][16][17][18]와 CNSS (Committee on National Security Systems)의 정책과 연계하여, 시험평가의 합리성과 효율성을 극대화 하였다[19]. Fig. 1.은 미국 사이버 보안관련 문서들의 관계를 설명한다.

미국 국방부(Department of Defense, 이하 DoD)에서는 무기체계에 사이버보안을 실현하기 위해 국방 획득 체계, 위험 관리 프레임워크(Risk Management Framework, 이하 RMF), 사이버 보안 시험 평가 체계가 통합되어 있으며[20], 각 지침에 대한 내용은 Table 1.과 같다.

미국은 위의 3가지 주요 체계 중, 무기체계 내 전반적인 사이버보안을 다루기 위해 사이버보안 시험평가 프로세스를 수행하고 있다. 이 프로세스는 국방획득체계 중 소요 분석 단계부터 생산 및 배치 단계까지 빠짐없이 연속으로 진행되며 시스템 공학 및 RMF 프로세스 과정과 통합하여 진행된다[6]. 이러한 시험평가 프로세스는 총 6단계로 다음과 같이 수행된다.

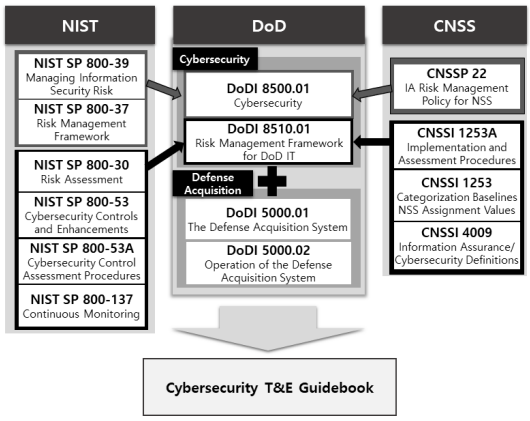


Fig. 1. Relations between Cybersecurity documents in U.S.

Table 1. Guidelines related to U.S. Cybersecurity

No	Title	Contents
DoDI 5000.02 [21]	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 [22]	Risk Management Framework for DoD Information Technology	Guidelines are provided for RMF for DoD IT and related cyber security policy establishment
DoDI 8500.01 [23]	Cybersecurity	General Guidelines are provided for protection and defence of DoD IT

- **1단계, 사이버보안 요구사항 이해**: 가능한 모든 대상 시스템 관련 문서를 살펴봄으로써 사이버보안 요구사항을 이해하는 단계
- **2단계, 사이버 공격표면 식별**: 공격자가 시스템을 악용할 수 있는 공격표면(접근 및 악용 가능한 취약점이 발생할 수 있는 부분)을 식별하는 단계
- **3단계, 협업을 통한 취약점 식별**: 시험, 분석, 수정, 재시험 과정을 통해 시스템 개발 전반에 걸쳐 사이버보안 취약점을 식별하는 단계
- **4단계, 적대적 사이버 보안 개발시험평가:** 이전 사이버보안 시험평가 단계에서 산출된 취약점 분석·평가 보고서, 보안평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행하는 단계
- **5단계, 협업을 통한 취약점 평가 및 침투 평가:** 취약점이 발생할 수 있는 환경을 임의로 구축하여 시험평가를 진행하며, 이를 통해 대상 시스템에 적용된 사이버보안 정도를 파악하는 단계
- **6단계, 적대 평가:** 공인된 취약점 침투 테스트 팀이 이전 사이버보안 시험평가 단계에서 도출된 사이버 위협에 대한 대응방안을 평가하는 단계

2.2.2 韓, 군 사이버보안 시험평가 체계

우리 군의 경우 무기체계 획득 시, 그 기본 지침을 '국방전력발전업무훈령'[7] 으로 하고 있다. '국방전력발전업무훈령'은 무기체계의 소요, 획득, 운영유지를 포함하는 무기체계 관련 전반적인 생명주기 전체를 다루고 있다. 특히, 무기체계 도입 시 아래와 같이 사이버 보안을 적용하기 위한 지침을 제공한다.

