사이버안보연구, 3집 1호 2026 여름, 089-129

모빌리티 사이버보안 법제 현황 및 시사점:

육상·해상·항공 모빌리티를 중심으로

최영한 | 국가보안기술연구소(제1저자, 교신저자)
김덕진 | 국가보안기술연구소

논문접수일 2026년 5월 12일 | 논문심사일 2026년 6월 5일 | 게재확정일 2026년 6월 16일

논문 요약

최근 모빌리티는 자율주행자동차, 자율운항선박, 드론, 도심항공교통 확산으로 국가 핵심 인프라로 부상했으나, 관련 특별법은 산업진흥과 규제완화에 치우쳐 사이버보안 규율은 부차적 지위에 머무르고 있다. 자율주행자동차 영역에서는 『자동차관리법』이 UNECE R155·R156 등을 수용해 CSMS·SUMS 체계를 도입함으로써 차량·백엔드·통신채널을 포괄하는 비교적 구체적 규범을 마련했지만, 자율운항선박은 『해사안전기본법』과 해사 관련 사이버안전 관리지침, IACS UR E26·E27 등으로 사이버복원력을 부분적으로만 규율하고, 드론·도심항공교통은 항공 4법과 『드론법』, 『도심항공교통법』이 물리적 안전과 산업육성에 집중해 사이버보안 규정이 초기 단계에 머물러 있다. 『인공지능기본법』은 교통수단·시설·체계에 활용되는 인공지능을 고영향 인공지능으로 규정하고 투명성·안전성·신뢰성 의무와 영향평가를 부과하지만, 인공지능을 겨냥한 사이버공격, 데이터·모델 탈취, 적대적 입력 교란 등 위험을 구조화한 규범은 미비하다. 이에 논문은 『모빌리티혁신법』과 『인공지능기본법』을 상위 구조로 하여 모빌리티 전 영역에 공통 적용 가능한 전 생명주기 기반 사이버보안 기본원칙과 최소 기준을 제안하고, 『자동차관리법』, 『해사안전기본법』, 항공 4법 등 개별 기본법에 모빌리티 수단별 기술·운영 특성을 반영한 차등적 사이버보안 의무를 내재화하는 법제 방향을 모색하였다.

주제어 모빌리티, 자율주행자동차, 자율운항선박, 드론, 도심항공교통, 사이버보안

Ⅰ. 서론

1. 연구 방향

최근 모빌리티 산업은 사람과 화물을 운송하는 기존의 교통체계를 혁신하고 새로운 산업 생태계를 형성함으로써 인간의 생활 전체를 하나로 묶는 전략적 성장 분야로 부상하고 있다.[1] 특히 첨단기술이 기반이 되는 자율주행자동차(Autonomous Vehicle, AV), 자율운항선박(Maritime Autonomous Surface Ship, MASS), 드론, 도심항공교통(Urban Air Mobility, UAM) 등의 모빌리티는 이동의 효율성과 안전성, 접근성 향상을 높이는 한편, 센서·통신·소프트웨어·인공지능 등이 결합된 복합시스템으로 사회와 경제 전반의 혁신을 견인할 핵심 인프라로 인식되고 있다. 이와 같은 흐름 속에서 정부는 모빌리티 혁신을 국가 성장전략과 연계하고, 관련 인프라 투자 및 규제개선 정책을 단계적으로 추진하고 있다.[2]

모빌리티는 운영되는 공간을 기준으로 육상·해상·항공 교통으로 나눌 수 있다.[3] 최근 육상에서는 자율주행자동차, 해상에서는 자율운

1) 미래 모빌리티, 스마트 모빌리티 등 다양한 용어가 사용되고 있으나, 본 논문에서는 『모빌리티 혁신 및 활성화 지원에 관한 법률』(이하 『모빌리티혁신법』) 에 정의된 "모빌리티"로 통일 한다.

2) "AI 선도 프로젝트 추진계획"(관계부처합동, 2025)과 "2030 모빌리티 혁신성장 로드맵"(국토교통부, 2026)은 자율주행, 자율운항선박, 드론 도심항공교통을 미래를 위한 국가 전략적 육성 산업으로 삼고 있다.

3) 『국가통합교통체계효율화법』(이하 『통합교통체계법』)에서는 국가 교통체계를 육상교통 · 해상교통 · 항공교통으로 분류하고 있다.

항선박, 항공에서는 드론·도심항공교통이 교통 수단으로 많은 관심을 받고 있다. 자율주행자동차 분야에서 정부는 2027년 완전자율주행 상용화를 목표로 자율주행 핵심기술 개발 및 인프라구축에 역량을 집중할 계획이다(국토교통부 2026, 6-13).[4] 자율운항선박은 인적 해양 사고, 해운 인력 수급 부족 등의 문제를 해결하기 위한 핵심 기술로 떠오르고 있다. 정부는 완전자율운항을 위해 자율운항선박 기술개발사업(2020년~2025년)을 수행하였으며, 현재는 AI 완전자율운항선박 기술개발사업(2026년~2032년)을 시작하였다(산업통상부 2025). 자율운항선박은 스마트항만, 디지털 물류체계 등과 연계되고 육상 모빌리티에서 해상 모빌리티로 확장되고 있다. 항공은 무인으로 동작하는 드론에서 사람이 탑승한 후 공중에서 이동을 할 수 있는 도심항공교통 중심의 새로운 항공 모빌리티 시장이 점점 형성되고 있다(국토교통부 2026, 14-20). 저고도 공역을 활용하는 도심항공교통은 전통적인 항공체계와는 달리 도심 및 근교 지역을 직접 연결하고, 이는 전기에너지를 동력으로 사용하는 수송기기 eVTOL(electric Vertical Take-Off and Landing)과 수송기기의 이착륙을 위한 인프라 시설인 버티포트(Vertiport) 기술 개발을 통해 가능해졌다.

이처럼 육상·해상·항공 모빌리티 분야의 자율주행자동차, 자율운항선박, 드론, 도심항공교통 기술에 대한 시장 수요와 정책적 관심은 빠르게 확대되고 있으며, 국가 차원에서 기술개발 지원, 실증사업, 규제 샌드박스 등을 통해 상용화를 촉진하기 위해 정부에서는 다양한

4) 자율주행자동차 관련 정부 추진 세부 목표는 다음과 같다. ①자율주행차 실증 본격화, ②자율주행 AI 인프라 확충 및 기술 고도화 지원, ③자율주행 규제 합리화, ④자율주행 서비스산업 생태계 육성.

특별법을 제정하였다.[5] 이러한 법령들은 모빌리티 기술의 개발·실증·사업화를 촉진하고, 안전기준 및 책임체계를 일정 부분 마련함으로써 산업 성장을 뒷받침한다는 점에서 중요한 의의를 가진다. 그러나 산업과 시장 활성화 관점에서의 논의가 우선시 되다 보니, 안전한 모빌리티를 위한 필수 구성 요소 중 하나인 사이버보안에 대한 체계적 논의는 후순위로 밀려 있는 실정이다. 자율주행자동차의 경우는 『자동차관리법』에 사이버보안 관련 요소가 반영되어 있으나, 자율운항선박 및 드론·도심항공교통의 경우는 미비하다고 할 수 있다. 이와 함께 자율 주행·운항·비행을 목표로 하는 모빌리티는 인공지능이 사람의 역할을 대체하게 되며, 이동 중 잘못된 판단은 큰 인명 피해를 야기할 수 있다. 인공지능 전반을 다루고 있는 『인공지능 발전과 신뢰 기반 조성 등에 관한 기본법』(이하 『인공지능기본법』)이 제정되어 2026년 시행되고 있지만, 인공지능의 안전성과 신뢰성을 확보하기 위한 규정은 있으나 아직은 초기 단계라 실질적인 방안이 필요하다고 하겠다. 향후 모빌리티가 국가의 핵심 사회기반시설로 정착할 경우, 해당 시스템에 대한 사이버공격은 단순한 기술적 장애를 넘어 대규모 인명 피해와 직결되는 안전사고는 물론, 물류·교통·에너지 등 연계 산업 전반에 걸친 경제적 손실과 사회적 혼란을 초래할 가능성이 크다. 특히 초연결·자율화된 모빌리티 환경에서는 공격의 전파 속도와 영향 범위가 기하급수적으로 확대될 수 있어, 개별 시스템의 취

5) 『모빌리티혁신법』, 『자율주행자동차 상용화 촉진 및 지원에 관한 법률』(이하 『자율주행자동차법』), 『자율운항선박 개발 및 상용화 촉진에 관한 법률』(이하 『자율운항선박법』), 『드론 활용의 촉진 및 기반조성에 관한 법률』(이하 『드론법』), 『도심항공교통 활용 촉진 및 지원에 관한 법률』(이하 『도심항공교통법』) 등

약성이 곧 국가 전체의 리스크로 확산될 수 있다. 이러한 점에서 모빌리티 분야의 사이버보안 문제는 더이상 산업 차원의 관리 과제가 아니라, 국가 기능의 연속성과 공공 안전을 직접적으로 위협하는 사이버안보 사안으로 인식될 필요가 있다.

위와 같은 문제의식을 바탕으로, 본 논문은 다음과 같은 내용을 포함한다. 첫째, 육상·해상·항공 모빌리티의 주요 수단인 자율주행자동차, 자율운항선박, 드론·도심항공교통의 기술과 사이버위협을 체계적으로 정리한다. 둘째, 관련 국내 법제와 국제규범을 검토하여 각 분야별 규율 수준을 분석한다. 셋째, 이러한 분석을 토대로 모빌리티 사이버보안 법제의 개선 방향을 제시한다. 특히 본 논문은 새로운 법체계를 별도로 새로 도입하기보다는, 공통원칙을 제시하는 기본법과 분야별 특수성을 반영한 개별법, 그리고 이를 구체화하는 기술기준 간의 기능적 조화를 통해 법제의 정합성을 확보하는 것이 중요하다는 점을 기술하고자 한다.

