IDAP INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2026, Vol. 9, No. 2, 15-39.

https://doi.org/10.37944/advmil.9.2.202610.002

Threat Classification of Multi-Domain Unmanned Systems and the Design of an Integrated Counter-Unmanned Systems (C-US) Framework: A Conceptual Study on Linking Capability Gaps to Response Components

Kwon Hyuk-Jin* · Kim Hyungsuk** · Kim Jang-Yeop***

ABSTRACT

Unmanned system threats are expanding from the air into the land, maritime, subsurface, and space domains, yet discussion of countermeasures has centered on aerial threats. An integrated Counter-Unmanned Systems (C-US) concept spanning multiple domains and a multi-domain threat classification framework have each been proposed. However, neither has addressed which component of the operational concept closes the capability gaps they identify. This conceptual study addresses that linkage problem. It first consolidates a classification framework built on four classification axes and the concept of cross-domain threats, refining the recording unit of the operational-domain axis and the definition of cross-domain relationships.

The study then identifies four constraint-driven capability gaps, which arise when threat attributes structurally exclude available countermeasures. It maps these gaps to the four components of the C-US operational concept: multi-domain integrated command and control, organization, doctrine and procedures, and technical support. The result is a gap-response matrix. The analysis shows that three gaps can be addressed by specific components: the neutralization of RF-based countermeasures, the limits of simultaneous engagement, and the compounding of constraints. The gap arising from the difficulty of cross-domain handling, however, requires a multi-domain integrated command and control system. To allow future research to test these linkages, the study presents five testable propositions with falsification conditions, and the appendix contains a two-round Delphi survey design for evaluating them. Establishing expert consensus and empirically verifying response effectiveness remain tasks for future research.

www.kci.go.kr

Keywords : Counter-Unmanned Systems (C-US), Cross-Domain Threat, Constraint-Driven Capability Gap, Gap-Response Matrix, Conceptual Study

* (First Author) Department of Defense Acquisition Program, Kwangwoon University, kadiakorea@gmail.com, https://orcid.org/0009-0000-8461-6838.

** (Co-Author) Director, Drone Center, Korea Anti Drone Industry Association, kimhs01@gmail.com, https://orcid.org/0009-0001-2844-5824.

*** (Corresponding author) Professor and Chair, Department of Defense Acquisition Program, Kwangwoon University, jykim1670@kw.ac.kr, https://orcid.org/0000-0001-7258-3928

www.kci.go.kr

Ⅰ. 서 론

1.1 연구 배경 및 목적

러시아-우크라이나 전쟁을 거치며 무인체계(unmanned systems)는 보조 전력에서 주요 무기체계의 하나로 자리 잡았다. 공중의 드론뿐 아니라 흑해의 무인수상정, 지상의 무인차량이 실제 전투에 투입되었고, 값싼 상용 부품으로 만든 무인 자산이 고가의 유인 전력을 잡는 일이 드물지 않게 되었다[1].

그러나 이러한 무인체계에 대한 대응 논의는 대부분 공중의 드론 위협을 막는 문제에 머물러 있다. 이 한계를 넘기 위해 영역 구분 없이 무인체계의 위협을 다루는 통합 무인체계 대응(Counter-Unmanned Systems, C-US) 개념과 운용개념(Concept of Operations, CONOPS)이 제안되었고[2], 대응의 전제가 되는 위협을 다섯 개 작전 영역에 걸쳐 분류하면서 영역 횡단 위협(Cross-Domain Threat)을 따로 설정한 분류체계도 제시되었다[3].

두 논의는 같은 문제의식에서 출발하였으나 따로 전개되었다. 분류체계에서 도출한 능력 공백과 운용개념의 구성요소는 각각 정리되어 있지만, 소요를 검토할 때 먼저 필요한 연결, 곧 특정 공백을 어느 구성요소가 메우는지는 양쪽 모두 다루지 않았다. 또한 분류축과 위협 범주가 공개출처정보(Open Source Intelligence, OSINT)를 바탕으로 한 정성적 판단에 기대고 있다는 점도 한계로 볼 수 있다.

본 연구는 이 두 논의를 하나의 틀로 묶어 확장한 개념적 연구(conceptual study)이다. 먼저 분류 틀을 정리하고 적용 규칙을 보완한 뒤, 분류에서 도출되는 제약 기반 능력 공백(constraint-driven capability gap)을 C-US 운용개념의 구성요소에 대응시킨 공백–대응 매트릭스를 제시한다. 그리고 이 연결이 실제로 성립하는지를 후속 연구에서 확인할 수 있도록 검증 명제와 조사 설계를 함께 제시한다.

1.2 문제 제기 및 연구 질문

기존 논의에서 먼저 드러나는 한계는 대응의 분절이다. 가장 널리 쓰이는 무인기 분류(Group 1～5)는 중량과 운용고도를 기준으로 하므로 공중 이외의 무인체계에는 적용되지 않는다. 대드론체계 연구 역시 공중 위협인 드론 대응에 집중되어 왔다. C-US 개념 연구가 이 분절을 문제 삼았지만 위협 분류와 대응 설계가 따로 제시되면서, 정작 둘을 잇는 고리는 비어 있다.

검증도 문제로 남아 있다. 영역 횡단 위협을 독립 범주로 설정한 분류체계는 전문가 검토를 거치지 않았고, 무엇을 확인해야 이 분류가 타당하다고 말할 수 있는지도 정리되어 있지 않다.

위의 문제를 바탕으로 본 연구에서는 다음의 네 가지 연구 질문을 설정하였다. Q1과 Q2는 기존 분류 논의에서 다룬 질문을 이어받아 적용 규칙을 보완한 것이고, Q3과 Q4는 본 연구에서 새로 제기한 질문이다.

www.kci.go.kr

Q1. 공중・지상・수상・수중・우주의 무인체계 위협을 어떤 기준으로 분류하고, 한 체계가 여러 영역에 걸칠 때 이를 어떻게 기록할 것인가?
Q2. 기존 분류가 영역의 경계를 넘나드는 위협을 포착하지 못하는 이유는 무엇이며, 영역 횡단 위협을 운용 영역 축과 어떤 관계로 정의할 것인가?
Q3. 분류 속성에서 도출되는 능력 공백은 통합 C-US 운용개념의 어떤 구성요소에 의해 해소되는가?
Q4. 분류–공백–대응의 연결을 후속 실증에서 확인하려면 어떤 검증 명제로 정식화하고, 어떤 절차로 평가해야 하는가?

1.3 연구 범위, 방법 및 구성

본 연구의 분석 대상은 공중, 지상, 수상, 수중, 우주의 다섯 개 영역에서 운용되는 무인체계로 한정하였다. 사이버 영역은 물리 영역의 위협을 매개하는 수단으로 보고 독립된 영역으로 다루지 않는다.

연구는 문헌과 OSINT를 바탕으로 한 개념적 연구 방법을 사용하였다. 개념적 연구는 새 자료를 수집하는 대신 기존 개념을 통합하거나 개념 사이의 관계를 모형으로 제시하는 방식이다[4]. 본 연구는 두 선행 개념을 하나의 설명 구조로 묶는 통합(theory synthesis)과, 구성요소 간 관계를 제시하는 모형(model) 방식을 함께 사용한다. 델파이 조사는 수행하지 않았으며, 5장의 명제를 평가하기 위한 조사 설계만 부록 A에 수록하였다.

본 연구는 1장 서론에 이어 2장에서는 다영역작전, 무인체계 위협 분류, 대드론체계에 관한 국내외 연구를 검토한다. 3장은 분류 틀을 정리하면서 운용 영역 축과 영역 횡단 위협의 관계를 보완하고, 4장은 능력 공백을 도출하여 C-US 구성요소와 연결한다. 5장에서 검증 명제를 제시하고, 6장과 7장에서 한반도 안보환경에 대한 함의와 결론을 다룬다.

Ⅱ. 이론적 배경 및 선행 연구

2.1 다영역작전 개념과 무인체계 위협 분류

다영역작전(Multi-Domain Operations, MDO)은 지상, 해양, 공중, 우주, 사이버 영역의 능력을 통합・동기화하여 적 체계에 효과를 내는 작전 개념이다. 미 육군은 2022년 10월 개정한 야전교범 FM 3-0(Operations)에서 다영역작전을 기본 교리로 채택하였다[5],[6]. 이 교리는 여러 영역에서 동시에 작전하는 것(operating in multiple domains)과 영역 간 효과를 통합해 적 체계에 작용시키는 것(multi-domain operations)을 구분하는데[7], 본 연구가 영역 횡단 위협을 바라보는 관점은 후자에 유사하다.[1)]

1) Army FM 3-0은 2025년 3월에 개정판이 공개(https://smallwarsjournal.com/2025/04/13/army-fm-3-0-march-2025/)

www.kci.go.kr

미 의회조사국(Congressional Research Service, CRS) 자료에 따르면 미 육군은 정찰, 타격, 교란을 조율하는 다영역임무부대(Multi-Domain Task Force, MDTF)를 편성하고 있으며, 이 부대는 무인항공체계와 궤도 센서 등을 활용해 적의 반접근·지역거부(Anti-Access/Area Denial, A2/AD) 체계에 대응한다[8]. 미국의 개념에서는 무인체계가 한 영역에 묶인 자산이 아니라, 영역을 넘나들며 효과를 전달하는 수단으로 쓰이고 있는 것이다.