- **제56조(탐색개발 수행)** ① 방사청은 연구개발 주관기관으로 하여금 탐색개발을 추진하도록 조치하고 탐색개발 결과를 검토한 후, 다음 각 호의 사항을 포함하는 탐색개발결과보고서를 합참 및 소요군에 통보한다.
  8. 무기체계의 정보시스템 및 내장형SW에 대한 기무사의 보호대책 검토결과.
- **제57조(체계개발 수행)** ② 방사청은 체계개발 착수 전 기무사에 무기체계의 정보시스템 및 내장형SW에 대한 보호대책 검토를 의뢰하고 검토결과를 체계개발 계획에 반영한다.
  ④ 방사청은 체계개발단계에서 작전운용성능 변경이 요구되거나, 합동성·상호운용성에 영향을 미치는 경우 등 개발계획의 변경이 요구되는 경우에는 국본(정보화기획관실), 합참, 소요군과 사전 협의하고 기무사에 무기체계의 정보시스템 및 내장형SW에 대한 보호대책 검토를 재의뢰하여야 한다.

'국방전력발전업무훈령' 제12조에 의하면, 정보시스템 및 내장형SW에 대한 보호대책 검토는 기무사가 담당하고 있으며 체계개발 착수 전까지 반복하여 검토를 수행한다. 이 외에도 제8절 제82조의4(개발시험평가계획 수립), 제82조의5(운용시험평가계획 수립) 지침에 '안전 및 보안대책' 문구를 포함하여 무기체계 개발·운용시험평가 시, 보안대책(해당 무기체계 및 연동체계와 관련되는 보안기능에 대한 대책, 정보보호, 연동성 등 암호기능에 관련되는 성능에 대한 대책을 포함)을 고려하도록 명시하고 있다.

이와 더불어, '국방사이버안보훈령'[8]은 군 사이버무기체계 사이버 안보 관련 보호 대책 수립 및 관리 지침을 규정하고 있다. 해당 지침에서는 무기체계의 소요 단계, 탐색개발 단계, 체계개발 단계, 운용 및 유지 단계에서 수행할 사이버보안 업무 및 참여기관 별 무기체계 사이버보안 보호대책 수립 및 관리 훈령을 명시하고 있다.

위의 2.2.1, 2.2.2를 종합하였을 때 한·미 사이버보안 프로세스는 Fig. 2.와 같이 그려진다. 미국은 무기체계 초기부터 체계적으로 사이버보안 시험평가가 진행되는 반면, 국내는 사이버보안 프로세스가 미흡하며, 무기체계 획득 및 사이버보안 프로세스와의 연계성이 존재하지 않아 무기체계 내 사이버보안 적용 유무를 알 수 없는 문제점이 존재한다. 이와 같은 사항은 다음 장에서 설명하도록 하겠다.