2. 모빌리티 범위 및 대상

『모빌리티혁신법』은 모빌리티를 다양한 이동수단과 기반시설, 서비스가 결합하여 이동 가능성과 편의성을 제공하는 포괄 개념으로 이해한다〈그림 1〉. 모빌리티는 이동 수요를 가진 주체의 관점에서, 다양한 교통수단과 시설, 서비스가 결합하여 제공하는 이동 가능성과 편의성, 접근성을 포괄하는 개념이다.[6] 따라서 모빌리티는 전통적인

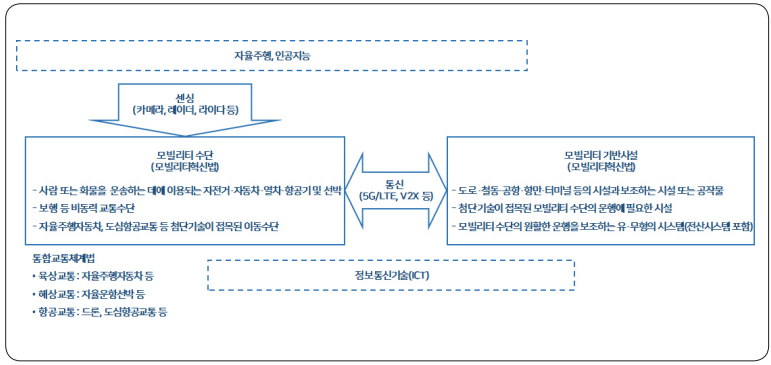
6) 『모빌리티혁신법』제2조제1호 "모빌리티".

교통 개념보다 넓은 범위를 가지며, 물리적 인프라와 디지털 인프라, 운영·관리 시스템, 서비스 플랫폼을 모두 포함하는 복합적 구조로 이해된다. 모빌리티는 이동의 주체가 되는 '모빌리티 수단'과 이를 돕기 위한 '모빌리티 기반시설'로 크게 나눌 수 있다.[7] '모빌리티 수단'은 사람 또는 화물을 운송하는 데에 이용되는 자전거, 자동차, 열차, 항공기, 선박 등을 의미하며, 이는 육상·해상·항공 영역에 걸쳐 다양한 형태로 존재한다. 오늘날 자율주행자동차, 자율운항선박, 드론, 도심항공교통 등 첨단기술이 접목된 '모빌리티 수단'으로 인해 '모빌리티 기반시설'은 물리적 시설에 한정되지 않고, 첨단기술이 접목되어 '모빌리티 수단'의 운행에 필요한 각종 전자·통신·제어 시설, 데이터센터 및 클라우드 인프라, 관제 및 운영시스템 등 유무형의 시스템까지 포괄하는 방향으로 확대되고 있다.

국가 교통체계는 '모빌리티 수단'이 운영되는 영역에 따라 육상·해상·항공 교통으로 나누고 있다. 육상 모빌리티는 도로·철도 인프라를 기반으로 하는 자전거, 자동차, 버스, 트럭, 열차 등 각종 교통수단과 관련 시설을 포함하고, 해상 모빌리티는 항만·해상 교통로를 기반으로 하는 여객선, 화물선, 선박 및 관련 항만시설 등을 포함한다. 항공 모빌리티는 공항, 도심항공교통 버티포트 등과 이를 이용하는 항공기, 헬리콥터, 무인항공기 등을 포함하는 영역으로 이해할 수 있다.

7) 『모빌리티혁신법』제2조제2호 "모빌리티 수단", 제2조제3호 "모빌리티 기반시설".

〈그림 1〉 모빌리티 구성 요소



첨단모빌리티는 육상·해상·항공 모빌리티에 자율주행, 인공지능, 정보통신기술(Information and Communications Technology, ICT) 등의 첨단기술이 접목되어, 기존 교통체계의 교통수단·기반시설·서비스와 비교해 혁신적인 기술적 변화가 일어난 모빌리티를 가리킨다.[8] 정보통신기술은 '모빌리티 수단'과 '모빌리티 기반시설'의 연결을 급속히 향상시켜 서비스로서 전체 시스템이 유기적으로 동작을 할 수 있도록 하였다. 육상에서는 자율주행자동차, 지능형 도로, C-ITS(Cooperative-Intelligent Transport Systems) 등이, 해상에서는 자율운항선박, 스마트항만, 해상교통관제시스템 등이, 항공에서는 도심항공교통, 무인기 관제시스템, 항공정보통합시스템 등이 첨단모빌리티의 사례라고 하겠다. 자율주행을 포함한 인공지능 기술은 인간의 개입 없이 시스템 스스로 인지(Perception)·판단(Decision)·행동(Action)을 가능하게

8) 『모빌리티혁신법』제2조제5호에서 첨단기술로 자율주행, 인공지능, 정보통신기술 등을 언급하고 있다.

만들었다. 특히 모빌리티는 이동이라는 물리 세계와 밀접하게 관련이 있어, 피지컬 AI 기술과 깊은 관계가 있다고 하겠다(Yingbo Li et al. 2023). 카메라, 레이더, 라이더 등과 같은 센서로 '모빌리티 수단'의 주변 환경을 인식하고 인공지능이 안전하면서 최적의 이동 경로를 분석 및 판단한 후 자율주행차, 자율운항선박, 드론, eVTOL 등에서 움직임을 수행한다.

본 논문에서는 모빌리티 사이버보안 관련 법제를 분석하기 위해 분석 대상을 '모빌리티 수단'이 동작하는 영역을 기준으로 육상·해상·항공으로 나누어 육상 모빌리티(자율주행자동차 등), 해상 모빌리티(자율운항선박 등), 항공 모빌리티(드론, 도심항공교통 등)로 분류하였다. 각각의 '모빌리티 수단'에 대해서는 정보통신기술과 인공지능 기술의 관점으로 살펴보았다〈표 1〉. 정보통신기술은 기존 시스템·네트워크를 대상으로 성능 향상과 모든 요소들의 연결성을 목표로 하고 있으며, 통상 사이버보안은 이러한 기술을 대상으로 한 규제·법제로 이해할 수 있다. 인공지능 기술은 자율 주행·운항·비행을 위한 기본 기술로 최근 들어 그 중요성이 점점 커지고 있다.

〈표 1〉 모빌리티 수단 및 기술 분류

	분류
모빌리티 수단	육상(자율주행자동차 등), 해상(자율운항선박 등), 항공(드론, 도심항공교통 등)
기술	정보통신기술(ICT), 인공지능(자율주행 포함)

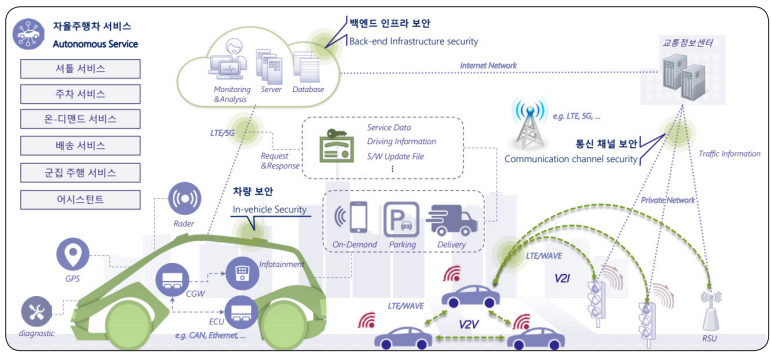
Ⅱ. 육상·해상·항공 모빌리티 기술 및 사이버보안

1. 육상 모빌리티: 자율주행자동차

1) 기술

자율주행자동차는 대표적인 육상 모빌리티이다. 최근 자동차는 연결을 중시하는 커넥티드카(Connected Car), 소프트웨어 관점에서 바라본 소프트웨어 정의 차량(Software Defined Vehicles, SDV) 등 다양하게 불리고 있으며, 자율주행자동차는 인간의 운전을 대신하는 인공지능에 초점을 맞춘 개념이라 할 수 있다. 이들은 별개의 시스템이 아니라 동일한 차량을 바라보는 기술적 관점의 차이라고 할 수 있다.

〈그림 2〉 자율주행차 서비스 구성도



출처: 과학기술정보통신부, 한국인터넷진흥원 2022a, 16.

자율주행자동차 서비스는 3요소인 '모빌리티 수단'인 차량, '모빌

리티 기반시설'인 백엔드 인프라, 그리고 '모빌리티 수단'의 외부 통신을 담당하는 '통신 채널'로 이루어져 있는데 정보통신기술과 관련이 있다〈그림 2〉. 차량 내부 통신은 CAN(Controller Area Network) 기반으로 이루어지고 있으나 자율주행을 위해 대량으로 데이터가 전송되다 보니 이더넷 기반으로 통신이 이루어진다. 자율주행을 위한 외부 데이터는 라이다, 카메라, 레이더, GPS 등 센서로 수집하고 있다. 이 밖에도 제어기(제동, 조향, 동력제어), 인포테인먼트, 텔레매틱스 등 수많은 부품들이 서로 통신을 하며 유기적으로 동작한다. 외부 통신은 V2X[9], 셀룰러(LTE/5G), 와이파이, 블루투스, GNSS(Global Navigation Satellite System) 등을 통해 이루어진다. 백엔드 인프라에는 OTA(Over-The-Air) 소프트웨어 업데이트 서버, ITS(Intelligent Transport Systems) 등이 있다. ITS는 교통수단과 교통시설에 정보통신기술을 적용해 교통 정보를 수집·가공·제공함으로써 교통 체계의 운영 효율성과 안전성을 향상시키는 지능형 교통 체계를 말하는데, V2X 기술이 접목되어 실시간 정보 공유를 통해 교통 안전성과 이동성을 더욱더 향상 시킨 C-ITS가 있다.

자율주행자동차의 자동화 수준은 SAE(Society of Automotive Engineers)에서 제시한 기준에 따라 레벨 0부터 레벨 5(완전자율주행)까지 여섯 단계로 구분되며, 레벨이 높아질수록 운전을 수행하는 주체가 운전자에서 자동화 시스템으로 점진적으로 이전된다.[10] 자율주행자

9) V2X(Vehicle-to-Everything)는 차량이 주변의 모든 대상과 통신을 수행해 정보를 주고받는 기술로, V2V(Vehicle-to-Vehicle), V2I(Vehicle-to-Infrastructure), V2P(Vehicle-to-Pedestrian) 등 차량과 통신 대상에 따라 다양하게 분류된다.

