Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 6 pp. 230-238, 2024

https://doi.org/10.5762/KAIS.2024.25.6.230
ISSN 1975-4701 / eISSN 2288-4688

MITRE 프레임워크 기반 무기체계 사이버 능력 확보 방안 연구

서석호[1], 성시일[2], 김도훈[3*]
[1]국방기술품질원, [2]경기대학교 산업시스템공학과, [3]경기대학교 AI컴퓨터공학부

A Study on to Secure Cyber Capabilities of Weapon System based on the MITRE Framework

Sukho Seo[1], Siil Sung[2], Dohoon Kim[3*]
[1]Defense Agency for Technology and Quality
[2]Department of Industrial Systems Engineering, Kyonggi University
[3]Department of AI Computer Engineering, Kyonggi University

요 약 전시와 평시를 막론하고 사이버 공간 작전의 중요성이 커지고, 사이버위협이 증가함에 따라 사이버 안보 대응역량 강화 필요성이 증대되고 있다. 이러한 측면에서, 사이버 공간을 활용하는 무기체계의 연구개발이 중요시되고 있으며, 소프트웨어 중심 무기체계의 사이버 능력을 평가하는 방안 마련이 필요한 시점이다. 본 연구는 사이버 공간을 활용하는 무기체계의 보안성을 고려하여 체계개발 방안을 제안한다. 특히, 무기체계 개발 단계에서 국제적으로 인정받는 MITRE 프레임워크를 적용하고, 개발 과정(SRR, SSR, PDR/CDR, TRR)에서의 업무를 단계별로 구체화한다. 이를 통해, 보안위협 식별, 보안기술 및 리스크 평가를 수행하고, MITRE 프레임워크를 활용하여 각 단위 모듈에 대한 공격/방어 트리와 시나리오를 구성한다. 또한, 구성된 시나리오를 기반으로 한 시험평가를 통해 무기체계의 사이버 능력을 검증한다. 본 연구는 사이버 공간을 활용한 무기체계의 품질평가 방안을 개발하기 위한 선행연구이며, 기존에 다루지 않았던 새로운 요소를 제시함으로써, 향후 중·장기적으로 도입될 사이버 무기체계 획득 시 품질관리 방안으로 활용 가능할 것으로 판단된다.

Abstract Recently, as cyber operations and cyber threats have increased regardless of wartime or peacetime, the need to strengthen cyber security capabilities is increasing. In this respect, research and development of weapon systems that utilize cyberspace is becoming important, and it is time to prepare a method to evaluate the cyber capabilities of weapon systems. This paper proposes a system development method that considers the security of weapon systems utilizing cyberspace. In particular, the internationally recognized MITRE framework is applied at the weapons system development stage (SRR, SSR, PDR/CDR, and TRR), and the tasks to be performed at each stage are presented. Through this, security threat identification, security technology, and risk assessment are performed, and then using the MITRE framework, attack/defense trees and scenarios for each unit module are constructed. In addition, the cyber capabilities of the weapon system are verified through tests and evaluation based on the configured scenario. This study is a preliminary study to develop a quality evaluation method for weapon systems using cyberspace. By presenting new measures that have not been previously addressed, it is believed this method can be used as a quality control measure for cyber weapon systems that will be introduced in the mid-to-long term.

Keywords : Weapon System, Cyber Weapon, System Development, Quality, MITRE Framework

*Corresponding Author : Dohoon Kim(Department of AI Computer Engineering, Kyonggi University)
email: karmy01@kyonggi.ac.kr
Received March 27, 2024 Revised April 24, 2024
Accepted June 7, 2024 Published June 30, 2024

1. 서론

근래 획득되어 운용되는 다양한 무기체계는 소프트웨어의 중요성이 증대됨과 동시에 네트워크 의존도가 매우 높으며, 이에 기반한 다양한 사이버위협에 노출될 가능성이 높다. 특히 고도화된 사이버전의 수행으로 전·평시 사이버 공간 작전의 중요성이 확대되고 DDoS, APT 등 다양한 사이버위협이 증대되고 있음에 따라[1,2], 대응방안 마련이 시급하다고 할 수 있다.