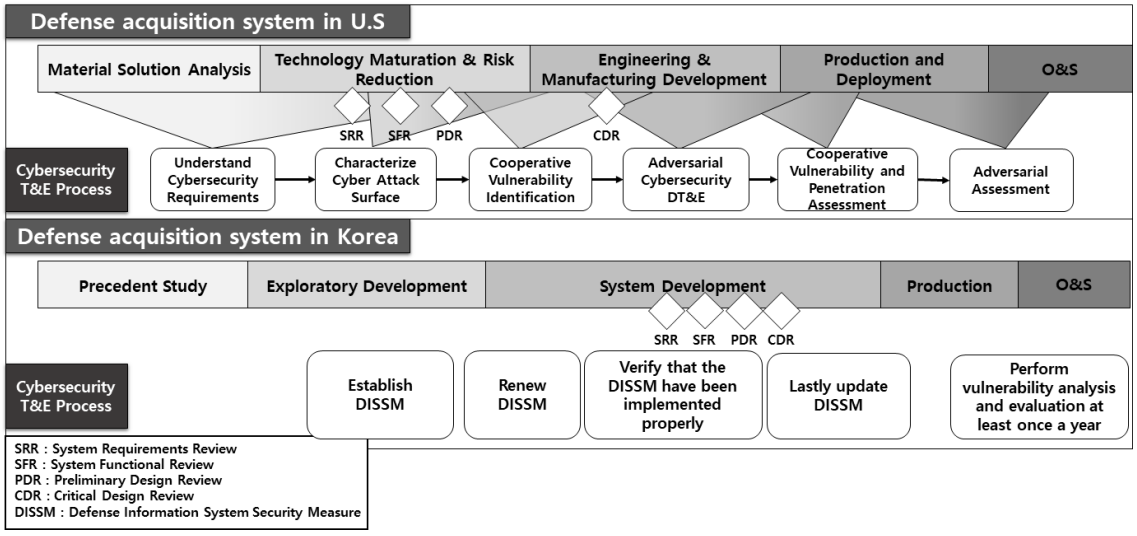


Fig. 2. Comparison of Cybersecurity T&E system between U.S. and Korea

III. 군 무기체계 획득 제약사항 : 사이버보안 관점으로

3.1 무기체계 획득 간 세부 사이버보안 프로세스 미흡

'국방전력발전업무훈령'의 제12조에서는 '국방사이버안보훈령' 관련하여 기무사가 무기체계 탐색개발 및 체계개발 단계에서 무기체계의 정보시스템 및 내장형 SW에 대한 보호대책을 검토하도록 명시하고 있다. 이와 관련하여 제56조(탐색개발 수행), 제57조(체계개발 수행)에서 기무사가 무기체계의 정보시스템 및 내장형SW에 대한 보호 대책을 검토하도록 하고 있다. 또한 제82조 4, 5항에서 무기체계의 개발·운용시험평가 단계에 사이버보안을 적용하기 위한 방안으로 '안전 및 보안 대책'라는 항목이 존재한다. 그러나 무기체계 시험평가의 바탕이 되는 문서인 '시험평가기본계획서'[13]에는 사이버보안과 관련한 사항이 반영되지 않았다. 또한 '국방사이버안보훈령'[8]에서는 국방정보시스템 보호대책서 수립, 갱신, 구현 적절성·적합성 검증 등 사이버보안 시험평가 방법이 모호하여 평가자의 주관에 따라 평가 방법·방향이 달라질 수 있다. 그러므로 무기체계 도입 시부터 사이버보안 문제가 생기게 되면, 사후 대처가 미약할 것으로 판단된다.

3.2 사이버보안 지침과 무기체계 획득 프로세스와 연계성 제한

모든 무기 체계는 사이버보안을 위해 '국방정보시스템 보호대책서'[8]를 작성하게 된다. 위 문서는 보호목적, 시스템 환경, 시스템 아키텍처, 보안 요구사항 및 보안대책, 개선 방안 등으로 구성되어 있다. 그러나, '시험평가기본계획서'와 '국방정보시스템 보호대책서'는 연계가 없는 별도 프로세스로 관리되어 있어 도입 당시부터 무기체계 내 사이버 보안의 적용 유무를 알 수 없다. 그러므로, '국방정보시스템 보호대책서'는 무기체계 획득 프로세스와 연계되어 관리되어야 한다. 또한, 세부적인 무기체계의 보안성 강화를 위해 '시험평가기본계획서'에 사이버보안 항목이 구체적으로 반영되어야 한다.

