방산안보연구
Journal of Defense Industrial Security

방산안보연구, 1권 1호, 2025년 3월, 87-99면.
Journal of Defense Industrial Security, Volume 1, Issue 1, March 2025, Pages 87-99.
https://doi.org/10.?????/jdis.2025.1.1.6

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

# 상용 무인이동체 군 도입간 시험절차방안 연구

**김대근[1], 김은영[2], 오복주[3]**

[1]테르텐 부사장
[2]테르텐
[3]켄코아에어로스페이스 부장

교신저자: 김대근 (segovia65@teruten.com)

## 요약

새롭게 등장한 드론은 국내외에서 큰 주목을 받으며, 군을 비롯한 다양한 분야에서 그 활용범위와 시장규모가 빠르게 확대되고 있다. 최근, 우크라이나-러시아 전쟁에서 확인된 바와 같이 군사용 드론은 미래전의 핵심 전력으로 점점 더 많이 활용되고 있다. 특히, 네트워크와 연결된 드론은 적 종심까지 은밀히 침투하여 적 상황을 신속하게 파악하여 지휘관에게 전달할 수 있어 그 어느 때보다 지휘관이 실시간 의사 결정을 내릴 수 있게 되었다. 이렇게 군에서의 작전 활용도가 높아짐에 따라 드론에 대한 사이버보안 위협도 증가하고 있다. 오늘날 이러한 사이버보안 위협에 대응하기 위해서는 운용을 위한 보안 솔루션이 아닌 시스템 수명주기 전반에 걸쳐 드론을 무기체계로 개발하거나 상용 드론을 군에 도입할 때 체계적이고 절차적인 보안 개념을 구현해야 한다. 이 문서에서는 드론을 군에 도입 또는 개발할 때 사이버 위협으로부터 생존성을 보장하기 위한 사이버보안을 평가하기 위한 체계적인 시험절차를 연구하였다.

**핵심어**

무인이동체, 사이버보안, 취약점 진단 도구, 시험평가 도구, 위험평가 도구

## 차례

1. 서론
2. 미군과 한국군의 무인 이동체 사이버보안 T&E
  2.1. 미군의 무인 이동체 사이버보안 T&E
  2.2. 한국군의 무인 이동체 사이버보안 T&E
3. 사이버보안 취약점 진단 도구 개발 방안
  3.1. 취약점 진단 도구
  3.2. 시험평가 도구
  3.3. 위험평가 도구
4. 무인 이동체 한국군 사이버보안 T&E 절차 적용 방안
5. 결론

Open Access

**접수일:** 2024년 11월 14일
**수정일:** 2025년 03월 17일
**게재승인일:** 2025년 03월 17일
**출판일:** 2025년 03월 31일

Original Article

# Research on the Test Procedures between the Introduction of Military for Commercial UAV

**Daegeun Kim[1], Eunyoung Kim[2], Bokju Oh[3]**

[1]Vice President, Teruten, Republic of Korea
[2]Teruten, Republic of Korea
[3]Department Head, Kencoa Aerospace, Republic of Korea

Corresponding Author: Daegeun Kim (segovia65@teruten.com)

## ABSTRACT

The newly introduced drones have gained significant attention both domestically and internationally, with their applications rapidly expanding across various sectors, including the military, and the market size growing swiftly. Recently, as confirmed in the Ukraine-Russia war, military drones are increasingly being used as a core power for future warfare. In particular, drones connected to the network can secretly penetrate the enemy's core, quickly grasp the enemy situation, and deliver it to the commander, allowing the commander to make real-time decisions more than ever.As the use of operations in the military increases, cybersecurity threats against drones are also increasing. Today, in order to cope with these cybersecurity threats, it is necessary to implement a systematic and procedural security concept when developing drones as weapons systems throughout the system life cycle or introducing commercial drones into the military, rather than security solutions for operation.In this paper, a systematic test procedure was studied to assess cybersecurity to ensure viability from cyber threats when introducing or developing drones into the military.

**KEYWORDS**

Unmanned Mobile, Cybersecurity, Vulnerability Assessment Tool, Test Evaluation Tool, Risk Assessment Tool

## 1. 서론

첨단 과학기술이 발전하고 있는 현 시점에서 드론에 대한 중요성은 날로 커가고 있는 상황이며, 한국군은 드론 및 무인항공기 등 무인 이동체 도입을 적극적으로 추진하고 있다. 이러한 상황 속에서 사이버보안의 중요성은 더욱 커지고 있는 것도 현실이다. 따라서 한국군에 적용 가능한 상용 사이버보안 시험 및 평가(Test and Evaluation, 이하 T&E로 표기함) 절차 정립이 절실한 상황이다.

무인 이동체는 그 특성상 민간 영역에서 설계 및 개발되어 군사 작전에 필요한 보안 요건을 모두 충족하지 못하는 경우가 많으며, 이러한 이유로 군 도입 시 체계적인 시험절차를 통한 보안 검증이 필수적이다. 본 연구는 상용 무인 이동체의 군 도입 시 요구되는 사이버보안 T&E 절차를 심층적으로 분석하고, 취약점 진단 도구, 시험평가 도구, 위험 평가 도구를 함께 개발해 이를 기반으로 군의 특수한 작전 환경과 보안 요건을 고려하여 시험절차 방안이 효과적으로 적용될 수 있도록 구체화할 예정이다. 무인 이동체의 군에서 운용은 다양한 작전 환경과 위협 요소에 노출되기 때문에 사이버보안 측면에서 철저한 검증이 필요하다.