이에 現 정부에서는 사이버위협에 대한 신속대응 및 예방체계 구축 강화를 목표로 국정과제로 '국가 사이버 안보 대응역량 강화'를 추진하고 있다. 즉, 기존 전장 영역(지상·해상·공중)을 사이버 공간이 포함된 전장 영역으로 확대 설정하고, 종래의 기동, 항공, 함정 등 무기체계를 포함하는 8대 무기체계에서 '사이버 무기체계'를 포함한 확대된 10대 무기체계로 재분류하는 등[3] 대응역량 강화를 위한 기반을 마련하고 있다. 특히 DARPA(美 고등연구계획국) Plan X, XD3와 같은 다양한 사이버 기술 프로그램의 연구개발을 진행하고 있는 추세를 고려할 때[4], 사이버 공간을 활용하는 무기체계에 대한 연구개발이 증가하고 있다. 이러한 상황은 사이버 안보 대응역량을 실질적으로 강화할 필요성을 부각시키며, 사이버 방어/능동대응 능력을 갖춘 사이버 무기체계의 개발과 획득을 중장기적으로 추진하는 방향으로 이어지고 있다. 이는 사이버 전장 관리체계와 전술 네트워크를 포함하여 사이버 공간을 활용하는 무기체계의 획득을 위한 연구개발 노력을 강화하고 있음을 의미한다.

이처럼 '사이버 무기체계'의 신설, 중·장기 무기체계 획득사업 반영 및 연구개발사업의 착수 등 사이버 공간을 활용하는 무기체계의 도입이 시작됨에 따라 향후 전력화 운용 시 일관된 성능 구현 및 서비스 제공을 위해서 체계특성에 맞는 품질관리 방안의 마련이 필수적이라고 할 수 있다. 특히 사이버 공간을 활용하는 무기체계는 하드웨어 중심으로 구성된 기존의 무기체계와는 달리 소프트웨어의 비중과 네트워크 의존도가 높고, 전술 네트워크상에서 작전 수행 및 지속 발생하는 사이버위협에 대한 침해영향 최소화 등 위험요소에 대한 관리가 중요한 특성에 따라 필연적으로 보안성이 고려된 품질관리 방안 마련이 필요하다.

본 연구에서는 사이버 공간을 활용하는 무기체계의 품질관리 방안을 확보하기 위하여, 사이버 능력에 기인하여 보안성을 고려한 체계개발 절차를 제안하고자 한다. 무기체계 사이버 능력이란 무기체계 내 소프트웨어를 대상으로 하는 사이버위협으로부터 체계를 보호하기 위한 기술을 의미하며, 보안성 확보를 중점적으로 고려한다. 특히 사이버 위협행위의 전술, 기술 등의 다양화 및 예측불가 악성 행위 증가로 인하여 이에 대한 능동적 대응을 위하여 전술, 기술, 절차에 따른 TTPs(Tactics, Techniques, Procedures) 기반 전략의 구성이 필요하다. 새롭게 제시하는 개발절차는 MITRE 프레임워크에 기반한 테스트 수행방안이며, 체계개발 간 수행할 업무를 제안한다. 2장을 통해 기존 무기체계 소프트웨어 품질관리 절차와 MITRE 프레임워크 기반 공격트리(AT) 및 방어트리(DT) 구성요소 검토방안을 살펴보고 3장을 통하여 기존 체계공학 활동에 더불어 무기체계 사이버 능력 확보를 위하여 수행해야 할 업무를 각 단계(SRR, SSR, PDR/CDR, TRR)별로 제안한다.

2. 관련연구

2.1 기존 무기체계 소프트웨어 품질관리

무기체계 연구개발은 소요제기부터 소요결정, 선행연구, 탐색개발 및 체계개발 단계로 구성된다. 그중 체계개발단계는 선행연구 및 탐색개발 과정 간 도출된 체계 요구성능을 달성하기 위하여 체계설계, 시제품 생산, 시험평가 등의 절차를 거치게 되며, 단계별 기술검토회의를 통하여 요구사항의 분석, 구체화, 위험감소 등의 행위를 수행한다. 기술검토회의는 개발의 완성도를 평가 및 검증하고 차후 단계로의 진입 가능성을 검증하는 체계공학 활동으로 체계요구사항검토(SRR), 체계기능검토(SFR), 기본설계검토(PDR), 상세설계검토(CDR), 시험준비상태검토(TRR) 등으로 분류하며 Fig. 1을 통하여 확인할 수 있다[5].

특히 일반적으로 내장형 소프트웨어가 포함된 무기체계는 체계개발 간 소프트웨어 요구사항 분석, 소프트웨어 구조설계 및 소프트웨어 상세설계 단계를 접목하며, 개발 시 방위사업청 '무기체계 소프트웨어 개발지원에 관한 규정' 및 소프트웨어의 체계적인 개발 및 관리를 위한 프로세스와 산출물 작성표준 지침인 '무기체계 소프트웨어 개발 및 관리 매뉴얼'[6] 등에 따라 소프트웨어 품질을 확보한다.

