www.eai.or.kr

EAI 워킹페이퍼

유럽의 AI 안보전략: EU·NATO·영국·프랑스·독일의 공식문서 분석과 한국의 선택

조은정(국가안보전략연구원)

EAI
동아시아연구원

EAI

EAI 워킹페이퍼

유럽의 AI 안보전략:
EU·NATO·영국·프랑스·독일의 공식문서 분석과 한국의 선택

조은정
국가안보전략연구원 지정학센터장

Ⅰ. 문제 제기: 유럽의 AI 전략을 어디에서 읽어야 하는가?

유럽을 인공지능 경쟁의 규제자로만 이해하면 두 가지 중요한 변화가 시야에서 사라진다. 하나는 AI를 실제 산업과 공공서비스에 적용하기 위한 자원 동원이며, 다른 하나는 AI를 군사적 판단과 행동에 연결하는 조직적 전환이다. 2025년 유럽연합(European Union, EU)의 「AI 대륙 행동계획」(AI Continent Action Plan)과 NATO의 2024년 「개정 AI 전략」(Revised Artificial Intelligence Strategy)은 서로 다른 권한과 목적을 가진 문서이지만, 기술의 존재와 사용 가능한 능력 사이의 간극을 줄이려 한다는 점에서는 문제의식을 공유한다. 러시아의 우크라이나 전면 침공 이후 방위 대비태세가 유럽 정책의 전면에 오르면서, 이 간극을 줄이는 일은 산업정책을 넘어 안보 과제가 되었다. 따라서 유럽이 더 이상 규제만 하지 않는다는 관찰에서 멈출 것이 아니라, 누가 어떤 권한과 자원을 이용하여 AI를 안보능력으로 전환하는지를 물어야 한다(European Commission 2025a; North Atlantic Treaty Organization 2024, 5-6).[1]

조은정·윤정현(2025)은 EU 「인공지능법」(Artificial Intelligence Act, 이하 AI Act)을 위험에 비례한 규제체계인 동시에 유럽의 규범경쟁과 산업적 이해가 결합된 제도로 분석했다. 이러한 접근은 AI 규제를 기술에 대한 중립적 행정절차로 보지 않고 국제정치적 영향력의 수단으로 파악한다는 장점이 있다. 다만 그 문제의식을 오늘의 안보환경에 적용하려면 법률이 시장에 미치는 효과와 군사조직이 AI를 도입하는 경로를 분리한 뒤 다시 연결할 필요가 있다. 시장을 규율하는 법이 군사적 전력화를 자동으로 이끄는 것은 아니며, 민간의 안전·기본권 보호를 위해 설계한

1 NATO 개정 전략 공개 요약.

통제방식과 군사 임무의 승인·수행을 위한 절차는 목적과 권한이 다르기 때문이다.

AI의 국제정치적 효과를 이해하는 데에는 기술 자체보다 그것을 흡수하고 활용하는 조직에 주목한 연구도 유용하다. 호로위츠(Horowitz 2018)는 AI를 특정 무기와 동일시하기보다 여러 군사능력을 가능하게 하는 범용적 기술로 보면서, 조직의 적응과 활용방식이 상대적 이익을 좌우할 수 있다고 설명했다. 이 관점에서 중요한 것은 유럽이 미국과 동일한 규모의 범용모델을 보유했는지가 아니라, 필요한 데이터와 연산자원에 접근하고 이를 임무체계에 결합하며 지속적으로 통제할 수 있는 지이다. 모델의 기술적 성능은 그 가운데 중요한 요소이지만, 곧바로 국가의 군사적 효과를 의미하지는 않는다.[2]

이 같은 문제의식 아래 본 연구는 다음 질문에 답하고자 한다. 유럽의 AI 정책은 기술적 자율성을 강화하면서도 동맹의 공동작전에 필요한 상호운용성을 어떻게 제고하고 있는가? 그리고 두 목표가 충돌할 때 무엇이 새로운 안보 취약성이 되는가? 이를 위해 EU와 NATO를 상하 관계에 있는 기관처럼 배열하지 않는다. 영국은 EU 밖의 주요 유럽 안보행위자이며, NATO에는 미국과 캐나다가 포함된다. EU의 산업정책, NATO의 공동운용 기준, 각국의 국방정책은 권한의 범위도 참여자도 다르다. 분석의 대상은 통일된 하나의 '유럽 AI 전략'이 아니라, 서로 연결되면서도 경쟁하는 전략들의 관계이다.

본 연구에서 'AI 안보'는 ① 군사 AI의 도입·승인·통제, ② AI가 증폭하는 사이버·기반시설 위험에 대한 대응, ③ 연산·데이터·클라우드와 이를 개발·유지하는 인력으로 이루어진 공급망의 전략적 자율성을 아우르는 개념이다. 세 영역을 함께 다루는 이유는 유럽의 정책문서들이 이들을 별개의 의제로 다루면서도 실제로는 같은 연산기반과 공급자, 인력에 의존하기 때문이다.

시간 범위는 2024년 AI Act 발효 전후부터 2026년 10월 19일까지를 중심으로 하되, 정책의 연속성을 파악하기 위해 영국의 2022년 「국방 AI 전략」(Defence Artificial Intelligence Strategy)과 프랑스의 2019년 국방 AI 전략(L'intelligence artificielle au service de la défense) 등 선행 문서도 검토한다. 자료는 법령, 전략문서, 국방부 지침과 공식 사업 발표를 우선한다. 특히 법적 의무, 정치적 목표, 기관·시설의 설치, 구매계약 체결, 검증된 작전효과를 동일한 증거로 취급하지 않는다. 공개자료로 확인할 수 있는 것은 정책의 방향과 일부 제도화 과정이며, 실제 군사적 성과와 비공개 체계의 신뢰성까지 확인한 것으로 확대 해석하지 않는다. 이 구분은 본문 전체에 적용되므로 이하에서는 문단마다 되풀이하지 않고, 필요한 경우에만 각주에서 근거의 성격을 밝힌다.

2 "AI Is an Enabler, Not a Weapon" 절 및 "Organizational Politics and Artificial Intelligence" 절.

ⓒ EAI 2025

본 연구의 주장은 세 가지이다. 첫째, 유럽의 AI 안보정책은 규제에서 군사화로 옮겨 가는 과정이 아니라 기술주권과 동맹 상호운용성을 함께 추구하는 과정이며, EU·NATO·국가의 역할은 '분업'보다 '중첩'에 가깝다. 둘째, EU의 대표적 AI·사이버 '법제'가 군사 목적을 적용범위에서 제외한 자리에서는 '재원'의 적격 요건, '동맹 네트워크'의 참여 요건, 국가별 조달·보증 '절차'가 사실상의 규범으로 작동한다. 셋째, 그 결과 생기는 의존은 공급자의 '국적'보다 계약과 아키텍처가 배분하는 접근·결합·통제의 '권한'에 따라 관리 가능 여부가 갈린다. 이하 Ⅱ장은 분석틀을 제시하고, Ⅲ-Ⅴ장은 EU, NATO, 영국·프랑스·독일을 차례로 검토한다. Ⅵ장은 안보적 함의를, Ⅶ장은 한국의 정책과제를 다루며, Ⅷ장은 결론과 함께 이 틀이 놓치기 쉬운 인적 공급망의 문제를 제기한다.

Ⅱ. 유럽 AI 전략의 개관: 접근·결합·통제의 다층 구조

1. EU·NATO·국가의 역할: 분업보다 중첩

EU는 AI를 적용할 시장과 산업기반을 형성하면서 규제와 지원정책을 함께 운용한다. NATO는 회원국의 디지털 능력이 공동작전에서 작동하도록 공통의 기술·운용 조건을 정한다. 개별 국가는 군사 데이터와 기밀, 조달예산, 병력 운용 및 사용 승인에 관한 권한을 보유한 상태에서 기술을 전력으로 전환한다. 이러한 구분은 각 행위자의 상대적 강조점을 파악하는 데 유용하지만, 고정된 기능 분담은 아니다. EU의 「AI 적용 전략」(Apply AI Strategy)에는 방위·안보·우주 분야가 포함되고 2025년 「유럽 방위 대비태세 2030 공동백서」(Joint White Paper for European Defence Readiness 2030)는 AI를 우선 역량분야로 지정했다. NATO는 산업과 민간 혁신기업의 참여를 넓히고 있고, 각국은 독자적인 윤리·법적 관리체계를 마련한다(European Commission 2025b; European Commission and High Representative 2025a; North Atlantic Treaty Organization 2026e; Ministry of Defence 2024).[3]

3 AI 적용 전략의 부문별 조치; NATO 산업협력 전략; JSP 936의 거버넌스 지침.

ⓒ EAI 2025

〈표 1〉 주요 행위자의 AI 안보전략 비교[4]

행위자	정책의 중심 과제	대표 문서•제도	안보 분석의 핵심 질문
EU	규칙·연산기반·산업적용·방위산업 재원·민간 회복력	AI Act(2024)·AI 디지털 옴니버스(2026); AI 대륙 행동계획·AI 적용 전략(2025); 방위백서·SAFE·대비태세 로드맵(2025); 기술주권 패키지·사이버안보 및 AI 행동계획(2026)	역내 역량 확대가 공급망과 시장접근 조건을 어떻게 바꾸는가
NATO	공동운용·데이터·시험검증·신속 도입	개정 AI 전략(2024); 데이터 전략·신속도입 행동계획(2025); 동맹 디지털 전략·DTIS 2.0·산업협력 전략(2026)	누가 어떤 조건으로 공동 디지털 체계에 참여하는가
영국	통합 전투체계와 책임 있는 도입	국방 AI 전략(2022); JSP 936(2024); SDR(2025); 국방투자계획·TF RAID(2026)	속도 향상과 사용 책임을 어떻게 함께 확보하는가
프랑스	민감 데이터·연산기반·조직적 주도권	국방 AI 전략(2019); 국방부 AI 전략·AMIAD 설립(2024); ASGARD 가동(2025); LPM 개정(2026)	어떤 자원을 직접 통제해야 자율적 운용이 가능한가
독일	군 전체의 도입·승인·위험관리·다국적 호환	국방 AI 개념서 K-9000/102 (2026년 4월 효력, 8월 공개본)	규범과 조달절차를 어떻게 전력화 과정에 내장하는가

[4] European Commission (2025b); North Atlantic Treaty Organization (2026a); Ministry of Defence (2025); République française (2024); Bundesministerium der Verteidigung (2026). 갱신 항목은 European Parliament and Council of the European Union (2026); European Commission and High Representative (2025a, 2025b); European Commission (2026c); North Atlantic Treaty Organization (2025a, 2025b, 2026c, 2026e); Ministry of Defence (2026a, 2026b); Ministère des Armées (2019); République française (2026) 참조. 각 행위자의 공식문서에 근거해 필자 정리. 개별 전략과 사업의 출처는 본문의 해당 절 및 참고문헌 참조. 국가별 특징은 상대적 강조점이다. 표의 약어와 문서명 원문은 본문에서 처음 언급할 때 병기했다.

ⓒ EAI 2025

따라서 EU가 규범을 제공하고 NATO가 이를 군사적으로 실행한다는 직선적 설명은 적절하지 않다. 협력의 접점이 형성되어도 양 기관의 목표가 항상 일치하는 것은 아니다. 유럽산 기술을 우대하는 산업정책은 빠르게 사용할 수 있는 동맹국 상용기술을 도입하려는 수요와 충돌할 수 있다. 국가별 기밀보호와 데이터 통제는 공통 상황인식에 필요한 정보공유를 제약할 수 있다. 반대로 기술적 호환성을 높이는 공통 플랫폼은 단기적인 작전 효율을 개선하면서 장기적으로 특정 공급자에 대한 변경 비용을 키울 수 있다. 이처럼 협력의 확대와 의존의 심화는 함께 발생할 수 있다는 것이 본 연구의 분석적 출발점이다.

2. AI 안보능력을 판단하는 세 가지 기준

첫째는 접근이다. 필요한 연산자원과 데이터, 모델, 통신서비스를 평시뿐 아니라 위기에서도 사용할 수 있어야 한다. 둘째는 결합이다. 접근 가능한 자원을 센서, 지휘체계, 군수지원과 다른 국가의 체계에 연결할 수 있어야 한다. 셋째는 통제이다. 무엇을 학습시키고 어떤 상황에서 사용하며 언제 수정·중단할지 결정할 수 있어야 한다. 외국 모델을 사용해도 통제조건을 확보한 경우와 국내에서 개발했지만 핵심 부품이나 원격 서비스 없이는 유지할 수 없는 경우를 구분하려면 이러한 기준이 필요하다. 여기서 주권은 모든 구성요소의 국산화를 뜻하기보다, 중요한 임무에 관한 선택권을 잃지 않는 상태로 정의한다. 본 연구는 이를 '선택권으로서의 주권'이라 부르기로 한다.