이에 본 논문은 상용 무인이동체 군 도입간 시험절차 방안을 제시하고자 한다. 논문의 구성은 II장에서는 미군과 한국군의 무인 이동체 사이버보안 T&E에 대해 서술하였으며, III장에서 사이버보안 취약점 진단 도구 개발 방안을 제시하여 사이버보안 취약점을 보완하고자 한다. 또한 미군과 한국군의 사이버보안 시험 및 평가 검증에 요구되는 프로세스 비교 분석을 통해 IV장에서 무인이동체 한국군 사이버보안 T&E 절차 적용방안을 제안하였다.

## 2. 미군과 한국군의 무인 이동체 사이버보안 T&E 비교

### 2.1. 미군의 무인 이동체 사이버보안 T&E

미군의 사이버보안 T&E 단계는 요구사항 이해, 사이버 공격표면 특성화, 협력적 취약점 식별, 적대적 사이버보안 DT&E, 협력적 취약점 침투평가, 적대 평가 등 6개 단계로 구성되어 있으며 각 단계 수행 시마다 1단계와 2단계는 지속적으로 각 활동의 계획 및 분석에 포함된다. 표 1은 미군의 DoDI 5000.02에서 규정하고 있는 획득 수명주기에 따른 사이버보안 T&E 단계를 보여준다.[1][2]

표 1. 수명주기에 따른 사이버보안 T&E 단계

| 구분 | 평 가 내 용 | 세 부 내 용 |
|---|---|---|
| 1단계 | 사이버보안 요구사항 이해 | 평가 대상 시스템의 문서를 살펴봄으로써 사이버보안 요구사항을 이해 |
| 2단계 | 사이버 공격표면 식별 | 공격자가 시스템을 악용하여 접근 및 침투가 가능한 취약점이 발생할 수 있는 공격표면을 식별 |
| 3단계 | 협업을 통한 취약점 식별 | 시험, 분석, 수정, 재시험 과정을 통해 시스템 개발 전반에 걸쳐 사이버보안 취약점을 식별 |
| 4단계 | 적대적 사이버보안 개발시험평가 | 3단계에서 작성된 취약점 분석·평가 보고서, 보안평가 보고서 및 개발시험평가 산출물 등을 활용하여 시스템 시험 평가 수행 |
| 5단계 | 협업을 통한 취약점 평가 및 침투 평가 | 취약점이 발생할 수 있는 임의의 환경에서 시험평가, 이를 통해 대상 시스템에 적용된 사이버보안 수준을 파악 |
| 6단계 | 적대 평가 | 공인된 취약점 침투 테스트 팀이 이전 사이버보안 시험평가 단계에서 도출된 사이버 위협에 대한 대응 방안을 평가 |

도입될 시스템의 보안 기능 및 보증에 대한 평가는 획득 프로세스 전체에서 세부적으로 이루어지고 있다. 그럼에도 불구하고 이러한 획득 체계는 전통적으로 무기체계의 사이버보안 측면보다는 성능과 운용성에 중점을 두었다. 사이버보안을 강화하기 위해 획득 체계를 변경하는 대신 기존 체계에 C&A(Certification and Accrediation)와 같은 프로세스를 혼합하여 사이버보안 수준을 높이는 방향으로 발전하였으며 평가를 위해 국방부 정보 기술 보안 인증 및 인증 프로세스(DITSCAP)[1]를 만들었다. 이후 국방부는 DITSCAP의 단점을 극복하기 위해 위험 관리 프레임워크(RMF)[2]를 운영하고 있다.[3][4] 현재 미국에서 그림 1과 같이 RMF를 적용한 사이버보안 강화 국방획득 체계를 설명하였다.

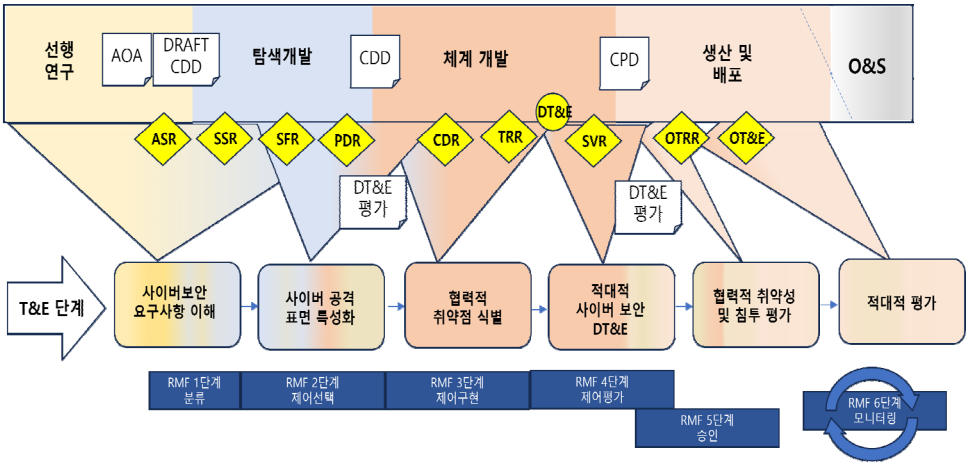


그림 1. 획득 체계 內 RMF 프로세스

그러나 위와 같은 프로세스는 무기체계 개발에 중점을 갖고 있어 부품 구매 및 완성품 구매 등에 적용하기에는 어려운 점이 있다. 그래서 드론과 같은 소형 시스템의 경우 신속 획득 절차에 맞춰 사이버보안 활동을 하고 있다. 특히, 상용 드론의 경우보다 신속하게 군에 도입할 수 있도록 Blue UAS[3] 라는 사전 인증 프로그램을 두고 있다. Blue UAS는 군에 도입되는 상용 무인항공기 및 관련 기술의 사이버보안 기능을 검증하고 관리하는 프로그램으로 표 2와 같이 5가지의 중요 프로세스로 구성되어 있다.