무기체계 소프트웨어는 Fig. 2의 절차에 따라 체계 공학 프로세스와 연계된 형태의 소프트웨어 개발 프로세스로 구현되며, 주요 체계개발 단계는 소프트웨어 요구사항분석, 소프트웨어 구조설계, 소프트웨어 상세설계, 소

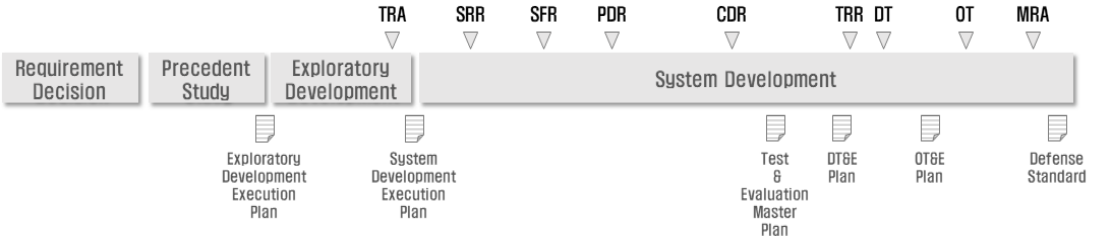

Fig. 1. Research and development step of weapon system[5]

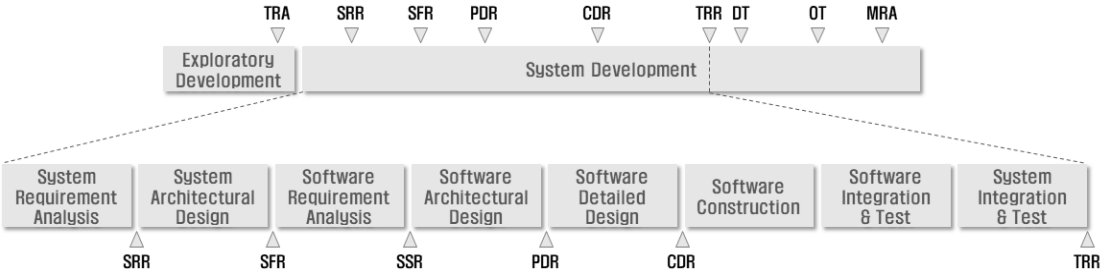

Fig. 2. System development step of embedded software[6]

프트웨어 구현 및 통합시험 등으로 구성되어 있다. 각 단계 수행 간 체계요구사항 명세서, 소프트웨어 개발계획서, 소프트웨어 요구사항 명세서, 소프트웨어 설계기술서, 소프트웨어 목록명세서 등의 산출물을 작성하게 된다. 산출물 작성, 검토 시 소프트웨어 보안성 구현 계획 및 시험방안과 절차 등의 기술 여부와 보안 요구사항의 반영 및 구현 여부 등에 대한 검토를 수행하게 된다. 또한, 개발 간 국방사이버안보훈령, 국방보안업무훈령 등 다양한 보안 관계 지침에 따라 소프트웨어 취약점 점검/제거 및 정적, 동적 소프트웨어 신뢰성 시험 등을 수행하고 있으며, 이러한 일련의 절차를 수행함으로써 무기체계 내장형 소프트웨어 품질을 확보하고 있음을 확인할 수 있다. 다만 상기 기존의 소프트웨어 품질확보를 위한 명세기반의 개발절차는 최근 고도화 및 다각화되는 사이버 작전 공간과 그 공간을 활용하는 사이버 무기체계 개발을 위한 품질관리 프레임워크로 적용 및 활용에 대한 연구가 부족한 실정이다. 특히 미션크리티컬(mission critical)한 특징을 갖는 사이버 무기체계의 특성상 위협기술의 다변화에 따른 능동적 대응전략을 내포하고 있어야 함에 따라 무기체계 위험관리 차원의 적합한 보안성 확보를 위한 품질관리 방안 마련이 필수적이라고 할 수 있다.

2.2 MITRE ATT&CK / D3FEND FRAMEWORK

일반적으로는 무기체계 내 소프트웨어의 신뢰성과 안전성 확보를 위한 체계적인 개발이 이루어지지만, 무기체계의 사이버 능력에 기인한 보안성을 확보할 수 있는 품질관리를 위해서는 이에 맞는 분석, 테스트 및 검증 평가방안이 요구된다. 이를 위해 무기체계 내 소프트웨어가 위협행위에 노출될 가능성을 가정하고 개발 시 위협요소 식별, 위협 시나리오 설계 및 이에 기반하는 테스트 및 평가 수행이 필수적이다. 이에 따라 실질적인 보안위협, 대응방안 등 TTP기반 전략, 전술을 제공하는 MITRE 프레임워크를 활용하고, 체계개발 간 MITRE 프레임워크에 기반한 공격트리(AT: Attack Tree)/방어트리(DT: Defend Tree)를 구성하는 방안을 제안한다. MITRE 프레임워크는 사이버보안 분야에서 널리 사용되는 프레임워크 중 하나로 공격 및 방어 전략을 평가하고 개선하기 위해 설계되었다[7].