무인체계의 위협은 무인체계 분류에서 출발한다. 가장 많이 인용되는 것은 미 국방부의 5개 그룹 분류(Group 1～5)이다. 최대이륙중량, 운용고도, 비행 속도를 기준으로 무인항공체계를 다섯 등급으로 나눈 것으로[9], 군용 무인기를 국가 공역 체계(National Airspace System)에 편입시키려는 목적에서 만들어졌다[10]. 이 분류는 획득과 공역 관리에는 유용하지만 위협 분석에 그대로 쓰기는 어렵다. 제원 중심의 기준으로는 위협 행위의 유형이나 통신·자율성 의존 구조를 구분할 수 없고, 애초에 항공기를 대상으로 설계되어 다른 영역의 무인체계를 포함하지 못한다. 국내 연구도 사정이 크게 다르지 않다. 강한태[11]는 미래전에 대비한 무인기 운용 방향을 다루면서 무인기를 원격조종 항공기(Remotely Piloted Aircraft, RPA)로 보아야 한다고 제안하였는데, 논의의 대상은 아군 무인항공기의 운용이었다.

2.2 통합 대응 개념 및 선행 연구의 공백

대응체계 연구는 주로 탐지–추적–식별–대응으로 이어지는 처리 절차 또는 킬체인을 정형화하고, 단계별 센서와 대응 수단을 분석하는 방향으로 진행되어 왔다[12],[13]. Tan 등[14]은 이러한 연구가 탐지·식별 기술과 킬체인 내 인간 개입 문제에 치우쳐 있고, 인접 우군과 민간을 포함한 체계 수준의 분석은 부족하다고 지적하였다.

국내에서는 소형 드론 위협과 대드론체계를 다룬 연구가 늘고 있으나 대부분 공중 영역에 한정되어 있다. 심준학 등[15]은 미국과 이스라엘 사례를 바탕으로 군, 경찰, 공공기관, 민간 기업, 지역사회가 역할을 나누는 거버넌스 기반의 국가중요시설 대드론체계를 제안하였다. 여러 주체의 책임을 조정한다는 점에서 본 연구의 문제의식과 닿아 있으나, 대상은 공중 드론 위협이다. 여러 영역의 자산을 하나의 체계로 검증하는 문제와 관련해서는, 인공지능 등 신기술을 적용한 무기체계의 야전운용시험에 디지털 트윈을 활용하는 방안이 제시된 바 있다[16]. 통합 대응체계의 성능을 실제 교전 이전에 확인하는 데 참고할 만한 접근이지만, 무인 위협의 분류와 직접 연결된 연구는 아니다.

다영역의 관점을 대드론체계에 적용한 국내 연구도 나오고 있다. 서강일 등[17]은 러시아-우크라이나 전쟁에서 양국이 운용한 대드론체계를 지상, 공중, 사이버, 전자기 스펙트럼 영역으로 나누어 분석하고, 하드킬과 소프트킬 무기체계를 여러 영역에 걸쳐 융복합하되 저가형 고효율 체계를 민군융합형으로 구축해야 한다고 제언하였다. 이 연구에서 다영역은 대응 수단이 운용되는 영역을 가리키며, 대응의 대상은 여전히 공중의 무인기이다.

되었으나, 다영역작전의 개념을 2022년 2월의 내용을 계승하여 사용하고 있다.

www.kci.go.kr

위협의 영역을 공중 밖으로 넓힌 연구로는 전창빈[18]이 있다. 이 연구는 공중의 군집 드론과 북한의 수중 무인체계를 함께 다루면서 거부적・응징적 억제 이론을 분석 틀로 삼았다. 이를 바탕으로 기존 감시 자산에 AI를 통합하는 단계적 획득, 드론작전사령부를 다영역 합동 교육・훈련 및 개념발전 컨트롤 타워로 전환하는 조직 개편, 통신 단절에 대비한 조건부 타격 권한 위임 등을 제시하였다. 위협을 수중까지 넓히고 조직・교리 차원의 대응을 제시하였다는 점에서 본 연구와 문제의식이 가장 가깝다. 다만 위협을 공통의 기준으로 분류하는 틀은 제시하지 않았고, 도출한 취약점을 대응체계의 어느 구성요소가 메우는지도 다루지 않았다. 이처럼 대응 수단을 다영역으로 확장하거나 위협의 영역을 넓힌 연구는 이루어지고 있으나, 영역을 넘나드는 무인 위협을 분류하고 이를 하나의 대응체계 설계로 연결한 연구는 [2],[3]을 제외하면 아직 제한적이다.

C-UAS(Counter-Unmanned Aerial Systems)의 공중 편중을 극복하려는 시도로 무인항공기(UAV), 무인지상차량(UGV), 무인수상정(USV), 무인수중정(UUV)을 하나의 대응체계로 다루는 C-US 개념이 제안되었다[2]. 이 개념은 탐지, 식별, 추적, 대응의 네 기능을 모든 영역에 공통으로 적용하고, 다영역 통합 지휘통제(Multi-Domain Command and Control, MD-C2), 조직(통합대응팀), 교리・절차, 기술지원의 네 구성요소가 이를 뒷받침하도록 구성되어 있다. 영역 경계에서 벌어지는 복합 공격에 방공 중심 체계가 취약하다는 점도 지적하였으나, 그러한 위협을 식별하고 분류하는 틀까지 제시하지는 않았다.

위협 분류 측면에서는 운용 영역, 통신・자율성 의존 구조, 위협 행위 유형, 영역 고유 제약의 네 축으로 구성된 다축 분류체계가 제시되었다[3]. 이 분류체계는 영역을 넘나드는 위협을 영역 횡단 위협으로 정의하고 세 가지 양상으로 나누었다. 또한 능력 공백의 원인을 기술의 미성숙보다는 위협의 분류 속성이 특정 대응 수단을 구조적으로 배제하는 데서 찾고, 이를 제약 기반 능력 공백이라 하였다.

선행연구의 내용을 나란히 놓으면 비어 있는 곳이 드러난다. 분류에서 도출한 네 가지 능력 공백과 운용개념의 네 구성요소가 각각 정리되어 있지만, 어떤 공백을 어떤 구성요소가 메우는지는 설명되지 않았다. 본 연구는 이 연결을 4장의 공백–대응 매트릭스로 다룬다. 분류축과 영역 횡단 양상이 정성적 판단에 근거한다는 문제도 남아 있다. 선행연구 [3]은 전문가 조사를 후속 과제로 제안하였으나 무엇을 어떤 기준으로 검증할지는 정하지 않았다. 본 연구도 검증은 수행하지 않았으며, 5장에서 검증 명제를 정리하는 데 그쳤다.

Ⅲ. 다영역 무인체계 위협 분류 프레임워크

3.1 분류 설계 원칙과 방법론적 근거

공중, 지상, 수상, 수중, 우주의 다섯 영역 위협을 하나의 틀에서 비교하려면 공통의 축으로 정렬하면서도 영역별 성격 차이를 구분할 수 있어야 한다. 분류 틀은 이를 위해 세 가지 원칙에 따라

www.kci.go.kr

설계되었다. 먼저 영역 비교 가능성(cross-domain comparability)은 분류 축이 특정 영역의 제원이 아니라 다섯 영역 모두에 적용할 수 있는 차원이어야 한다는 원칙이다. 대응 연계성(response relevance)은 위협의 외형보다 대응 수단의 선택을 좌우하는 속성을 축으로 삼아야 한다는 것으로, 분류가 대응 설계로 이어지게 하는 원칙이다. 제약 명시성(constraint explicitness)은 부수피해, 식별 곤란, 통신·탐지의 물리적 한계, 국제법처럼 대응을 구속하는 영역 고유 제약을 별도 차원으로 드러내야 한다는 원칙이다.