표 2. Blue UAS 프로세스 구성

| NO | 프로세스 | 세 부 내 용 |
|---|---|---|
| 1 | Blue UAS Cleared List | 진화하는 사이버보안 요구에 맞는 국방부 승인 드론목록이 정기적으로 업데이트 된다. 이러한 드론은 보안 및 비행 안전성을 검증받았으며, 정부에서 구매 및 운용할 수 있다. |
| 2 | Blue UAS On-Ramp | 간소화된 승인 및 심사 프로세스이며 군 및 정부기관에서 드론 구매 시 검증된 제품을 제공할 수 있다. |
| 3 | Blue UAS Hub | 업계 및 정부 이해관계자를 위해 블루 UAS 리소스에 대한 종합적인 정보를 한 곳에서 제공하는 정부 웹사이트이다. |

1) DITSCAP(DoD Information Technology Security Certfication and Accrediation Process) : 국방부 정보 기술 보안 인증 및 인증 프로세스
2) RMF(Risk Management Framework) : 위험 관리 프레임워크
3) 미국 국방부 산하 DIU(Defense Innovation Unit)에서 진행하고 있는 프로그램으로, 상용 UAS(Unmanned Aircraft System, 무인 항공기 시스템) 및 관련 기술의 사이버보안 기능을 검증하고 관리하여 상용 UAS가 군에 납품될 때 신속하게 도입될 수 있도록 관리하는 프로그램

| | | |
|---|---|---|
| 4 | Blue UAS Foundry | Blue UAS 파운드리는 DIU[4]의 프로토타이핑 프로세스이다. 디자인 팀은 연방 사용자의 '제안 상자'에서 다양한 아이디어를 실험하여 요구사항을 충족하는 최종 제품을 만든다. |
| 5 | Blue UAS Framework | 이 단계에서 구성 요소 및 소프트웨어 개발이 이루어진다. DIU는 업체에 기준을 충족할 수 있는 정보를 제공한다. |

위와 같은 프로세스에 의해 검증된 문서는 RMF 프로세스에 의해 위험 평가를 수행하고 공급망 보안과 비밀 통제 방안 등을 검토한 후 승인된 제품에 대하여 ATO(Authorization to Operate) 프로세스를 거쳐 군에 납품된다.

미군의 국방획득 시스템에서의 사이버보안은 위험 관리 프레임워크와 사이버보안 테스트 및 평가가 무기체계 개발 수명주기 전반에 걸쳐 수행되고 있음을 알 수 있으며 무기체계의 기능적 부분의 위험 관리뿐만 아니라 공급망, 인적자원 등 비기능적 측면 등 폭넓게 적용되고 있다.

## 2.2. 한국군의 무인 이동체 사이버보안 T&E

한국군의 무인 이동체 획득은 매우 빠른 신속 프로세스에 의해 이루어진다. 그에 따라 보안대책 없이 무분별하게 드론 등이 도입되는 것을 방지하기 위해 2021년 12월에 국방부에서는 '국방 드론 보안 가이드라인'을 발간했다.[6] 가이드라인에 의하면 군에 도입되는 비밀드론은 암호장비를, 평문드론은 KCMVP 검증 암호모듈을 탑재하도록 하는 등 보안대책을 적용하고 있다. 표 3은 한국군 사이버보안 T&E를 설명한 것이다.[1]

표 3. 한국군 사이버보안 T&E 단계

| 구분 | 평가내용 | 세부내용 |
|---|---|---|
| 1단계 | 사이버보안 요구사항 파악 | 모든 대상 시스템 관련 문서를 살펴봄으로써 사이버보안 요구사항을 파악하고 사이버보안 시험평가 수행을 위한 초기 접근 및 계획 개발 |
| 2단계 | 사이버 공격표면 식별 | 공격자가 대상 시스템의 네트워크나 하드웨어, 펌웨어, 물리적 인터페이스, 소프트웨어 등의 접근 가능한 공격 경로를 식별하고 해당 경로에서 발생 가능한 취약점 파악 |
| 3단계 | 사이버보안 개발시험평가 | 취약점 분석·평가 보고서, 보안 평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행 |
| 4단계 | 사이버보안 운용시험평가 | 취약점 분석·평가 보고서, 사이버보안 개발시험평가 산출물 등을 참고하여 공격자 입장으로 취약점 침투 테스트를 수행하고 대상 시스템의 사이버보안 정도를 평가 |

한국군의 획득 프로세스는 미군의 획득 프로세스와 유사하나 사이버보안 T&E는 미군에 비해 간소화되어 있다. 한국 군이 미군보다 간소회된 사이버보안 시험절차를 적용하는 이유는 군사운영 환경, 자원사용의 효율성, 보안 요구사항의 차이, 그리고 국방 정책의 차이에서 비롯된 것으로 보이며 이는 자국의 특성에 맞춘 시험과 평가 절차로 필요 이상의 복잡한 과정을 피하고 제한된 자원을 최대한 효율적으로 활용하기 위한 전략으로 볼 수 있다.