10) 레벨 0은 비자동화(No Automation), 레벨 1은 운전자 지원(Driver Assistance), 레벨 2는

동차의 인공지능 기술은 카메라·레이더·라이다·초음파 센서와 지도·통신 데이터로부터 주행환경 정보를 수집한 뒤, 딥러닝 기반 인지 모듈로 도로 구조·차량·보행자·신호를 인식하고 고정밀지도와 결합한 위치추정 및 주변 객체의 거동 예측을 수행하며, 이를 토대로 경로 계획·차선변경·속도조절·충돌회피 등을 결정하는 의사결정 모듈과 조향·가감속·제동을 수행하는 제어 모듈을 통해 인간 운전자의 주행 행위를 모사·대체하는 통합 지능 시스템을 의미한다(안성원 2017).

2) 사이버위협

자율주행자동차는 연결성과 복잡성의 증가로 인해 심각한 사이버 보안 위협에 직면해 있다.[11] 초기 차량은 외부와 격리된 CAN과 같은 내부 네트워크에 의존하여 주로 물리적 공격에 취약했으나, 현대의 자율주행자동차는 V2X 등의 통신 기술 도입으로 원격에서 공격을 수행할 수 있는 지점이 대폭 확대되었다(Amal Yousseef et al. 2025). 내부 네트워크인 CAN 버스는 암호화 및 인증 메커니즘이 부족하여 인젝션 공격에 매우 취약하며, 이를 통해 공격자는 조향, 제동, 가속과 같은 핵심 기능을 임의로 제어할 수 있다. 센서 스푸핑 및 재밍 위협이 있을 수 있으며, 소프트웨어 및 펌웨어의 보안 취약점이 있을 수

부분 자동화(Partial Automation), 레벨 3은 조건부 자동화(Conditional Automation), 레벨 4는 고도 자동화(High Automation), 레벨 5는 완전 자동화(Full Automation)이다. 레벨 2까지는 운전자의 보조 기능으로 간주되며, 레벨 3부터 자율주행의 시작으로 보고 있다.

11) 『자동차 사이버보안 관리체계 인증 등에 관한 고시』에서는 사이버위협을 다음과 같이 분류하였다. ①자동차와 관련된 백엔드 서버에 대한 사이버공격·위협, ②자동차 통신채널과 관련된 사이버공격·위협, ③업데이트 절차와 관련된 사이버공격·위협, ④의도하지 않은 행동으로 인한 사이버공격·위협, ⑤자동차의 외부 연결에 대한 사이버공격·위협, ⑥자동차 데이터·코드에 대한 사이버공격·위협, ⑦악용될 수 있는 잠재적 취약점.

있다. 특히 안전하지 않은 OTA 소프트웨어 업데이트 메커니즘은 공격자가 시스템에 대한 지속적인 제어권을 획득할 수 있는 경로를 제공한다(과학기술정보통신부, 한국인터넷진흥원 2022b, 18-21). 2015년 지프 체로키의 인포테인먼트 대상 해킹은 원격으로 차량을 제어할 수 있음을 Black Hat 시연에서 보여 주었으며, 그 후 실제 차량 대상 다양한 해킹 공격에 대한 기술 개발이 급속도로 이루어지고 있다(Alex Drozhzhin 2015).

자율주행차에서 인공지능 도입에 따른 위협으로 적대적 머신러닝(Adversarial machine learning), 데이터 중독(Data poisoning), 모델 탈취, 입력 조작에 의한 오동작 등이 발생할 수 있다(ENISA 2021, 31-42). 적대적 머신러닝은 공격자가 특수하게 조작된 입력을 제시하여, 인공지능이 신호등과 표지판을 잘못 인식하도록 유도한다. 데이터 중독은 학습 데이터셋에 악의적 샘플을 삽입하여, 특정 상황에 대해 잘못된 행동을 학습하게 한다. 모델 탈취·역공학은 API 호출 패턴 분석 등을 통해 모델 구조·파라미터를 유추한 뒤, 이를 활용해 보다 정교한 공격을 수행한다. 추론 단계 조작은 추론 엔진이 실행되는 차량 내 시스템을 악성코드로 오염시켜, 인공지능 출력값을 변조하거나 특정 상황에서만 오동작하도록 한다.

2. 해상 모빌리티: 자율운항선박

1) 기술

해상 모빌리티의 대표적인 영역인 자율운항선박은 전통적인 선박 시스템에 센서·통신·인공지능 기반 의사결정 기능이 결합된 구조로서, 선박 내부 시스템, 해상·육상 간 통신망, 육상 관제 인프라가 긴밀

히 연결된다. 자율운항선박이라고 하면 '모빌리티 수단'인 자율운항선박과 '모빌리티 기반시설'인 원격운항센터 등을 포함한 전체 환경을 가리키며, 〈표 2〉와 같은 핵심 기술 요소로 구성된다.

〈표 2〉 자율운항선박의 핵심 기술 요소

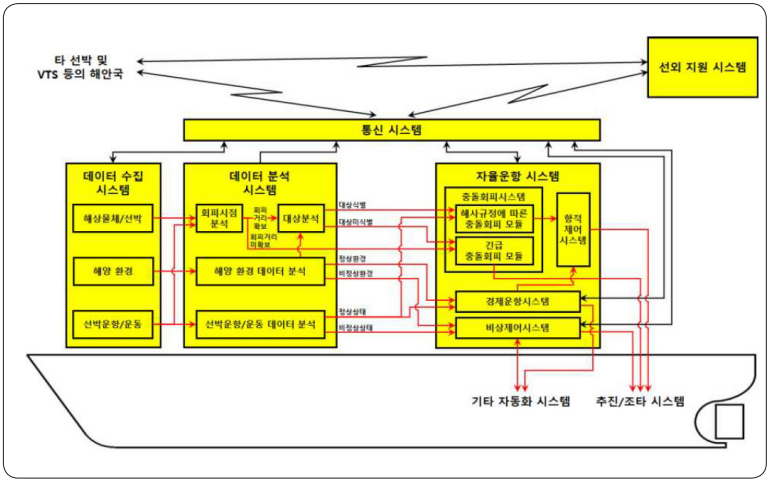
기술 요소	내용
지능항해시스템	선박 주변의 해상 상황을 실시간으로 인지하고 충돌 및 사고를 방지하는 시스템
기관자동화시스템	엔진, 발전기 등 핵심 기관의 상태를 실시간 모니터링하고 고장을 예측·진단하여 운항 신뢰성을 확보하고 원격 유지보수를 지원
디지털 브릿지	자율운항 관련 모든 시스템의 데이터를 통합하고 제어하는 선박 내 중앙 플랫폼
에너지통합관제시스템	선내 에너지 효율을 최적화하고 환경 규제 준수를 지원
해상광대역통신 및 사이버보안시스템	위성통신(VSAT), VDES(VHF Data Exchange System), 5G/LTE-M 등을 통해 선박과 육상 간의 대용량 데이터를 안정적으로 통신하고, 이 과정에서의 보안을 담당
원격운항센터	육상에서 선단을 실시간으로 모니터링하고, 필요시 원격 제어하며, 수집된 운항 데이터를 분석하여 선단 운영을 최적화하는 중앙 통제소

출처: 과학기술정보통신부 외 2025, 16-20

자율운항을 위한 자율화시스템을 살펴보면 선박의 외부상황과 선박의 운항정보와 같은 내부상황을 인식하기 위한 '데이터 수집 및 분석 시스템', 내외부 상황을 고려하여 운항 계획을 세우고 선박을 제어하는 '자율운항시스템', '통신시스템', 자율운항선박의 운항정보를 모니터링하고 제어하는 '선외 지원 시스템'의 요소로 분류할 수 있다 〈그림 3〉. International Maritime Organization(IMO)은 자율운항 수준을 4단계로 나누었는데, 레벨 1은 운항의 의사결정을 도와주고(Ship

with automated processes and decision support), 레벨 2는 선원이 있지만 원격으로 제어하며(Remotely controlled ship with seafarers on board), 레벨 3은 원격으로 무인 선박을 제어하고(Remote controlled ship without seafarers on board), 레벨 4가 되면 인공지능 기반으로 완전히 자율운항을 한다(Fully autonomous ship)(IMO 2018, 1).

〈그림 3〉 자율화시스템의 일반적인 구성



출처: 한국선급 2024, 11-12.

2) 사이버위협

정보통신기술 관점에서 자율운항선박에 대한 사이버공격을 살펴보면 선박의 시스템에 허위 정보를 입력하여 시스템이나 센서를 속이는 스푸핑 공격(Spoofing Attacks), 간섭 신호를 방출하여 통신 신호를 방해하는 재밍 공격(Jamming Attacks), 해상 모바일 서비스 식별 번호의 취약점을 이용하는 조정된 공격(Coordinated Attacks), 시스템 자

원을 고갈시켜 정상적인 사용자의 접근을 차단하는 서비스 거부 공격(DoS Attacks), 기술적으로 오류가 없으나 내용상 불가능한 메시지를 보내는 논리적으로 유효하지 않은 데이터 인코딩(Logically Invalid Data Encoding), 플로팅 차트나 레이더 화면에 표시되는 시각 정보를 속이는 시각 항법 방해(Visual Navigation Disruption) 등과 같이 다양한 방법들이 있다(Nimra Tabish, Tsai Chaur-Luh 2024, 17120-17124). 이러한 기술을 이용하여 전세계적으로 해사 대상 사이버공격이 이루어지고 있으며, Maritime Cyber Attack Database에서는 총 447건(2026.6.12. 기준)의 크고 작은 실제 사이버공격 사례를 정리하고 있다(MACD).

자율운항선박의 인공지능 대상 사이버공격은 학습 단계에서 데이터에 노이즈를 추가하는 포이즈닝(Poisoning) 공격을 통해 인공지능이 장애물이나 위협을 오판하도록 유도하는 선박 데이터셋 공격(Ship Dataset Attack), AIS(Automatic Identification System), GNSS, 카메라 등 센서 데이터에 스푸핑, 재밍, DoS 공격 등을 가해 인공지능이 잘못된 판단을 내리게 하거나 운항을 방해하는 센서 데이터 공격(Sensor Data Attack), 신경망 알고리즘 자체에 대한 해킹(무차별 대입, 버퍼 오버플로우 등)을 통해 인공지능의 안정성을 해치고 정상적인 제어를 불가능하게 만드는 인공 신경망 공격(Artificial Neural Network Attack) 등이 있다(Ji-woon Yoo, Yonghyn Jo 2023, 5-10).