MITRE의 ATT&CK 프레임워크는 공격자의 행동을 분석하고 모델링하는 데 도움이 되며, 공격트리 구성에 유용할 수 있다. 반면 MITRE의 D3FEND 프레임워크는 방어 전략에 중점을 두며, 방어트리 구성에 이용될 수 있다. 사이버 공간을 활용하는 무기체계는 보안성이 중요한 이슈임에 따라 MITRE 프레임워크를 활용한 공격트리와 방어트리의 구성을 통하여 무기체계의 보안을 강화

Table 1. MITRE ATT&CK Framework[8]

Category	Details
Tactics	· 40 Tactics are provided (Enterprise: 14, Mobile: 14, ICS: 12) · Represents actions according to the attack goal / Higher category for Technique
Techniques	· 340 Techniques are provided (Enterprise: 196(Sub-Tech: 411), Mobile: 66(Sub-Tech: 41), ICS: 81) · As a method to achieve the tactic, it specifies the results that occur through the technique
Mitigations	· 104 Mitigations are provided (Enterprise: 41, Mobile: 11, ICS: 52) · Actions that can be taken to prevent and detect attacks · It can be applied overlapping against attacks(Technique)
Groups	· 138 Groups are provided · Providing information and attack techniques on publicly-named hacking groups · Identifying hacking organizations based on main attack methods, activities, etc
Software	· 740 Attack tool information are provided · Lists basic tools and Open Source S/W included in the OS

Table 2. MITRE D3FEND Framework[8]

Category	Details
Hardening	· Reduce attack surfaces and emphasize limited access and monitoring · Focus on updates and patches to reduce vulnerabilities and reflect security protocols and regulations for authentication and access control
Detection	· Focus on analyzing identified threats based on the MITRE Attack Framework · Includes file, identifier, process and user behavior analysis and platform monitoring(Includes SIEM, MDR)
Isolation	· Focus on isolating vulnerable or infected hosts · Continuous traffic monitoring and DNS/IP filtering
Deception	· Focus on deception across the entire IT environment, including network resources, files, users, etc · The goal is to trick the attacker into a fake environment
Eviction	· Strengthen security profiles by shutting down vulnerable and infected components

하고, 잠재적인 위협을 식별하며, 대응전략을 개발하기 위한 효과적인 방법을 제공할 수 있다[8]. MITRE ATT&CK 프레임워크는 Table 1과 같이 Tactics, Techniques, Mitigations 등으로 구성되며, 공격 전술, 기술 및 완화 기법 등의 최신화된 정보를 제공한다. Tactics 및 Techniques은 공격트리의 '구성요소'로 대응 가능하며 대상체계에 대한 보안위협 요소로서 공격행위를 위한 전술, 기술, 수단으로 활용할 수 있다. MITRE D3FEND 프레임워크는 ATT&CK 프레임워크와 유사하게 Tactics과 Techniques으로 구성되며, Table 2와 같이 Hardening, Detection, Isolation 등의 방어 전술을 최상위 계층으로 분류하여 기술 및 하위기술의 정보를 제공한다. 마찬가지로 Tactics 및 Techniques은 방어트리의 '구성요소'로 대응 가능하며, 대상체계에 대한 보안위협을 방어할 수 있는 보안기술로 보안위협을 완화하는 요소로 활용할 수 있다. 특히 MITRE D3FEND는 MITRE ATT&CK의 완화기술(mitigation)과 대응하는 방어기술을 구성하여 계층적으로 제공함에 따라 사이버 능력에 기인한 무기체계 보안성 확보를 위한 다양한 방어 요소들을 TTPs로 개념화할 수 있으며, 이를 ATT&CK 전술, 기술 및 절차에 매핑하여 예방적이고 위협에 기반한 방어 전략을 구현하도록 할 수 있다.

2.3 공격트리(AT) / 방어트리(DT)

공격트리 및 방어트리는 공격목표 및 방어목표를 최상위 노드로 구성하고 그 목표을 달성하기 위한 공격 및 방어 전략, 기술 등을 하위단계로 작성하는 계층 트리(multi-layer)를 의미한다. 공격 및 방어트리는 그림, 텍스트형식 등으로 작성 가능하며, 공격 및 방어경로를 시각적으로 표현하는 방법이라고 할 수 있다. 공격 트리와 방어 트리는 시스템, 네트워크 등의 보안상태를 평가·분석하기 위하여 사용되는 구조화된 방법론으로 공격 트리는 공격자 목표 중심의 가능한 공격 경로를 조직하며, 방어 트리는 이에 대한 대응전략과 방법을 조직한다.