간소화된 사이버보안 시험절차 단점으로는 세부검증 부족으로 미세한 보안 취약점을 놓칠 가능성이 있으며 긴급한 보안 업데이트 대응 부족을 들 수 있다. 지속적인 보안 개선의 어려움이 있고 새로운 위협에 대한 취약성 등이 그 예이다. 또한 국제 표준과의 차이로 국제 연합작전에서의 어려움이 발생될 수 있으며 장비 복잡성에 대한 대응 부족으로 복잡한 시스템에 대한 대응 한계 및 다양한 형태의 드론이나 무인 이동체의 도입시 이들 시스템에 맞는 보안 평가를 세부적으로 진행하기 어려운 확장성 문제에 부딪힐 수 있다. 이러한 단점들을 보완하기 위해 일부 중요한 테스트에서는

4) DIU(Defense Innovation Unit) : 국방 혁신부

추가적인 검증이나 세부적인 평가 단계를 포함하는 것도 좋은 방법이 될 수 있다.

그림 2는 한국군 획득 시험평가 간 한국군의 사이버보안 활동에 대해 설명하였다.

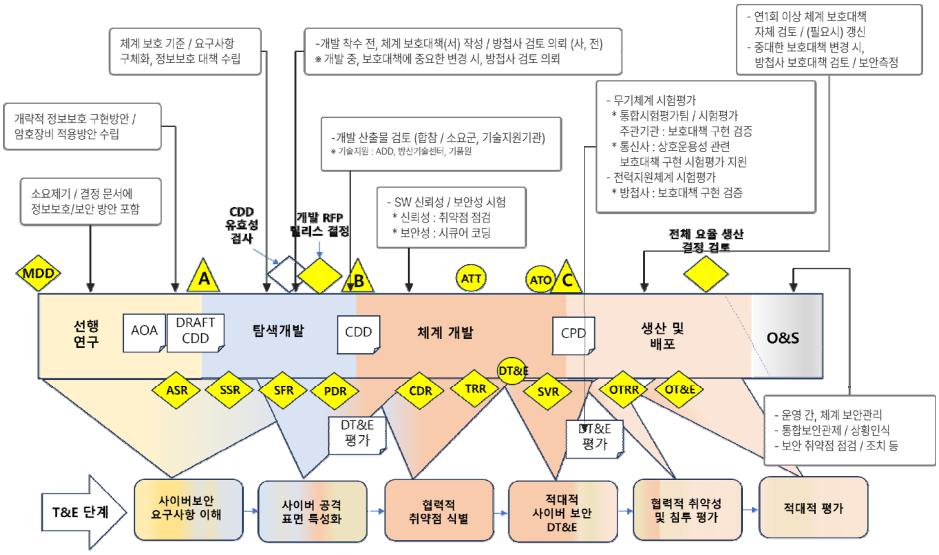


그림 2. 한국군 획득 시험평가 간 한국군의 사이버보안 활동

특히 정보보호 시스템 또는 네트워크 시스템이 포함될 경우에는 보안적합성 검토 및 소프트웨어(S/W) 신뢰성 시험을 별도로 수행하게 된다. 체계 개발이 완료되면 상호운영성 센터에서 상호운영성 평가 항목 각 분야별로 평가를 수행하고 수행한 결과는 시험평가 결과에 반영하여 전력화 여부를 판단한다. 이때 적대적 사이버보안 평가를 위해 사이버사에서는 모의침투 테스트를 수행한다. 운영 전 평가대상 부대(서)에서는 방첩사에 보안측정을 의뢰하고 방첩사에서 보안측정 결과 이상이 없을 경우 평가대상 부대(서)에서는 전력화를 추진한다. 표 4는 국방상호운용성관리지시에 명시된 무기체계에 대한 정보보호 시험평가 세부 항목이다.

표 4. 상호운용성 사이버보안 관련 평가 항목

| 구 분 | 평 가 내 용 | 세 부 내 용 |
|---|---|---|
| 사이버 보안 | 정보보호수준 | 정보보호 수준의 적절성 |
| | 네트워크 정보보호 | 네트워크 정보보호 대책 수립 / 구현의 적절성 |
| | 관제 체계 구축 | 관제 체계 구축 방안 수립/구현의 적절성 |
| | 키 관리체계 구축 | 키 관리체계 구축 방안 수립/구현의 적절성 |
| | 응용체계 정보보호 | 응용 체계 정보보호 대책 수립/구현의 적절성 |
| | 서버 정보보호 | 서버 정보보호 대책 수립/구현의 적절성 |
| | 단말기 정보보호 | 단말기 정보보호 대책 수립/구현의 적절성 |
| | 암호장비 적용 | 암호장비 적용계획/적용의 적절성 |
| | 사이버전 대비 능력 | 신분 위장 위협 대응 능력 |
| | | 데이터 변조 위협 대응 능력 |
| | | 공격행위 부인 위협 대응 능력 |
| | | 정보 유출 위협 대응 능력 |
| | | 서비스 거부 위협 대응 능력 |
| | | 권한 상승 위협 대응 능력 |
| | | 시큐어코딩 규칙 적용 적절성 |
| | | 오픈소스 취약점 및 공개 취약점 제거 적절성 |

## 3. 사이버보안 취약점 진단 도구 개발 방안

무인 이동체에서는 물리적 제어 시스템과 실시간 통신의 보안 평가 필요성이 핵심이다. 무인 이동체는 제어 신호, 실시간 통신, 센서 데이터의 무결성을 보호하는 것이 필수적이며, 사이버보안 시험절차는 더 복잡하고 공격 시나리오가 훨씬 다양하며 물리적 시스템의 안정성까지 고려해야 한다.

무인 이동체의 사이버보안 시험 및 평가 절차는 기존의 사이버보안 시험 및 평가 절차와 비교할 때 다소 차이가 있다. 대부분의 무기체계는 개발 기간이 상당히 길어 사이버보안 시험평가를 위해 준비할 수 있는 충분한 시간이 보장되는 반면 무인 이동체는 구매 후 운용까지 빠른 시간 內 도입이 이루어져 사이버보안 평가를 위한 충분한 시간이 보장되지 않는다. 따라서 무인 이동체의 사이버보안 시험평가를 체계화된 프로세스 없이 진행할 경우 매우 위험한 취약점에 노출될 수도 있다.