접근·결합·통제는 서로 대체되지 않는다. 고성능 모델이 있어도 기밀 데이터에 접근하지 못하면 임무 수행에 한계가 있고, 데이터를 확보해도 타국 체계와 연결되지 않으면 공동작전에서 활용범위가 줄어든다. 반대로 결합이 매우 잘되어 있어도 갱신과 운용 승인에 대한 권한을 공급자에게 지나치게 의존하면 독자적 판단이 제약될 수 있다. 패럴과 뉴먼(Farrell and Newman 2019)의 상호의존의 무기화(weaponized interdependence) 논의는 효율적인 네트워크의 중심에 위치한 행위자가 비대칭적 영향력을 가질 수 있음을 보여준다. 본 연구는 이를 AI 동맹에 그대로 대입하여 이미 강압이 발생했다고 주장하는 대신, 연결구조의 효율성과 통제권의 분배를 함께 살펴보는 분석적 단서로 활용한다.

이 기준은 국산과 외산의 구분이 놓치는 차이를 드러낸다. 예를 들어 독자 모델을 확보했더라도 그 모델을 수정할 인력과 재평가할 데이터가 없다면 통제능력은 제한된다. 반면 외부에서 개발한 모델을 활용하더라도 임무에 필요한 검증과 변경, 대체가 가능하다면 일정한

ⓒ EAI 2025

자율성을 유지할 수 있다.

Ⅲ. EU: 규제·산업역량·회복력을 함께 구축하는 전략

1. AI Act의 적용과 군사적 예외의 구분

AI Act는 EU의 AI 정책을 조직하는 중요한 법적 기반이지만, 이를 유럽 군사 AI의 직접적인 통제법으로 이해해서는 안 된다. 제2조 제3항은 군사·방위·국가안보 목적에만 사용되는 AI 시스템을 적용 대상에서 제외한다. 따라서 NATO나 회원국의 무기체계가 AI Act의 고위험 분류와 적합성 평가를 그대로 적용 받는다는 설명은 잘못이다. 동시에 국방기관이 사용한다는 이유만으로 모든 AI가 제외되는 것도 아니다. 민간 목적이나 혼합된 목적의 사용에 대해서는 사용 용도와 관련 조항을 별도로 판단해야 한다. 조직의 이름이 아니라 시스템의 목적과 사용 맥락이 법적 적용을 가르는 핵심이다(European Parliament and Council of the European Union 2024a, 제2조 제3항 및 전문 제24항).[5]

시행 시점도 단계별로 구별해야 한다. 금지된 AI 관행과 AI 리터러시 관련 규정은 2025년 2월, 범용 AI(general-purpose AI) 및 거버넌스 규정은 같은 해 8월부터 적용되었으며, 투명성 등을 포함한 일반 적용 시점은 2026년 8월이다. 그러나 2026년 7월 27일 발효한 「AI 디지털 옴니버스」 규정(Digital Omnibus on AI, Regulation (EU) 2026/1744)에 따라 부속서 Ⅲ의 고위험 AI 의무는 2027년 12월 2일로, 부속서 Ⅰ의 규제 대상 제품에 내장되는 고위험 AI 의무는 2028년 8월 2일로 연기되었다. 2025년 11월의 개정안은 적용 시점을 조화표준(harmonised standards) 등 이행 지원수단의 준비와 연동하려 했으나, 최종 규정은 확정 일자를 택했다. 연기의 배경에는 표준화 지연이라는 기술적 요인과 함께, 2025년 11월 독일과 프랑스가 공동 개최한 「유럽 디지털주권 정상회의」(Summit on European Digital Sovereignty)에서 양국이 고위험 AI 규정 준수의 12개월 유예를 공동으로 요청한 데서 보듯 산업경쟁력이라는 정치적 요인도 작용했다. 그렇더라도 이를 규제 포기로 읽기보다는 법적 원칙을 실행 가능한 검사기준과 감독능력으로 전환하는 과정의 조정으로 보는 편이 타당하다(European Commission n.d.b; European Parliament and Council

5 조문은 EU AI Act Service Desk의 공식 법문과 대조.

ⓒ EAI 2025

of the European Union 2026; Bundesregierung 2025; Présidence de la République 2025b).[6]

이러한 조정에서 한국이 주목해야 할 점은 유럽의 영향력이 법률의 선언에만 머무르지 않는다는 것이다. 제품과 서비스가 어떤 요건을 충족했는지 판단하는 시험방법, 문서화 방식, 책임주체의 지정은 규칙의 실제 효과를 결정한다. 안보 측면에서 중요한 질문은 법적 적용 예외의 존재 자체보다, 예외 영역에서 어떤 대체적 책임·검증체계가 마련되는가이다. 영국과 독일의 군사 AI 지침은 바로 이 문제를 국가적 차원에서 다룬다(European Commission n.d.b; Ministry of Defence 2024; Bundesministerium der Verteidigung 2026).[7]

2. AI 대륙 행동계획·AI 적용 전략: 지원정책과 수요정책의 결합

2025년 4월의 「AI 대륙 행동계획」은 유럽이 AI 경쟁에서 규칙을 제시하는 데 그치지 않고 필요한 생산기반을 확보해야 한다는 방향을 분명히 한다. 연산 인프라, 데이터, 인재, 산업적 활용 및 규제 이행 지원을 함께 추진하는 구조이다. 특히 AI 팩토리(AI Factories)와 AI 기가팩토리(AI Gigafactories)는 모델 개발자에게 연산자원을 제공하는 동시에 연구기관·기업·사용 부문을 연결하려는 장치로 이해할 수 있다. 다만 최대 7곳의 기가팩토리를 선정하는 유럽 고성능컴퓨팅 공동사업(EuroHPC Joint Undertaking)의 공모는 2026년 7월 30일 개시되어 11월 12일 마감되므로, 기준일 현재 선정된 시설은 없다(European Commission 2025a).[8]

같은 해 10월 발표된 AI 적용 전략은 공급기반에 더해 사용 수요를 조직한다. 산업과 공공부문이 AI를 어디에 어떻게 적용할지 지원하고, 전략 부문에서 실증과 도입을 촉진하며, 유럽의 경쟁력과 기술주권을 연결한다. 방위·안보·우주가 적용 대상에 포함된다는 점은 EU를 순수한 민간 규제자와 동일시하기 어렵게 만든다. 여기서 공공부문과 주요 산업의 구매는 단순한 소비가 아니라

6 "When will the AI Act be fully applicable?"; "Governance, enforcement, and implementation." 변경 가능한 집행 안내이므로 조회일을 명시했다. 고위험 의무의 적용 연기는 모든 AI Act 규정의 적용 연기를 의미하지 않는다. 옴니버스는 이 밖에 기존 시스템에 대한 합성 콘텐츠 표시의무(제50조 제2항)의 경과기간과 AI 리터러시 의무(제4조)의 완화도 담고 있으나 본 연구의 범위 밖이다.

7 JSP 936, 제99–114항, 제202–209항; 독일 개념서, 제3·4장.

8 기가팩토리 공모 현황은 EuroHPC Joint Undertaking (2026).

ⓒ EAI 2025

기술의 개선 방향을 정하고 공급자의 성장기회를 형성하는 수단이 된다. '유럽산 구매'(buy European) 방향의 실제 효과는 개별 사업의 자격과 조달조건에 따라 달라진다(European Commission 2025b).[9]

이 두 전략을 함께 보면 EU의 관심은 규범적 신뢰성과 산업적 역량을 대립시키기보다 상호 보강하는 데 있다. 신뢰성 요구가 일정 수준의 검증비용을 만들더라도, 예측 가능한 규칙과 공동 시험환경은 사용기관의 불확실성을 낮출 수 있다. 공공 수요가 안정적으로 형성되면 기업은 보안성과 유지관리 능력에 투자할 유인을 갖는다. 반대로 도입 지원이 특정 기업이나 기술구조에 고착되면 시장의 다양성과 교체 가능성을 약화시킬 수도 있다. 그러므로 EU 정책의 안보적 평가는 투자 규모뿐 아니라 공급자의 다양성, 기술의 이전 가능성, 위기 시 서비스 지속성까지 포함해야 한다. 이 점에서 한국의 대 유럽 협력도 연산자원의 공동 활용, 산업별 실증, 규제준수 지원을 하나의 시장진출 경로로 연결할 필요가 있다. 단지 유럽의 규정을 충족하는 완제품을 판매하는 것과 유럽의 연구·검증·운영 과정에 참여하는 것은 서로 다른 수준의 협력이다. 후자는 접근 기회를 넓힐 수 있지만 데이터와 지식재산의 배분 조건을 더 정교하게 협의해야 한다.

2026년 6월 3일 집행위원회가 제안한 「기술주권 패키지」(Tech Sovereignty Package)는 이 흐름을 연산·클라우드에 대한 통제의 문제로 끌어올렸다. 패키지의 중심인 「클라우드·AI 개발법」(Cloud and AI Development Act, CADA)안은 데이터센터 확충과 함께 EU 차원의 단일한 '클라우드·AI 주권 평가체계'와 공공부문 도입 메커니즘을 제시한다. 아직 입법 제안 단계이지만, 공공 수요를 주권성 평가와 연결하려 한다는 점에서 본 연구의 접근·통제 기준과 직접 맞닿아 있다. 앞서 2025년 11월 베를린에서 열린 유럽 디지털주권 정상회의도 주권적 유럽 AI 모델 개발을 위한 공동 이니셔티브('European Frontier AI')와 공공조달에서의 유럽 우선을 제기했다(European Commission 2026c; European Parliament 2026; Bundesregierung 2025; Présidence de la République 2025b).[10]

---

9 AI 적용 전략 원문 및 집행위원회의 "Apply AI" 정책 설명. 문서의 채택일은 2025년 10월 8일이다. 전략적 방향과 개별 조달사업의 법적 참여조건을 구별한다.

10 CADA는 COM(2026) 502로 제안되었으며, 기준일 현재 유럽의회 소관 위원회(ITRE(Committee on Industry, Research and Energy)·IMCO(Committee on the Internal Market and Consumer Protection) 공동)의 보고서 초안은 나오지 않았다. 이니셔티브의 명칭은 정상회의 결과문서를 따랐다. 메르츠 총리는 기자회견에서 'Next-Frontier-AI-Initiative'라고 표현했다.

ⓒ EAI 2025

3. AI 안전에서 사이버·물리적 회복력으로

2026년 7월의 「사이버안보 및 AI 행동계획」(EU Action Plan on Cybersecurity and Artificial Intelligence)은 고도화된 AI가 방어능력과 공격능력을 함께 변화시킨다는 문제를 전면에 제시했다. 집행위원회는 AI를 통한 취약점 탐지와 공격 자동화의 확대를 경계하면서, 기존 AI·사이버 법제와 회원국·산업계의 능력을 연계하여 안전하고 책임 있는 활용을 지원하려 한다. 구체적으로는 EU 시장 출시 전 AI 모델 평가역량의 강화, EU 사이버보안청(European Union Agency for Cybersecurity, ENISA)과 함께 마련할 사이버보안용 첨단 AI 접근에 관한 유럽 청사진, 핵심부문을 위한 보안 시험 플랫폼, AI를 활용한 취약점의 신속한 탐지·대응을 제시한다. 군사 지휘체계가 아니라 민간 회복력을 겨냥한다는 점에서 NATO의 AI 전략과는 성격이 다르다(European Commission 2026b).[11]

이러한 방향은 제품 보안과도 연결된다. 「사이버복원력법」(Cyber Resilience Act, CRA)에 따라 적극적으로 악용되는 취약점과 중대한 보안사고에 대한 보고의무가 2026년 9월 11일부터 적용되었다. 주요 의무는 2027년 12월 11일부터 전면 적용된다. 이는 소프트웨어와 연결기능을 갖춘 제품의 보안을 판매 이후의 임의적 서비스가 아니라 제조자의 지속적인 책임으로 다루는 변화이다. 한국에서는 AI 모델을 개발하는 기업뿐 아니라 산업용 장비와 관련 소프트웨어를 공급하는 기업의 대응도 중요해진다. 의료기기·자동차·민간항공·선박장비처럼 별도 부문법이 규율하는 제품은 적용에서 제외되며(제2조 제2-4항), 국가안보·국방 목적으로만 개발·개조된 제품도 제외된다(제2조 제7항). AI Act와 마찬가지로 CRA도 군사 영역을 명시적으로 비켜 간다(European Commission n.d.a; European Parliament and Council of the European Union 2024b, 제2조 제2-4항·제7항, 제71조).

2026년 10월 9일 집행위원회가 소집한 AI Act상 독립 전문가 과학패널(Scientific Panel of Independent Experts)의 특별회의는 규범에서 평가와 감독으로 이어지는 움직임을 보여준다. 비르쿠넨(Henna Virkkunen) 집행부위원장은 개회사에서 올해에만 20건이 넘는 '통제 상실(loss-of-control)' 사고가 기록되었다고 밝혔다. 10월 12일 공개된 결과 요약에 따르면 패널은 ① 개발·시험 단계에 있는 내부 모델의 위험 관리, ② 사고의 탐지·평가·조사 역량 강화, ③ 정보공유와 공통 요건, 공동 위기대응을 위한 국제 이니셔티브, ④ 감시 가능성을 떨어뜨리는 학습기법과 구조에 대한 심사 강화를 권고했다. AI사무국(AI Office)은 이미 제공자들에게 보안 관행에 관한 정보제공을

11 비입법 행동계획이다.