IV. 제안하는 무기 획득 사이버보안 시험평가체계

이 장에서는 미국의 문서, 지침을 응용하여 국내에 적합한 무기체계의 사이버보안 시험평가 방안을 제안하고자 한다. 국내 무기체계 시험평가의 변형을 최소화하면서 사이버보안을 고려하기 위해 무기체계 시험평가 단계와 제안한 사이버보안 시험평가 단계를 별개로 진행되도록 구성하였다. 이에 따라 '국방사이버안보훈령' 내 '국방정보시스템 보호대책서'를 최대한 활용한 사이버보안 시험평가체계를 제안한다.

현재 국내 무기체계 시험평가는 체계개발 단계까지 이루어지므로[13] 국방획득체계 전 범위로 작용하는 미국 사이버보안 시험평가체계 6단계를 맞추어 적용하기 어렵다. 따라서 제안한 사이버보안 시험평가체계는 Fig. 3.과 같이 4단계로 구분하였으며 기존의 국내 시험평가체계를 기준으로 작성하였다.

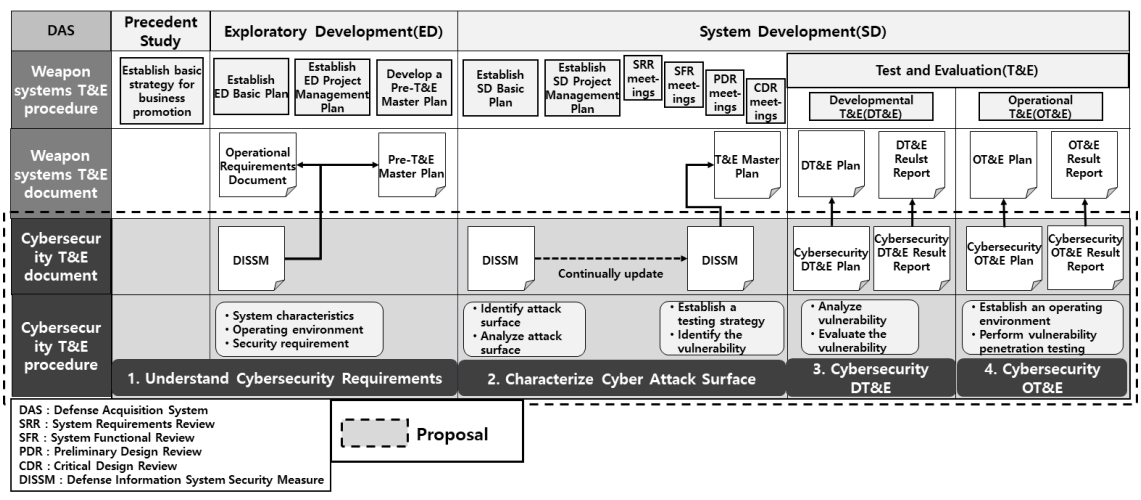


Fig. 3. Proposed Weapon Systems Cybersecurity T&E process

제안 방안에서 3.1의 세부 사이버보안 프로세스 미흡 문제는 국방획득체계 내 사이버보안 단계를 4단계로 구분하고, 각 단계에 수행해야 할 프로세스를 제시하여 사이버보안 프로세스를 체계적으로 수행되도록 하였다. 또한 개발·운용시험평가 단계에 취약점 분석·평가 및 취약점 침투 시험, 사이버보안 평가 항목을 추가함으로써 문제점을 해결하였다. 3.2의 사이버보안 지침과 무기체계 획득 프로세스와 연계성 제한 문제는 사이버보안 시험평가 관련문서 및 '국방정보시스템 보호대책서'와 무기체계 기반 문서(운용요구서, 시험평가기본계획서, 개발·운용시험평가 계획서, 결과보고서)를 연계함으로써 해결하였다.