이러한 점을 보완하기 위해 본 연구 간 개발 중인 취약점 진단 도구, 시험평가 도구, 위험 평가 도구를 개발하여 적용해야 한다.

### 3.1. 취약점 진단 도구

취약점 진단 도구는 UAV(Unmanned Aerial Vehicle) 및 UAV와 연결된 장비의 취약점을 진단하고 분석하는 도구이며, 주요기능은 UAV에서 사용하는 대표적인 공격 표면(Attack Surface, RF, Wi-Fi, USB 등)에서 발생할 수 있는 취약점을 분석한다. 사용자의 편의성을 위한 웹 기반으로 개발되었으며 사용자 권한에 따라 로그뷰어 및 사용자 수정 기능, 선택한 취약점에 대한 공격의 성공 여부를 확인하여 정밀한 취약점 분석이 가능하다는 특징이 있다. 그림 3은 취약점 진단 도구 구성도이다.

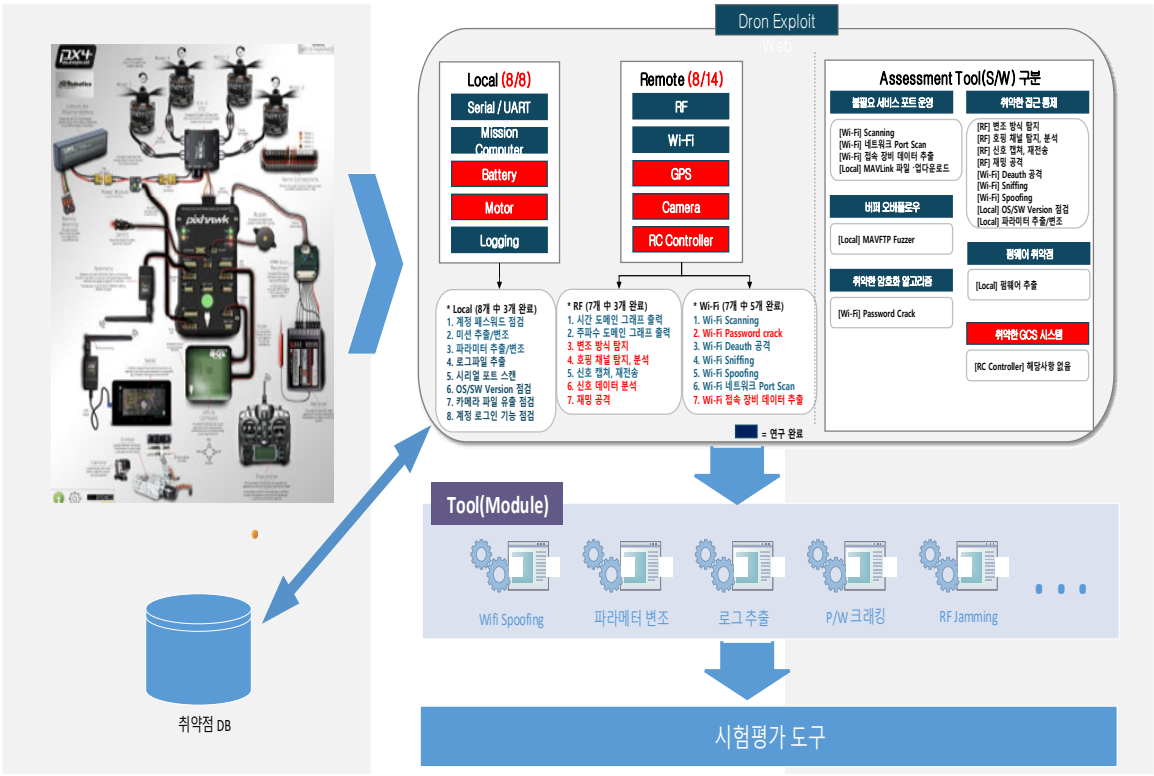


그림 3. 취약점 진단 도구 구성도

### 3.2. 시험평가 도구

시험평가 도구는 UAV의 사이버보안 시험평가를 수행할 수 있도록 지원하는 도구이며, 주요기능으로는 사이버보안 위협이 발생할 수 있는 공격 표면, 체크리스트(평가요소) 자동산출이 되며 킬 체인(Kill-Chain)[9] 구성을 돕기 위한 취약점 매트릭스 및 우선 조치할 취약점이 표기된다. 또한, 진단 결과 중 취약한 항목에 대하여 커스터마이징이 가능한 조치 가이드가 제시되며, 프로파일 기반 진단 수행으로 자산에 대한 빠른 진단 지원이 가능하다. 지금까지의 타 취약점 진단 솔루션과는 다르게 14단계로 구분된 공격 단계에 따른 취약점 매트릭스를 제시함으로써 실질적으로 실현 가능한 위협인 킬 체인에 대한 선제적대응을 지원하며, 시험평가에 대한 특화된 점수 산정식 적용으로 우선조치 취약점에 대한 정보를 별도로 제시한다. 그림 4는 시험 평가 도구 구성도이다.