ⓒ EAI 2025

요청했으며, 패널과 함께 마련한 질의를 담아 사고에 관한 추가 요청을 보낼 예정이다. 이 사례의 중요성은 유럽이 원칙을 선언하는 데서 더 나아가 모델의 위험을 평가하고 사업자에게 설명을 요구하는 역량을 제도화하려 한다는 데 있다. 군사 AI에 대한 직접 규제는 아니지만, 관련 평가기법과 전문인력이 민군 양쪽에서 중요해질 수 있다는 점은 주목할 만하다(European Commission 2026a, 2026d; Virkkunen 2026).[12]

4. 방위산업 정책: AI를 역량 우선순위와 공동재원에 편입

EU의 AI 안보정책을 시장규칙과 민간 회복력으로만 보면 2025년 이후 가장 큰 변화를 놓친다. 2025년 3월의 「유럽 방위 대비태세 2030 공동백서」는 일곱 개 우선 역량분야의 하나로 'AI·양자·사이버·전자전'을 지정했고, 같은 해 5월 채택된 「유럽안보행동」(Security Action for Europe, SAFE) 규정(Council Regulation (EU) 2025/1106)은 1,500억 유로 규모의 공동조달 대출 대상에 AI와 전자전 역량을 포함했다. 10월의 「방위 대비태세 로드맵 2030」(Preserving Peace – Defence Readiness Roadmap 2030)은 유럽 드론방어 이니셔티브(European Drone Defence Initiative), 동부측면 감시(Eastern Flank Watch), 유럽 방공방패(European Air Shield), 유럽 우주방패(European Space Shield)를 선도사업으로 제시하면서, 방위기술 경쟁에서 AI가 결정적 요인이 될 것이라고 보고 AI 학습·검증용 데이터셋에 대한 접근을 간소화하겠다고 밝혔다(European Commission and High Representative 2025a, 2025b; Council of the European Union 2025b).[13]

이로써 EU 안에는 민간 AI는 법으로 규율하고 군사 AI는 재원으로 지원하는 이원 구조가 형성되고 있다. AI Act와 CRA가 군사 목적을 적용범위에서 제외하는 동안, 방위산업 정책은 바로 그 영역에 공동재원을 투입한다. 그리고 재원에는 조건이 붙는다. SAFE는 AI·전자전을 방공·미사일방어, 중대형 드론, C4ISTAR(Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, and Reconnaissance) 체계 등과 함께 '두 번째 범주'의 방위제품으로 분류한다. 이 범주의 공동조달에서 계약자는 제3국이나 제3국 주체의 제한 없이 제품 설계의 정의·조정·발전을 결정할 수 있어야 하고, 제3국 제한을 받는 부품을 교체하거나 제거할 법적

12 개회사는 OpenAI, Anthropic, Google DeepMind, Meta와 독립 평가기관을 사고 관련 주체로 언급했다. 결과 요약은 기업이나 모델을 특정하지 않는다.

13 로드맵의 AI 관련 서술은 JOIN(2025) 27 final 참조.

ⓒ EAI 2025

권한을 가져야 한다(제16조 제11항). EU·EEA-EFTA(European Economic Area-European Free Trade Association)·우크라이나 밖에서 생산된 부품의 비용은 최종 제품 부품 비용 추정치의 35%를 넘을 수 없다(제16조 제10항). 본 연구의 용어로 말하면 EU는 군사 AI의 통제 기준을 법률이 아니라 대출의 적격 요건에 써넣은 것이다. 2026년 10월 12일 이사회가 최종 승인한 1억 1,500만 유로 규모의 「민첩·신속 방위혁신 프로그램」(Programme for Agile and Rapid Defence Innovation, AGILE)도 같은 재원 경로에 속한다(Council of the European Union 2025b, 제1조 제2문, 제16조 제10·11항; 2026b; European Council 2026).[14]

한국에는 SAFE가 EU와 안보·국방 파트너십(Security and Defence Partnership)을 맺은 제3국에 별도 협정을 통한 참여 경로를 열어 두었다는 점이 중요하다(제17조). 이 협정은 부품 원산지 규칙과 제3국 제한에 관한 조건을 정해야 하므로, 참여는 시장 접근이면서 위의 통제 기준을 받아들이는 문제이기도 하다. 제3국으로는 캐나다가 처음으로 참여협정을 맺었다(2025년 12월 회원국 승인, 2026년 2월 이사회 서명 승인). 영국은 2025년 11월 분담금 문제로 협상이 결렬된 뒤 기준일 현재 합의에 이르지 못했다. 한국은 2024년 11월 EU와 안보·국방 파트너십을 출범시켰지만, 기준일 현재 SAFE 참여협정 협상에 착수했다는 공식 발표는 없다. 협정이 없는 한 한국산 부품은 역외 부품으로 계산되어 35% 상한의 적용을 받는다(Council of the European Union 2025a; 2025b, 제17조; 2026a, 2026c).[15] 세 기준으로 정리하면, EU는 연산기반과 공동조달로 접근과 결합의 조건을 넓히는 한편, 군사 영역의 통제 기준은 법률이 아니라 재원의 적격 요건에 맡기고 있다.

14 '법률이 아니라 대출의 적격 요건'이라는 평가는 필자의 해석이다. 2026년 10월 16일 유럽이사회 결론은 드론·대드론, 동부측면 감시, 유럽방위산업프로그램(European Defence Industry Programme, EDIP)과 AGILE을 다루었지만 AI를 따로 언급하지 않았다. AI가 독립된 정치 의제보다 역량 사업의 구성요소로 다루어지고 있음을 보여준다(필자 해석).

15 영국 협상 결렬은 언론 보도에 따른 것이다. 2025년 12월 집행위원회 대변인은 일본의 참여 요청을 '한국, 튀르키예와 마찬가지로' 검토하겠다고 언급한 것으로 보도되었으나, 한국의 요청을 확인하는 공식 문서는 찾지 못했다.

ⓒ EAI 2025

Ⅳ. NATO: AI를 연결하고 사용할 수 있는 동맹으로

1. 개정 AI 전략의 핵심: 원칙의 폐기가 아니라 실행조건의 구체화

NATO가 2024년 7월 공개한 개정 AI 전략 요약은 신속한 도입과 책임 있는 사용을 동시에 강조한다. 2021년 제시한 합법성, 책임성과 설명책임, 설명가능성과 추적가능성, 신뢰성, 통제가능성, 편향 완화라는 여섯 가지 '책임 있는 사용 원칙'(Principles of Responsible Use: Lawfulness, Responsibility and Accountability, Explainability and Traceability, Reliability, Governability, Bias Mitigation)을 유지하면서, 생성형 AI를 포함한 기술 변화에 대응하고 동맹 전반의 활용을 확대하려는 것이다. 특히 시험·평가·검증·타당성 확인(Testing, Evaluation, Verification and Validation, TEV&V), 양질의 데이터, 상호운용성 및 관련 생태계의 구축을 주요 과제로 명시한다. 따라서 변화는 윤리적 제한에서 해방된 군사적 활용이라기보다, 원칙을 충족하는 AI를 어떻게 더 신속하게 도입할 것인가에 가깝다(North Atlantic Treaty Organization 2024, 제1-2항, 제5-6항, 제8항, 제10-13항).[16]

이 전략을 동맹의 관점에서 읽으면 검증은 국내 인증을 넘어 협력의 신뢰를 형성하는 작업이다. 한 국가가 개발한 AI의 오류 특성이나 사용 한계를 다른 국가가 이해하지 못한다면, 공동 상황인식이나 의사결정 지원에 그 결과를 활용하기 어렵다. 다만 같은 원칙을 승인했다는 사실만으로 모델 간 신뢰가 자동 형성되는 것은 아니다. 데이터의 품질, 평가 환경, 허용된 사용 목적, 갱신 이후의 재검증이 구체적으로 확인되어야 한다. 공통의 윤리 언어는 협력의 출발점이고, 서로 검토할 수 있는 증거는 실제 사용의 조건이라는 구분이 필요하다.

이후 NATO는 실행조건을 데이터와 획득 속도의 두 방향에서 구체화했다. 2025년 2월 북대서양이사회가 승인한 「동맹 데이터 전략」(Data Strategy for the Alliance, DaSA)은 다섯 가지 목표와 일곱 가지 데이터 원칙을 제시하고, 동맹 데이터 공유 생태계(Alliance Data Sharing Ecosystem)를 통한 AI·머신러닝 모델의 공유를 언급한다. 같은 해 6월 헤이그 정상회의가 승인한 「신속도입 행동계획」(Rapid Adoption Action Plan)은 신기술 제품의 획득과 통합 착수를 원칙적으로 24개월 안에, 해결책 식별 후의 시험·통합을 12개월 안에 마치도록 하는 기준을 제시했다. 「헤이그 정상회의 선언」(The Hague Summit Declaration)은 2035년까지 GDP의 5%를

16 공개 요약.

ⓒ EAI 2025

국방 및 안보 관련 지출에 투입하기로 하면서, 그중 최대 1.5%를 기반시설 보호, 네트워크 방어, 혁신, 방위산업 기반 강화 등에 쓸 수 있도록 했다(North Atlantic Treaty Organization 2025a, 2025b, 2025c).[17]

2. 디지털 전략: 모델보다 데이터와 네트워크의 연결조건 강조

2026년 1월의 「동맹 디지털 전략」(Alliance Digital Strategy)은 AI를 별도 사업이 아니라 데이터·클라우드·네트워크와 결합된 공동운용의 일부로 다룬다. 전략 제8항은 NATO 기구에는 전략 목표의 이행을 요구하는 한편, 회원국과 연합임무네트워킹(Federated Mission Networking, FMN) 참가국에는 정렬을 '권고하고 강력히 독려'하되 전략적 정치·군사 협의와 NATO 주도 작전을 위해 구성된 연합(federated) 네트워크에 참여하는 경우에는 정렬을 의무로 규정한다. 이는 AI 시대의 표준이 단지 권장 기술사양에 머무르지 않고 특정 공동운용 환경에 참여하는 조건이 될 수 있음을 보여준다(North Atlantic Treaty Organization 2026a, 제8항).[18]

같은 전략은 통신이 교란되거나 제한되는 상황에서도 데이터를 처리할 수 있도록 클라우드와 전술 엣지(tactical edge)의 연산능력을 함께 다룬다. 중앙에 모든 것을 모으는 방식이 아니라, 보안등급과 임무환경이 다른 체계들을 연합하고 필요한 기능을 현장에 배치하는 접근이다. 여기서 AI의 효과는 모델의 평균 정확도만으로 결정되지 않는다. 필요한 정보가 제때 도착하는지, 연결이 끊겼을 때 어떤 기능이 유지되는지, 지연된 정보와 최신 정보가 구분되는지에 따라 달라진다. 전략 제11항이 전술 엣지에 추론형 AI를 배치해 전투원의 상황인식과 실시간 결심을 지원하도록 한 것도 같은 맥락이다. 전술 엣지 연산의 핵심은 경량 모델 자체가 아니라 연결 실패를 전제한 설계에 있다(North Atlantic Treaty Organization 2026a, 제10-11항).[19]

---

17 신속도입 행동계획 제16항, 제23항; 헤이그 정상회의 선언 제2-3항. 신속도입 행동계획 자체는 AI를 명시하지 않는다.

18 해당 문맥의 의무는 연합 네트워크 참여에 관한 것이며 동맹 조약상의 권리·의무와 동일하지 않다.

19 federated platforms, hybrid cloud, tactical edge, data as a strategic asset.

ⓒ EAI 2025

2026년 5월 공개된 「디지털 전환 이행전략 2.0」(Digital Transformation Implementation Strategy 2.0, DTIS 2.0)은 2023년 승인된 첫 이행전략을 개정한 문서로, 이러한 구상을 사람·절차·기술과 자원 배분의 문제로 구체화한다. 디지털 기반망을 국가와 보안경계를 넘어 센서, 의사결정자, 행동 주체를 연결하는 기반으로 설명하고, 2030년까지의 5개년 전망을 해마다 갱신하며 2035년까지 연장하는 이동 계획기간(rolling-horizon) 방식을 채택한다. 이 문서가 AI를 직접 언급하지 않는다는 점도 눈여겨볼 만하다. 이행의 단위가 개별 AI 사업이 아니라 디지털 기반망 전체로 설정되어 있기 때문이다. 실제 도입률과 임무효과는 이와 별도로 평가해야 한다(North Atlantic Treaty Organization 2026c, 제4-6항, 제13-17항, 제19-25항).[20]

2026년 7월 「앙카라 정상회의 선언」(The Ankara Summit Declaration)은 이 방향을 정상 차원에서 확인했다. 여섯 개 항에 불과한 선언은 '상호운용 가능한 대서양 전투 클라우드(transatlantic warfighting cloud)'를 개발하고 '강력한 AI 모델(powerful AI models)'을 도입하고 있다고 명시했다. NATO의 AI 논의가 원칙과 전략문서의 단계를 지나 전력화 일정의 단계로 들어섰음을 보여주는 대목이다(North Atlantic Treaty Organization 2026b, 제3항).