구성 절차는 최상위 수준에서 최종목표(root node)를 구성하고 하위 수준으로 목표를 달성하기 위한 단계를 트리의 'Leave' 형태로 계층별로 세분화한다. 하위단계 트리 세분화 시 AND/OR 로직을 사용하여 단계 간 관계를 복잡화 또는 단순화할 수 있고, 트리 'Leave' 레벨을 심화함으로써 최종목표를 달성하기 위한 전략, 기법을

Table 3. Example of Security Threat and Security Technology of Weapon System

Domain	Component	Security Threats	Security Tech.
Weapon System	Component 1 - 2 Component 2 - 3	Firmware Tampering	Secure Flash
		Remete Control Hacking	SecOC
		DoS	IDS
		...	...
Communication System	Component 1 - 3	Wiretapping	IPSec, TLS
	Component 1 - 2	False Information	
	Component 2 - 4	Message Forgery and Alteration	
	...	...	...
Back-End Infrastructure	N/A	Information Leakage	UTM
		Privilege Escalation	Access Control
		.....	.....

다양하게 구성할 수 있다. 특히, MITRE 프레임워크 매트릭스에서 식별된 공격 및 방어 전략 및 기술을 적용하여 하위단계 트리를 보다 상세하게 구성할 수 있으며, 공격트리와 방어트리의 연계를 통하여 공격자의 행위와 방어 조치 간의 상호작용을 이해할 수 있다.

3. 무기체계 체계개발 단계 제안

본 논문에서 제안하는 MITRE 프레임워크 기반 테스트 수행방안은 사이버 능력에 기인한 보안성 확보를 위하여 위협모델링 기반 보안위협과 보안기술을 식별하고 단위 모듈별 공격 및 방어트리의 구성으로 공격 및 방어 시나리오를 작성하고 이를 기밀성, 무결성, 가용성을 고려한 시나리오 위험도 기반 사이버 능력을 테스트하는 방안이다. 개발 간 체계공학 활동에 더불어 사이버 능력 확보를 위하여 수행해야 할 업무를 각 단계(SRR, SSR, PDR/CDR, TRR)별로 제안한다.

(1) 무기체계 요구조건검토(SRR)

SRR(System Requirements Review)은 사용자의 요구사항이 무기체계에 대한 요구조건으로 정의된 체계 요구사항명세서(SSRS)에 반영 여부를 확인하고, 체계 설계과정으로의 진입 여부를 결정하게 되는 절차이다. 특히, 체계 안전 및 보안을 위한 요구조건의 적절성을 검토함에 따라 본 단계에서 제안하는 대상 무기체계의 보안위협 사항 및 해당 기술을 식별하는 과정으로 적절하다.

이에 본 단계는 공격트리 및 방어트리를 구성하기 위한 준비단계에 해당하며, 무기체계 사이버 능력에 대한 위협과 위험에 대한 심각성(severity), 발생확률(probability of exposure), 제어 가능성(controllability)을 분석하고 궁극적으로 보안위협 사항과 이에 대응하는 보안기술을 식별하는 단계이다. 무기체계 사이버 능력요소를 검토하기 위하여 대상 영역별 사이버위협 모델링을 가정하고 영역별 구성요소를 '컴포넌트' 단위로 분류한다. 컴포넌트 간의 관계를 분석하고 이를 통한 보안위협 식별과 이에 대응하는 보안기술을 다음 Table 3과 같이 도출한다. 이러한 과정은 대상 시스템의 아키텍처 및 소프트웨어의 구성요소 등에 대한 충분한 이해가 선행되어야 하며, MITRE ATT&CK 프레임워크의 공격 전술과 기술 및 공격 단체, 도구에 대한 정보 요소를 기반하여 보안위협을 식별할 수 있다. 예를 들어 MITRE ATT&CK 프레임워크의 Privilege Escalation(Tactic ID: TA0004) 및 Exploitation for Privilege Escalation(Technique ID: T1068)은 공격자가 시스템 또는 네트워크 등의 취약점을 악용하여 권한을 얻기 위한 전술과 기술이며, 이를 시스템 및 구성 소프트웨어에 대한 보안위협 사항으로 판단하였다면, 보안위협 목록으로 식별 및 구성할 수 있다.

(2) 소프트웨어 요구사항검토(SSR)

SSR(Software Specification Review)은 소프트웨어 요구사항을 정의, 분석 및 확정하고 소프트웨어 분야 요구사항이 소프트웨어 요구사항명세서(SRS)에 기술되었는지를 확인하며, 소프트웨어 구조설계 단계로의 진입을 결정하는 단계이다. 특히, 체계요구사항명세서(SSRS) 및 체계설계기술서(SSDD) 등 체계요구사항에 기반한 소프트웨어 형상항목(CSCI : Computer Software Configuration Item)이 식별되며, 무기체계 소프트웨어 개발 요구사항에 대한 공식적인 검토가 이루어지는