3. 항공 모빌리티: 드론·도심항공교통

1) 기술

드론은 촬영, 측량, 감시 등 제한된 용도로 활용되던 단계에서, 배터리 및 전기추진 기술의 발전을 계기로 활용 영역이 점차 확대되었

으며, 이러한 기술적 진전과 더불어 도심 교통 혼잡과 환경 문제를 완화할 필요성이 제기되면서, 드론과 유사한 eVTOL를 활용해 사람과 화물을 도심 상공에서 수송하려는 도심항공교통 개념이 부상 하였다(이중현 2021, 10-12). 결과적으로 드론 분야에서 축적된 전기추진·자율비행·통신 기술은, 버티포트·전용회랑·교통관리시스템을 포함하는 도심항공교통 체계로 확장되며 대중교통 수준의 안전성과 신뢰성을 요구받는 항공 모빌리티로 진화하고 있다.

드론은 조종사가 직접 탑승하지 않고 무선으로 원격 조정을 하거나 입력된 프로그램에 따라 비행이 가능한 비행체를 말하며, 드론 서비스는 '드론', '지상제어장치', '정보제공장치', '서비스 제공자', '서비스 요청자'로 구성된다(한국인터넷진흥원 2020, 14-15). 지상제어장치(Ground Control Station, GCS)는 C2(Command and Control) 링크를 통해 드론에서 명령을 전달하고 원격 제어하는 장치이며, 정보제공장치는 드론 서비스와 관련된 정보를 제공하는 장치이다. 드론 기반의 서비스를 제공하는 기관은 서비스 제공자 또는 사업자로 구분할 수 있으며, 드론 서비스를 요청하는 서비스 요청자 또는 사용자로 구분할 수 있다. 도심항공교통은 도심 내 활용이 가능하고 배출가스가 없는 친환경 eVTOL 등을 이용하여 승객이나 화물 운송 등을 목적으로 하는 항공체계 기반 모빌리티로(UAM Team Korea 2025, 9), 드론에 수송·여객의 역할이 확장되었다고 할 수 있다. 도심항공교통의 핵심은 eVTOL로 대표되는 도심형항공기와 eVTOL이 이착륙할 수 있는 시설로 사람과 물품을 실을 수 있는 공간인 버티포트이다.

드론과 도심항공교통의 자율비행 레벨과 관련하여 명확하게 분류한 것은 없으나 정부문서 등의 자료에서 분류 기준을 찾아볼 수 있다. 드론에서는 조종의 단계를 5단계로 나누고 있으며, 사람이 직접 조종

하는 1단계(원격조정), 고난도 임무만 사람이 직접 조종하는 2단계(부분 임무위임), 부여받은 임무만 자동비행하는 3단계(임무위임), 자율비행을 하면서 필요시 사람이 개입하는 4단계(원격감독), 완전 자율비행을 하는 5단계(완전자율)로 나누고 있다(관계부처 합동 2025, 4). 도심항공교통은 기장의 운용 방식에 따라 조종사가 탑승하는 초기(On-Board), 원격조종사 도입 및 원격조종사 기능 미지원시 조종사가 탑승하는 성장기(Remote), 무인 자율비행이 도입되는 성숙기(Autonomous)로 구분하고 있다(UAM Team Koera 2025, 13-15). 이는 자율 운전·운항의 단계를 보조·원격조종·자율로 보는 자율주행자동차와 자율운항선박의 자율화 레벨 분류 접근 방식과 유사하다.

2) 사이버위협

드론과 도심항공교통은 운영 환경이 항공이라는 점만 다를 뿐, 앞에서 살펴본 육상·해상 환경에서 자율주행자동차와 자율운항선박의 사이버위협 유형과 유사하다고 할 수 있다. 드론 대상 사이버위협은 드론, 통신, 조종·운영시스템에서 발생한다. 드론을 대상으로 GPS 재밍, 제어신호 전파 방해, GPS 위장 교란, 센서 교란, 데이터 유출, 암호키 노출, 악성코드 감염, 펌웨어 변조, 업데이트 결함, SW 오류 등이 있으며, 통신에 대해서는 세션 하이재킹, 제전송 공격, 중간자 공격, 메시지 위변조 등이 있다(한국인터넷진흥원 2020, 35). 도심항공교통에서는 드론과 유사하게 공격 벡터로 네트워크 공격, 악성 소프트웨어, IoT 조작, 승인 오용, 소셜 엔지니어링 및 피싱 공격이 있다(김경욱 2023, 20-22).

4. 모빌리티 사이버보안을 위한 공통 요소

자율주행자동차, 자율운항선박, 드론 및 도심항공교통과 관련된 사이버 위협은 주로 모빌리티 수단 자체, 이를 지원하는 모빌리티 기반 시설, 그리고 이들을 연결하는 무선통신망을 공격 대상으로 삼는다. 육상·해상·항공으로 구분되는 물리적 운행 환경은 다르지만, 이러한 이질적인 모빌리티 환경 전반에서 사이버보안을 실질적으로 향상시키기 위해서는 설계·개발·운영·유지관리·폐기에 이르는 전 생명주기에 걸쳐 체계적으로 사이버보안 요소를 통합하는 공통된 접근이 요구된다.

설계 단계에서는 모빌리티 환경과 위협 모델을 반영해 보호 대상과 공격 경로를 식별하고 이에 기초한 보안 요구사항을 구조 설계에 내재화한다. 개발 단계에서는 안전한 개발 원칙과 보안 코딩·시험을 통해 설계된 보안 요구사항이 구현물과 통합 과정에 충실히 반영되도록 한다. 운영 단계에서는 실제 운행 환경에서의 위협·취약점을 지속적으로 모니터링하고 이상 탐지·사고 대응을 통해 공격의 영향을 최소화한다. 유지관리 단계에서는 정기 점검·업데이트·취약점 관리 등을 통해 시스템의 보안 수준을 계속 유지·개선한다. 폐기 단계에서는 운행 종료·설비 폐기 과정에서 데이터와 보안 설정 정보가 유출·악용되지 않도록 안전한 삭제·파기와 분리 조치를 시행한다.

Ⅲ. 모빌리티 사이버보안 법제 분석: 국내법과 국제규범

1. 모빌리티 관련 사이버보안 법제

모빌리티 분야의 주요 법률인 『모빌리티혁신법』, 『자율주행자동차법』, 『자율운항선박법』, 『드론법』, 『도심항공교통법』등은 전반적으로 산업육성을 위한 성격이 강해 규제 완화, 실증 특례, 인프라·사업 지원 등 산업 경쟁력 강화에 초점이 맞추어진 특별법의 성격을 강하게 가진다. 이들 법률은 새로운 모빌리티 산업의 성장과 상용화 촉진에 중요한 역할을 하지만, 사이버보안에 관한 규율은 분야별로 편차가 크며 상당 부분이 개별법이나 고시· 지침, 국제기준의 수용을 통해 보완되고 있다. 따라서 모빌리티 사이버보안 법제를 검토할 때에는 특별법만이 아니라, 영역별 일반법·기본법, 행정규칙·지침, 국제규범을 입체적으로 살펴보아야 한다.

『모빌리티혁신법』은 모빌리티 사업의 활성화와 민간 혁신 촉진에 초점을 두고 설계되어, 규제 완화 및 지원체계 구축에 입법 목적이 집중되어 있다.[12] 이에 따라 모빌리티 서비스 및 기반시설에 내재된 사이버보안 위협을 독립된 규율 대상으로 설정하거나, 안전·보안 측면

12) 『모빌리티혁신법』제1조(목적) 이 법은 모빌리티의 혁신을 체계적으로 수행하고 활성화하기 위한 기반 조성 및 지원 등에 필요한 사항을 규정하여 새로운 모빌리티 수단 · 기반시설 · 서비스 및 기술의 도입 · 확산을 도모함으로써 국민 이동성의 획기적인 증진에 이바지함을 목적으로 한다.

에서의 체계적인 관리·통제 메커니즘을 마련하는 규정은 사실상 부재하다는 한계를 가진다. 한편 '모빌리티 기반시설'은 도로·공항·항만 등 교통 인프라와 이를 운영·관리하는 각종 전산·통신 시스템이 포함되어 있고 이용자·운행 데이터, 위치정보, 교통관제 정보 등을 대규모로 처리·전송한다는 점에서 『개인정보 보호법』, 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』(이하 『정보통신망법』), 『위치정보의 보호 및 이용 등에 관한 법률』(이하 『위치정보법』) 등의 법률로 규율을 받고 있다. 또한 도로·공항·항만 등은 정보통신기반 보호법상 주요정보통신기반시설로 지정될 수 있는 교통시설에 해당 되어, 관련 기반시설과 관제·운영 시스템은 『정보통신기반 보호법』에 따른 취약점 분석·평가 및 보호대책 수립·이행 의무의 영향권 안에 놓이게 된다. 본 논문에서는 모빌리티와 관련된 특례법과 영역별 기본법, 그리고 『인공지능기본법』을 위주로 논의를 하였으며, 『개인정보 보호법』, 『정보통신망법』 등의 일반 정보보호 법률은 배경 규범으로 전제한다.

〈표 3〉 모빌리티 관련 사이버보안 국내외 법제

대상	법제
모빌리티	• 『모바일혁신법』, 『통합교통체계법』 등 • 『개인정보 보호법』, 『정보통신망법』, 『정보통신기반 보호법』 등
자율주행자동차	• 『자율주행자동차법』, 『자동차관리법』, 『자동차 및 자동차부품의 성능과 기준에 관한 규칙』(이하 『자동차규칙』),『자동차 사이버보안 관리체계 인증 등에 관한 고시』 등 • UNECE R156, R155, R157, R171 등
자율운항선박	• 『자율운항선박법』, 『해사안전기본법』 등 • 『해사 사이버안전 관리지침』, 『선박 및 시스템의 사이버복원력 지침』, 『해상 사이버보안 시스템 지침』, 『자율운항선박 지침』 등 • IACS UR E26, E27 등

대상	법제
드론 도심항공교통	• 『드론법』, 『도심항공교통법』 등 • 『항공안전법』, 『항공사업법』, 『공항시설법』, 『항공보안법』 등
인공지능	• 『인공지능기본법』 등 • EU AI Act(이하 EU AIA) 등

2. 자율주행자동차 사이버보안 법제

자율주행자동차 영역은 육상·해상·항공 모빌리티 분야 중 사이버보안 규율이 가장 구체적으로 형성된 분야이다. 국내 자율주행자동차 법제는 자율주행차 대상 『자율주행자동차법』과 차량 관리의 일반법인 『자동차관리법』이 있다. 이들 법에 UNECE(UN Economic Commission for Europe) WP.29 체계의 국제규범이 영향을 미치고 있다.