3. 상용 AI의 도입: 기술 주권 vs. 상호 운용성

기술의 '전략적 구상'과 '실제 획득' 사이의 간극을 보여주는 사례는 NATO 통신정보청(NATO Communications and Information Agency, NCIA)이 2025년 4월 발표한 Maven Smart System NATO의 구매이다. 공식 발표에 따르면 NCIA는 같은 해 3월 25일 연합작전사령부(Allied Command Operations, ACO)를 위한 Palantir 체계의 획득을 완료했으며, 요구 제기에서 획득까지 6개월이 걸렸다. 이 사례에서 확인할 수 있는 것은 NATO가 민간기업의 AI 기반 체계를 공동 군사능력에 도입하기로 결정했다는 사실이다. 이 구매는 국방 AI의 발전이 군 내부의 독자적 개발만으로 이루어지지 않음을 보여주는 구체적 제도화 사례이다(NATO Communications and Information Agency 2025).

이 사례의 쟁점은 유럽의 기술주권과 미국 기업 기술의 활용이 모순되는가가 아니다. 검증된 상용체계를 도입하면 개발 시간을 줄이고 기존 운용자와 연결하기 쉬울 수 있다. 문제는 그 대가로 어느 수준의 '의존성'을 수용하는가이다. 데이터 구조와 업무절차가 특정 제품을 중심으로 정착되면

20 이동 계획기간 방식(제20항)과 공동재원·다국적·국가 사업의 구분(제14항).

ⓒ EAI 2025

나중에 공급자를 바꾸는 비용이 증가할 수 있다. 반대로 개방된 인터페이스와 데이터 이전권, 독립적인 검증권한을 확보한다면 같은 외국 기술도 보다 통제 가능한 의존으로 관리할 수 있다. 결국 안보적 평가는 공급자의 국적만이 아니라 계약과 아키텍처가 배분하는 권한을 함께 보아야 한다. 이러한 의존성은 최초 구매의 순간보다 운용 경험이 축적되는 과정에서 커질 수 있다. 특정 제품에 맞춰 인력을 교육하고 데이터를 정리하며 다른 체계를 연결할수록 공급자의 교체는 소프트웨어 구매를 넘어 조직의 재학습을 요구하기 때문이다. 따라서 조달정책과 조직학습을 함께 보아야 실제 전환 비용을 평가할 수 있다.

2026년 7월 앙카라 정상회의에서 승인된 「산업-NATO 협력 전략」(Strategy for Industry-NATO Cooperation)은 직접적인 재원이나 법적 효력이 없는 자발적 문서이지만, 이러한 변화를 조달과 산업 생태계의 문제로 확대한다. 산업과의 조기 협력, 실험·시범·훈련, 표준과 기술의 검증을 연계하려는 방향은 구매자가 완성품을 받아 사용하는 전통적인 조달관계보다 더 긴밀한 상호작용을 요구한다. AI가 자주 수정되고 운영환경에 적응해야 한다면, 구매 이후의 갱신과 평가가 전력의 일부가 되기 때문이다. 다만 도입 속도를 높이는 것과 공급자에 대한 견제 능력을 유지하는 것은 별개 과제이다. 빠른 계약은 성과일 수 있으나, 접근권과 변경권을 제대로 확보하지 못한 빠른 계약은 장기적 자율성의 비용을 남길 수 있다(North Atlantic Treaty Organization 2026e, 2026f).[21]

세 기준으로 보면 NATO는 결합의 조건을 가장 구체적으로 정하고 있지만, 접근은 상당 부분 상용 공급자에, 통제는 회원국의 승인권에 맡겨 두고 있다. 공동운용의 확대가 통제의 집중으로 이어질지는 이 분산 구조가 유지되는지에 달려 있다.

21 산업과의 협력, 실험·시범·훈련 및 표준 검증에 관한 항목. 재정·법적 효력이 없다는 점은 부속서 1의 원칙 2. 정상회의 승인 사실은 정상회의 선언이 아니라 NATO 발표문에서 확인된다. 전략 본문에서 AI는 부속서 2에서 한 차례 언급된다.

ⓒ EAI 2025

V. 주요국의 전력화 경로: 영국·프랑스·독일

1. 영국: 통합작전의 속도와 책임 있는 사용을 함께 제도화

영국의 2022년 국방 AI 전략은 AI 준비태세를 갖춘 조직, 신속하고 광범위한 도입, 산업·연구 생태계와의 협력, 국제적 안전과 가치의 수호라는 네 가지 목표를 제시했다. 이 전략은 무기체계에 AI를 부착하는 일만을 다루지 않는다. 의사결정 지원과 군수·행정의 효율화, 인력과 교육, 조직문화의 전환을 함께 다룬다는 점에서 부처 전체의 변화에 가깝다. 따라서 영국의 접근을 군사적 치명성의 추구로만 요약하면, 실제 도입의 기반인 데이터와 인력, 조직적 책임을 놓치게 된다(Ministry of Defence 2022).[22]

2025년 「전략방위검토」(Strategic Defence Review, SDR)가 제시한 디지털 표적화 웹(Digital Targeting Web, DTW)은 이를 작전 수준으로 연결한다. 센서, 판단 주체, 효과수단을 공통 데이터 환경에서 연결하여 필요한 정보를 적절한 행동과 결합하려는 구상이다. 여기서 '효과수단'은 단순히 하나의 무기를 뜻하지 않으며, 네트워크의 목적도 모든 판단을 AI에 일임하는 데 있지 않다. 보고서는 2027년 구축을 목표로 제시했다. 중요한 변화는 개별 플랫폼의 우수성보다 플랫폼 사이의 정보와 판단의 연결을 전투력의 핵심으로 위치시킨다는 점이다(Ministry of Defence 2025).[23]

2026년 6월 30일 발표된 「국방투자계획」(Defence Investment Plan, DIP)은 이 구상을 예산과 일정에 연결했다. DIP는 DTW의 기반이 될 국방 전체의 비밀 클라우드(Defence-wide Secret Cloud)의 최소기능제품(minimum viable product, MVP)을 2026년 중 내놓고, 2030-35년 디지털 기간망(Digital Backbone)과 표적화 웹에 최소 170억 파운드를 투입하겠다고 밝혔다. 같은 달 출범한 신속 AI 전력화 태스크포스(Taskforce RAID: Rapid AI Delivery)에는 4년간 1억 파운드를 배정했다. TF RAID는 9월 영국-우크라이나 AI 협력의 첫 사업으로 AI 군집 경연(Avengers)을 공고했다. DIP는 흩어진 사업을 묶을 새로운 「국방 AI 전략적 접근」(Defence Strategic Approach to AI)도 예고했으나 기준일 현재 공개되지 않았다. 영국 국방 AI 정책의 무게중심이 2022년 전략과 2024년 지침(Joint Service Publication, JSP 936, 후술)의 원칙

22 "Our vision"; "Strategic objectives"; "AI-ready organisation."

23 제4.1절, Box 5 "The Digital Targeting Web" 및 권고 5.

ⓒ EAI 2025

정립에서 예산·사업 단위의 전력화로 옮겨 가고 있는 것이다(Ministry of Defence 2026a, 2026b, 2026c).[24]

이 구상이 실효성을 가지려면 연결의 확대만큼 오류와 책임의 전파도 관리되어야 한다. 예컨대 하나의 잘못된 분류가 여러 부대의 공통 상황도에 반영되더라도, 정보가 공유되었다고 해서 정확해지지는 않는다. 오히려 동일한 판단에 대한 집단적 의존이 확대될 수 있다. 따라서 네트워크의 성과는 전달속도뿐 아니라 원자료의 출처를 확인할 수 있는지, 서로 다른 해석을 유지할 수 있는지, 불확실성을 사용자가 이해할 수 있는지에 의해 평가되어야 한다.

영국의 2024년 지침 「국방 분야의 신뢰할 수 있는 인공지능」(Dependable AI in Defence, JSP 936)은 이러한 문제를 구체적인 관리절차로 다룬다. AI의 전체 생애주기에 관한 책임과 보증 활동을 규정하고, 고위 책임자와 개발·사용 주체의 역할을 연결한다. 특히 외부에서 개발한 AI도 책임자가 영국의 '야심차고 안전하며 책임 있는'(Ambitious, Safe, Responsible: ASR) 정책 충족 여부를 확인해야 한다는 원칙(제113항)과, 계약에서 데이터·모델·알고리즘에 대한 접근 및 지식재산권을 고려하도록 하는 지침(제203항)이 중요하다. 외국 수출통제가 데이터를 포함해 AI의 유지·운용에 가하는 제약도 평가하도록 한다(제204항). 빠른 도입을 추구하면서도 운용상의 자율성을 계약 단계에서 확보하려는 것이다(Ministry of Defence 2024, 18-19, 제99-114항(특히 제113항); 31, 제202-209항(특히 제203-204항)).[25]

영국의 사례가 한국에 주는 시사점은 전투속도와 규범의 양립 가능성이다. 검증되지 않은 AI를 신속하게 배치하면 사용자가 결과를 신뢰하지 못해 오히려 절차가 지연될 수 있다. 반대로 사용 한계와 책임이 명확하면 각 단계에서 반복되는 승인 비용을 줄일 여지가 있다. 그러나 검증절차가 곧 속도 향상을 보장하는 것은 아니며, 지나치게 경직된 심사 역시 기술 갱신을 막을 수 있다. 필요한 것은 모든 AI에 동일한 절차를 적용하는 방식이 아니라 임무의 위험과 변경의 정도에 비례한 보증체계이다. 예컨대 동일한 분석 보조도구라도 단순한 행정업무에 쓰일 때와 시간에 민감한 군사적 판단에 쓰일 때 요구되는 근거는 달라질 수 있다. 기술명보다 의도된 사용과 실패의 결과를 기준으로 심사 강도를 조절해야, 반복적인 승인 부담과 과소 검증의 위험을 동시에 줄일 수 있다.

---

24 DIP 제25-26항, 제31항, 제39항. 요약부의 2억 파운드는 TF RAID와 Project FRONTIER를 합한 금액이다.

25 인쇄면 기준.

ⓒ EAI 2025

2. 프랑스: 주권적 연산기반과 전담기관을 통한 전력화

프랑스는 2019년 첫 국방 AI 전략을 발표한 데 이어 2024년 3월 8일 「국방부 AI 전략」(Stratégie ministérielle sur l'intelligence artificielle)을 새로 공개했다. 이 전략의 중심에는 민감한 데이터와 핵심 기술에 대한 독자적 관리능력이 놓여 있다. 정부는 연구와 생산 역량을 결집하는 전담기관의 신설과 기밀 정보를 처리할 연산기반을 제시했다. 여기서 주권은 단순한 자국산 브랜드의 보유가 아니라, 외부 서비스 이용조건에 전적으로 종속되지 않고 국방 목적의 개발과 사용을 결정할 수 있는 능력이다(Gouvernement français 2024).[26]

이 전략은 2024년 4월 23일자 법령(Décret n° 2024-376)으로 국방인공지능청(Agence ministérielle pour l'intelligence artificielle de défense, AMIAD)을 설치하면서 조직적 기반을 갖추었다. AMIAD는 2024년 5월 1일 출범했다. 전담기관은 군의 수요를 개발과 연결하고, 분산된 전문성을 결집하며, 반복되는 문제를 공통 기반으로 해결할 수 있다. 동시에 모든 업무가 소수 전문인력과 중앙조직에 집중되면 현장의 요구 변화에 뒤처질 위험도 있다. 따라서 이 모델의 성패는 중앙집중의 정도보다 공통 기반과 임무별 재량을 어떻게 배분하는가에 달려 있다(République française 2024, 제1-2조).[27]

프랑스 국방부는 2025년 9월 4일 몽발레리앵 요새에서 AMIAD가 운영하는 기밀 AI 슈퍼컴퓨터 ASGARD를 가동했다. 이 사실은 주권적 AI가 모델 개발의 언어를 넘어 연산시설과 정보보호의 문제로 구체화되고 있음을 보여준다. 전략적 의미는 기밀 데이터를 외부의 일반 상용환경으로 이전하지 않고 개발·시험할 기반을 확보하려는 데 있다. 이러한 기반은 민간에서 범용기술이 개발되더라도, 군사적 활용 단계에서 별도의 환경과 통제체계가 필요할 수 있음을 시사한다(Ministère des Armées 2025a, 2025b).[28]

---

26 정부 설명자료의 최초 게시일은 2024년 3월 11일이며, 페이지는 2025년 6월 4일 수정되었다. 2019년 전략은 Ministère des Armées (2019).

27 시행 안내 포함. 법령은 2024년 5월 1일 시행을 명시한다.

28 국방부의 2025년 9월 5일 발표는 9월 4일의 출범 행사를 소개한다. ASGARD라는 명칭과 AMIAD의 운영 주체 지위는 2025b에서 확인된다. 영국 육군의 Project ASGARD(DTW의 일부)와는 별개 사업이다.