Table 4. Example of Security Risk Assessment of Weapon System

Domain	Component	Security Threats	Security Risk	Details	Security Tech.
Weapon System	Component 1 - 2 Component 2 - 3	Firmware Tampering	...	...	Secure Flash
		Remete Control Hacking	...	...	SecOC
		DoS	C: Low I: Low A: High	System availability is reduced due to DoS attacks. Weapon system software is interrupted and mission performance becomes impossible. through this, Availability is greatly damaged.	IDS
		...	...	...	...
Communication System	Component 1 - 3	Wiretapping	...	...	IPSec, TLS
	Component 1 - 2	False Information		...	
	Component 2 - 4	Message Forgery and Alteration	C: High I: Mid A: Low	If the communication message is forged or altered, the attacker can log into the system and access confidential information. through this, Confidentiality is greatly damaged.	
	...	...	...	...	...

단계임에 따라 이전 (1)SRR 단계에서 언급된 무기체계 사이버 능력을 위한 보안 요구사항(보안위협 및 보안기술)들의 보안리스크를 평가해야 하는 단계로서 적절하다고 할 수 있다.

이에 본 단계에서는 (1)SRR 에서 식별된 보안 요구사항들을 기준으로 다음 Table 4와 같이 대상 무기체계의 보안리스크를 사이버 능력 기준으로 평가할 수 있는 보안의 3요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)으로 정의하고, 이를 통하여 사이버 능력의 위험도를 검토한다. 기밀성은 무기체계 소프트웨어에 저장된 중요한 정보가 무단으로 액세스되지 않도록 보호해야 함을 의미한다. 기밀성 확보를 위해서는 접근제어, 데이터 암호화 등의 조치를 고려할 수 있다. 무결성은 무기체계 소프트웨어의 데이터가 무단으로 변경되거나 손상되지 않도록 보호해야 함을 의미한다. 무결성 확보를 위하여 데이터 무결성 검사, 변경 로깅 등의 조치를 고려할 수 있다. 가용성은 무기체계 소프트웨어와 관련된 기능 및 서비스가 필요할 때 언제든지 사용 가능해야 함을 의미한다. 가용성 확보를 위하여 재해복구 계획 수립, 부하분산 등의 조치를 고려할 수 있다. 보안의 3요소에 기반한 보안리스크 평가를 통하여 구성요소별 사이버 능력 위험도를 도출할 수 있으며 이를 통하여 궁극적인 사이버 능력 요소를 식별할 수 있다. 본 단계를 통하여 식별된 사이버 능력 요소는 추후 PDR/CDR 단계에서 공격 및 방어트리 구성에 활용할 수 있다.

(3) 기본설계검토(PDR) / 상세설계검토(CDR)

PDR(Preliminary Design Review)은 체계 형상품목에 대한 기본설계 완전성을 검토하고, 상세설계로 진행 가능함을 확인하는 절차이며, CDR(Critical Design Review)은 체계요구조건, 기능요구조건이 하드웨어 설계기술서(HDD), 소프트웨어 설계기술서(SDD), 인터페이스설계기술서(IDD) 등에 반영 여부를 확인하고 요구조건을 충족하는 시제제작, 체계통합 및 시험단계로 진행 가능함을 공식적으로 확인하는 절차이다. 특히 소프트웨어 구성요소를 상세히 설계하고 소프트웨어 신뢰성 및 보안성 시험을 위한 대상, 종류 등 계획을 구체화하는 단계임에 따라 식별된 사이버 능력요소에 대한 보안성 평가를 위한 공격 및 방어트리를 구성하는 단계로서 적절할 것으로 판단된다.

이에 본 단계는 식별된 사이버 능력 요소에 대한 보안성 평가를 위한 Table 5 및 Table 6과 같은 공격트리 및 방어트리를 구성하는 단계에 해당한다. 앞서 (1)SRR 및 (2)SSR 단계를 통하여 무기체계의 공격/방어 자산식별(영역별 컴포넌트)과 위협사항에 대한 보안리스크 평가를 완료하였다. 이를 기반으로 사이버 능력요소를 식별하였으며, 이를 활용하여 대상 무기체계의 공격트리와 방어트리를 구성할 수 있다. 우선, 대상 무기체계의 최종 공격 및 방어목표를 설정할 수 있으며. 이는 이전 단계로 식별된 자산 등으로 설정할 수 있다. 최종 공격 및 방어목표를 루트노드(level 0)로 설정하고 루트노드를 달성하기 위한 세부절차인 서브 트리(level n)를 구성한다. 서

Table 5. Example of Attack Tree

	Level 3	Level 4	Level n	MITRE ATT&CK Technique ID	Security Risk
Attack Tree (AT)	[AM1]	[AM11]	[AM1n]	MITRE - T1XXX	C(High/Mid/Low) I(High/Mid/Low) A(High/Mid/Low)
	[AM2]	[AM21]	[AM2n]		
	.....	.....	.....		
	[AMm]	[AMn1]	[AMnm]		