차량과 연결된 인프라 전반의 사이버보안의 대응하기 위한 법제·규정을 보면 국제적으로 UNECE Regulation No. 155(Cybersecurity Management System, CSMS)와 UNECE R156(Software Update Management System, SUMS)이 마련되어 있으며, 이를 국내 법제에 반영한 『자동차관리법』이 있다. R155는 자동차 사이버보안 및 사이버보안관리체계(CSMS)에 관한 규정으로, 자동차 제조사가 차량과 그 생태계 전반에 대해 사이버위험을 조직적으로 식별·분석·관리하는 체계를 수립·운영하고, 이를 독립적인 형식승인 절차를 통해 입증받도록 요구한다. R156는 소프트웨어 업데이트 및 보안(SUMS)에 관한 규정으로, 차량에 적용되는 소프트웨어 업데이트 특히 OTA 방식의 원격 업데이트에 대해 무결성·진정성·추적 가능성을 보장하도록 관리할 것을 요구한다. 두 규정은 유럽형식승인 체계에서 차량 판매의 필수 요건으로 기능하고 있으며, 실질적으로 글로벌 자동차 산업 전반에 적용

되는 사이버보안·소프트웨어 업데이트 규범으로 자리 잡았다.

우리나라는 이들 국제 규제를 수용하기 위해, 상위법인 『자동차관리법』과 그 하위 규범을 단계적으로 정비하는 방식으로 자동차 사이버보안 법제를 구축해 왔다. 『자동차관리법』에 자율주행자동차 및 커넥티드카를 포함한 자동차 전반에 대하여, 자동차 제작자 등이 사이버보안 관리체계를 갖추고 자동차의 사이버위협을 관리해야 한다는 취지의 근거 규정이 도입되었다.[13] 『자동차관리법』의 위임을 받아 제정·개정된 『자동차규칙』에 자동차 및 자동차의 부품 또는 장치의 안전 및 성능 시험에 적용할 기준 및 방법을 정하고 있는데, 이 중에 사이버보안 관련 기준을 규정하고 있다.[14] 이를 근거로 『자동차 사이버보안 관리체계 인증 등에 관한 고시』에 구체적인 기준과 절차를 제시하고 있으며, 제13조에 자동차 사이버공격·위협[15]과 제14조에 자동차 사이버공격·위협에 대한 보안조치[16]가 UNECE R155 등의 규정을

13) 『자동차관리법』제30조의9(자동차 사이버보안 관리체계 인증 등), 제30조의10(자동차 사이버보안 관리체계 관련 자료의 제출 요구), 제30조의11(자동차 사이버보안 관리체계 인증의 취소 등), 제30조의12(자동차 사이버공격·위협의 신고 등).

14) 『자동차규칙』제18조의4(사이버보안) 자동차 사이버공격 · 위협과 관련된 자동차의 전기 · 전자장치는 법 제30조의9제1항에 따른 자동차 사이버보안 관리체계 인증을 받은 내용에 따라 다음 각 호의 기준에 적합해야 한다.

15) UNECE R155 Annex 5의 Part A. Vulnerability or attack method related to the threats를 참조하고 있으며 사이버공격·위협을 다음과 같이 분류하였다. ①자동차와 관련된 백엔드 서버에 대한 사이버공격·위협, ②자동차 통신채널과 관련된 사이버공격·위협, ③업데이트 절차와 관련된 사이버공격·위협, ④의도하지 않은 행동으로 인한 사이버공격·위협, ⑤자동차의 외부 연결에 대한 사이버공격·위협, ⑥자동차 데이터/코드에 대한 사이버공격·위협, ⑦ 악용될 수 있는 잠재적 취약점.

16) UNECE R155 Annex 5의 Part B. Mitigations to the threats intended for vehicles 및 Part C. Mitigations to the threats outside of vehicles를 참조하고 있으며 사이버공격·위협에 대한 보안 조치를 다음과 같이 분류하였다. ①자동차 통신채널과 관련된 위협에 대한 보

참조하였다. 자동차 사이버공격·위협은 환경을 자동차, 백엔드, 통신 채널로 분류하여 이들 사이에서의 연결 및 각자 요소에 대한 사이버 공격·위협을 정의하고 있다.

한편 자율주행과 관련된 국내외 법제·규정을 보면 『자율주행자동차법』과 UNECE R157(Automated Lane Keeping Systems)와 R171(Driver Control Assistance Systems)이 있다. 『자율주행자동차법』은 2019년에 제정되어 2020년부터 시행되면서, 자율주행자동차의 상용화 촉진과 안전한 운행 기반 조성을 위한 기본 법적 틀을 마련하였다. 이 법은 초기에 시범운행지구 지정, 실증 특례 부여 등 행정적·재정적 지원 근거를 규정하였으나, 이후 개정에서는 성능인증 및 적합성 승인 제도가 도입 되었다.[17] 자율주행자동차의 성능인증을 위해 레벨 4 이상의 자율주행에 대한 안전기준을 마련하기 위해 『자율주행자동차 성능인증 및 적합성 승인 등에 관한 규정』을 제정하였다.[18] R157과 R171은 자율주행 기능 상용화를 위해 단계별 안전 요구사항과 책임 범위를 규정하는 국제 기준이다. R157은 레벨 3 대상 조건부 자율주행용

안 조치, ②업데이트 절차와 관련된 위협에 대한 보안 조치, ③의도하지 않은 행동으로 인한 위협에 대한 보안 조치, ④자동차의 외부 연결과 관련된 위협에 대한 보안 조치, ⑤ 자동차 데이터/코드와 관련된 위협에 대한 보안 조치, ⑥악용될 수 있는 잠재적 취약점에 대한 보안 조치, ⑦ 차량 데이터 손실 및 데이터 유출과 관련된 위협에 대한 보안 조치, ⑧시스템의 물리적 조작과 관련된 위협에 대한 보안 조치, ⑨자동차와 관련된 백엔드 서버의 위협에 대한 보안 조치, ⑩데이터의 물리적 손실에 대한 보안 조치.

17) 『자율주행자동차법』제40조(자율주행자동차의 성능인증)는 『자동차관리법』제30조(자동차 자기인증)와 관련한 조항이다.

18) 『자율주행자동차 성능인증 및 적합성 승인 등에 관한 규정』제6조(제작방법) 제3항에서는 자율주행시스템의 고장 · 기능장애 · 사이버 보안 위험등 비상상황 대비에 관한 기준을 제시한다. 해당 기준에서는 자율주행자동차 대상 사이버공격·위협 방지를 위한 대책 수립·적용·검증을 요구하고 있다.

자동 차선 유지 시스템 관련 규정이며, R171은 레벨 2에 해당하는 조향·가감속 보조 기능을 탑재한 M(사람 수송)·N(화물 수송)형 차량의 형식승인을 위한 일관된 안전·성능 요구사항을 위한 규정이다.

이와 같이 자율주행자동차 사이버보안 법제는 R155와 R156의 수용과 『자동차관리법』과 『자율주행자동차법』의 연계를 통해 CSMS·-SUMS 중심의 관리체계와 형식승인 구조를 비교적 정교하게 구축하였다는 점에서 다른 모빌리티 영역에 비해 진전된 모습을 보인다. 그럼에도 불구하고 이 법제는 적대적 머신러닝, 데이터 중독, 모델 탈취, 추론 단계 조작 등 인공지능 고유의 위협을 독립된 규율 축으로 구조화하지 못하고 있고, CAN 버스 인젝션, 센서 스푸핑·재밍, OTA 공급망 공격 등 차량·센서·백엔드·통신채널 전반의 위협에 대해서도 구체적 기술요건의 상당 부분을 하위 기술기준과 국제표준에 위임하고 있어 규율의 범위와 강행성이 분야와 요소별로 편차를 보인다는 한계를 가진다.

3. 자율운항선박 사이버보안 법제

자율운항선박 분야는 자율주행자동차에 비해 사이버보안 국내 법제의 성숙도가 낮은 편이며, 국내 법률과 정책지침, 선급 기준, 국제규범이 병존하는 구조를 가진다.

해사안전 전반을 포괄하던 종전 『해사안전법』은 2023년 전부개정을 통해, 해사안전 정책·시책 등 기본 사항을 규율하는 『해사안전기본법』과 수역·해상교통·선박 안전관리 및 항법을 규율하는 『해상교통안전법』으로 분법 되었다. 『해사안전기본법』은 해양사고 예방, 해상교통 안전 및 위험관리 체계 구축을 위하여 국가, 지방자치단체 등

의 책무를 규정하고, 해사안전종합계획과 연도별 시행계획을 통해 다양한 해상 위험요인을 종합적으로 관리하기 위한 기본 법적 틀을 제시하고 있으며, '해사 사이버안전'의 정의와 해사 사이버안전 관리를 위한 시책을 수립·시행하도록 명시하고 있다.[19] 해양수산부는 『해사안전법』을 상위 근거로 하여 『해사 사이버안전 관리지침』을 제정·고시하였고, '해사 사이버 공격·위협'의 개념을 구체화 하였다.[20] 동 지침에서는 식별·보호·탐지·대응·복구의 다섯 단계로 구성된 해사 사이버안전 관리 기능을 제시하여 선박 및 관련 사업장에서 구현해야 할 사이버보안 관리체계의 기능적 요소를 구조화하고 있다.[21]

선박과 항만의 보안을 규율하는 『국제항해선박 및 항만시설의 보안에 관한 법률』(이하『국제선박항만보안법』)은 IMO의 International Ship and Port Facility Security Code(ISPS Code)[22]를 수용하기 위해 제정된 법으로, 선박·항만시설 출입통제, 경비 인력 배치, 울타리·감

19) 『해사안전기본법』제3조(정의). "해사 사이버안전"이란 사이버공격으로부터 선박운항시스템을 보호함으로써 선박운항시스템과 정보의 기밀성 · 무결성 · 가용성 등 안전성을 유지하는 상태를 말한다.
『해사안전기본법』 제4조제2항. 국가 및 지방자치단체는 해양사고를 예방하고 해상교통환경의 변화에 대응할 수 있도록 해양시설의 관리, 해상교통망의 구축 및 관리, 해상교통 관련 신기술의 개발 · 기반조성 지원, 해사 사이버안전 관리 등을 위하여 필요한 시책을 수립 · 시행하여야 한다.