ⓒ EAI 2025

주권적 기반은 2026년 「군사계획법」(Loi de programmation militaire, LPM) 개정으로 한층 확대되었다. 8월 16일 공포된 개정법(Loi n° 2026-791)은 2024-2030년 국방예산을 360억 유로 늘려 총 4,360억 유로로 조정했다. AMIAD와 미래전투사령부(Commandement du combat futur, CCF)가 공동 주도하는 로봇화 부대 사업(Pendragon)은 2026년 첫 작전 시연과 2027년 초기 배치를 목표로 한다. 기밀 연산시설에서 출발한 주권적 기반이 무인체계의 전력화로 이어지고 있는 셈이다(République française 2026; Sénat 2026; Ministère des Armées 2026).[29]

기밀 연산환경은 접근과 통제의 측면에서 이점이 있지만, 상호 운용성의 측면에서는 추가 비용을 만들 수 있다. 외부 모델과 데이터의 도입이 제한되고, 새로운 소프트웨어를 검증하는 데 시간이 필요하며, 동맹과 공유할 결과를 별도로 가공해야 할 수 있기 때문이다. 따라서 프랑스의 주권적 접근과 NATO의 연합체계는 어느 한쪽이 다른 쪽을 대체하는 관계가 아니다. 중요한 과제는 기밀을 보호하면서도 필요한 검증 결과와 정보가 동맹 내부에서 교환될 수 있도록 경계를 설계하는 것이다. 자율성의 확보는 협력의 거부가 아니라 협력할 조건을 자국이 결정할 수 있는 능력으로 평가해야 한다. 무엇을 보호하고 무엇을 설명할지를 구분하지 못하면 주권적 기반은 고립된 체계로 굳어질 수 있다(정책적 함의는 Ⅶ.3 참조).

3. 독일: 산업정책의 주변이 아니라 군 전체의 승인·운용체계

독일을 AI 산업과 연구에는 적극적이지만 군사 AI 전략에는 소극적인 국가로 고정하는 설명은 2026년 공식문서를 반영하지 못한다. 독일 국방부(Bundesministerium der Verteidigung, BMVg)의 AI 개념서(KI-Konzeption, 문서번호 K-9000/102)는 개발·도입·사용을 전략적으로 관리하기 위한 문서이며, 표지에 효력 개시일(Datum Gültigkeitsbeginn)을 2026년 4월 9일로 기재하고 있다. 국방부는 같은 해 8월 12일 공개본(Öffentliche Fassung)을 발표하면서 AI를 국가·동맹 방위(Landes- und Bündnisverteidigung)와 다영역작전(Multi-Domain Operations)을 위한 요소로 명시했다. 따라서 독일의 차이는 군사 AI의 부재가 아니라, 이를 어떤 절차와 책임 구조를 통해 군 전체에 도입하려 하는 가에서 찾아야 한다(Bundesministerium der Verteidigung 2026; Manthey 2026).[30]

---

29 증액 규모는 상원의 법률 해설, Pendragon의 일정과 주관 기관은 국방부 육군 발표(2026년 4월 17일) 기준.

30 개념서 표지의 효력 개시일; 국방부 2026년 8월 12일 설명자료. 개념서의 유효 시작일과 공개 설명자료의 발표일을 구별한다.

ⓒ EAI 2025

독일 개념서는 '책임 있는 AI 사용' 행동영역(Verantwortungsvolle Nutzung von Künstlicher Intelligenz, 제3.3절) 아래 위험관리, 투명성·추적성·문서화, 훈련·검증·확인·시험, 적합성 검사와 사용·운용 승인, 인간의 통제, 신뢰성·강건성·보안·데이터 보호를 하나의 절차로 연결한다. 이러한 요구는 기술 연구의 부수적인 윤리절차가 아니라 개발에서 구매와 사용에 이르는 과정의 일부이다. 국방부 설명자료는 이러한 요건이 성능 명세서, 계약, 인수 절차에도 적용된다고 밝힌다. 따라서 독일의 군사 AI 정책은 규범과 작전 사이에서 선택하는 모델보다, 책임 있는 사용의 요건을 전력화 과정에 편입하는 모델로 해석할 수 있다(Bundesministerium der Verteidigung 2026, 제3장 제3.3절(제3.3.1-3.3.6절), 23-33).[31]

거버넌스에서도 중앙 조정과 분산 실행을 결합한다. 개념서는 'CAIO 협의체'(Chief Artificial Intelligence Officer Council)와 통합과업팀(Integrierte Aufgabenteams, IAT)을 통해 전략적 방향과 조정을 수행하되 기존 업무별 책임과 절차를 대체하지 않는다고 명시한다. 이는 새로운 위원회를 만든 사실보다 중요한 부분이다. AI 관련 의사결정이 모두 한곳에 집중되는 것도 아니고, 각 부대와 기관이 독립적으로 위험을 감수하도록 방치되는 것도 아니다. 기존 지휘·관리 책임을 유지하면서 AI와 데이터의 문제를 조율하려는 구조이다. 다만 이러한 설계가 실제 부처 간·군종 간 조정에서 얼마나 효과적인지는 향후 집행자료와 사례를 통해 평가해야 한다(Bundesministerium der Verteidigung 2026, 제4.1절, 34-36).[32]

독일의 사례는 EU AI Act와 군사 AI의 관계도 선명하게 한다. 개념서 부속서(제5.1절)는 AI Act '영역 예외'(Bereichsausnahme)의 범위에 관한 국방부의 2025년 1월 30일자 입장을 별도로 수록하고 있다. 군사적 예외가 존재한다고 해서 아무런 규범이 적용되지 않는 것은 아니다. 오히려 목적별로 EU법의 적용 여부를 판단하고, 예외 영역에서는 국제법과 국가적 통제, NATO와의 협력 기준을 적용하는 별도의 작업이 필요하다. 이러한 구조는 유럽 전체에서 규제와 군사화가 단순히 반대 방향으로 움직인다는 설명에 대한 반례이다. 군사적 활용이 확대되는 바로 그 과정에서 승인과 기록, 책임을 더욱 구체화할 수 있기 때문이다(Bundesministerium der Verteidigung 2026, 부속서 제5.1절(제5.1.1절 '2025년 1월 30일 국방부 입장' 포함), 38-44).[33]

---

31 인쇄면 기준. 계약·인수 적용은 Manthey (2026)와 대조.

32 인쇄면 기준.

33 인쇄면 기준.

ⓒ EAI 2025

4. 국가별 비교 분석: 차이는 목표보다 전환 경로

세 나라 모두 효율적인 작전, 신뢰할 수 있는 기술, 동맹과의 협력을 추구한다. 따라서 '영국은 속도, 프랑스는 주권, 독일은 윤리'라는 배타적 분류는 각국 문서의 복합성을 훼손한다. 더 적절한 비교는 전력화 과정에서 어느 부분을 먼저 조직하는가이다. 영국은 통합 전투체계와 이를 뒷받침하는 보증 절차를, 프랑스는 전담기관과 민감 데이터·연산기반을, 독일은 군 전체의 개발·조달·승인·사용을 연결하는 체계를 상대적으로 전면에 둔다. 이는 국가의 본질을 설명하는 고정 유형이 아니라, 검토한 공식문서에서 확인되는 정책적 강조점이다.

규범외교에서는 세 나라의 위치가 오히려 엇갈린다. 2025년 2월 프랑스가 발표한 'AI 기반 무기체계에 대한 인간 통제 유지에 관한 파리 선언'(Paris Declaration on Maintaining Human Control in AI enabled Weapon Systems)에는 독일을 포함한 27개국이 참여했지만 영국은 참여하지 않았다. 반면 2026년 2월 스페인 아코루냐에서 열린 제3차 「인공지능의 책임 있는 군사적 이용에 관한 고위급회의」(Responsible AI in the Military Domain, REAIM)의 결과문서('Pathways to Action')는 영국·프랑스·독일과 한국이 모두 지지했고 미국과 중국은 지지하지 않았다. 또한 2025년 유엔총회에서 핵무기 지휘·통제·통신체계에 AI를 통합하는 위험을 다룬 결의안(Possible risks of integration of artificial intelligence in command, control and communication systems of nuclear weapons)에는 영국·프랑스·미국이 함께 반대했다. 독일은 반대국에 포함되지 않았다. 영국과 프랑스는 미국이 반대한 군사 AI·자율무기체계 결의안에는 반대하지 않았다. 군사 AI의 일반 원칙에서는 미국과 거리를 두면서도, 핵억제와 직결되는 영역에서는 핵보유국으로서 미국과 보조를 맞추는 이중적 모습이다(Présidence de la République 2025a; Ministerio de Asuntos Exteriores, Unión Europea y Cooperación 2026; United Nations 2025).[34]

이러한 차이는 한국에 단일한 유럽 모델을 모방하기보다 문제별로 협력 상대와 수단을 선택해야 함을 시사한다. 통합체계의 시험과 운영상 보증은 영국, 기밀 환경에서의 개발·운영 통제는 프랑스, 조달과 승인절차의 연계는 독일의 경험이 유용한 비교대상이 될 수 있다. 그러나 외국 제도의 명칭을 수입하는 것만으로 동일한 효과를 얻을 수는 없다. 각국의 제도는 기존 조직과 산업기반에 연결되어 있으므로, 한국의 권한 배분과 조달·보안 환경에서 어떤 문제를 해결할

34 총회 본회의 표결 기준 핵 지휘통제 결의안(A/C.1/80/L.56)은 118-9-44였다. REAIM 2026 결과문서 지지국은 회의 종료 시 35개국, 기준일 현재 스페인 외교부 명단 기준 45개국이다.

ⓒ EAI 2025

것인지부터 설정해야 한다.

〈표 2〉 접근·결합·통제 기준에 따른 행위자별 비교[35]

행위자	접근	결합	통제	주된 긴장
EU	AI 팩토리·기가팩토리, CADA안(역내 연산·클라우드)	AI 적용 전략의 부문별 실증, SAFE 공동조달	AI Act·CRA(민간, 군사 목적은 적용 제외), SAFE 설계 권한(제16조 제11항)	역내 우대 ↔ 동맹 상용기술 수요
NATO	공동재원 사업, 상용 체계 획득 (Maven Smart System NATO)	연합 네트워크 정렬 의무(FMN), 데이터 전략	책임 있는 사용 원칙·TEV&V, 각국 승인권 유지	공통 플랫폼 효율 ↔ 공급자 의존
영국	국방투자계획, TF RAID	디지털 표적화 웹(센서–판단–효과수단)	JSP 936 생애주기 보증, 계약상 데이터·지식재산권 접근	전력화 속도 ↔ 보증 부담
프랑스	기밀 AI 슈퍼컴퓨터 (ASGARD), LPM 증액	동맹과 공유할 결과의 경계 설계	AMIAD 중심의 개발·운용 통제	주권적 폐쇄성 ↔ 연합 결합 비용
독일	개념서의 AI 인프라 항목(제3.2.3절)	동맹 방위·다영역 작전 연계	위험관리–승인–인간 통제의 조달 내장, CAIO 협의체	절차적 엄격성 ↔ 도입 속도

[35] 필자 정리. 본문에서 검토한 공식문서의 내용을 세 기준에 따라 재분류한 분석적 요약이다.

ⓒ EAI 2025

Ⅵ. 안보적 함의: 더 빠른 AI보다 통제 가능한 연결

1. 상호운용성은 효율성과 영향력의 배분 문제

AI를 결합한 공동운용은 여러 국가가 동일한 모델을 구매하는 문제와 다르다. 서로 다른 모델을 사용하더라도 결과의 의미와 불확실성을 이해하고, 필요한 데이터를 교환하며, 갱신 이후의 변화를 확인할 수 있다면 협력이 가능하다. 반대로 같은 공급자의 제품을 사용해도 정보 접근권과 운영규칙이 다르면 실질적 상호운용성은 제한될 수 있다. 이 점에서 NATO의 디지털 전략이 제시하는 연합 네트워크의 공통 요건은 기술사양인 동시에 참여자들 사이의 권한과 책임을 정하는 장치로 읽을 수 있다(North Atlantic Treaty Organization 2026a, 제8항, 제10-11항).[36]

공통 기준은 협력을 가능하게 하지만, 그 기준을 누가 수정하고 예외를 누가 승인하는지도 중요하다. 네트워크에 연결되었다는 사실과 그 네트워크의 방향을 결정할 수 있다는 사실은 같지 않다. 향후 AI 동맹의 내부 격차는 기술의 보유 여부뿐 아니라 데이터에 대한 접근, 검증기준의 형성, 오류 발생 시의 이의 제기와 수정 권한에서 나타날 가능성이 있다. 이는 앞으로 동맹 내 위계와 자율성을 평가할 때 확인해야 할 변수이다.

이 변수는 미국의 정책 변화로 더 현실적인 문제가 되었다. 미국은 2025년 유엔총회에서 '군사 영역의 인공지능과 국제평화·안보에 대한 함의'(Artificial intelligence in the military domain and its implications for international peace and security) 결의안과 '치명적 자율무기체계'(Lethal autonomous weapons systems) 결의안에 모두 반대했고, 2026년 REAIM 결과문서도 지지하지 않았다. 반면 NATO가 도입한 대표적 상용 AI 체계는 미국 기업의 제품이며, 앙카라 정상회의가 내세운 대서양 전투 클라우드도 미국과의 기술적 결합을 전제한다. 유럽은 기술적으로는 미국 중심 플랫폼과의 결합을 심화하면서 규범적으로는 미국과 다른 경로를 걷고 있다. 본 연구는 이를 '기술적 결합과 규범적 분기'라 부른다. 동맹 표준을 "누가 정하고 예외를 누가 승인하는가?"라는 질문은 이 괴리 속에서 가설이 아니라 현재의 쟁점이 된다(United Nations 2025; Ministerio de Asuntos Exteriores, Unión Europea y Cooperación 2026; NATO Communications and Information Agency 2025; North Atlantic Treaty Organization 2026b).[37]

---

36 분석적 해석.