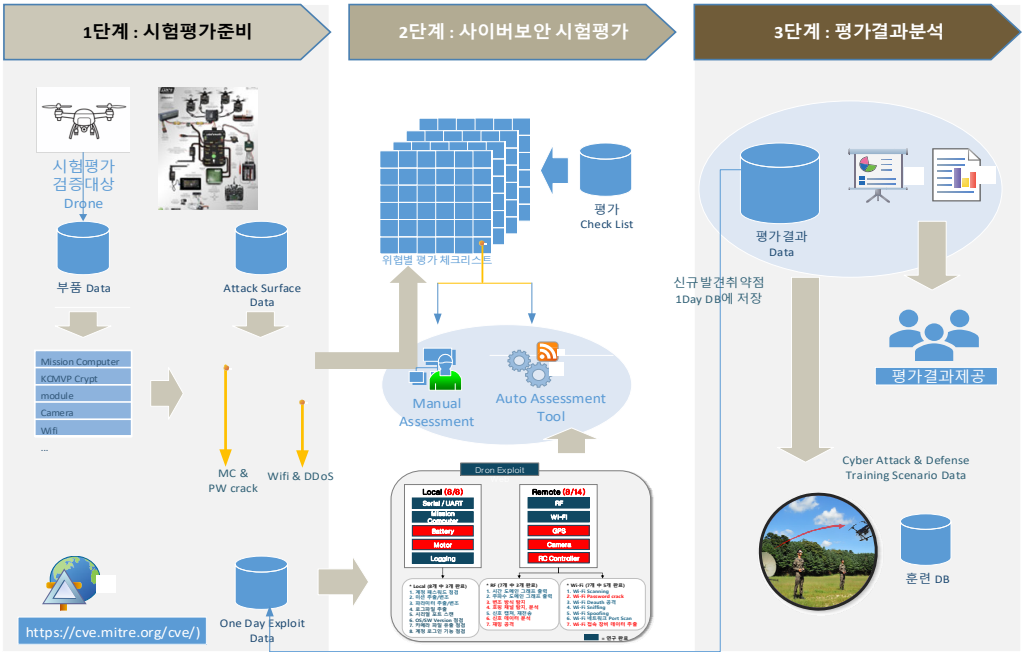


그림 4. 시험 평가 도구 구성도

### 3.3. 위험 평가 도구

위험 평가 도구는 군에서 도입하려는 드론에 산재한 사이버보안 취약점의 위험도를 평가하고, 수용 · 완화 여부를 결정하는데 도움을 주기위한 도구이며, 주요기능으로는 평가대상 드론의 페이로드를 선택하고, 선택 결과에 따라 사이버보안 위협이 발생할 수 있는 공격 표면을 산출해 준다. 또한, 평가대상 드론 특화 킬 체인 목록을 생성해 주며 영향, 가능성, 위협원 분류별 평가를 진행하며, 평가 도구 내 자체 알고리즘에 따라 평가대상 드론에 대한 위험도 점수(평가결과 점수)가 도출된다. 기존 진단 방식과는 차별화된 K-RMF 수명주기 전반에 걸쳐 시나리오 기반 평가 지원 및 각 위협에 따른 위협 완화 방법을 제시한 것이 특징이다. 그림 5는 위험 평가 도구 구성도이다.


그림 5. 위험 평가 도구 구성도

## 4. 무인 이동체 한국군 사이버보안 T&E 절차 적용 방안

사이버보안 시험절차는 사이버보안 시험 및 평가를 위한 구체적인 방법론과 테스트 방법을 정의하고 이를 실행하는 단계이다. 즉, 시스템의 보안 요구사항의 충족 여부를 기술적으로 검증하는 단계라고 볼 수 있다. 시험절차의 목적은 시스템의 보안성, 안정성을 시험하는 구체적인 방법론을 정립하고, 각 단계에서 어떻게 보안을 검증할지 정의하는 것으로, 일련의 계획된 테스트 절차를 따르며, 특정 보안 요구사항을 만족하는지 확인한다.

미군의 6단계와 달리 한국군의 무인 이동체 사이버보안 시험 및 평가 검증에 요구되는 프로세스는 임무 기반의 무기체계 사이버보안 시험평가 적용 연구에서 4단계로 구분하였다. 그러나 첨단 과학기술이 적용된 드론 등 도입시 4단계를 적용하기에는 취약점 등을 분석하기에 한계가 있다고 판단된다. 또한, 취약점 등을 파악하기 위한 도구가 부재한 상황이다.

따라서 본 연구에서는 이러한 취약점을 보완하기 위해서 취약점 진단 도구, 시험평가 도구, 위험평가 도구를 제시하였으며, 이것을 사이버보안 실험 및 평가 절차에 적용하여 보았다.

본 연구에서는 취약점 진단 등 3가지 진단 도구를 제시하면서 임무 기반의 무기체계 사이버보안 시험평가 적용 연구에서 제시한 4단계에서 장비 및 소프트웨어 취약점 평가를 추가하여 5단계로 제시하였다. 표 5는 한국군 사이버보안 T&E 절차 적용 방안을 제시한 것이다.

표 5. 한국군 사이버보안 T&E 절차 적용 방안

| 구분 | 평가내용 | 세부내용 |
|---|---|---|
| 1단계 | 사이버보안 요구사항 파악 | 모든 대상 시스템 관련 문서를 살펴봄으로써 사이버보안 요구사항을 파악하고 사이버보안 시험평가 수행을 위한 초기 접근 및 계획 개발 |
| 2단계 | 사이버 공격표면 식별 | 공격자가 대상 시스템의 네트워크나 하드웨어, 펌웨어, 물리적 인터페이스, 소프트웨어 등의 접근 가능한 공격 경로를 식별하고 해당 경로에서 발생 가능한 취약점 파악 |
| 3단계 | 장비 및 소프트웨어 취약점 평가 | 취약점 진단, 시험평가, 위험 평가 도구를 이용하여 장비 및 사이버보안 취약점을 진단하고 취약점 항목에 대한 커스터마이징이 가능한 가이드 제시 |
| 4단계 | 사이버보안 개발시험평가 | 취약점 분석·평가 보고서, 보안 평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행 |
| 5단계 | 사이버보안 운용시험평가 | 취약점 분석·평가 보고서, 사이버보안 개발시험평가 산출물 등을 참고하여 공격자 입장으로 취약점 침투 테스트를 수행하고 대상 시스템의 사이버보안 정도를 평가 |