4.1 사이버보안 요구사항 파악

무기체계 선행연구부터 탐색개발 단계는 무기체계가 보유해야 하는 정보처리 능력, 무기체계 간 상호운용성 등을 정의하고 무기체계 획득 시 운용 유지를 위한 운용환경 분석을 수행한다. 이를 기반으로 개발대상 체계가 만족해야 하는 기능 및 성능, 체계개념, 제약사항을 수집하여 사용자 요구사항을 개발하고 있으며, 대상 체계의 전체 수명주기 전반에 대한 체계요구사항을 도출한다. 이러한 사항을 운용요구서, 예비시험평가기본계획서에 반영하고 있다. 한편, 탐색개발 단계에는 사이버보안 시험평가 수행을 위한 '국방정보시스템 보호대책서' 수립 및 검토가 포함된다.

제안한 사이버보안 요구사항 파악은 모든 대상 시스템 관련 문서를 살펴봄으로써 사이버보안 요구사항을 파악하고 사이버보안 시험평가 수행을 위한 초기 접근 및 계획을 개발하는 단계이다[6]. 위의 선행연구, 탐색개발 단계를 살펴보았을 때, 체계 개념 및 기능, 요구사항, 제약사항 등을 파악할 수 있으므로 이에 맞추어 시험평가와 관련된 모든 이해관계자가 대상 시스템의 시험평가를 위한 사이버보안 요구사항을 파악하는 것이 적합하다고 판단된다.

구체적으로 사이버보안 요구사항은 국방정보시스템 보호대책서에 작성하도록 하며, 이를 운용요구서(대상 시스템의 운용능력, 위협, 취약점, 요구사항 등을 기술한 문서), 예비시험평가 기본계획서에 반영하도록 한다. 사이버보안 요구사항에는 대상 시스템의 특성(예를 들어 네트워크 환경, 운영체제 환경 등), 운용환경, 아키텍처, 보호요구사항(사이버보안 관련 법령/규정, 보호통제항목 등)과 같은 항목을 작성한다.

4.2 사이버 공격표면 식별

체계개발 초기부터 상세설계검토(CDR, Critical Design Review) 회의 전까지는 이전 단계에서 도출된 사용자 요구사항, 체계요구사항을 무기체계의 구성요소에 할당하며, 각각의 체계요구사항이 구현 가능한지 확인한다. 이후 무기체계 구성요소의 검증 과정을 통해 무기체계 설계를 확정하고 사용자 요구사항, 체계요구사항을 충족하도록 기능 설계를 수행한다. 이와 더불어 체계개발 단계 초기부터 시험평가 전까지 '국방정보시스템 보호대책서'의 지속적인 갱신, 검토 과정이 포함된다.

제안한 사이버 공격표면 식별은 공격자가 대상 시스템의 네트워크나 하드웨어, 펌웨어, 물리적 인터페이스, 소프트웨어 등의 접근 가능한 공격 경로를 식별하고 해당 경로에서 발생 가능한 취약점을 파악하는 단계이다[6]. 공격표면 및 취약점 식별 시 전문지식, 기술문서, 국가 취약점 데이터베이스(NVD, National Vulnerability Database), 기타 참고문헌을 이용할 수 있다. 위의 체계개발 초기, CDR 회의 전 단계를 살펴보았을 때, 무기체계의 구성요소 검증, 기능 설계를 수행하며 무기체계 설계도면 등의 정보를 용이하게 파악할 수 있으므로 이에 맞추어 사이버 공격표면, 취약점에 관한 정보를 획득·탐지하는 것이 적합하다고 판단된다.

구체적으로 사이버 공격표면 및 취약점 식별 결과, 사이버보안 시험평가 전략은 '국방정보시스템 보호대책서'에 작성하도록 하며, 이를 '시험평가기본계획서'에 반영하도록 한다.