이 세 원칙은 선행 분류 연구에서 독자적으로 제안된 것이다. 분류체계 개발에 관한 방법론 문헌에 비추어 보면 각 원칙이 어떤 역할을 하는지 설명할 수 있다. Nickerson 등[19]은 분류체계를 개발할 때 분류의 목적에서 메타특성(meta-characteristic)을 먼저 정하고, 모든 차원이 이 메타특성에서 도출되도록 할 것을 요구한다. 본 분류에서 메타특성은 '대응 수단의 선택에 영향을 주는 위협 속성'이며, 대응 연계성 원칙이 이 역할을 맡는다. 같은 문헌은 모든 대상이 각 차원에서 하나의 특성값만 갖도록 차원을 구성할 것을 요구하는데, 영역 비교 가능성은 이 조건을 다섯 영역 전체에 걸쳐 적용하려는 원칙으로 볼 수 있다. 영역 고유 제약은 한 대상에서 제약이 겹쳐 나타날 수 있어 이 조건의 예외로 두었다.

분류체계가 대상을 기술하는 데서 그치지 않고 그 성질을 설명해야 한다는 설명력(explanatory) 조건은 제약 명시성 원칙과 맞닿아 있다. 다차원 유형론의 구성 방식은 Bailey[20]를 참고하였다. 다만 Nickerson 등이 제시한 반복적 개발·평가 절차를 본 연구에서 모두 수행한 것은 아니다. 위의 대응 관계는 원칙의 근거를 설명하기 위한 것이다.

3.2 네 개 분류 축

네 분류 축은 다음과 같다. 축 1 운용 영역(Operating Domain)은 공중, 지상, 수상, 수중, 우주로 구분한다. 축 2 통신·자율성 의존(Communication-Autonomy Dependency)은 전파 의존형(무선주파수·위성항법 신호), 유선 연결형(광섬유 케이블 등), 모선 의존형(상위 통신중계 자산에 의존), 완전 자율형(관성항법·탑재 자율판단)으로 나눈다. 축 3 위협 행위 유형(Threat Behavior)은 정찰·표적지정, 자폭·직접타격, 인프라 사보타주, 항법·통신 교란, 통신중계·다영역 협업의 다섯 가지이다. 축 4 영역 고유 제약(Domain-Specific Constraint)은 부수피해 제약, 식별 곤란, 통신·탐지 물리 한계, 국제법·관할권 제약으로 구분한다. 다음의 표는 선행연구[3]를 바탕으로 정리한 다영역 무인체계 위협의 분류 축이다.

초기 분류에서는 위협 하나에 운용 영역 하나를 부여하였는데, 수상에서 수중으로 들어가는 양용 무인체계나 공중 중계기와 함께 움직이는 무인수상정처럼 한 영역에 넣기 어려운 사례[2]가 적지 않았다. 그래서 축 1의 값을 '특정 플랫폼이 특정 임무 단계에서 주로 운용되는 물리 영역'으로 정의하

2) 한경BUSINESS(2026.9.25.). 수중에서 벌어지는 무인 전쟁[테크트렌드]. https://magazine.hankyung.com/business/article/202609171291b

www.kci.go.kr

였다. 한 플랫폼이 임무 중에 영역을 바꾸면 단계별로, 여러 플랫폼이 협업하면 플랫폼별로 값을 기록한다. 위협 하나에 축 1의 값이 여러 개 붙을 수 있지만, 기록 단위(플랫폼・단계) 하나에는 값이 하나만 붙는다. 축 2와 축 3도 기록 단위 하나에 값 하나를 부여한다. 축 4는 부수피해 제약과 식별 곤란처럼 한 기록 단위에서 제약이 겹쳐 나타날 수 있으므로 복수의 값을 허용한다.

〈Table 1〉 Classification axes for multi-domain unmanned systems threats

Classification axis	Classification criteria and categories
Axis 1: Operating Domain	Air, land, surface, underwater, space
Axis 2: Communication-Autonomy Dependency	RF(Radio Frequency)-dependent, wire-linked, mothership-dependent, fully autonomous
Axis 3: Threat Behavior	Reconnaissance and target designation, one-way attacks and direct strikes, infrastructure sabotage, navigation and communication disruption, communication relay and multi-domain cooperation
Axis 4: Domain-Specific Constraint	Collateral-damage constraints, identification difficulties, physical limitations on communication and detection, international law and jurisdictional constraints

네 축을 조합하면 개별 위협을 다차원으로 기술할 수 있다. 광섬유 유선 일인칭시점(First-Person View, FPV) 자폭 드론[3]은 <공중, 유선 연결형, 자폭・직접타격, 부수피해 제약>으로, 항만 침투형 자폭 무인수중정은 <수중, 완전 자율형 또는 모선 의존형, 자폭・직접타격, 통신・탐지 물리 한계>로 기술된다. 두 위협은 모두 자폭・직접타격형이지만, 앞의 것은 전파 탐지와 재밍이 통하지 않고 뒤의 것은 소나 외에 마땅한 탐지 수단이 없다는 점에서 대응 수단이 갈린다.

3.3 영역 횡단 위협과 운용 영역 축의 관계

영역 횡단 위협은 단일 무인체계 또는 여러 무인체계의 협업이 둘 이상의 작전 영역을 통과・연계・전이하면서 형성되는 위협으로, 식별과 대응의 책임이 한 영역의 자산이나 주체에 온전히 귀속되지 않는 위협을 말한다. 이런 위협을 하나의 영역에 귀속시키면 위협의 실체와 대응 요구가 왜곡된다.

이에 따라 본 연구에서는 영역 횡단을 축 1의 여섯 번째 값으로 보지 않고, 기록 단위 사이의 관계로 정의하였다. 축 1은 각 기록 단위가 어느 영역에 있는지를 나타낸다. 영역 횡단은 영역값이 다른 두 기록 단위(단계 또는 플랫폼), 혹은 효과가 발생한 영역과 피해가 나타난 영역 사이의 연결을 나타낸다. 영역값이 서로 다른 기록 단위가 있다고 해서 모두 영역 횡단 위협이 되는 것은 아니다. 그 연결 때문에 식별과 대응책임이 한 영역에 귀속되지 않을 때에 한하여 영역 횡단 위협으로 본다.

이 정의에 따르면 세 양상은 관계의 양 끝이 무엇이냐로 구분된다. 플랫폼 양용형(platform

3) KBS뉴스(2025.6.23.). 전장의 지배자 '광섬유 드론'…러시아 진격의 비밀? [특파원 리포트]. https://news.kbs.co.kr/news/pc/view/view.do?ncd=8285285

www.kci.go.kr

dual-medium)은 한 플랫폼이 영역 경계에서 운용 매질을 바꾸는 경우로, 같은 플랫폼의 두 임무 단계가 양 끝이 된다. 협업 연계형(collaborative relay)은 서로 다른 영역의 무인체계가 통신중계로 협업하여 단독으로는 얻을 수 없는 지속성과 사거리를 확보하는 경우이며, 두 플랫폼이 양 끝이다. 영향 전이형(effect propagation)은 한 영역에서 발생한 효과가 다른 영역의 자산에 미치는 경우로, 효과의 발생 영역과 피해 영역이 양 끝이 된다. 우주 기반 위성항법(Global Navigation Satellite System, GNSS) 신호를 대상으로 한 교란·스푸핑이 영향 전이형의 대표적인 예이다. 교란원은 주로 지상에 있으나 영향을 받는 것은 위성에서 내려오는 항법 신호이며, 피해는 그 신호에 의존하는 여러 영역의 자산에 나타난다. <표 2>는 선행연구[3]의 세 양상을 위 정의에 맞추어 다시 정리한 것이다.

〈Table 2〉 Three manifestations of cross-domain threats

Manifestation	Relational endpoints	Core mechanism	Representative examples
Platform dual-medium	Two mission phases of the same platform	Transition between operating media	A surface-underwater unmanned system that reduces its radar cross-section and acoustic signature before submerging
Collaborative relay	Two platforms operating in different domains	Cooperation through communication relays between assets in different domains	UAV-USV/UUV communication relays, UAV-USV cooperation in providing targeting support against surface fleets
Effect propagation	The domain in which an effect originates and the domain in which harm occurs	Separation between the domain of origin and the affected domain	GNSS jamming and spoofing with simultaneous effects on navigation-dependent assets across the air, land, surface, and underwater domains

세 양상에서는 공통적으로 대응 책임의 공백(responsibility gap)이 생긴다. 양용형은 영역이 바뀌는 순간 탐지 책임의 인계가 끊기기 쉽다. 협업 연계형은 위협의 핵심이 영역 사이의 연결에 있어서 한 영역의 자산만으로는 대응이 완결되지 않는다. 영향 전이형은 효과가 발생한 곳과 피해를 입은 곳이 달라서, 누가 대응 주체인지를 정하는 일부터 쉽지 않다.