20) 『해사 사이버안전 관리지침』제2조(정의), "해사 사이버 공격 · 위협"이란 해킹, 컴퓨터 바이러스, 서비스 거부, 전자기파 등 전자적 수단으로 선박운항시스템 또는 이와 관련된 정보시스템을 침입 · 교란 · 마비 · 파괴하거나 정보를 위조 · 변조 · 훼손 · 훔치는 행위 및 그와 관련된 위협을 말한다.

21) 선박 사이버보안은 궁극적으로 사이버복원력을 목표로 하고 있으며, 이를 위한 식별·보호·탐지·대응·복구의 5단계 기능이 기본 틀이 된다.

22) ISPS Code는 국제해사기구(IMO)가 제정한, 선박과 항만시설을 테러·해적·무단침입 등 보안 위협으로부터 보호하기 위한 국제선박 및 항만시설 보안규칙이다.

시카메라·경보장치 등 물리적·운영상의 보안 조치를 중심으로 규율 체계가 설계되어 있다. ISPS Code 자체가 테러·불법 침입·화물 취급 과정의 파괴 행위 등 물리적 위협을 주된 규율 대상으로 삼았기 때문에, 이를 국내법으로 이행한 『국제선박항만보안법』 역시 해상 사이버 위협 보다는 물리·인적 보안에 치우친 구조를 유지하고 있다(박제영 외 2025). ISPS Code와 International Safety Management Code(ISM Code)[23]의 국제 규범을 준수하기 위해 한국선급에서 『해상 사이버보안 시스템 지침』을 마련하였으며, 사이버보안을 사이버공격에 대해 예방·탐지·대응 수행하는 일련의 프로세스로 정의 내리고 있다. 『해사 사이버안전 관리지침』에서의 '해사 사이버안전'은 『해사안전기본법』 체계 하에서 국가·지자체·선사 등의 책무, 계획, 시책까지 포함하는 정책·법제 용어라고 본다면, 『해상 사이버보안 시스템 지침』의 '해상 사이버보안'은 선박·항만 등 해상 분야에 IT·OT 시스템에 대한 보다 구체적인 기술 및 활동을 가리키는 기술 용어로 볼 수 있다.

선박은 해외에서 운항이 되기 때문에 국제 규제에 영향을 많이 받는다. 국제선급협회(International Association of Classification Societies, IACS)의 UR(Unified Requirement) E26(Cyber Resilience of Ships)와 UR E27(Cyber Resilience of On-Board Systems and Equipment)는 해상 분야 사이버복원력 규제의 핵심 기준이다. UR E26은 선박 전체를 하나의 통합된 사이버 시스템으로 보고 설계·건조·시운전·운항 전 생애주기에 걸친 사이버복원력 확보를 요구하며, IT·OT 시스템을 대상으로 식별·보호·탐지·대응· 복구의 다섯 기능 영역에 따라 요구사항을 구

23) ISM Code는 선박의 안전한 관리·운항과 해양오염방지를 위한 국제표준을 정한 규약이다.

조화한다. UR E27은 선내 개별 시스템·장비 수준에서 사이버복원력을 확보하기 위한 기준을 제시하는 것으로, 시스템 구성·네트워크 흐름, 보안이 반영된 개발수명주기 문서, 유지관리·복구 계획, 시험 및 운용 매뉴얼, 변경관리 절차 등 문서화와 보안 기능 구현을 장비 공급자의 책임으로 요구한다. 한국선급의 『선박 및 시스템의 사이버복원력 지침』은 UR E26·E27의 구조와 요구사항을 반영하여 신조선과 주요 선내 시스템이 해당 통일규칙에서 규정하는 사이버복원력 수준을 충족하도록 설계·통합·시험, 문서 제출, 검증 방법을 세부적으로 제시하는 기술 지침이며, 특히 『선박 자동화 시스템의 사이버복원력 승인/검사 가이드』는 자동화·제어 시스템을 대상으로 UR E26·E27의 요구사항을 승인·검사 관점의 시험 항목·절차·입회 방식으로 구체화하고 있다.[24)]

『자율운항선박법』은 자율운항선박의 기술 및 핵심기자재 개발을 촉진하고 자율운항선박의 안전 운항 기반을 조성하여 상용화를 지원하기 위한 법률로 제정되었으며, 제19조에 따라 해양수산부장관은 시범운항 및 실증에 필요한 경우 자율운항선박 및 기자재의 안전성 평가를 시행할 수 있도록 규정하고 있으나 사이버보안이나 사이버안전보다는 안전성에 대한 전반을 규율하고 있다. 이에 비해 한국선급의 『자율운항선박 지침』은 자율운항선박 및 기자재의 안전성 평가 시 적용되는 기술 지침으로서, 사이버공격에 대응하는 사이버보안 기술을 적용하여 시스템의 가용성·기밀성·무결성에 대한 인증을 받

24) IACS UR27의 보안 기능 요구사항인 30개의 필수 보안 기능 요구사항과 11개의 추가 보안 기능 요구사항이 반영되어 있다.

도록 하고 있으며, 이를 위해 자사의 『해상 사이버보안 시스템 지침』이 제시한 요건을 따르도록 하고 있다.

이처럼 자율운항선박 관련 국내 법제에는 사이버보안 관련 항목이 일부 반영되어 있음에도 불구하고, 다양한 정보통신기술·인공지능 기반 위협을 법률 수준에서 직접 다루는 규정은 아직 미비한 상황이다. 『해사안전기본법』과 『해사 사이버안전 관리지침』이 정책·관리체계 차원에서 해사 사이버안전을 포괄하고, 『국제선박항만보안법』이 물리·인적 보안을 규율하며, IACS UR E26·E27 및 한국선급 지침이 선박·선내 시스템의 사이버복원력을 기술적으로 뒷받침하고 있다는 점에서, 자율운항선박 사이버보안 규율은 법률, 정책지침, 선급 기준, 국제규범이 다층적으로 결합된 구조로 이해될 수 있다. 그러나 이 구조에서는 사이버보안 관련 핵심 의무가 어디까지 법률에 의해 직접 부과되고, 어디서부터 선급·지침의 재량에 맡겨지는지 경계가 불명확하다는 한계를 지닌다. 또한 적대적 머신러닝·데이터셋 공격·센서 데이터 공격·신경망 공격 등 인공지능 고유의 위협은 주로 복원력와 관리체계의 일반 범주에 흡수되어 있을 뿐, 자율운항선박법령 체계에서 독립된 규율 축으로 구조화되어 있지 않다. 결국 현재 자율운항선박 사이버보안 법제는 UR E26·E27을 중심으로 한 국제 규범과 한국선급 지침이 선박 관련 사이버복원력의 근간을 이루고 있으나, 국내 법률 차원에서 정보통신기술·인공지능 기반 위협을 직접 규정하고 구속력 있는 의무와 책임체계를 부과하는 수준까지는 아직 나아가지 못한 상태라고 평가할 수 있다.

4. 드론·도심항공교통 사이버보안 법제

우리나라의 항공 관련 기본 일반법은 항공 4법으로, 항공기 등의 안전한 운항 기준과 의무를 정하는 『항공안전법』, 항공사업의 성장·경쟁력·이용자 편의를 위한 『항공사업법』, 공항·항공기 등에 대한 불법 방해행위방지를 위한 『항공보안법』, 공항·항행 안전시설의 설치·운영 기준을 정하는 『공항시설법』이 있다. 이들 법들을 기본법으로 하여 특별법인 드론 산업 활성화를 위한 『드론법』과 도심항공교통 산업 활성화를 위한 『도심항공교통법』이 제정되어 있다. 항공 4법과 특별법 모두 항공기·공항에서의 물리적 안전에 초점을 맞추고 있으며, 사이버보안 요소는 미비하다.

드론은 조종자가 탑승하지 않은 상태에서 항행하는 비행체를 의미하며,[25] 도심항공교통에서 도심형항공기는 『항공안전법』에서 항공기, 경량항공기, 초경량비행장치 중 하나에 해당하는 항공기 또는 이에 준하는 기기로, 도심 운항에 적합한 형태로 규정된다.[26] 이처럼 드론과 도심형항공기가 서로 다른 용어와 법적 범주로 분류되고 있어, 사이버보안 규율의 적용 대상을 일관되게 설정하는 데에는 복잡성이

25) 『드론법』제2조제1호. "드론"이란 조종자가 탑승하지 아니한 상태로 항행할 수 있는 비행체로서 국토교통부령으로 정하는 기준을 충족하는 다음 각 목의 어느 하나에 해당하는 기기를 말한다.
가. 「항공안전법」 제2조제3호에 따른 무인비행장치
나. 「항공안전법」 제2조제6호에 따른 무인항공기
다. 그 밖에 원격 · 자동 · 자율 등 국토교통부령으로 정하는 방식에 따라 항행하는 비행체

26) 『도심항공교통법』제2조제2호, "도심형항공기"란 「항공안전법」 제2조제1호에 따른 항공기 또는 이에 준하는 기기 중 도심에서도 운항하기에 적합한 기기로서 국토교통부장관이 「국가통합교통체계효율화법」 제106조에 따른 국가교통위원회(이하 "국가교통위원회"라 한다)의 심의를 거쳐 고시한 것을 말한다.

존재한다.

드론과 도심항공교통에 대해 사이버보안을 규제할 수 있는 법률은 『항공보안법』 제33조(항공보안 감독)를 근거로 제정된 『국가항공보안 수준관리지침』이다. 동지침의 제5조(적용규정)에 포함된 ICAO(International Civil Aviation Organization) 부속서에 있는 '사이버 위협 관련 조치' 규정을 보면, 각 체약국이 중요 정보·IT/ICT 시스템과 데이터를 식별하고 위험평가에 따라 보호조치를 시행하도록 하는 표준 1개와, 기밀성·무결성·가용성 확보를 위해 설계·공급망·네트워크·원격접근 보안을 권고하는 권고사항 1개가 규정되어 있다(정원희 2020, 27). 드론 대상 안전성인증을 살펴보면 『항공안전법』제124조(초경량비행장치 안전성인증)를 근거로 한 『초경량비행장치 기술기준』에 무인비행장치에 대한 기술기준이 제시되어 있다.[27] 동기술기준에는 무인비행장치로서 적절한 임무를 수행할 수 있는 물리적 기준 인증에 초점을 맞추고 있으나 사이버보안 요소는 미비하다. 도심형항공기 경우는 현재 실증사업·시범운영 단계로 활성화를 위해 산업 진입을 하기 위한 물리적 인증기준만 제안하고 있는 상황이다(국토교통부 2023, 1-4).