4.3 사이버보안 개발시험평가

무기체계 개발시험평가 단계는 제품에 대한 기술상의 성능(신뢰도, 적합성, 내환경성, 안전성 등)을 측정하고 무기체계 획득과정에 있어 기술적 개발목표가 충족되었는지 결정하기 위해 수행된다. 이는 시험일정, 비용, 평가항목, 평가방법 및 절차 등을 고려하여 수행된다. 이와 더불어, 개발시험평가 단계에서 대상 시스템의 사이버보안을 달성하기 위해 보호대책 구현기능 및 성능의 적절성·적합성을 검증하도록 한다. 이와 더불어, 개발시험평가 단계에서 대상 시스템의 사이버보안을 달성하기 위해 보호대책 구현기능 및 성능의 적절성·적합성을 검증하도록 한다.

제안한 사이버보안개발시험평가는 취약점 분석·평

가 보고서, 보안평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행하는 단계이다[6]. 위의 개발시험평가 단계를 살펴보았을 때, 무기체계의 기술상 성능을 위한 시험평가는 진행되고 있으나 사이버보안 방법이 모호하다. 그러므로 사이버보안을 보완하기 위해 이전 단계의 결과물을 활용하여 평가 계획을 세우고, 대상 시스템의 취약점을 분석·평가하는 것이 적합하다고 판단된다.

구체적으로 실효성 있는 사이버 보안 개발시험평가를 위해, 무기체계 시험평가 계획 시, 사이버보안 개발시험평가 계획서를, 개발 시험평가 시 사이버보안 개발시험평가 결과 보고서에 작성하도록 한다. 또한, 이를 무기체계의 개발시험평가 계획서, 개발시험평가 결과 보고서에 반영하도록 한다. 또한 실제 무기체계의 사이버 보안 안전성을 검증을 위해, 취약점 분석·평가가 가능한 별도의 사이버보안 개발시험평가 팀을 구축, 임무 수행해야 한다[24].

4.4 사이버보안 운용시험평가

무기체계 운용시험평가 단계는 제품에 대하여 실제 작전환경과 유사한 운용환경에서 작전운용성능 충족여부와 운용적합성, 효율성, 안전성 등을 평가한다. 이와 동시에, 사이버보안 운용시험평가를 수행한 후 '국방정보시스템 보호대책서'를 최종 갱신한다.

제안한 사이버보안 운용시험평가는 취약점 분석·평가 보고서, 사이버보안 개발시험평가 산출물 등을 참고하여 공격자 입장으로 취약점 침투 테스트(Penetration Test)를 수행하고 대상 시스템의 사이버보안 정도를 평가하는 단계이다[6]. 또한 유사시 사이버 공격으로부터 무기체계를 안전하게 보호할 수 있는 능력을 갖추기 위해 별도의 사이버보안 네트워크 방어 팀을 구성하여 보안위협 탐지 능력, 사이버 공격으로 인해 손실되거나 저하된 시스템을 복구하는 능력을 평가한다. 위의 운용시험평가 단계를 살펴보았을 때, 평가 범위와 평가 내용에 있어 미국과 유사한 부분이 많으므로 해당 단계에 미국 국방부의 지침을 참고하여 사이버보안 운용시험평가를 진행하는 것이 적합하다고 판단된다.

구체적으로 시험평가 계획, 시험평가 결과는 각각 사이버보안 운용시험평가 계획서, 사이버보안 운용시험평가 결과 보고서에 작성하도록 하며, 이를 무기체계의 운용시험평가 계획서, 운용시험평가 결과 보고서에 반영하도록 한다. 원활한 운용시험 평가를 위해 대상 시스템의 취약점 분석·평가가 가능한 별도의 사이버보안 운용시험평가 팀을 구축해야 한다[24]. 이 팀은 개발시험평가 팀이 미처 확인하지 못한 잠재적인 위협을 이중으로 식별하기 위한 목적으로 구성된다.