3.4 영역별 위협 분류의 적용

네 축을 다섯 영역에 적용한 결과는 <표 3>과 같다. 공중에서는 광섬유 유선 드론, FPV 자폭 드론, 배회형 탄약(loitering munition), 군집 드론이, 지상에서는 자폭 UGV, 무인전투차량(Robotic Combat Vehicle, RCV), 자율 보급후송 UGV가 대표 체계이다. 수상에서는 자폭 USV, 중형 자폭 USV, 자율 호위함급 무인함, 군집 USV가, 수중에서는 소형 자율수중정(Autonomous Underwater

www.kci.go.kr

Vehicle, AUV), 글라이더형 UUV, 초대형 무인수중정(Extra-Large UUV, XLUUV), 항만 침투형 자폭 UUV가 해당한다. 우주에서는 군집 소형위성, 자율 궤도 근접기동체(Rendezvous and Proximity Operations, RPO),[4] 대위성무기(Anti-Satellite, ASAT),[5] GNSS 교란・스푸핑을 들 수 있다. GNSS 교란・스푸핑은 그 자체로 무인체계가 아니고 발신원도 대부분 지상에 있다. 다만 선행연구[3]와의 일관성을 위해, 우주 기반 항법 신호를 겨냥한 위협으로 보아 우주 영역에 함께 기록하였다.

〈Table 3〉 Representative threat systems and classification attributes by domain

Attribute	Air	Land	Surface	Underwater	Space
Representative systems	FPV drones, loitering munitions, wire-linked drones, drone swarms	One-way attack UGVs, RCVs	One-way attack USVs, frigate-class autonomous USVs, USV swarms	AUVs, XLUUVs, one-way attack UUVs	Small-satellite swarms, RPO, ASAT, GNSS jamming/ spoofing
Communication-autonomy dependency (Axis 2)	Mix of RF-dependent, wire-linked, and fully autonomous systems	RF-dependent and fully autonomous systems	RF-dependent and fully autonomous systems	Fully autonomous systems	Mothership-dependent and fully autonomous systems
Threat behavior (Axis 3)	One-way attacks and direct strikes	One-way attacks and direct strikes	One-way attacks and direct strikes	Reconnaissance and target designation, infrastructure sabotage	Navigation and communication disruption (effect propagation)
Domain-specific constraints (Axis 4)	Physical limitations on communication and detection (small targets)	Collateral-damage constraints, identification difficulties	Identification difficulties (civilian vessels), collateral-damage constraints	Physical limitations on communication and detection	International law and jurisdictional constraints (orbital debris)

자폭・직접타격형은 공중・지상・수상에서 대응 시급성이 가장 높은 위협 행위이다. 통신・자율성 측면에서는 영역을 가리지 않고 완전 자율형 쪽으로 옮겨 가고 있다[1]. 완전 자율화가 진행되면 통신을 끊는 방식의 소프트킬은 어느 영역에서든 효과가 떨어진다. 반면 영역 고유 제약(축 4)은 영

4) ZDNETKorea(2026.9.22.). 나라스페이스, 초소형위성 자율 근접운용 기술 개발 나선다. https://zdnet.co.kr/view/?no=20260922175325

5) TWZ10(2026.8.13.). New Anti-Satellite Weapons Now Officially A Top U.S. Priority. https://www.twz.com/space/new-anti-satellite-weapons-now-officially-a-top-u-s-priority

www.kci.go.kr

역마다 달라서, 대응 수단의 선택을 실제로 가르는 것은 이 축인 경우가 많다.

Ⅳ. 제약 기반 능력 공백과 공백-대응 매트릭스

4.1 제약 기반 위협-대응 정합성

위협-대응 정합성은 두 단계로 나누어 볼 수 있다. 탐지 정합성은 위협을 식별·추적할 수 있는 탐지 원리가 있는지의 문제이고, 무력화 정합성은 식별된 위협에 쓸 수 있는 대응 수단이 있는지의 문제이다. 대드론체계의 표적 처리 절차에 대입하면 탐지·추적·식별 단계가 앞의 것에, 대응 단계가 뒤의 것에 해당한다.

이 분석틀의 특징은 정합성을 위협의 분류 속성에 따라 달라지는 변수로 본다는 데 있다. 통신·자율성 의존 구조(축 2)는 소프트킬이 통하는지를 좌우하고, 영역 고유 제약(축 4)은 하드킬과 탐지의 적용 범위를 제한하며, 위협 행위(축 3)는 대응이 얼마나 급한지를 정한다. 이렇게 보면 능력 공백은 어떤 장비가 없어서 생긴다기보다, 위협의 속성 조합이 쓸 수 있는 수단을 구조적으로 배제할 때 생긴다고 할 수 있다.

4.2 탐지와 무력화의 정합성

탐지 정합성은 영역과 통신 의존 구조에 따라 달라진다. 전파 의존형 위협은 전파 탐지와 방향탐지로 식별할 수 있으나, 전파가 혼잡한 환경에서는 정확도가 떨어진다. 유선 연결형 드론은 전파를 쓰지 않으므로 전파 탐지가 통하지 않고 광학·음향·열영상 탐지에 의존해야 한다. 수중에서는 전파가 감쇠하여 음향(소나)에 기댈 수밖에 없는데, 저소음 무인수중정은 소나로도 잡아내기 어렵다. 우주에서는 거리와 궤도 환경 때문에 평시의 근접기동(RPO)과 정상 운용을 구분하기가 쉽지 않다. 이런 한계를 보완하려면 전파·레이더·EO·IR·음향 센서를 융합해야 하는데, 이는 통합 지휘통제 기반과 센서 간 데이터 표준화가 먼저 갖추어져야 가능하다.

무력화 정합성은 소프트킬과 하드킬로 나누어 볼 수 있다. 소프트킬이 통하는지는 축 2에 달려 있다. 전파·위성항법 재밍은 전파 의존형에는 유효하지만 유선 연결형에는 효과가 없고, 완전 자율형에는 통신을 끊는 방식 자체가 작동하지 않는다. 사이버 침투는 상용 프로토콜 기반 체계에 한정되며 군용 암호화 체계에는 적용이 제한된다. 하드킬의 적용 범위는 축 4가 정한다. 기관총·포, 근접방어무기체계(Close-In Weapon System, CIWS), 함포는 직접 파괴가 가능하지만 도심이나 임해 시설 인근에서는 부수적인 피해 우려로 사용이 제한된다. 요격 드론, 고출력 마이크로파(High-Power Microwave, HPM), 레이저 무기는 유선 연결형과 군집에도 쓸 수 있다. 레이저는 기상의 영향을 받

www.kci.go.kr

고, HPM과 레이저는 대용량 전력과 냉각 설비를 갖추어야 한다. 수중의 대잠 어뢰·폭뢰는 탐지 한계에, 우주의 운동성 ASAT는 국제법 제약과 궤도 잔해 문제에 묶여 있다.

4.3 네 가지 제약 기반 능력 공백

탐지와 무력화의 분석을 종합하면 <표 4>의 네 가지 능력 공백으로 정리된다. ①~③은 한 영역 안의 정합성에서 생기고, ④는 영역 사이의 연계에서 생긴다. ①과 ③은 기록 단위 하나의 속성값(축 2, 축 4)에서 비롯되지만, ④는 기록 단위 사이의 관계에서 비롯된다. ②의 원인인 동시 운용 규모는 네 축 어디에도 값으로 들어 있지 않다. 본 연구에서는 이를 운용 형태로 따로 다루었으며, 규모를 별도 축으로 둘지는 부록 A의 B5 문항에서 확인한다.

〈Table 4〉 Constraint-driven capability gaps by threat attribute

Capability gap	Associated threats	Attributes giving rise to the gap	Measures rendered ineffective	Required response direction
1. Neutralization of RF-based countermeasures	Wire-linked drones	RF detection and jamming rendered ineffective simultaneously (Axis 2)	RF detection, jamming	Optical and acoustic detection, physical and directed-energy neutralization
2. Limits of simultaneous engagement	Swarms	Concurrent operation of multiple platforms exceeds the capacity of a single response system (operational scale, an attribute outside the four axes)	Single-target response systems	Wide-area neutralization, integrated employment of multiple assets
3. Compounding of constraints	Underwater and seabed threats	Physical limitations on communication and detection compounded by identification difficulties (Axis 4)	Soft-kill measures, long-range detection	Fixed acoustic surveillance, physical protection of infrastructure
4. Inability to handle cross-domain threats	Cross-domain threats	Linkages between two or more domains (a relational attribute)	Single-domain response assets	Sensor fusion, integrated command and control, integration of responsibilities

www.kci.go.kr

4.4 공백-대응 매트릭스

<표 4>의 공백을 C-US 운용개념의 네 구성요소[2]에 대응시키고, '위협 분류 → 능력 공백 → C-US 구성요소 → 세부 대응수단'의 순서로 정리한 것이 <표 5>의 공백–대응 매트릭스이다. <표 5>의 열은 왼쪽부터 능력 공백, 대응 방향, 담당 구성요소, 대응 수단 · 절차, 조직 · 기술 기반의 순이다. 공백 ①의 경우 유선 연결형 드론이 전파 탐지와 재밍을 함께 무력화하므로, 전파에 의존하지 않는 탐지와 물리적 무력화가 필요하다. 이는 기술지원, 구체적으로는 신규 전력 도입의 영역이며 요격드론, HPM, EO/IR(electro-optical/infrared) · 음향 통합 탐지로 구현할 수 있다.