1단계 사이버보안 요구사항 파악은 드론을 도입하기 위한 군과 계약업체의 사이버보안 T&E 수행을 위한 초기 및 후속 접근 방식과 계획과 관련된 여러 가지 요건들을 검토하는 것이다. 이 단계에서 시스템의 사이버보안, 시스템 사이버 생존 가능성, 운영 복원력 요건 등을 검토하여 사전에 인증받은 제품을 도입하거나 기존 상용 제품에 새로운 기능을 일부 탑재하여 제작, 도입하거나 새로운 제품을 개발하거나 하는 결정을 내린다. 표 6은 보안대책 검토시 보호 대책 검토 내용이다.

표 6. 보호 대책 검토 내용

| No | 구분 | 세부내용 |
|---|---|---|
| 1 | 네트워크 보호 | 네트워크 경계의 방어, 네트워크 내부 보호, 네트워크 연동 통제 |
| 2 | 서버 보호 | 식별 및 인증, 접근통제, 로그 관리, 서버 보호 프로그램 적용 |
| 3 | 단말기 보호 | 식별 및 인증, 단말기 보호 프로그램 적용 |
| 4 | 응용체계 보호 | 식별 및 인증, 접근통제, 로그 관리, 데이터 보호, 응용 서비스 보호 |
| 5 | 보호 관리 | 비상계획 수립, 사이버 위협 대응, 암호 기술, 정보보호 체계, 형상 관리, 물리적 보호 |

2단계 사이버 공격표면 식별은 시스템 시험 책임자는 알려진 취약점을 식별하고 공격자가 어떻게 접근하는지 설명하기 위한 활동을 수행한다. 그림 6은 드론 사이버 공격표면 개념도이다.

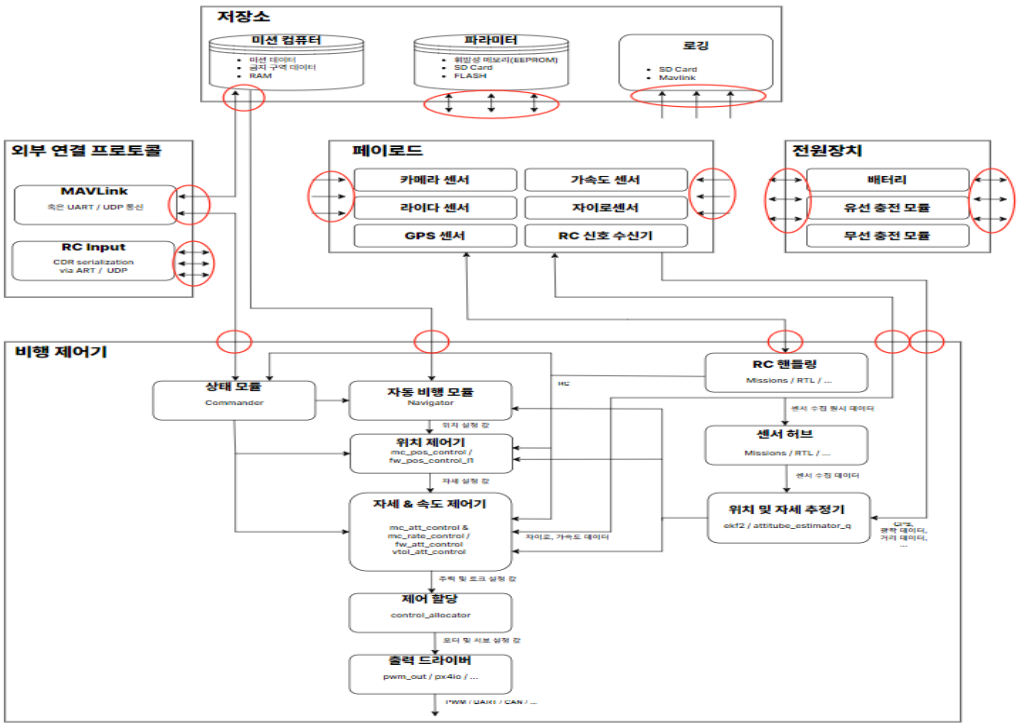


그림 6. 드론 사이버 공격표면 개념도

3단계 장비 및 소프트웨어 취약점 평가는 취약점 진단, 시험평가, 위험 평가 도구를 이용하여 UAV 및 UAV와 연결된 장비의 취약점을 진단하고 분석하고, 14단계로 구분된 공격 단계에 따른 취약점 매트릭스를 이용하여 사이버보안 시험평가를 수행할 수 있도록 지원하며, 드론에 산재한 사이버보안 취약점의 위험도를 평가한다.

4단계 사이버보안 개발시험평가는 하드웨어, 소프트웨어, 인터페이스, 운영 및 아키텍처에서 알려진 사이버보안 취약성을 식별하고, 이러한 취약성과 관련된 임무 위험을 평가하며, 위험을 줄이기 위한 적절한 완화 또는 대응책을 결정하기 위한 것이다. 그림 7은 취약점 분석 평가 시험절차이다.