37 총회 본회의 표결 기준 군사 AI 결의안(A/C.1/80/L.46)은 167-5-5, 자율무기체계 결의안(A/C.1/80/L.41)은

ⓒ EAI 2025

2. 기술주권은 민간기업과의 관계를 재설계하는 문제

국방 AI의 기반을 민간기업이 제공할수록 국가안보의 통제대상도 넓어진다. 모델의 기능뿐 아니라 학습 데이터의 처리방식, 공급망 변경, 원격 지원, 갱신 주기, 서비스 중단과 계약 종료 이후의 권리가 중요해진다. 영국 JSP 936이 데이터·알고리즘·모델의 접근과 외국 수출통제를 계약의 문제로 다루는 것은 이러한 변화의 구체적인 사례이다. 따라서 기술주권을 국내 기업의 매출이나 모델 이름으로 측정하기보다, 중요한 임무에서 유지·수정·교체·중단을 결정할 수 있는 권한의 묶음으로 파악할 필요가 있다. 공급자가 누구인가 뿐 아니라 그 공급자를 위해 코드를 쓰고 갱신하는 사람이 누구인가도 이 권한의 일부이다(Ministry of Defence 2024, 31, 제203-204항; Ⅷ장 참조).[38]

그렇다고 모든 외국 기술의 사용을 취약성으로 간주하면 선택지가 지나치게 좁아진다. 공동의 공급망과 시장은 비용을 분담하고 기술 수준을 높일 수 있으며, 중복된 개발을 줄일 수도 있다. 문제는 의존을 제거하는 것이 아니라 관리 가능한 형태로 만드는 것이다. 완전한 국산화를 주장하면서 실제 운영은 소수 외부 서비스에 묶여 있다면 명목상의 주권과 실질적인 선택권은 달라진다.

3. 전술적 속도 향상과 위기안정성은 별개의 성과

AI가 센서 정보를 더 빠르게 정리하고 의사결정 선택지를 제시하면, 지휘관은 정보 과부하를 줄이고 대응시간을 확보할 수 있다. 그러나 그 시간상의 이익이 항상 안정성으로 이어지는 것은 아니다. 더 빠른 체계를 전제로 상대도 대응을 서두르면 검토 가능한 시간이 줄어들 수 있고, 여러 체계가 동일한 오인에 반응하면 상황이 급격히 악화될 수 있다. 윤정현(2026)은 전략적 비핵무기체계의 AI 전환이 야기하는 결심시간 압축과 자동화의 얽힘에 주목하며, 최소한의 판단 여지, 교차확인과 안전장치를 제안한다. 이 문제의식은 유럽의 AI 기반 통합작전체계를 평가하는 데에도 유용하다.[39]

164-6-7로 채택되었다.

38 인쇄면 기준.

39 본 연구의 유럽 적용은 필자의 해석이다.

ⓒ EAI 2025

따라서 '인간이 최종 승인한다'는 문장만으로 통제가 보장되지는 않는다. 사용자가 결과의 불확실성을 이해하지 못하거나 대안을 검토할 시간이 없다면 승인은 형식적인 절차가 될 수 있다. 그렇다고 모든 자동화에 동일한 숙고 시간을 요구하는 것도 적절하지 않다. 즉각적인 방어반응과 정치적으로 중대한 무력사용 결정은 서로 다른 시간구조를 갖는다. 필요한 것은 임무와 위험 수준에 따라 인간에게 남겨야 할 판단 기능, 자동화의 허용 범위, 이견이 발생했을 때의 중단과 상급 검토 절차를 구분하는 것이다. AI의 속도를 늦추는 것이 목표가 아니라, 속도 향상이 어떤 결정권도 무의미하게 만들지 않도록 하는 것이 목표이다.

4. AI 회복력은 디지털 기술과 물리적 기반시설 모두에 핵심

AI의 안보적 가치를 높이는 연결은 동시에 의존경로를 늘린다. 연산시설과 통신망, 전력, 위치·시각 정보가 불안정해지면 모델 자체가 정상이어도 임무는 실패할 수 있다. ENISA가 2026년 6월 10–11일 실시한 「Cyber Europe 2026」 훈련은 철도·해상교통의 동시 장애가 무역과 군사기동, 위기 대응에 미치는 영향을 모의했다. 민간 교통망의 장애를 안보 기능의 중단과 연결해 연습했다는 점이 핵심이다. AI 작전체계의 회복력도 이러한 물리적 의존을 포함해서 평가해야 한다(European Union Agency for Cybersecurity 2026).[40]

2026년 2월 공개된 EU 「해저케이블 보안 툴박스」(Submarine Cable Security Toolbox) 역시 데이터와 전력 케이블의 취약성, 의존관계, 복구 능력을 함께 다룬다. 케이블 정책이 AI를 위해 만들어진 것은 아니지만, AI 활용이 확대될수록 기존의 기반시설과 상호 운용성은 새로운 임무와 결합한다. 중요한 것은 유럽이 기술·기반시설·군사 기능의 연쇄를 함께 관리하기 시작했다는 점이다. 한국에서도 AI 방어체계의 성능을 측정할 때 정상적 통신환경뿐 아니라 서비스 제한과 복구 상황을 포함할 필요가 있다(European Commission 2026e).[41]

40 훈련일 2026년 6월 10–11일; "A glimpse of the scenario" 및 군사기동 관련 설명.

41 2026년 2월 5일 공개, 3월 16일 수정본.

ⓒ EAI 2025

5. 규범의 영향력은 평가와 조달을 통하여 작동

EU, NATO, 영국과 독일의 사례를 종합하면 규범은 군사적 활용의 반대편에만 있는 것이 아니다. 어떤 위험을 허용하고 어떤 증거를 요구하며 누가 승인할지를 정하면, 그 기준은 개발 방향과 구매 가능성을 함께 바꾼다. 이는 윤리원칙이 기술적 검증으로 완전히 환원된다는 뜻은 아니다. 민간인의 보호나 무력사용의 정당성처럼 검사 성적으로 대체할 수 없는 판단이 남는다. 그러나 그러한 규범적 판단을 실제 설계와 사용 절차에 연결하지 못하면, 원칙은 도입을 정당화하는 언어로만 남을 위험이 있다(North Atlantic Treaty Organization 2024; Ministry of Defence 2024; Bundesministerium der Verteidigung 2026).[42]

향후 유럽 전략의 성과를 판단하려면 최소한 세 가지를 확인해야 한다. 도입이 늘어날수록 오류와 갱신을 추적할 능력도 함께 늘어나는가? 공동운용이 확대될수록 참여국이 결과와 한계를 이해하는 능력도 높아지는가? 연산·데이터 기반에 대한 투자가 위기 시 서비스 지속성과 교체 가능성으로 이어지는가? 이 질문에 대한 답이 없다면 전략 발표와 기관 설치를 성공의 대리 지표로 사용하는 데 그치게 된다. 유럽을 새로운 AI 군사강국으로 선언하기보다, 이러한 전환 조건이 충족되고 있는지를 추적하는 것이 더 생산적인 연구 과제이다.

Ⅶ. 한국의 선택: 독자적 판단과 선택적 연결을 함께 확보하기

한국의 유럽 AI 협력은 새로운 제도를 처음부터 만드는 문제만은 아니다. NATO의 공식 안내에 따르면 한국은 2023년 7월 합의한 개별 맞춤형 파트너십 프로그램(Individually Tailored Partnership Programme, ITPP)을 바탕으로 사이버 방위, 신기술, 상호운용성 등에서 협력하고 있으며, 2025년 3월에는 스위스·우크라이나와 함께 NATO 과학기술기구(Science and Technology Organization, STO)의 '과학기술 강화 파트너십'(S&T Enhanced Partnership)에 참여했다. EU와는 디지털 파트너십 이사회(Digital Partnership Council)를 운영하고(2025년 11월 제3차 회의) 2025년 호라이즌 유럽(Horizon Europe) 제2축(Pillar Ⅱ)에 준회원국으로 가입했으며, 2026년 6월 제11차 한-EU 정상회의에서는 AI 협력약정(Cooperation Arrangement on AI) 체결과 정보보호협정(Security of Information Agreement, SIA) 협상 개시 추진에 합의했다. 다만 협력

42 NATO 책임 있는 사용 원칙; JSP 936의 보증체계; 독일 개념서 제3·4장에 대한 비교 해석.

ⓒ EAI 2025

채널의 존재가 특정 기금이나 조달사업의 자동 참여, 기밀 정보 접근, 인증의 포괄적 상호인정을 의미하지는 않는다. 필요한 것은 기존 채널 안에서 어떤 기능을 제공하고 어떤 권한을 확보할지 구체화하는 일이다(North Atlantic Treaty Organization 2025d, 2026d; European Commission 2025c; Council of the European Union 2026a).[43]

한국은 이 분야의 규범 형성에서도 이미 행위자이다. 2024년 9월 서울에서 제2차 REAIM 고위급회의를 공동 주최해 '행동을 위한 청사진'(Blueprint for Action)을 이끌어냈고, 네덜란드와 함께 2024년(결의 79/239)과 2025년 유엔총회의 군사 AI 결의를 주도했다. 다만 2025년 프랑스 주도의 파리 선언에는 참여하지 않았다. 국내적으로는 2026년 1월 시행된 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 제4조 제2항이 국방 또는 국가안보 목적으로만 개발·이용되는 인공지능으로서 대통령령으로 정하는 것을 적용에서 제외한다. EU AI Act 제2조 제3항과 같은 구조이다. 따라서 Ⅲ장에서 EU에 던진 질문, 즉 예외 영역에서 어떤 대체적 책임·검증체계를 마련할 것인가는 한국에도 그대로 적용된다. 2026년 2월 여야 의원 33명이 공동발의를 발표한 「국방인공지능법」 제정안은 기준일 현재 국회 국방위원회에 계류 중이다. 국제적으로는 2026년 9월 특정재래식무기금지협약(Convention on Certain Conventional Weapons, CCW) 정부전문가그룹이 자율무기체계에 관한 문서의 '요소'를 합의한 보고서를 채택했으나 협상 권한은 부여하지 않았고, 향후 작업 방식은 11월 16–20일 제7차 평가회의(Seventh Review Conference)의 합의에 맡겨졌다. 이것이 이하 정책과제의 국내외 맥락이다(대한민국 2025, 제4조 제2항; United Nations General Assembly 2024; United Nations 2025; Présidence de la République 2025a; Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems 2026, 제25-45항).[44]

---

43 NATO "Key areas of cooperation"; 호주(2015)와 일본(2020)은 이 파트너십의 기존 참여국이다; 제3차 한-EU 디지털 파트너십 이사회 공동성명(2025년 11월 28일); 제11차 한-EU 정상회의 공동성명(2026년 6월 10일).

44 「국방인공지능법」 제정안은 유용원·부승찬 의원 공동대표발의(2026년 2월 발표)이며, 계류 상황은 언론 보도 기준이다.

ⓒ EAI 2025

1. 임무별 자율성 지도와 생애주기 조달권리

영국 JSP 936과 프랑스의 기밀 연산기반은 서로 다른 방식으로 같은 질문에 답한다. 어떤 기능을 독자적으로 통제해야 하는가? 한국에 필요한 첫 작업은 AI 기술 목록이 아니라 임무별 자율성 지도이다. 각 임무에 필요한 데이터, 연산자원, 통신과 업데이트가 어디에 의존하는지 점검하고, 위기 시 이를 사용할 수 없을 때의 영향을 평가해야 한다. 모든 구성요소의 국산화보다 반드시 독자적으로 유지해야 할 기능과 공동 활용이 유리한 기능을 나누는 편이 실행 가능하다. 예컨대 민감한 판단과 승인에 필요한 데이터는 독자적으로 관리하되, 일반적 분석 도구나 비 기밀 시험환경은 국제협력을 활용할 수 있다. 이러한 구분은 실제 업무와 보안 검토를 거쳐 확정해야 한다.

이 지도는 구체적인 조달계약으로 이어져야 한다. AI 조달계약에는 구매가격과 최초 성능 외에 데이터의 반출·이전 가능성, 모델 변경 통지, 평가자료에 대한 접근, 지원 종료 이후의 유지방안, 공급자 교체 시 필요한 정보가 포함되어야 한다. 핵심은 모든 기술의 소유권이 아니라 임무 지속에 필요한 운영상의 선택권이다. JSP 936의 계약 지침(제203-204항), 독일 개념서가 성능 명세서·계약·인수 절차에 책임 있는 사용 요건을 적용한 방식, SAFE의 설계 권한 조항은 좋은 비교기준이다. 다만 한국의 관련 법제와 보안요건에 맞게 조정해야 한다. 초기에는 소수 사업을 대상으로 계약과 운영상의 취약성을 점검하고, 그 결과를 표준계약의 개선으로 연결하는 방식이 적절하다.