Table 6. Example of Defend Tree

	Level 3	Level 4	Level n	MITRE D3FEND		ATT&CK ID (ATT&CK Mitigation)
				Control ID	Control Name	
Defend Tree (DT)	[DM1]	[DM11]	[DM1n]	D3-ANCI D3-DTP D3-UAP D3-LFP	.....	M1013, M1015, M1016, M1020, M1021, M1022 .....
	[DM2]	[DM21]	[DM2n]			
	.....	.....	.....			
	[DMm]	[DMn1]	[DMnm]			

브 트리 작성을 위하여 MITRE TTPs를 분석하고 세부기법, 절차 및 완화 기술을 도출한다. TTPs(Tactics, Techniques, Procedures)는 서브트리 구성 시 활용되며 세부기법의 확장 및 경로 변형 등에 활용할 수 있다. Tactic을 통하여 루트노드를 달성하기 위한 공격 및 방어 전략을 설정할 수 있으며 이를 서브트리(level n)의 최상단 노드로 구성한다. Technique는 해당 전략을 달성하기 위한 다양한 기술이며 이를 최상단 노드의 하위 노드로 구성할 수 있다. Procedure를 통하여 각 Technique에 대해 구체적인 공격 절차를 도출할 수 있으며, Technique 노드의 하위로 다양한 경로 절차구성 및 경로 확장 시 활용할 수 있다. 특히 공격의 완화기술은 방어의 완화전략으로 적용 가능함에 따라 방어트리 구성 시 활용할 수 있다.

(4) 시험준비상태검토(TRR)

TRR(Test Readiness Review)은 시험평가 단계로 진입 전 시험절차, 방법, 계획 등이 사용자 요구조건 및 체계요구 조건에 대한 만족 여부를 검증할 수 있는지를 확인하는 단계로 시험평가 계획서를 작성, 검토, 확정하는 절차이다. 특히 시험평가 시 사용되는 데이터, 시나리오, 중요기술 검증방법 등의 적절성을 확인하는 단계로 본 연구에서 제안하는 사이버 능력 요소에 대한 평가 시나리오를 구성 및 적절성을 검토하는 단계로 적절하다고 할 수 있다.

본 단계는 공격트리와 방어트리를 기반으로 사이버 능력 요소에 대한 평가 시나리오를 구성하고 적절성을 검토하는 단계이다. 이전 (3)PDR/CDR 단계를 통하여 공격 및 방어트리를 작성함으로써 최종목표 달성을 위한 다양한 세부절차를 구성하였고, 각 세부절차를 공격 및 방어목표 달성을 위한 전체 또는 부분 시나리오로 활용하며, 시나리오 집단을 구성할 수 있다. 각 시나리오는 시험평가를 위한 테스트 시나리오로 사용하며, 시나리오 유효성 및 안전성 검토 등을 통하여 적절성을 검증하고 선별된 시나리오를 시험평가 항목으로 선정한다. 적절성 검증 시 최신 MITRE TTPs 분석을 통하여 최신 기법, 기술, 프로세스를 반영하고 새로운 위협과 변화를 파악함으로써 시나리오의 유효성을 확보한다. 또한, 시나리오 요소의 잠재 위협사항과 취약점을 검토함으로써 리스크를 분석하고, 구성된 시나리오가 체계의 보안성을 저해하지 않는지에 대한 검토를 통하여 시나리오의 안전성을 확보한다. 특히 기밀성(C), 무결성(I), 가용성(A) 모델에 기반한 CVE (Common Vulnerabilities and Exposures)연계를 통하여 취약점을 분석하고, 위험도를 보안 3요소(기밀성, 무결성, 가용성)에 기반하여 정량화함으로써 시나리오의 우선순위를 도출할 수 있으며, 이를 고려하여 시험평가 시나리오를 선정한다. 선정된 시나리오는 시험평가를 수행함에 앞서 개발시험평가계획서 및 운용시험평가계획서에 반영할 수 있으며, 시험평가를 통하여 해당 시나리오에 대한 평가를 수행한다. 이를 통해 사이버 능력 요소를 검증 및 평가할 수 있으며, 대상 체계의 기능, 성능 등 체계 요구사항 충족 여부 평가 시 활용할 수 있다.