〈Table 5〉 Mapping constraint-driven capability gaps to components of the integrated C-US concept of operations (gap-response matrix)

Capability gap	Required response direction	C-US component	Response measures and procedures	Organizational and technological support
1. Neutralization of RF-based countermeasures	Integration of optical and acoustic detection, physical and directed-energy neutralization	Technical support (introduction of new capabilities)	Interceptor drones, HPM and laser weapons, integrated EO/IR and acoustic detection	Sensor-fusion platforms, proactive investment in research and development
2. Limits of simultaneous engagement	Wide-area neutralization, integrated employment of multiple assets	Organization (integrated response teams) + MD-C2	Procedures for simultaneous engagement of multiple targets, integrated command of the air-defense network, automated priority recommendations	Joint integrated response teams comprising Air Force air-defense, Army/Marine Corps base-defense, and Navy coastal-defense elements
3. Compounding of constraints	Fixed acoustic surveillance, physical protection of infrastructure	Technical support + doctrine and procedures	Subsea cable surveillance networks, enhanced port and coastal security, countermeasures using small torpedoes and depth charges, civilian-military information-sharing procedures	Information-sharing arrangements among civilian and military infrastructure owners, revision of relevant legal and institutional frameworks
4. Inability to handle cross-domain threats	Sensor fusion, integrated command and control, integration of responsibilities	MD-C2 itself	Common operational picture (COP), procedures for coordinating responsibilities across domains, joint training	National-level governance, data standardization

www.kci.go.kr

<표 5>에서 공백 ①~③은 각각 한두 개의 구성요소에 배정된다. 공백 ④는 여기에 들어맞지 않는다. 기록 단위 사이의 관계에서 생기는 공백이어서 센서나 무기를 하나 더한다고 메워지지 않으며, 수단들을 잇는 지휘통제 구조, 곧 MD-C2 자체가 대응이 되어야 한다. 분류에서 '관계'로 정의한 속성이 대응 설계에서는 '연결 구조'에 대한 요구로 이어진 것이다.

다만 ①~③도 배정된 구성요소만으로 완결되지는 않는다. 공백 ①에 요격드론이나 HPM을 도입하더라도 센서 융합 플랫폼이 없으면 교전할 표적 정보를 얻기 어렵다. 여기서 MD-C2는 주된 대응 수단은 아니지만 다른 구성요소가 작동하기 위한 기반이 된다. <표 5>의 배정이 실제 운용에서 성립하는지는 5장의 P4와 P5로 확인한다.

4.5 구성요소별 구현

통합 운용개념은 영역별로 나누어 지휘하던 관행에서 벗어나, 다영역 상황을 한 곳에서 인식하고 결심하는 체계를 지향한다. 조직 면에서는 작전지역이나 기지 단위로 C-US 통합대응팀을 편성하는 방안을 생각할 수 있다. 공군 방공, 육군・해병대 기지 경계, 해군 해안방어 인원이 한 팀으로 평시에 함께 훈련하고 위협이 나타나면 함께 대응하는 방식이다. 교리・절차 면에서는 다영역 경보 전파, 교전 지침, 자원 할당 원칙을 담은 통합 대응 교범이 있어야 한다. 공중 드론이 탐지되면 그 정보를 지상・수상 부대에 바로 전파하고, 해안에서 수상 위협이 포착되면 방공 부대도 경계 수준을 높이는 상호 공조 절차가 여기에 해당한다.

통합 C-US는 센서 데이터의 실시간 공유와 인공지능(AI) 기반 위협평가・권고 체계를 전제로 한다. 여러 영역의 자산을 하나의 체계로 묶으려면 센서와 지휘통제 데이터의 형식과 의미를 통일해야 하고, 실제 교전 이전에 통합 체계의 성능을 확인할 시험평가 수단도 마련되어야 한다[16]. 제도 측면에서는 영공・영해에서의 드론 대응 권한, 재밍・스푸핑 관련 규제, 치안・대테러 대응과 군사작전 사이의 공조 체계를 정비할 필요가 있다. 국가중요시설의 드론 대응을 위해 중앙 통제본부, 정기 합동훈련, 정보공유 플랫폼, 법・제도 개선을 제시한 연구[15]는 공중 영역에 한정된 것이지만, <표 5>에서 공백 ④에 배정한 범국가적 거버넌스를 구체화할 때 출발점으로 삼을 수 있다. 동맹 차원에서는 한미 연합훈련에서 미측의 합동전영역지휘통제(Joint All-Domain Command and Control, JADC2)와 한국의 통합 C-US 체계를 연계하여 상호운용성을 점검할 수 있을 것이다.

V. 검증 명제와 후속 실증 설계

개념적 연구의 결과는 후속 연구가 검증할 수 있는 명제로 제시될 때 활용 가치가 커진다[21]. 이에 따라 3장의 분류와 4장의 매트릭스에 담긴 주장을 다섯 개의 명제로 <표 6>에 정리하였다. P1~

www.kci.go.kr

P3은 이어받은 분류 틀에 관한 것이고, P4와 P5는 본 연구가 새로 제시한 연결에 관한 것이다. 각 명제에는 어떤 결과가 나오면 명제를 받아들이기 어려운지를 함께 정리하였다. 다섯 명제 가운데 논증의 무게가 가장 큰 것은 P5이다. P5가 기각되면 영역 횡단 위협을 별도 범주로 둘 이유(P2)도 약해지므로, 두 명제는 함께 평가하는 것이 바람직하다.

〈Table 6〉 Research propositions and illustrative falsification conditions

Proposition	Statement	Illustrative falsification conditions	Survey items (Appendix A)
P1	The four classification axes are necessary for distinguishing multi-domain unmanned systems threats, and the subcategories within each axis reflect differences that determine the choice of countermeasures.	A prevailing judgment that omitting a particular axis would not change the choice of countermeasures.	B1-B5
P2	Cross-domain threats need to be treated as a relational category distinct from single-domain classifications, and the three manifestation patterns encompass currently observed cross-domain threats.	Repeated identification of cases that fall outside the three patterns, such as cyber-physical convergence threats.	C1-C4
P3	The four capability gaps are perceived in practice within current countermeasure systems.	A prevailing judgment that a particular gap has already been closed in practice or is not perceived in practice.	D1-D5
P4	Gaps 1-3 can be closed primarily through the components assigned in Table 5, with MD-C2 serving as their enabling foundation.	A prevailing judgment that a component not assigned to the gap should provide the primary response.	E1-E3, E6
P5	Gap 4 cannot be closed by individual countermeasures and requires integration at the MD-C2 level.	A prevailing judgment that the gap can be closed solely through an individual countermeasure, such as adding a particular sensor.	E4a, E4b, E6

명제의 평가 방법으로는 전문가 델파이 조사를 설계하였다. 조사는 구조화 설문을 쓰는 2라운드 델파이[22]로 하고, 패널은 군, 국방연구기관, 방산업체, 학계의 무인체계 · 대드론체계 전문가 15～20명으로 구성한다. 문항의 내용타당도는 Lawshe의 내용타당도비율(Content Validity Ratio, CVR)[23],[33]로, 패널 간 순위 일치도는 Kendall의 일치계수 W[24]로 판정한다. 1차 설문은 5개 부문 26개 문항이며 부문 B～E가 명제 P1～P5에 대응한다. 절차와 합의 기준, 전체 문항은 부록 A에 실었다.

www.kci.go.kr

Ⅵ. 한반도 안보환경에 대한 함의

한반도에서 무인체계 위협은 공중에서 먼저 드러났다. 2022년 12월 26일 북한 무인기 5대가 군사분계선을 넘었고, 그중 1대는 서울 상공에 들어와 대통령 집무실 인근 비행금지구역의 북측 가장자리를 일시 통과하였다[25],[26]. 군은 전투기와 공격헬기를 투입하고 경고사격을 하였으나 무인기를 격추하지 못하였다. 항공기와 미사일에 맞춰진 방공체계가 소형 무인기에는 제대로 작동하지 않았다는 점이 드러난 사건이었다. 본 연구의 틀에서 보면 이는 소형 공중 위협에 대한 탐지 정합성의 문제로, 4.2절에서 다룬 탐지 한계가 실제 상황에서 드러난 사례이다.