2. 모델 성적표를 넘어 검증 근거와 공동 시험환경

NATO가 책임 있는 사용 원칙을 유지하면서 TEV&V를 전략의 중심 과제로 올린 것은 원칙의 공유만으로는 상호 신뢰가 생기지 않음을 보여준다. 한국은 AI를 수출하거나 연합체계에 연결할 때 함께 제출할 검증 근거를 정형화해야 한다. 의도된 사용 범위, 시험환경, 알려진 한계, 오류 처리, 변경 이력과 책임주체를 설명하는 자료 묶음은 한국 기업과 사용기관이 공동으로 준비할 수 있는 정책도구이다. 이는 REAIM과 유엔총회 결의로 쌓아 온 한국의 규범외교를 원칙의 선언에서 서로 검토할 수 있는 증거의 교환으로 발전시키는 수단도 된다.

기밀 데이터를 직접 이전하지 않는 공동 시험도 설계할 수 있다. 비 기밀·합성 데이터와 공통 시나리오를 사용하여 오류 발견, 재 검증, 갱신 후 변화 탐지의 절차를 비교하는 방식이다. 협력의 성과는 행사 개최나 양해각서 수가 아니라, 같은 문제를 서로 다르게 판단했을 때 원인을

ⓒ EAI 2025

설명하고 평가절차를 개선할 수 있는 지로 측정해야 한다. 이 방식은 한국이 모든 분야에서 최고 성능의 모델을 확보해야만 협력할 수 있다는 전제를 완화하고, 단순한 보조 공급자를 넘어 사용의 근거를 함께 형성하는 역할을 열어 준다.

3. 상호운용 가능한 설계와 등급별 데이터 협력

NATO 디지털 전략 제8항이 보여주듯 연합 네트워크의 기술 요건은 참여의 조건이 될 수 있다. 한국의 AI 체계는 필요한 외부 체계와 연결되면서도 특정 제품에 과도하게 묶이지 않도록 설계되어야 한다. 인터페이스 문서화, 데이터 형식의 명확화, 구성요소의 교체 가능성을 사업 초기부터 검토할 필요가 있다. 목표는 FMN을 비롯한 NATO의 디지털 요건을 일괄 수용하는 것이 아니라 실제 협력이 예정된 임무에서 필요한 요건을 식별하는 것이다. 호환성을 이유로 불필요한 기능과 비용을 추가하는 것도 경계해야 한다.

데이터 협력은 전면 공유와 전면 차단의 이분법을 벗어나야 한다. 프랑스의 기밀 연산기반이 드러내듯, 무엇을 보호하고 무엇을 설명할지 구분해야 주권적 기반이 고립되지 않는다. 원자료를 공유하지 않더라도 평가결과, 오류 유형, 변경 이력, 특정 조건에서의 작동 여부는 교환할 수 있다. 반대로 결과만 공유하면 상대가 판단 근거를 검증할 수 없는 경우도 있으므로, 임무별로 필요한 정보의 수준을 합의해야 한다. 정보공유의 범위와 승인 주체, 재사용 조건을 구분하는 것은 보안의 완화가 아니라 협력의 지속성을 높이는 수단이다. 2026년 6월 한-EU 정상회의가 협상 개시를 추진하기로 한 정보보호협정(SIA)과, 같은 해 9월 8일 한국과 프랑스 국방부가 서명한 개정 군사비밀정보보호협정은 이러한 등급별 공유의 법적 토대가 될 수 있다(Council of the European Union 2026a, 제8항; Présidence de la République 2026).

4. 판단시간의 보호와 오류를 알리는 협력

영국의 DTW처럼 센서와 판단, 효과수단을 하나의 네트워크로 묶는 구상은 처리시간을 줄이는 만큼 판단의 여지를 압박한다. 한국은 AI 도입의 성과지표에 인간의 판단 가능성을 포함해야 한다. 처리시간 단축과 함께 사용자가 불확실성을 이해하는지, 대안을 검토할 수 있는지, 오류를 발견했을 때 개입할 수 있는지를 측정하고, 위험이 큰 결정에서 독립적인 확인과 상급 검토가 실제로

ⓒ EAI 2025

작동하는지를 시험평가 항목으로 삼아야 한다.

AI 관련 오류와 사고를 알리는 협력절차도 필요하다. 모델을 공동 개발하지 않더라도 오류 유형과 사고 통지의 공통 형식을 만들고, 잘못된 신호가 다른 체계로 전파되는 상황을 함께 연습할 수 있다. EU 과학패널이 사고의 탐지·조사 역량과 국제적 정보공유 이니셔티브를 권고한 것은 민간 영역에서 같은 방향의 제도화가 시작되었음을 보여준다. 초기에는 협력국과 비 기밀 환경에서 시작하고, 위험 감소의 효과가 확인되는 범위에서 확대하는 접근이 적절하다. 한반도에서는 이를 곧바로 적대 당사자 간 기술협력으로 연결하기보다, 우선 동맹과 파트너 사이에서 오인과 과잉반응을 줄이는 절차를 정교화해야 한다. 윤정현(2026)의 위기안정성 논의를 정책화 할 때도 기술 도입과 위험소통을 별도 사안으로 두지 않는 것이 중요하다.

5. 민군 기반시설 훈련과 사업별 협력전략

ENISA의 Cyber Europe 2026은 민간 교통망의 장애를 군사기동과 위기 대응의 문제로 연습했다. 한국도 민간 기반시설의 장애가 AI 관련 임무에 미치는 영향을 공동으로 연습해야 한다. 전력·통신·물류의 일부가 제한될 때 어떤 기능을 우선 유지하고 언제 수동 또는 대체 체계로 전환할지 확인하는 것이 핵심이다. 훈련의 목적은 특정 시설의 취약점을 공개하는 것이 아니라, 기관별로 분리된 대응절차가 실제 임무의 흐름에서 충돌하는지를 점검하는 데 있다.

마지막으로 한–EU·한–NATO 협력을 사업 단위로 구체화해야 한다. 산업진출, 연구협력, 군사적 상호운용성, 국제규범 참여는 필요한 자격과 기대효과가 다르다. 방산 협력에서는 SAFE 참여협정과 정보보호협정이, 연구협력에서는 호라이즌 유럽 제2축과 한–EU AI 협력약정이, 군사적 상호운용성에서는 ITPP와 연합 네트워크 참여 수준이 각각 관건이 된다. 각 사업에서 한국이 제공할 자원, 얻을 권리, 부담할 비용과 정보보호 조건을 구분해야 한다. 한국이 제공할 자원에는 기술과 시장만이 아니라 북한의 사이버·위장취업 활동에 관한 식별 정보와 대응 경험도 포함될 수 있다(Ⅷ장 참조). 이를 조정하는 실무체계는 새로운 대규모 조직보다 기존 협력 채널과 관련 기관의 역할을 연결하는 데서 출발할 수 있다. 우선순위는 협력 선언의 확대가 아니라 공동 시험, 계약 개선, 임무별 상호운용성처럼 확인 가능한 결과를 만드는 것이다.

ⓒ EAI 2025

Ⅳ. 결론: 기술주권과 동맹 상호운용성의 동시 추구

유럽의 최근 AI 전략을 규범에서 군사화로의 이동이라는 한 방향의 변화로 설명하기는 어렵다. EU는 규칙의 적용과 함께 산업적 활용·기반시설·방위산업 재원을 조직하고, NATO는 공동작전에 필요한 데이터·네트워크·검증의 조건을 구체화하며, 주요국은 AI를 개발·도입·승인·운용하는 조직과 절차를 정비하고 있다. 이 과정은 상호 보완적이지만 자동적으로 조화롭지는 않다. 특히 EU의 재원은 제3국 제한에서 자유로운 설계 권한을 보상하는 반면 NATO의 연결은 미국 기업의 플랫폼 위에서 넓어지고 있어, 기술적 자율성을 높이려는 정책과 공통 플랫폼을 활용하려는 정책이 서로 다른 수준에서 의존과 선택권을 재 배분한다.

본 연구가 강조한 것은 접근·결합·통제의 관계이다. 필요한 자원을 확보하는 것만으로 충분하지 않고, 연결 가능성만 높아져도 충분하지 않다. 어떤 상황에서 사용하고 변경하며 중단할지 결정할 수 있어야 한다. 규범과 보증절차도 이 관계 속에서 이해해야 한다. 적절한 기준은 협력의 불확실성을 줄이고 도입을 촉진하지만, 형식적인 인증이나 불투명한 플랫폼 의존은 책임과 자율성을 약화시킬 수 있다. AI의 군사적 가치는 최고 성능의 기술 하나보다 사용 가능한 능력을 신뢰성 있게 구성하고 유지하는 데서 나온다.

마지막으로 본 연구의 틀이 놓치기 쉬운 영역을 짚어 둔다. 유럽의 전략문서들은 통제를 주로 계약, 플랫폼, 연산시설, 보증절차의 문제로 다룬다. 그러나 AI와 소프트웨어를 개발하고 갱신하는 사람이 누구인지도 통제의 일부이다. 북한 IT 인력의 원격 위장취업이 이를 보여준다. 구글 위협정보그룹(Google Threat Intelligence Group, GTIG)은 2025년 4월, 미국에서 단속과 경각심이 높아지자 북한 IT 인력이 활동 무대를 넓히면서 특히 유럽에 주목하고 있다고 분석했다. 2024년 말 한 인물은 유럽과 미국에서 최소 12개의 가상 신원을 운용하며 유럽의 방위산업 기반과 정부 부문 기관에 취업을 시도했고, 영국에서 수행한 사업에는 AI 웹 애플리케이션 개발도 있었다. 2026년 7월 프랑스·독일·이탈리아·네덜란드·영국이 한국·미국·일본 등과 함께 발표한 11개국 공동 경보는 이들이 대규모 언어모델로 그럴듯한 이력을 만들고 조작된 영상으로 면접을 통과하며, 그 자체로 '내부자 위협'이 된다고 명시했다. 이들은 해킹이 아니라 고용계약을 통해 코드 저장소와 개발환경에 접근한다. 생성형 AI는 위장의 비용을 낮추고, 원격근무는 신원 확인의 영토적 전제를 약화시킨다. 다시 말해, 접근의 경로가 인력 시장을 통해 열리고 갱신 권한이 신원이 확인되지 않은 개발자에게 넘어가는 것이다(Collier 2025; Auswärtiges Amt 2026; Office of Financial Sanctions

ⓒ EAI 2025

Implementation 2024; Bundesamt für Verfassungsschutz 2024).[45]

유럽의 대응은 아직 이 연결을 충분히 다루지 않는다. EU 대외관계청(European External Action Service, EEAS)은 2026년 7월 북한의 IT 인력 계획을 명시하며 제재 수단을 더 활용하겠다고 밝혔다. 그러나 같은 달 발표된 「사이버안보 및 AI 행동계획」은 프런티어 모델의 방위 분야 배치에 따른 위험은 다루면서도 채용·신원 확인이나 내부자 위험은 다루지 않는다. 네트워크·정보보안지침(Directive on Measures for a High Common Level of Cybersecurity across the Union, NIS2)의 인적 보안 조항과 그 이행규정의 배경 확인 요건이 가장 가까운 법적 근거이지만, AI 공급망의 인적 구성을 겨냥한 장치는 아니다. 집행도 비대칭적이다. 북한 IT 인력에게 대리 신원을 제공한 우크라이나 국적의 조력자는 2024년 폴란드에서 체포되었지만 기소와 선고는 미국에서 이루어졌다. 이 공백은 한국이 고유하게 기여할 수 있는 영역이기도 하다. 한국은 독자적인 주의보를 내고 11개국 공동 경보에도 참여해 왔다. 위장취업의 탐지 경험과 식별 정보의 공유는 접근권과 기밀을 요구하는 한-EU·한-NATO 협력에서 한국이 내놓을 수 있는 실질적인 자산이다(European External Action Service 2026; European Parliament and Council of the European Union 2022, 제21조 제2항 (i)호; European Commission 2024, 부속서 10.2; 2026b; U.S. Department of Justice 2026).[46]

한국의 선택은 독자적인 AI 강국과 외부 생태계의 참여자라는 양자택일이 아니다. 독자적으로 판단해야 할 영역을 분명히 하되, 국제협력에서는 접근권과 검증능력, 교체 가능성을 확보해야 한다. 유럽에서 배울 것은 특정 기관이나 전략의 이름이 아니라, 기술을 실제 능력으로 바꾸는 과정에서 권한·책임·의존을 어떻게 배분하는가이다. AI 안보협력의 핵심은 더 많이 연결하는 데 있지 않다. 연결된 상태에서도 필요한 판단과 행동을 스스로 선택할 조건을 설계하는 데 있다.■

45 영국 금융제재실행청(Office of Financial Sanctions Implementation, OFSI)은 2024년 9월 영국 기업이 표적이 되고 있음이 '거의 확실하다'고 경고했고, 독일 연방헌법보호청(Bundesamt für Verfassungsschutz, BfV)은 같은 해 이들이 지식재산과 기업 내부 자료의 유출에 관여한다고 경고했다. 생성형 AI에 대한 의존 양상은 미국 사례를 다룬 Anthropic (2025) 참조. 이에 대한 자세한 분석은 저자의 EAI Global NK (2026.10.) 기고문을 참조.

46 행동계획에 관한 평가는 필자가 검토한 행동계획 본문 기준이다.