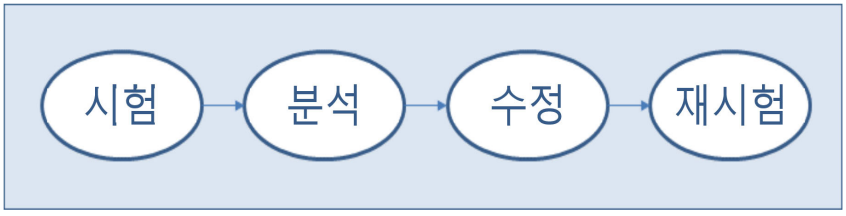


그림 7. 취약점 분석 평가 시험절차

5단계 사이버보안 운용시험평가는 운영 환경에서 현실적인 위협 익스플로어 기술을 사용하여 임무 상황에서 시스템의 사이버 생존 가능성과 운영 복원력을 평가하는 작업이 포함된다. 평가팀(사이버사 모의해킹팀)은 시스템 위협 평가 문서에 설명된 사이버보안 위협 공격자의 일반적인 방법을 사용한다.

## 5. 결론

무인 이동체란 외부로부터의 간섭, 조정이 없이 스스로 외부 환경을 인식하고 상황을 판단하여 이동하며, 필요시에는 작업을 수행하는 지상은 물론, 해상·공중을 망라하는 이동체를 의미한다. 도입될 시스템의 사이버보안 위협에 대한 보안 기능 및 보증에 대한 평가는 매우 중요하다. 특히, 군에서 운용되는 시스템은 대부분 무기체계로 높은 수준의 보안 적용을 요구한다. 한국군에서 무기체계 도입시 상호운용성평가 기준 지침에 따라 획득 단계별 평가 항목에 대한 세부 기준을 마련하여 적용하고 있다. 보안대책 검토, 보안측정을 통해 도입 체계에 대한 사이버 위험을 평가하고 있다.

그러나 첨단 과학기술이 적용된 무인 이동체에 대해서는 구체적인 사이버보안 시험평가 절차나 기준이 없어서 일반적인 정보체계에 적용하는 사이버보안 진단 도구 등을 이용하여 평가를 수행한다. 그러기 위해서는 무인 이동체 도입을 위한 사이버보안 시험 평가(T&E) 체계 도입이 필요하다.

이에 본 기관은 미군의 무인 이동체 사이버보안 T&E와 한국군의 사이버보안 T&E를 비교, 분석 후 드론의 사이버보안 시험절차에 대해 알아보았다. 무인 이동체의 사이버보안 시험절차는 기존의 사이버보안 시험절차와 비교할 때 다소 차이가 있다. 일반적인 정보체계나 무기체계는 사이버보안 시험절차가 숙달되어 있으나, 첨단 과학기술이 적용된 무인 이동체는 구매 후 운용까지 빠른시간內 이루어져야 하지만 사이버보안 시험을 위한 준비가 미비한 상황이다. 따라서 무인 이동체의 사이버보안 시험을 체계화된 프로세스 없이 진행할 경우 매우 위험한 취약점에 노출될 수도 있다. 본 연구는 미군 제도의 장점을 참조 및 한국군의 제도 운용 간 문제점을 식별 및 보완하고 무인 이동체의 시험절차를 어떻게 해야 하는지 그 방안에 대해 연구하였다.

본 연구에서는 미군의 무인 이동체 사이버보안 시험 및 평가 절차를 참조하여 우리 군에 최적화된 시험 및 평가 방안을 설계하여 사이버보안 취약점을 사전에 식별하고 이를 효과적으로 완화할 수 있는 일련의 검증 단계까지 포함하여 제시하였다.

다만, 제안된 절차의 실효성을 극대화하기 위해 지속적인 피드백과 실증 연구가 필요하며, 최신 사이버보안 위협에 대응하기 위한 개선 작업이 필수적이다. 향후 연구에서는 빠르게 변화하는 사이버 위협 환경을 반영한 시험절차의 지속적인 개선이 필요하며, 국제 표준 및 연합군과의 협력 강화를 통하여 보다 종합적이고 실전적인 사이버보안 전략이 개발될 수 있어야 할 것이다.

## Acknowledgement

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2023-00232964, 국방 무인이동체 사이버보안 검증 프레임워크 및 시험환경 개발).

## 참고문헌

[1] Kim I et al. A Study on the Application of Mission-based Weapon System Cybersecurity Test and Evaluation. Journal of Internet Computing and Services, Vol. 22, No. 6, pp. 71-81. 2021.

[2] USA DoDI 5000.02, Cybersecurity Test and Evaluation Guidebook 2.0, Change 1. 2020.

[3] NIST SP 800-37. Guide for Applying the Risk Management Framework to Federal

Information systems Rev. 1. 2010.

[4] Cho H et al. A Case Study on the Applicaion of RMF to Domestic Weapon System. Journal of The Korea Institute of Information Security & Cryptology, Vol. 29, No. 6. 2019.

[5] 김백중, 정석재. 국방 무기체계 시험평가 수행체계 개선방안 연구. 한국국방기술학회 논문지, 제5권 제2호, pp. 1-9. 2023.

[6] 국방부. 국방 드론 보안 가이드라인. 2021.

[7] 한국인터넷진흥원. 정보통신망 연결기기등 정보보호인증기준 상세 해설서(드론). 2024.

[8] 한국인터넷진흥원. 드론분야 ICT 융합 제품 · 서비스의 보안 내재화를 위한 드론 사이버보안 가이드. 2020.

[9] Lee J et al. A Study on Defense and Attack Model for Cyber Command Control System based Cyber Kill Chain. Journal of Internet Computing and Services, Vol. 22, No. 1, pp. 41-50. 2021.