4. 결론

본 연구에서는 사이버 공간을 활용하는 무기체계의 품질확보를 위하여 무기체계 사이버 능력에 기인한 보안성을 중심으로 MITRE 프레임워크에 기반한 체계개발 수행방안을 제시하였다. 체계 구성요소별 보안위협 및 보안기술의 식별과 이에 기반한 공격, 방어트리의 작성으로 공격 및 방어시나리오를 구성하는 방안은 무기체계 사이버 능력 확보를 위한 새로운 방법론이라고 할 수 있다. 본 방법론은 최근 다양해지고 예측 불가능한 사이버 위협행위에 대하여 능동적이고 효과적인 대응전략 마련을 위한 방안으로, 종래의 무기체계 획득 및 개발과정에서 다루지 않았던 부분을 새롭게 제시함으로써, 향후 중·장기적으로 도입될 사이버 공간을 활용하는 무기체계의 전략적 획득을 위한 방안으로 활용 및 응용 가능할 것으로 판단된다. 특히, 국제적으로 활용도가 높은 MITRE 프레임워크에 기반한 무기체계 개발 방안은 실시간으로 변화하고 행해지는 사이버 위협행위에 대한 대응전략 구성을 가능하게 함으로써, 실질적인 체계의 보안성 및 안전성을 확보할 수 있을 것으로 판단한다.

향후 본 연구가 제안하는 방법론을 기반으로 현재의 체계개발 단계를 개선하기 위한 구체적 연구를 계획하고 있다. 이는 방법론을 실행하는 주체, 절차 및 결과물의 상세화에 초점을 맞출 것이다. 또한, 개발이 완료된 후에는 사이버 능력의 지속 가능성을 유지하기 위해 무기체계의 제조성숙도 평가와 최초양산 단계와의 연계를 고려한 품질관리 방안연구를 진행할 예정이다. 이는 향후 도입될 시스템의 품질을 보장하기 위한 기반을 마련하는데 목적이 있다.

References

[1] J. K. Lee, "Cybersecurity Policy Trend of Weapon System", *REVIEW OF KIISC*, Vol.28, No.6, pp.83-87, 2018.

[2] J. S. Lee, S. Y. Cha, S. S Baek, and S. J. Kim, "Research for Construction Cybersecurity Test and Evaluation of Weapon System," *Journal of the Korea Institute of Information Security & Cryptology*, Vol.28, No.3, pp.765-774, 2018.
DOI: https://doi.org/10.13089/JKIISC.2018.28.3.765

[3] "National Defense Power Generation Business Instruction", Ordinance of the Ministry of National Defense No.2568, 2021, Korea

[4] M. Kim, "R&D Trend and Development Direction of Cyber Warfare Weapon System Technology" *Journal of the Korea Academia-Industrial cooperation Society*, Vol.23 No.5, pp.272-278, 2022.
DOI: https://doi.org/10.5762/KAIS.2022.23.5.272

[5] DTaQ, Weapon System Research and Development Quality Management Technical Support Guidebook, Defense Agency for Technology and Quality, Korea

[6] DAPA, Weapon System Software Development and Management Manual, Defense Acquisition Program Administration, Korea

[7] H. Kim, S. Lee and S. Y. Hong, "A Quantitative Security Metric Based on MITRE ATT&CK for Risk Management", *Journal of the Korea Institute of Information Security & Cryptology*, Vol.34, No.1, pp.53-60, 2024.
DOI: https://doi.org/10.13089/JKIISC.2024.34.1.53

[8] D. H. Kim, "A Method of MITRE Framework based Cyber Threats and its Defend Modeling with NIST 800-53", Korean Institute of Information Technology Magazine, Vol.21, No.1, pp.25-30, 2023.

서 석 호(Sukho Seo) [정회원]

- 2015년 2월 : 충남대학교 (공학사)
- 2017년 2월 : 충남대학교 (공학석사)
- 2017년 12월 ~ 현재 : 국방기술품질원(DTaQ) 선임연구원

〈관심분야〉
국방품질경영, K-RMF

성 시 일(Siil Sung) [정회원]

- 2007년 2월 : 고려대학교 (공학사)
- 2009년 2월 : 고려대학교 (공학석사)
- 2014년 2월 : KAIST (공학박사)
- 2014년 8월 ~ 2017년 1월 : 국방기술품질원(DTaQ)
- 2018년 3월 ~ 현재 : 경기대학교 부교수

〈관심분야〉
품질공학, 품질경영, 신뢰성공학

김 도 훈(Dohoon Kim) [정회원]

- 2005년 2월 : 고려대학교 수학/컴퓨터과학 (이학학사, 이중전공)
- 2007년 8월 : 고려대학교 컴퓨터과학 (이학석사)
- 2012년 2월 : 고려대학교 컴퓨터·전파통신학 (공학박사)
- 2012년 3월 ~ 2018년 2월 : 국방과학연구소 선임연구원 (사이버보안팀장)
- 2018년 3월 ~ 현재 : 경기대학교 AI컴퓨터공학부 부교수

〈관심분야〉
K-RMF, 국방/우주 사이버보안, 네트워크 보안, MTD 등