V. 국내 무기체계 시험평가와 제안 방안 비교평가

사이버보안 관점으로 국내 무기체계시험평가와 제안 방안을 비교하면 Table 2.와 같다. 먼저, 기존 무기체계에는 무기체계 기반 문서, 사이버보안 시험평가 관련 문서 간 연계성이 존재하지 않는다. 이를 개선하기 위해 국방정보시스템 보호대책서, 사이버보안 개발·운용시험평가 계획서를 활용하여 시험평가기본계획서, 개발·운용시험평가 계획서에 사이버보안을 적용하도록 제안하였다. 사이버보안 관련 문서를 무기체계 시험평가 문서와 연계한다면 체계화된 사이버보안 시험평가 수행이 가능할 것이다.

다음으로, 국내 사이버보안 시험평가 프로세스를 세부항목으로 나누었다. 탐색개발, 체계개발 단계의 '국방정보시스템 보호대책서 수립, 갱신'과 같이 간략하게 작성되어 있는 부분을 Fig. 3.의 사이버보안 시험평가 단계와 같이 상세하게 구분함으로써 시험평가 관련 인원들의 의견공유 및 각 단계에 적합한 효율적인 임무수행이 이루어질 것으로 판단된다.

또한 사이버보안 운용시험평가 시, 실 환경과 유사한 운용환경을 구축하여 취약점 침투 시험을 수행하도록

Table 2. Current korean weapon system T&E and proposal

	T&E system of Korea	Proposal
Weapon systems & Cybersecurity document connectivity	X	○
Cybersecurity T&E process	Succinct	Segmentat-ion
Construction of Cybersecurity T&E operating environment	X	○
Vulnerability analysis & evaluation	Once	3 times

하였다. 실제와 같은 환경에서 사이버보안 시험평가를 진행하므로 평가의 신뢰도가 높아질 수 있으며, 무기체계의 보안위협을 완화할 수 있을 것으로 기대된다.

마지막으로 개발·운용시험평가 단계에 취약점 분석·평가를 체계적으로 수행하도록 제안하였다. 기존에는 운영 및 유지보수 단계에서만 취약점 분석·평가를 수행하도록 명시하였으며, 개발·운용시험평가 단계는 이러한 과정이 존재하지 않는다. 또한 '국방정보시스템 보호대책서'에 별지로 취약점 분석·결과 보고서가 포함되어 있으나 각 문서가 어느 단계에서 작성되는지 명시되어 있지 않다. 따라서 제안 방안을 통해 취약점 분석·평가 방안을 개발·운용시험평가에 적용한다면 무기체계의 보안성이 향상될 것으로 기대된다.

Ⅵ. 결 론

본 논문에서는 국방획득체계의 무기시험평가에서 수행되고 있는 사이버보안 시험평가에 대해 미국과 국내로 나누어 비교·분석하고, 사이버보안 시험평가에 대한 문제점을 분석한 후 국내 실정에 맞는 사이버보안 시험평가 방안을 제안하였다.

제안한 사이버보안 시험평가 프로세스는 무기체계 개발단계와 발맞추어, 사이버보안 요구사항 파악을 통해 사이버보안 시험평가 수행을 위한 초기 접근, 계획 개발을 준비하고, 사이버 공격표면, 취약점 식별을 통해 대상 시스템의 취약점 완화대책을 효율적으로 세운다. 또한, 전문 취약점 분석 팀을 활용하여 대상 시스템의 사이버보안 개발시험평가를 수행하며, 실 운용환경과 유사한 환경에서 공격자 입장으로 취약점 침투 테스트를 수행하고 대상 시스템의 사이버보안 정도를 평가한다. 본 논문을 통해서, 무기체계 획득 프로세스와 사이버 보안에 대한 연계성을 높이고, 체계적인 검증이 가능할 것으로 판단된다.