『드론법』과 『도심항공교통법』은 입법 목적 단계부터 산업 진흥과 활용 촉진, 규제 완화를 통한 신산업 육성에 초점을 두고 있어, 모빌리티 체계의 디지털화·자율화로 인해 증대되는 사이버보안 위험을 충분히 반영하지 못하고 있다. 특히 기체·지상통제시스템·통신망이 유기적으로 연결되는 구조적 특성에도 불구하고, 사이버위협을 독립

27) 『항공안전법 시행규칙』제305조 제1항제4호 가목에 따른 무인비행기, 무인헬리콥터 또는 무인멀티콥터을 대상으로 하고 있다.

적인 규율 대상으로 설정하거나 위험관리 체계를 체계적으로 설계하지 않은 한계가 있다. 그 결과, 현행 법체계는 운항 안전성 확보와 사업 활성화를 위한 물리적·절차적 규율에는 비교적 충실하나, 해킹, 신호교란, 데이터 변조 등 사이버공격에 대한 예방 및 대응 체계는 미흡한 수준에 머무르고 있다. 이는 향후 드론 및 도심항공교통이 사회기반시설로 확장될 경우, 개별 시스템의 취약성이 전체 운항 안전과 공공 안전을 위협하는 사이버안보 리스크로 전이될 수 있다는 점에서 구조적 한계로 평가된다.

5. 인공지능 사이버보안 법제

국내 『인공지능기본법』은 2026년부터 시행되었으며 관련 법 체계를 구체화하기 위해 하위 법제가 순차적으로 마련되고 있다.[28] 동법은 '사람의 생명·신체의 안전 및 기본권에 중대한 영향을 미치거나 위험을 초래할 우려가 있는 인공지능 시스템'을 '고영향 인공지능'으로 정의하고, 사람의 생명·신체의 안전 및 기본권 보호가 필요한 영역을 열거하고 있다.[29] 고영향 인공지능으로 분류될 경우, 인공지능 사업자에게는 일반 인공지능 시스템보다 강화된 투명성 확보, 안전성·신뢰성 검증, 데이터·모델 관리체계 정비 의무가 부과되며, 사전·

28) 『인공지능기본법』제32조(인공지능 안전성 확보 의무)를 근거로 『인공지능 안전성 확보 의무의 이행방법 등에 관한 고시』와 제34조(고영향 인공지능과 관련한 사업자의 책무)를 근거로 『고영향 인공지능과 관련한 사업자의 책무 고시』가 행정예고 되었다.(2026.4.15. 기준)

29) 『인공지능기본법』제2조제4호. "고영향 인공지능"이란 사람의 생명, 신체의 안전 및 기본권에 중대한 영향을 미치거나 위험을 초래할 우려가 있는 인공지능시스템으로서 다음 각 목의 어느 하나의 영역에서 활용되는 것을 말한다.

사후 인공지능 영향평가와 위험관리, 이용자에 대한 사전 고지, 분쟁·사고 발생 시 책임추적 가능성을 담보하기 위한 기록·로그 관리 의무 등이 추가로 요구된다.[30] 다만 현행 규율 체계는 주로 물리적 안전성과 기능적 신뢰성을 중심으로 설계되어 있고, 인공지능 시스템을 겨냥한 사이버 공격, 데이터·모델 탈취, 적대적 예측 교란 등 사이버보안 위험을 독립된 규율 축으로 구조화하는 데에는 아직 미비한 측면이 있다.

모빌리티 분야에서 활용되는 자율주행자동차, 자율운항선박, 드론·도심항공교통과 관련된 인공지능 기반 교통수단·교통시설·교통관리체계는 교통·운항·비행 사고를 통해 다수의 생명·신체에 직접적인 위해를 초래할 수 있고, 대규모 도시 인프라와 연계된 연쇄 피해를 유발할 수 있다는 점에서 고영향 인공지능의 전형적 유형으로 간주된다.[31] 모빌리티 환경은 차량·선박·항공기와 지상 관제센터, 클라우드 기반 데이터·모델 서버가 네트워크로 상시 연결되어 있어 통신망 침입 등 다양한 사이버위협에 노출되어 있기 때문에 모빌리티 특유의 고영향 인공지능 규제 틀이 반영되어야 할 필요가 있다.

EU AIA는 국내 『인공지능기본법』과 유사하게 인공지능이 인간의 생명·신체 안전과 기본권에 미치는 위험을 기준으로 위험 기반 규율 체계를 구축하고 있다. EU AIA는 '고위험 인공지능(high-risk AI)'을 인

30) 『인공지능기본법』제31조(인공지능 투명성 확보 의무), 제32조(인공지능 안전성 확보 의무), 제33조(고영향 인공지능 확인), 제34조(고영향 인공지능과 관련한 사업자의 책무), 제35조(고영향 인공지능 영향평가)

31) 『인공지능기본법』제2조제4호 아목에서 「교통안전법」 제2조제1호부터 제3호까지에 따른 교통수단, 교통시설, 교통체계의 주요한 작동 및 운영에 사용되는 인공지능을 고영향 인공지능으로 분류하였다.

간의 건강·안전 또는 기본권에 중대한 위험을 초래할 수 있는 분야에 사용되어, 엄격한 사전 규제와 지속적 관리의 대상이 되는 인공지능 시스템으로 정의하고 있으며,[32] 중요 기반 시설(Critical Infrastructure)에 들어가는 교통 등의 모빌리티 영역도 고위험 인공지능에 포함된다.[33] 고위험 인공지능에 대해서는 시스템 제공자에게 사전 적합성 평가, 위험관리체계 구축, 데이터 거버넌스 및 품질관리, 인간의 감독(human oversight) 확보, 기술문서 및 로그 기록 의무 등을 부과한다.[34] EU AIA는 고위험 인공지능의 정확성·견고성·사이버보안 의무(제15조 등)를 중심축으로 삼으면서, 디지털 요소가 포함된 제품의 보안 요건을 규율하는 Cyber Resilience Act(CRA)와 중요 서비스·인프라 사업자의 사이버보안 거버넌스를 규율하는 NIS(Network Information Security) Directive 2와 상호 보완적 관계를 이루어, 인공지능 시스템 자체·탑재 제품·서비스 운영 단계 전반에 걸친 통합적인 위험관리·사이버보안 규율 체계를 형성하고 있다(구태언, 방석호 2026).

『인공지능기본법』은 사람의 생명·신체·기본권에 중대한 영향을 미칠 수 있는 시스템을 고영향 인공지능으로 규정하고, 이에 대해 투명성·안전성·영향평가 의무를 부과하고 있다. 모빌리티의 경우 자율주행·운항·비행 단계에서는 인간의 개입 없이 인공지능이 자동제어를 수행하게 되는데, 이는 고영향 인공지능에 해당하지만 이를 위한 규정이 법률에 충분히 반영되어 있지 않다. 현재 자율주행자동차·자

32) EU AIA, Article 6: Classification Rules for High-Risk AI Systems.

33) EU AIA, Annex III: High-Risk AI Systems Referred to in Article 6(2).

34) EU AIA, Chapter III: High-Risk AI System, Section 2: Requirements for High-Risk AI System, Articles 8-15.

율운항선박·드론·도심항공교통의 시스템·네트워크를 대상으로 사이버보안을 고려하여 이를 반영하려는 노력이 이루어지고 있으나, 『인공지능기본법』에서 제시하는 인공지능의 사이버보안에 대한 규범은 부재하다고 할 수 있다.

Ⅳ. 모빌리티 사이버보안 법제 시사점

모빌리티 기술이 디지털화·연결화되면서 기존의 물리적 안전 중심 규제만으로는 새로운 유형의 위험을 충분히 통제하기 어려워지고 있다. 차량·선박·항공기뿐 아니라 드론, 도심항공교통 등 다양한 수단이 네트워크와 인공지능에 의존하게 되면서, 사이버공격이 곧 물리적 사고와 인명 피해로 직결될 수 있는 구조가 형성되고 있다. 그럼에도 현행 법제는 운행 안전과 시설·사업 규제에 초점이 맞추어져 있어, 모빌리티를 다루고 있는 사이버보안 규제가 영역별로 불균등하게 형성되어 있으며 공통적으로 적용될 수 있는 최소 보안원칙도 명확히 정립되어 있지 않다. 자동차 분야는 CSMS·SUMS를 중심으로 비교적 구체적인 인증체계를 갖추고 있는 반면, 자율운항선박 분야는 지침과 국제기준 중심의 보완 구조를 보이고, 드론·도심항공교통 분야는 물리적 안전과 산업 활성화 중심의 법제가 우세하여 사이버보안 관련 의무가 미약하다. 본 논문은 이러한 문제의식을 바탕으로, 모빌리티 사이버보안 법제와 관련하여 세 가지 방향에서 체계정합성을 제고한 방안을 모색한다.

첫째, 『모빌리티혁신법』은 차량, 선박, 드론, 도심항공교통 등 다양한 이동수단을 포괄하는 일반법으로서, 모빌리티 수단·기반시설·서

비스와 이를 연결하는 통신·네트워크 인프라 전반에 공통 적용될 수 있는 사이버보안 목표와 기본원칙을 설계·개발·운영·유지관리·폐기 단계별로 제시될 수 있다. 이는 별도의 신규 법률을 제정하기보다는, 『통합교통체계법』이 육상·해상·항공 교통을 수평적으로 포괄해 공통 원칙을 제시하는 방식에 준하여, 『모빌리티혁신법』 내부에 모빌리티 관련 시스템 및 사이버보안의 정의, 설계 단계의 위협 모델링과 보안 요구 내재화, 개발·구축 단계의 안전한 구현과 취약점 제거, 운영 단계의 위협 모니터링·사고 대응, 유지관리 단계의 패치·업데이트·구성관리, 폐기 단계의 데이터·장비·계정의 안전한 종료를 포함하는 전 생명주기 기반 공통 보안원칙을 국가와 사업자의 기본 책무로 명시하는 방향으로 구체화될 수 있다. 이러한 단계별 원칙은 개별 교통수단이나 인프라에 관한 세부 기술기준을 한 법에 집중시키려는 것이 아니라, 모빌리티 관련 각 개별 법령(자동차, 해사, 항공 법제 등)이 설계부터 폐기까지 일관된 방향성을 유지하도록 상위에서 조정하고, 상호 간 규율 체계의 충돌을 최소화하며 정합성을 확보하는 공통 기준점으로 기능하게 된다.