북한의 위협은 공중에 한정되지 않는다. 2024년 5～6월과 11월에는 북한 발신으로 추정되는 위성항법 교란이 서해 일대 다수 항공기와 선박의 운항에 장애를 일으켰다[27],[28]. 교란원은 지상에 있고 영향을 받은 것은 항법 신호였지만, 피해는 공중과 해상의 자산에 함께 나타났다. 영향 전이형 영역 횡단 위협에 해당하는 사례로, 한 영역의 대응 자산만으로는 다루기 어렵다.

러시아-우크라이나 전쟁에서 자폭 무인수상정이 함정과 임해 시설을 공격한 사례[29],[30], 발트해에서 되풀이된 해저 인프라 손상[31],[32]은 한반도 해역에도 참고가 된다. 위협 행위자와 지리 조건, 국제법적 지위가 다르므로 이 사례를 그대로 대입할 수는 없다. 위협 유형의 참조 사례로 보는 것이 적절하다. 그렇지만 한국은 어항과 액화천연가스, 정유, 조선소 등 임해 산업 시설이 많고 해저 통신・전력 케이블에 의존하고 있어 비슷한 위협에 노출되어 있다. 공백 ③(제약 중첩)은 이런 인프라 방호 문제와 직접 맞닿아 있으며, 해저 인프라의 물리적 방호와 고정형 음향 감시망이 필요한 이유가 된다. 수상의 민간선 식별 곤란과 임해 시설 인근의 화력 제한도 대응 수단의 선택을 좁히는 요인이다.

분석 결과를 한국의 대응체계에 적용할 때, 위협 분석과 대비의 범위를 공중에서 다영역으로 넓혀야 한다는 점이 중요하다. <표 4>의 네 공백은 모두 한반도에서 나타날 수 있으며, 공백 ④는 군의 영역별 책임 분담 구조를 다시 검토하게 만든다. 통신 의존 구조의 변화도 고려해야 한다. 유선 연결형과 완전 자율형이 늘어날수록 전파 기반 대응의 효용은 줄어들기 때문에, 광학・음향 탐지와 물리・지향성 에너지 무력화 수단의 비중을 높일 필요가 있다. 시간이 가장 오래 걸릴 과제는 영역 횡단 위협에 대응할 통합 지휘통제와 책임 통합의 제도적 기반이다. 영역 간 책임을 조정하려면 법령과 조직, 교리를 함께 바꾸어야 하기 때문이다.

Ⅶ. 결 론

7.1 연구 요약과 기여

본 연구는 다영역 무인체계 위협의 분류와 통합 C-US 운용개념을 하나의 틀로 연결하고자 하였

www.kci.go.kr

다. 위협 분류에서는 운용 영역, 통신·자율성 의존, 위협 행위 유형, 영역 고유 제약의 네 축으로 다섯 영역의 무인 위협을 같은 기준 위에서 기술할 수 있었다. 운용 영역 축의 값을 플랫폼과 임무 단계 단위로 기록하자, 수상-수중 양용 체계나 이종 영역 간 협업처럼 한 영역에 넣기 어려웠던 사례도 무리 없이 기록되었다. 영역 횡단 위협은 운용 영역의 여섯 번째 값으로 보기보다 기록 단위 사이의 관계로 보는 편이 적절하였다. 다만 영역값이 다르다고 모두 영역 횡단 위협이 되는 것은 아니며, 그 연결 때문에 대응 책임이 한 영역에 귀속되지 않는 경우로 범위를 한정하였다.

능력 공백은 장비가 부족해서라기보다 위협의 속성이 대응 수단을 구조적으로 배제하는 데서 생겼다. 전파 기반 수단 무력화, 동시처리 한계, 제약 중첩의 세 공백은 한 영역 안에서 생기며, 각각 기술지원, 조직과 다영역 통합 지휘통제, 기술지원과 교리·절차에 대응시킬 수 있었다. 반면 영역 횡단 처리 불가 공백은 기록 단위 사이의 관계에서 비롯된다. 이 공백에는 특정 수단을 배정할 수 없었고, 수단들을 잇는 다영역 통합 지휘통제 구조 자체가 대응이 되어야 하는 것으로 분석되었다. 이 결과는 문헌과 OSINT에 근거한 개념 모형이다. 그래서 분류 틀의 타당성과 공백–대응 연결을 다섯 개의 검증 명제와 반증 조건으로 정리하였다.

본 연구는 학술적으로는 따로 제시되어 온 위협 분류와 대응 개념을 '분류 속성 → 능력 공백 → 대응 구성요소'의 경로로 이어, 분류가 대응 설계로 넘어가는 논리를 제시하였다. 공백–대응 매트릭스는 소요 기획 단계에서 공백별 담당 구성요소를 점검하는 목록으로 쓸 수 있고, 검증 명제와 반증 조건은 후속 조사가 확인할 대상을 정해 준다.

7.2 정책적 함의

특정 위협 대응을 위한 무기체계의 소요는 대체로 장비 단위로 제기된다. 어떤 탐지 레이더나 재밍 장비, 요격 수단을 들여올지가 먼저 논의되고, 그 장비들을 어떻게 연결할지는 전력화 이후의 과제로 미뤄지는 경우가 많다.[6] 위협의 통신·자율성 의존 구조와 영역 고유 제약이 특정 수단을 구조적으로 배제한다면, 개별 장비의 성능을 높여도 공백은 남는다. 소요를 제기하는 단위를 장비에서 능력 공백으로 바꾸고, 각 공백을 메우는 데 필요한 조직·절차·기술 요소를 함께 묶어 검토하는 방식을 생각해 볼 수 있다.

책임 배분의 문제도 제기된다. 현재의 대응책임은 대체로 영역과 기관을 기준으로 나뉘어 있다. 영역 횡단 위협은 그 경계에서 발생하므로, 경계 지점의 책임을 사전에 정해 두지 않으면 탐지 정보가 전달되지 않거나 대응 주체를 정하는 데 시간이 걸린다. 해안과 항만처럼 방공, 해안 경계, 해양 경찰, 시설 관리 주체가 겹치는 곳에서는 어느 단계에서 누가 탐지 정보를 넘기고 누가 교전을 결심하는지를 교리와 합동 절차로 명시하는 작업이 장비 도입과 함께 추진되어야 한다. 위성항법 교란처

6) DefenseNews(2020.6.27.). Army selects eight counter-drone systems for the joint force. https://www.defensenews.com/unmanned/2020/06/26/army-selects-eight-counter-drone-systems-for-the-joint-force/

www.kci.go.kr

럼 효과가 여러 영역에 동시에 미칠 때는 군뿐 아니라 전파 관리, 항공, 해양을 담당하는 부처 간 공조 체계도 고려해야 한다.

시험평가의 기준도 달라져야 한다. 개별 장비의 탐지 거리나 요격 확률만으로는 통합 대응체계의 성능을 판단하기 어렵다. 영역이 바뀌는 순간의 추적 인계, 다수 표적의 동시처리, 이종 센서 정보의 융합처럼 체계 수준에서 나타나는 성능을 평가 항목에 포함하고, 디지털 트윈과 같은 모의 환경에서 이를 사전에 확인하는 방안을 검토할 수 있다. 전력 증강 소요나 제도 개편의 근거로 활용하려면 제시한 검증 명제가 전문가 조사와 실증을 통해 먼저 확인되어야 한다.

7.3 연구의 한계와 후속 과제

이 연구의 가장 큰 한계는 실증이 제한된다는 점이다. 분류와 매트릭스는 문헌과 OSINT에 근거한 개념 모형이며, 전문가 합의나 대응 효과는 확인하지 않았다. 부록 A의 델파이 조사도 설계 단계에 머물러 있다. 델파이를 시행하더라도 얻을 수 있는 것은 내용타당도이고, 구성타당도나 기준타당도는 별도의 검증을 거쳐야 한다. 사이버 영역을 물리 영역과 분리하지 않은 점도 한계로 남는다. 사이버-물리 융합형 위협을 영역 횡단의 네 번째 양상으로 볼 수 있는지는 판단을 유보하였다.