References

[1] Jungho Kang, Hoedong Kim, Sunsoo Kim, and Jincheol Yoo, "Cyber Warfare Countermeasures by Comparison of Cyber Warfare Strategy and Technology of North Korea and other Major Country", *Journal of Security Engineering*, Vol.13, No.4, pp.287-298, 2016

[2] http://www.yonhapnews.co.kr/politics/2014/04/10/0505000000AKR20140410030651001.HTML?076fb838

[3] https://news.sbs.co.kr/news/endPage.do?news_id=N1003456392

[4] http://www.dt.co.kr/contents.html?article_no=2016120702109960813002

[5] "Integrated Air, Space and Missile Defense in 2025 and Beyond", *Space and Missile Defense symposium*, 2015

[6] "Cybersecurity Test and Evaluation Guidebook", *Department of Defense*, 2015

[7] "National Defense Power Generation Business Instruction", *Ordinance of the Ministry of National Defense No.2040*, 2017

[8] "National Defense Cyber Security Instruction", *Presidential Decree No. 1862*, 2015

[9] Carl E. Landwehr, "History of US Government Investments in Cybersecurity Research", *2010 IEEE Symposium on Security and Privacy*, 2010

[10] "Cybersecurity Policy", *National Security Presidential Directive-54 /Homeland Security Presidential Directive-23*, January 2008

[11] Wan Choung, "A Study on the Trend of Cyber-Security Legal Systems in Korean and the United States", *Kyung hee Law Journal*, pp.213-242, 2013

[12] National Cyber Security Management Regulation", *Presidential decree No.316*, 2013

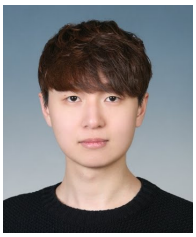
[13] "Weapon system Test & Evaluation Practical Guidebook", *Defense Acquisition Program Administration*, 2013

[14] "Guide for Conducting Risk Assessment", *NIST SP 800-30 Rev.1*, 2012

[15] "Guide for Applying the Risk Management Framework to Federal Information Systems", *NIST SP 800-37 Rev.1*, 2010

〔16〕 "Managing Information Security Risk", *NIST SP 800-39*, 2011
〔17〕 "Security & Privacy Controls for Federal Information Systems and Organizations", *NIST SP 800-53 Rev.4*, 2013
〔18〕 "Guide for Assessing the Security Controls in Federal Information Systems and Organizations", *NIST SP 800-53A Rev.1*, 2010
〔19〕 Cybersecurity and the Risk Management Framework, *Department of Defense*, http://slideplayer.com/slide/4575411/
〔20〕 Congressional Research Service, Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process, May 23, 2014
〔21〕 "Operation of the Defense Acquisition System", *DoDI 5000.02*, 2013
〔22〕 "Risk Management Framework for DoD IT", *DoDI 8510.01*, 2014
〔23〕 "Cybersecurity", *DoDI 8500.01*, 2014
〔24〕 "Information Assurance Certification Training", *DoDI 8570.01*, 2012

〈저자소개〉



이 지 섭 (Jiseop Lee) 학생회원
2016년 2월: 조선대학교 컴퓨터공학부 학사
2016년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 취약점 분석, 보안성분석평가

차 성 용 (Sungyong Cha) 학생회원
2004년 2월: 육군 사관학교 전산학과 전공
2008년 8월: 뉴욕 주립 대학교 전자공학과 석사
2015년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 C4I, 위험관리, 사이버보안 시험평가

백 승 수 (Seungsoo Baek) 학생회원
2002년 2월: 육군 사관학교 전산학과 전공
2007년 9월: 미국 해군대학원 컴퓨터공학 석사
2002년~2017년: 육군 전술통신 및 정보보증 담당 장교
2012년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 개인정보보호, 사이버 작전

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2017년~현재: 고려대학교 사이버무기시험평가연구센터(CW-TEC) 부센터장
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: (사)화이트해커연합 HARU 및 국제해킹대회 SECUINSIDE 설립자 및 이사
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 국방보안연구소 정보보호분야 자문위원
2017년~현재: 여신금융협회 신용카드 단말기 시험 인증위원회 위원
〈관심분야〉 보안공학 및 SDL, 위협 리스크 모델링, 보안성 평가/인증, 암호학, Usable Security