둘째, 자율 주행·운항·비행 체계에서 활용되는 인공지능에 대한 사이버보안은, 『인공지능기본법』의 고영향 인공지능 규율을 참조하되, 『모빌리티혁신법』에는 공통 원칙 수준에서 최소한으로 반영하는 것이 체계정합성 측면에서 타당하다. 구체적으로는, 『모빌리티혁신법』이 고영향 인공지능이 탑재된 모빌리티 수단·기반시설·서비스에 대하여 설계·개발·운영·유지관리·폐기의 전 생명주기에 걸쳐 인공지능으로 인한 안전·보안 위험을 식별·관리하고 관련 기록을 적정하게 보존·제공할 책무가 있음을 선언적·원칙적으로 규정하면서, 위험관리·영향평가·투명성·안전성·신뢰성 확보 등 보다 구체적인 요구

사항은 『인공지능기본법』에서 정한 고영향 인공지능 의무를 준수할 것을 모빌리티 분야 사업자의 공통 책무로 연결하는 방식이다. 이때 학습데이터 검증, 모델 업데이트, 인간 감독 절차, 로그 관리 등 세부 이행 방법은 각 개별 모빌리티 법령 및 하위 기준에서 정하도록 위임함으로써, 상위 기본법 간 역할 분담과 모빌리티 분야 특수성 반영을 동시에 담보할 수 있다.

셋째, 『모빌리티혁신법』을 중심으로 사이버보안 관련 공통 원칙과 목표 수준을 설정하는 것과 병행하여, 개별 '모빌리티 수단'별 기본법에 이를 구체화하는 작업이 이루어질 때 체계정합성이 실질적으로 확보된다. '모빌리티 수단'마다 기술적 특성과 운용 환경이 상이하다는 점을 고려하면, 자동차 분야는 『자동차관리법』, 자율운항선박은 『해사안전기본법』, 드론·도심항공교통은 항공 4법(『항공안전법』, 『항공사업법』, 『항공보안법』, 『공항시설법』)을 중심으로 사이버보안 관련 규정을 정비하되, 이를 『모빌리티혁신법』이 제시하는 전 생명주기 공통 보안원칙과 조화되도록 설계하는 것이 바람직하다. 이때 『모빌리티혁신법』은 엄격한 상위법이라기보다 공통원칙을 제시하는 기반법으로 이해하고, 각 개별 기본법이 이를 참조하여 인증·운항·관제·정비·원격제어·통신보안·사고대응 등 수단별 특성을 반영한 세부 의무와 기술기준을 설정하는 구조를 상정하는 것이 타당하다. 예를 들어, 『자동차관리법』에서는 차량 내부 네트워크, OTA 업데이트, V2X 통신 및 백엔드 연계에 대한 요구사항을, 『해사안전기본법』에서는 선박 내 IT·OT(Operational Technology) 융합 시스템과 위성·육상 통신망을 포함한 해사 사이버보안을, 항공 4법 체계에서는 비행제어시스템·지상관제·데이터링크·항공정보통신망에 대한 보안 요구를 구체화하는 방식이다.

V. 결론

본 논문은 자율주행자동차, 자율운항선박, 드론·도심항공교통을 중심으로 육상·해상·항공 모빌리티의 기술과 사이버위협, 그리고 국내외 법제의 현황을 분석하였으며, 그 결과 모빌리티 관련 특별법들이 기술개발·실증·상용화를 촉진하는 제도적 기반을 제공하지만 사이버보안 규범은 영역별 성숙도와 규율 범위에 큰 편차가 있고 통합적 체계가 미비하다는 점을 확인하였다. 자동차 분야는 『자동차관리법』을 통해 UNECE R155·R156을 수용하여 CSMS·SUMS 체계를 비교적 정교하게 도입한 반면, 자율운항선박은 『해사안전기본법』, 해사 사이버안전 관리지침, IACS UR E26·E27 등에 부분적으로 의존하고, 드론·도심항공교통은 항공 4법과 특별법이 물리적 안전과 산업진흥에 치우쳐 사이버보안 규정이 초기 단계에 머무르고 있다. 이와 함께 『인공지능기본법』이 교통수단·시설·체계에서 활용되는 인공지능을 고영향 인공지능으로 규정하고 투명성·안전성·신뢰성 의무와 영향평가를 부과하고 있음에도, 적대적 머신러닝, 데이터·모델 탈취, 입력 교란 등 인공지능 고유의 사이버위협을 독립된 규율 축으로 충분히 구조화하지 못하고 있다는 한계가 있음을 알게 되었다.

이에 논문은 『모빌리티혁신법』과 『인공지능기본법』을 상위 구조로 삼아 전 생명주기 관점의 공통 사이버보안 원칙과 최소 기준을 모빌리티 전 영역에 반영하고, 『자동차관리법』, 『해사안전기본법』, 항공 4법 등 수단별 기본법에 기술·운영 특성을 반영한 차등적 사이버보안 의무를 내재화하며, 자율 주행·운항·비행을 가능하게 하는 인공지능 사이버보안을 고영향 인공지능 규율과 연계해 통합적으로 설계하는 방향이 필요함을 모색하였다..

〈참고문헌〉

김경욱. 2023. “UAM 항공교통관리 인프라의 사이버보안 고려사항 및 대응방안.” 한국데이터전략학회 30(6): 17–29.

구태언·방석호. 2026. “고영향 AI사업자의 위험관리방안과 사이버보안의무.” 법률신문. https://www.lawtimes.co.kr/news/articleView.html?idxno=214825 (검색일: 2026.6.16.)

관계부처합동. 2025. “AI 선도 프로젝트 추진계획.”

과학기술정보통신부·한국인터넷진흥원. 2022a. “자율주행차 보안모델 PART I: 자율주행차 및 서비스.”

과학기술정보통신부·한국인터넷진흥원. 2022b. “자율주행차 보안모델 PART III: SUMS.”

과학기술정보통신부·한국인터넷진흥원·KR. 2025. “자율운항선박 보안모델.”

국토교통부. 2023. “도심형항공기 인증기준 안내서.”

국토교통부. 2026. “2030 모빌리티 혁신성장 로드맵.”

박제영·박치병·박한선. 2025. “해사 사이버 보안 규제 프레임워크 방향성 연구.” 대한조선학회논문집.

산업통상부. 2025. “AI 완전자율운항선박 기술개발 사업, 예비타당성 조사 면제 확정.” https://www.motir.go.kr/kor/article/ATCL3f49a5a8c/171162/view (검색일: 2026.4.21.)

안성원. 2017. “자율주행을 가능하게 하는 기반 기술들.” https://spri.kr/posts/view/21781?code=column (검색일: 2026.4.20.)

이중현. 2021. “도심 항공 모빌리티(UAM)의 미래.” 기술과 혁신.

정원희. 2020. “항공 사이버보안에 관한 공법적 연구.” 중앙대학교 대학원, 석사 학위논문.

한국선급. 2024. “자율운항선박 지침.”

한국인터넷진흥원. 2020. “드론 사이버보안 가이드.”

Alex Drozhzhin. 2015. “Black Hat USA 2015: The full story of how that Jeep was hacked.” https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/ (검색일: 2026.6.12.)

Amal Yousseef et al. 2025. “Autonomous Vehicle Security: Hybrid Threat Modeling Approach.” IEEE Open Journal of Vehicular Technology 6: 1774-1795.

ENISA. 2021. “Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving.”

EU Artificial Intelligence Act. https://artificialintelligenceact.eu/ (검색일: 2026.6.16.)

IMO. 2018. MSC 100/20/Add.1, Annex 2

Jiwoon Yoo, Yonghyn Jo. 2023. “Formulating Cybersecurity Requirements for Autonomous Ships Using the SQUARE Methodology.” Sensors 23(11).

MACD Maritime Cyber Attack Database. https://maritimecybersecurity.nl/ (검색일: 2026.6.12.)

Nimra Tabish, Tsai Chaur-Luh. 2024. “Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives.” IEEE Access 12: 17114-17136.

UAM Team Korea. 2025. “한국형 도심항공교통 운용개념서 1.5.”

Yingbo Li, et al. 2023. “Physical Artificial Intelligence (PAI) : The Next-Generation Artificial Intelligence.” Frontiers of Information Technology & Electronic Engineering 24(8): 1231-1238.

Mobility Cybersecurity Law
: Focusing on Land, Maritime, and Air Mobility

Young Han Choi | National Security Research Institute, First and Corresponding author
Deokjin Kim | National Security Research Institute

This paper analyzes the technological architectures and cybersecurity threats of land, maritime, and air mobility by focusing on autonomous vehicles, Maritime Autonomous Surface Ships (MASS), drones, and Urban Air Mobility (UAM), and surveys the related domestic and international legal frameworks. It finds that the Mobility Innovation Act and several special acts provide a basis for technology development, pilot projects, and commercialization, but that cybersecurity rules remain fragmented: the Vehicle Management Act has incorporated UNECE Regulations No. 155 and 156 to establish CSMS and SUMS, while the maritime domain relies on the Maritime Safety Framework Act, national maritime cybersecurity guidelines, and IACS UR E26 and E27, and the legal regime for drones and UAM still focuses on physical safety and industrial promotion. The AI Framework Act classifies AI used in transport vehicles, facilities, and systems as "high-impact AI" and imposes duties related to transparency, safety, reliability, and impact assessment, yet AI-specific cybersecurity risks such as adversarial attacks and data or model theft are not fully structured as a distinct regulatory pillar. Consequently, the paper proposes that the Mobility Innovation Act and the AI Framework Act together establish life-cycle-based cybersecurity principles and minimum requirements across all mobility domains. It further suggests that sector-specific base laws incorporate differentiated cybersecurity obligations reflecting the characteristics of cars, ships, drones, and UAM. In addition, it argues that cybersecurity for AI systems enabling autonomous driving, sailing, and flying should be regulated in an integrated manner under the high-impact AI framework, with detailed rules allocated to individual mobility laws and technical standards.

Keyword Mobility, Autonomous Vehicle, Maritime Autonomous Surface Ship(MASS), Drone, Urban Air Mobility(UAM), Cybersecurity