후속 연구에서는 우선 부록 A의 델파이 조사를 시행하여 P1~P5를 평가해야 한다. 그 결과를 바탕으로 능력 공백의 상대적 시급성을 계층분석법(Analytic Hierarchy Process, AHP) 등으로 정량화하면 대응 수단과 무기체계 확보의 우선순위를 도출할 수 있을 것이다. 영역 횡단 위협에 대응하기 위한 통합 지휘통제 구조와 영역 간 책임 배분의 거버넌스 모형도 별도의 연구가 필요한 주제이다.

www.kci.go.kr

Reference

[1] McAuliffe, A. (2026, September 22). Russia-Ukraine war is accelerating the dangerous race toward fully autonomous drones. The Conversation. https://theconversation.com/russia-ukraine-war-is-accelerating -the-dangerous-race-toward-fully-autonomous-drones-290877

[2] Kwon, H. J., & Kim, H. S.(2025). Establishing an integrated counter-unmanned systems (C-US) concept: Expanding from counter-UAS to multi-domain defense. Journal of the Korea Anti Drone Industry Association, 1(1), 119-132. https://kadiakorea.or.kr/cmnt/50926/boardInfo.do?bidx=1002559

[3] Kwon, H. J., & Kim, H. S.(2026). Multi-domain unmanned systems threat classification and counter-unmanned systems requirements: Focusing on the cross-domain threat concept. Journal of the Korea Anti Drone Industry Association, 2(1), 120-137https://kadiakorea.or.kr/cmnt/50926/boardInfo.do?bidx=1024605

[4] Jaakkola, E. (2020). Designing conceptual articles: Four approaches. AMS Review, 10(1-2), 18-26. https://doi.org/10.1007/s13162-020-00161-0

[5] U.S. Department of the Army. (2022, October 1). Operations (Field Manual 3-0). https://armypubs.army.mil /epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

[6] Stenson, R. (2022, October 11). TRADOC updates Army capstone doctrine, codifying shift to multidomain operations. Joint Base San Antonio. https://www.jbsa.mil/News/News/Article/3184208/tradoc-updates -army-capstone-doctrine-codifying-shift-to-multidomain-operations/

[7] Segal, R. (2023, March 10). Who “does” MDO? What multi-domain operations will mean for – and require of - the Army’s tactical units. Modern War Institute. https://mwi.westpoint.edu /who-does-mdo-what-multi-domain-operations-will-mean-for-and-require-of-the-armys-tactical-units/

[8] Feickert, A., & M’Bai, E. (2025, December 8). Defense primer: Army multi-domain operations (MDO) (CRS Report No. IF11409). Congressional Research Service. https://www.congress.gov/crs_external_products /IF/PDF/IF11409/IF11409.15.pdf

[9] Gettinger, D. M. (2024, October 25). Defense primer: Categories of uncrewed aircraft systems (CRS Report No. IF12797). Congressional Research Service. https://www.congress.gov/crs_external_products/IF/PDF/IF12797/IF12797.1.pdf

[10] Joint Chiefs of Staff. (2019, July 25). Joint air operations (Joint Publication 3-30). https://aerospace.csis.org/wp-content/uploads/2019/09/JointAirOperations_jp3_30.pdf

[11] Kang, H. (2019). Direction of operation of ROKA RPA for future warfare. The Quarterly Journal of Defense Policy Studies, 35(1), 7-33. https://doi.org/10.22883/jdps.2019.35.1.001

www.kci.go.kr

[12] Wang, J., Liu, Y., & Song, H. (2021). Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends. IEEE Aerospace and Electronic Systems Magazine, 36(3), 4-29. https://doi.org/10.1109/MAES.2020.3015537

[13] Khawaja, W., Ezuma, M., Semkin, V., Erden, F., Ozdemir, O., & Guvenc, I. (2026). A survey on detection, classification, and tracking of AAVs using radar and communications systems. IEEE Communications Surveys & Tutorials, 28, 3272-3310. https://doi.org/10.1109/COMST.2025.3554613

[14] Tan, C. S., Van Bossuyt, D. L., & Hale, B. (2021). System analysis of counter-unmanned aerial systems kill chain in an operational environment. Systems, 9(4), Article 79. https://doi.org/10.3390/systems9040079

[15] Sim, J.-H., Choi, W.-J., Lee, J.-Y., Lee, W.-W., & Kim, G.-S. (2025). Governance-based counter-drone system construction plan for national key infrastructure. The Journal of the Convergence on Culture Technology, 11(3), 149-156. https://doi.org/10.17703/JCCT.2025.11.3.149

[16] Kim, G., Jin, K., Cho, Y., & Won, K. (2022). Initial operational capability of future weapon systems and field test method using digital twin. Journal of Advances in Military Studies, 5(3), 1-22. https://doi.org/10.37944/jams.v5i3.167

[17] Seo, K. I., Kim, K.-W., Kim, J. H., Cho, S.-K., & Park, S.-H. (2023). A study on multi-domain counter-drone system in the Ukraine-Russia War. Journal of Military Robotics Society, 2(1), 25-32. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART003173234

[18] Yang, S., & Lim, Y. (2024). A study on the changes in the threat of asymmetric war in modern warfare and lessons: Focusing on the case of drone operation. Korea Maritime Security Review, 7(2), 29-52. https://doi.org/10.23270/kmsr.2024.7.2.002

[19] Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. European Journal of Information Systems, 22(3), 336-359. https://doi.org/10.1057/ejis.2012.26

[20] Bailey, K. D. (1994). Typologies and taxonomies: An introduction to classification techniques. SAGE Publications. https://doi.org/10.4135/9781412986397

[21] MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. Journal of Marketing, 75(4), 136-154. https://doi.org/10.1509/jmkg.75.4.136

[22] Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. Management Science, 9(3), 458-467. https://doi.org/10.1287/mnsc.9.3.458

[23] Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563-575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

[24] Kendall, M. G., & Babington Smith, B. (1939). The problem of m rankings. The Annals of

www.kci.go.kr

Mathematical Statistics, 10(3), 275-287. https://doi.org/10.1214/aoms/1177732186

[25] Ji, D. (2022, December 26). N. Korean drones cross border. The Korea Herald. https://www.koreaherald.com/article/3026653

[26] Al Jazeera. (2023, January 5). N Korea drone entered S Korea's presidential no-fly zone: Army. https://www.aljazeera.com/news/2023/1/5/north-korea-drone-entered-no-fly-zone-in-seoul-s-korea-military

[27] Agence France-Presse. (2024, November 9). North Korea jams GPS signals, affecting ships, aircraft in South. Voice of America. https://www.voanews.com/a/north-korea-jams-gps-signals-affecting-ships-aircraft-in-south/7858015.html

[28] The Associated Press. (2024, November 9). North Korean GPS manipulation disrupted dozens of planes and vessels, South Korea says. NBC News. https://www.nbcnews.com/news/world/north-korean-gps-manipulation-disrupted-dozens-planes-vessels-rcna179444

[29] Wertheim, E. (2025, September). Ukraine's Magura naval drones: Black Sea equalizers. Proceedings, 151(9). https://www.usni.org/magazines/proceedings/2025/september/ukraines-magura-naval-drones-black-sea-equalizers

[30] Butenko, V., Edwards, C., & Stambaugh, A. (2024, February 14). Ukraine says it has sunk another warship, disabling a third of Russia's Black Sea Fleet. CNN. https://www.cnn.com/2024/02/14/europe/ukraine-says-russian-warship-caesar-kunikov-destroyed-black-sea-intl-hnk/index.html

[31] Majcin, J. (2025, April 22). Battle of the Baltic: Safeguarding critical undersea infrastructure. European Policy Centre. https://www.epc.eu/publication/Battle-of-the-Baltic-Safeguarding-critical-undersea-infrastructure-645780/

[32] Jones, B. D. (2026, February 13). Seabed zero: Baltic sabotage and the global risks to undersea infrastructure. Bulletin of the Atomic Scientists. https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/

[33] Ayre, C., & Scally, A. J. (2014). Critical values for Lawshe's content validity ratio: Revisiting the original methods of calculation. Measurement and Evaluation in Counseling and Development, 47(1), 79-86. https://doi.org/10.1177/0748175613513808

원 고 접 수 일 2026년 09월 14일
원 고 수 정 일 2026년 09월 28일
게 재 확 정 일 2026년 09월 30일

www.kci.go.kr

부록 A. 검증 명제 평가를 위한 델파이 조사 설계

A.1 조사 개요

조사는 구조화 설문을 이용한 2라운드 델파이[22]로 설계한다. 목적은 <표 6>의 명제 P1～P5에 대한 전문가 합의 수준을 확인하는 것이다. 시행 전 기관생명윤리위원회(Institutional Review Board, IRB)의 심의를 받는다.

패널은 다음 세 기준 중 둘 이상을 충족하는 전문가로 구성한다. ① 국방학・군사학・방위사업학・항공우주공학 관련 석사 이상 학위, ② 무인체계・대드론체계 관련 연구・정책・야전 실무 경력 10년 이상, ③ 최근 5년 이내 무인체계 소요기획・전력화・정책연구 참여. 군(방공・정보・기갑・해군・우주 관련 분야), 국방연구기관, 방산업체, 학계에서 균형 있게 위촉하며 목표 규모는 15～20명이다. CVR 임계값은 라운드별 실제 응답자 수에 따라 적용하며, 15명이면 0.600(12명 이상 긍정 응답), 20명이면 0.500(15명 이상 긍정 응답)이다[23],[33].

사전 단계에서 패널을 위촉하고 핵심 용어 설명자료를 배포한다. 1라운드에서는 부문 A의 배경 정보와 부문 B～E의 평정 및 개방형 의견을 받는다. 라운드 사이에 A.2절의 기준으로 합의 여부를 판정하고, 미달 문항은 개방형 의견을 반영해 재정식화한다. 2라운드에서는 1라운드 통계와 익명 처리한 소수의견을 함께 제시하고, 미달 문항과 재정식화한 문항을 다시 평정받는다. 2라운드에서도 기준에 미달한 문항은 합의 미도달로 보고한다. 조사는 온라인으로 진행하며, 전체 기간은 약 11주(패널 위촉 2주, 1라운드 3주, 분석・재정식화 2주, 2라운드 3주, 최종 분석 1주)이다.

A.2 합의 기준

5점 평정 문항(B1, B2a, B2b, B3, B4, C1～C3, D1～D4, E1～E3, E4a, E4b)은 CVR, 평균, 사분위범위(Interquartile Range, IQR)의 세 기준으로 판정한다. CVR은 5점 척도의 4점과 5점을 긍정 응답으로 보아 산출하며, 라운드별 응답자 수에 해당하는 임계값을 적용한다[23],[33]. CVR이 임계값 이상이고 평균 3.5 이상, IQR 1.0 이하를 모두 충족하면 합의로 본다. 미달 문항은 개방형 의견을 반영해 재정식화하여 2라운드에서 다시 평정한다. 순위 문항(E5)의 패널 간 일치도는 Kendall의 W[24]로 산출하고 0.5 이상을 수용 가능한 수준으로 둔다. 명제별 판정은 <표 6>에서 해당 명제에 연결된 평정 문항이 모두 합의에 도달하면 “지지”, 절반 이상 도달하면 “부분 지지 및 재정식화”, 절반 미만이면 “기각 검토”로 한다. 서술형 문항(B5, C4, D5, E6)은 합의 판정에 포함하지 않으며, 응답 내용은 문항 재정식화와 분류 틀 보완의 근거로만 활용한다.

www.kci.go.kr

A.3 1차 설문 문항

〈 Table A1 〉 First-round survey items and corresponding propositions
(Scale for five-point items: 1 = Strongly disagree, 5 = Strongly agree)

Section (proposition)	Item	Content	Response format
A (Background)	A1	Affiliation (military / defense research institute / defense company / academia / other)	Multiple choice
	A2	Years of experience in unmanned systems and/or counter-drone systems	Numeric
	A3	Highest relevant academic degree and field of study	Open-ended
	A4	Participation in requirements planning, capability fielding, or policy research within the past five years	Yes/No
B (P1)	B1	Axis 1 (Operating Domain) is a necessary dimension for distinguishing unmanned systems threats.	5-point scale
	B2a	The four subcategories of Axis 2 (Communication-Autonomy Dependency) are mutually exclusive.	5-point scale
	B2b	The subcategories of Axis 2 reflect differences that determine the choice of countermeasures.	5-point scale
	B3	Axis 3 (Threat Behavior) encompasses currently observed threat behaviors.	5-point scale
	B4	Axis 4 (Domain-Specific Constraint) encompasses constraints that limit the choice of countermeasures in practice.	5-point scale
	B5	Classification axes that should be added to the existing four	Open-ended
C (P2)	C1	It is appropriate to treat threats that traverse, link, or propagate across two or more domains as a distinct relational category (cross-domain threats).	5-point scale
	C2	The three manifestation patterns encompass currently observed cross-domain threats.	5-point scale
	C3	Cyber-physical convergence should be added as a fourth manifestation pattern distinct from the existing three.	5-point scale
	C4	Manifestation patterns that should be added or revised	Open-ended
D (P3)	D1	A capability gap caused by the ineffectiveness of RF-based countermeasures against wire-linked threats is perceived in practice.	5-point scale
	D2	A capability gap is perceived in practice when swarm threats exceed the capacity of single-target countermeasure systems to handle simultaneous targets.	5-point scale
	D3	A capability gap is perceived in practice in responding to underwater and seabed threats, as physical limitations and identification difficulties jointly weaken both detection and neutralization.	5-point scale
	D4	A capability gap is perceived in practice when simply aggregating domain-specific assets is insufficient to counter cross-domain threats.	5-point scale
	D5	Additional capability gaps perceived in practice beyond the four specified above	Open-ended

www.kci.go.kr

Section (proposition)	Item	Content	Response format
E (P4, P5)	E1	Gap 1 can be closed primarily through the component assigned in Table 5 (technical support).	5-point scale
	E2	Gap 2 can be closed primarily through the components assigned in Table 5 (organization and MD-C2).	5-point scale
	E3	Gap 3 can be closed primarily through the components assigned in Table 5 (technical support; doctrine and procedures).	5-point scale
	E4a	Gap 4 cannot be closed through individual countermeasures, such as adding a particular sensor or weapon.	5-point scale
	E4b	Closing Gap 4 requires integration at the MD-C2 level.	5-point scale
	E5	Rank the four gaps in order of urgency for closure in South Korea's security environment.	Ranking
	E6	Additional comments or proposed revisions to the gap-response matrix	Open-ended

www.kci.go.kr

IDAP 광운대학교 방위사업연구소 INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2026, Vol. 9, No. 2, 15-39.

https://doi.org/10.37944/advmil.9.2.202610.002

다영역 무인체계 위협 분류와 통합 대응체계(C-US) 설계: 능력 공백-대응요소 연계에 관한 개념적 연구

권혁진* · 김형석 · 김장엽*****

국문초록

무인체계 위협은 공중에서 지상, 수상, 수중 및 우주로 넓어지고 있으나 대응체계에 대한 논의는 공중 위협을 중심으로 이루어져 왔다. 여러 영역을 포괄하는 통합 무인체계 대응(Counter-Unmanned Systems, C-US) 개념과 다영역 위협 분류체계가 각각 제안된 바 있지만, 도출된 능력 공백을 운용개념의 어느 구성요소가 메우는지는 다루어지지 않았다. 본 연구는 이 연결 문제를 다룬 개념적 연구이다. 네 개의 분류축과 영역 횡단 위협 개념으로 이루어진 분류 틀을 정리하면서 운용 영역 축의 기록 단위와 영역 횡단 관계의 정의를 보완하였다.

이어서 위협 속성이 대응 수단을 구조적으로 배제하여 생기는 네 가지 제약 기반 능력 공백을 C-US 운용개념의 네 구성요소인 다영역 통합 지휘통제, 조직, 교리 · 절차, 기술지원에 대응시켜 공백과 대응의 매트릭스를 구성하였다. 분석 결과 전파 기반 수단 무력화, 동시처리 한계, 제약 중첩의 세 공백은 특정 구성요소로 대응할 수 있으나, 영역 횡단 처리가 곤란한 공백은 다영역 통합 지휘통제 체계를 필요로 하는 것으로 분석되었다. 아울러 이 연결을 후속 연구에서 확인할 수 있도록 다섯 개의 검증 명제와 반증 조건을 제시하고, 이를 평가할 2라운드 델파이 조사 설계를 부록에 수록하였다. 전문가 합의와 대응 효과에 대한 실증은 후속 과제로 남는다.

주제어 : 통합 무인체계 대응(C-US), 영역 횡단 위협, 제약 기반 능력 공백, 공백-대응 매트릭스, 개념적 연구

* (제1저자) 광운대학교 방위사업학과, kadiakorea@gmail.com, https://orcid.org/0009-0000-8461-6838.
** (공동저자) 한국대드론산업협회 드론센터장, kimhs01@gmail.com, https://orcid.org/0009-0001-2844-5824.
*** (교신저자) 광운대학교 방위사업학과 주임교수, https://orcid.org/0000-0001-7258-3928.

www.kci.go.kr