ⓒ EAI 2025

Ⅵ. 참고문헌

대한민국. 2025. “인공지능 발전과 신뢰 기반 조성 등에 관한 기본법.” 법률 제20676호. 2025. 1. 21. 제정, 2026. 1. 22. 시행.

윤정현. 2026. “전략적 비핵무기체계의 AI 전환과 위기안정성 확보 방안.” 『INSS 전략보고』 409. 국가안보전략연구원. 9월 16일.

조은정·윤정현. 2025. “AI 규범경쟁의 서막: EU AI Act 발효(2024.8.)의 분석과 전망.” 『INSS 전략보고』 302. 국가안보전략연구원. 1월 10일.

Anthropic. 2025. “Threat Intelligence Report: August 2025.” August. https://www-cdn.anthropic.com/b2a76c6f6992465c09a6f2fce282f6c0cea8c200.pdf.

Auswärtiges Amt. 2026. “Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers.” Joint statement of Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, the Republic of Korea, the United Kingdom and the United States. July 31. https://www.auswaertiges-amt.de/en/newsroom/news/2780754-2780754.

Bundesamt für Verfassungsschutz. 2024. “Sicherheitshinweis für die Wirtschaft 02/2024: Nordkoreanische IT-Worker.” Verfassungsschutz Niedersachsen. https://www.verfassungsschutz.niedersachsen.de/startseite/spionageabwehr/cyberabwehr/weitere_informationen/sicherheitshinweis-des-bfv-fur-die-wirtschaft-nordkoreanische-it-worker-244997.html.

Bundesministerium der Verteidigung. 2026. “Künstliche Intelligenz (K-9000/102, Öffentliche Fassung).” April 9. https://www.bmvg.de/resource/blob/6143700/9954e2b6b993b17cd3d09ca31c506774/dl-ki-konzeption-data.pdf.

ⓒ EAI 2025

Bundesregierung. 2025. “Europa muss Führungsanspruch übernehmen.” Gipfel zur europäischen digitalen Souveränität. November 18. https://www.bundesregierung.de/breg-de/aktuelles/digitale-souveraenitaet-eu-2394404.

Collier, J. 2025. “DPRK IT Workers Expanding in Scope and Scale.” Google Threat Intelligence Group. April 1. https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale.

Council of the European Union. 2025a. “SAFE: Member States Endorse Agreement on the Participation of Canada.” Press release. December 19. https://www.consilium.europa.eu/en/press/press-releases/2025/12/19/safe-member-states-endorse-agreement-on-the-participation-of-canada/.

Council of the European Union. 2025b. “Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument.” *Official Journal of the European Union*, L, 2025/1106. https://eur-lex.europa.eu/eli/reg/2025/1106/oj.

Council of the European Union. 2026a. “Joint Statement Following the 11th European Union–Republic of Korea Summit (10316/26).” June 10. https://data.consilium.europa.eu/doc/document/ST-10316-2026-INIT/en/pdf.

Council of the European Union. 2026b. “Programme for Agile and Rapid Defence Innovation: Council Gives Final Green Light.” Press release. October 12. https://www.consilium.europa.eu/en/press/press-releases/2026/10/12/programme-for-agile-and-rapid-defence-innovation-council-gives-final-green-light/.

ⓒ EAI 2025

Council of the European Union. 2026c. "SAFE: Council Clears Path for Financial Assistance to Eight Member States and Concluding the Canada Agreement." Press release. February 11. https://www.consilium.europa.eu/en/press/press-releases/2026/02/11/safe-council-clears-path-for-financial-assistance-to-eight-member-states-and-concluding-the-canada-agreement/.

EuroHPC Joint Undertaking. 2026. "The EuroHPC Joint Undertaking Launches the AI Gigafactories Call." July 30. https://www.eurohpc-ju.europa.eu/eurohpc-joint-undertaking-launches-ai-gigafactories-call-2026-07-30_en.

European Commission. N.d.a. "Cyber Resilience Act—Reporting Obligations." https://digital-strategy.ec.europa.eu/en/policies/cra-reporting. (Accessed: October 19, 2026)

European Commission. N.d.b. "Navigating the AI Act." https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act. (Accessed: October 19, 2026)

European Commission. 2024. "Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures." *Official Journal of the European Union*, L, 2024/2690. https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj.

European Commission. 2025a. "The AI Continent Action Plan." April 9. https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

European Commission. 2025b. "Commission Communication: Apply AI Strategy." October 8. https://digital-strategy.ec.europa.eu/en/library/commission-communication-apply-ai-strategy.

ⓒ EAI 2025

European Commission. 2025c. "Joint Statement of the Third Meeting of the EU–Republic of Korea Digital Partnership Council." November 28. https://digital-strategy.ec.europa.eu/en/library/joint-statement-third-meeting-eu-republic-korea-digital-partnership-council.

European Commission. 2026a. "Commission Holds Special Meeting of Scientific Panel on Frontier AI Safety and Risks." October 9. https://digital-strategy.ec.europa.eu/en/news/commission-holds-special-meeting-scientific-panel-frontier-ai-safety-and-risks.

European Commission. 2026b. "EU Action Plan on Cybersecurity and Artificial Intelligence." July 7. https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence.

European Commission. 2026c. "Proposal for a Cloud and AI Development Act (CADA) (COM(2026) 502)." June 3. https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada.

European Commission. 2026d. "Special Meeting of the AI Scientific Panel." October 12. https://digital-strategy.ec.europa.eu/en/news/special-meeting-ai-scientific-panel.

European Commission. 2026e. "Submarine Cable Security Toolbox and Cable Projects of European Interest." February 5. https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest.

European Commission and High Representative. 2025a. "Joint White Paper for European Defence Readiness 2030 (JOIN(2025) 120 final)." March 19. https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-european-defence-readiness-2030_en.

ⓒ EAI 2025

European Commission and High Representative. 2025b. “Preserving Peace – Defence Readiness Roadmap 2030 (JOIN(2025) 27 final).” October 16. https://data.consilium.europa.eu/doc/document/ST-14416-2025-INIT/en/pdf.

European Council. 2026. “European Council Conclusions (EUCO 14/26).” October 16. https://www.consilium.europa.eu/media/4tglqede/en-20261016-european-council-conclusions.pdf.

European External Action Service. 2026. “DPRK: Statement by the Spokesperson on Cyber Activities.” July 31. https://www.eeas.europa.eu/eeas/dprk-statement-spokesperson-cyber-activities_en.

European Parliament. 2026. “Cloud and AI Development Act (Procedure File 2026/0138(COD)).” Legislative Observatory. https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2026%2F0138%28COD%29. (Accessed: October 19, 2026)

European Parliament and Council of the European Union. 2022. “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).” *Official Journal of the European Union*, L 333: 80-152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

European Parliament and Council of the European Union. 2024a. “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).” *Official Journal of the European Union*, L, 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

ⓒ EAI 2025

European Parliament and Council of the European Union. 2024b. "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)." *Official Journal of the European Union*, L, 2024/2847. https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

European Parliament and Council of the European Union. 2026. "Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)." *Official Journal of the European Union*, L, 2026/1744. https://eur-lex.europa.eu/eli/reg/2026/1744/oj.

European Union Agency for Cybersecurity. 2026. "Cyber Europe 2026: All Eyes on the EU's Collective Response and Resilience." June 11. https://www.enisa.europa.eu/news/cyber-europe-2026-all-eyes-on-the-eus-collective-response-and-resilience.

Farrell, Henry and Abraham L. Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security*, 44(1): 42-79. https://doi.org/10.1162/isec_a_00351.

Gouvernement français. 2024. "Défense : La stratégie ministérielle sur l'intelligence artificielle." March 11. https://www.info.gouv.fr/actualite/defense-la-strategie-ministerielle-sur-lintelligence-artificielle.

ⓒ EAI 2025

Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. 2026. "Report of the 2024–2025–2026 Sessions of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (CCW/GGE.1/2026/3, Advance Copy)." September 14. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2026)/CCW-GGE.1-2026-3-Advance_copy.pdf.

Horowitz, Michael C. 2018. "Artificial Intelligence, International Competition, and the Balance of Power." *Texas National Security Review*, 1(3): 36-57. https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/.

Manthey, F. 2026. "KI (Künstliche Intelligenz)-Konzeption: Zukunftsfähige Verteidigung mit Künstlicher Intelligenz." Bundesministerium der Verteidigung. August 12. https://www.bmvg.de/de/aktuelles/verteidigungsministerium-erlaesst-ki-konzeption-6140520.

Ministère des Armées. 2019. "L'intelligence artificielle au service de la défense: Rapport de la task force IA." September. https://www.vie-publique.fr/files/rapport/pdf/194000723.pdf.

Ministère des Armées. 2025a. "Inauguration du plus puissant supercalculateur classifié dédié à l'IA en Europe." September 5. https://www.defense.gouv.fr/actualites/inauguration-du-plus-puissant-supercalculateur-classifie-dedie-lia-europe.

Ministère des Armées. 2025b. "Le ministre des Armées inaugure le Commissariat au numérique de défense (CND) et le supercalculateur ASGARD." September 5. https://www.defense.gouv.fr/cnd/actualites/ministre-armees-inaugure-commissariat-au-numerique-defense-cnd-supercalculateur-asgard.

ⓒ EAI 2025

Ministère des Armées. 2026. “Pendragon : franchir un cap décisif dans la robotisation du combat terrestre.” April 17. https://www.defense.gouv.fr/terre/actualites/pendragon-franchir-cap-decisif-robotisation-du-combat-terrestre.

Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. 2026. “REAIM 2026: Pathways to Action (A Coruña Declaration).” https://www.exteriores.gob.es/en/REAIM2026/Paginas/default.aspx.

Ministry of Defence. 2022. “Defence Artificial Intelligence Strategy.” June 15. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy.

Ministry of Defence. 2024. “Dependable Artificial Intelligence (AI) in Defence: Part 1—Directive (JSP 936, Version 1.1).” November 13. https://assets.publishing.service.gov.uk/media/6735fc89f6920bfb5abc7b62/JSP936_Part1.pdf.

Ministry of Defence. 2025. “The Strategic Defence Review 2025—Making Britain Safer: Secure at Home, Strong Abroad.” June 2. https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad.

Ministry of Defence. 2026a. “The Defence Investment Plan.” June 30. https://www.gov.uk/government/publications/the-defence-investment-plan.

Ministry of Defence. 2026b. “New Taskforce to Put AI on the UK’s Frontline.” Press release. June 10. https://www.gov.uk/government/news/new-taskforce-to-put-ai-on-the-uks-frontline.

ⓒ EAI 2025

Ministry of Defence. 2026c. "TF RAID Avengers AI Swarming Competition." September 25. https://www.gov.uk/government/publications/tf-raid-avengers-ai-swarming-competition.

NATO Communications and Information Agency. 2025. "NATO Acquires AI-Enabled Warfighting System." April 14. https://www.ncia.nato.int/newsroom/news/nato-acquires-aienabled-warfighting-system.

North Atlantic Treaty Organization. 2024. "Summary of NATO's Revised Artificial Intelligence (AI) Strategy." July 10. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy.

North Atlantic Treaty Organization. 2025a. "Data Strategy for the Alliance." May 5. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/05/05/data-strategy-for-the-alliance.

North Atlantic Treaty Organization. 2025b. "Summary of NATO's Rapid Adoption Action Plan." June 25. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/summary-of-natos-rapid-adoption-action-plan.

North Atlantic Treaty Organization. 2025c. "The Hague Summit Declaration." June 25. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration.

North Atlantic Treaty Organization. 2025d. "The Republic of Korea Joins NATO Science & Technology Organization (STO) Partnership." March 19. https://www.nato.int/en/news-and-events/articles/news/2025/03/19/the-republic-of-korea-joins-nato-science-amp-technology-organization-sto-partnership.

ⓒ EAI 2025

North Atlantic Treaty Organization. 2026a. "Alliance Digital Strategy." January 13. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/01/13/alliance-digital-strategy.

North Atlantic Treaty Organization. 2026b. "The Ankara Summit Declaration." July 8. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/08/the-ankara-summit-declaration.

North Atlantic Treaty Organization. 2026c. "NATO's Digital Transformation Implementation Strategy 2.0." May 26. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy.

North Atlantic Treaty Organization. 2026d. "Relations with the Republic of Korea." July 1. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-the-republic-of-korea.

North Atlantic Treaty Organization. 2026e. "Strategy for Industry–NATO Cooperation." July 8. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/08/strategy-for-industry-nato-cooperation.

North Atlantic Treaty Organization. 2026f. "NATO Releases New Strategy for Industry Cooperation." News release. July 8. https://www.nato.int/en/news-and-events/articles/news/2026/07/08/nato-releases-new-strategy-for-industry-cooperation.

Office of Financial Sanctions Implementation. 2024. "North Korean IT Workers Advisory: Signs to Watch For." HM Treasury. September 12. https://www.gov.uk/government/publications/north-korean-it-workers-advisory-signs-to-watch-for.

ⓒ EAI 2025

Présidence de la République. 2025a. “Paris Declaration on Maintaining Human Control in AI Enabled Weapon Systems.” February 11. https://www.elysee.fr/emmanuel-macron/2025/02/11/paris-declaration-on-maintaining-human-control-in-ai-enabled-weapon-systems.

Présidence de la République. 2025b. “Sommet sur la souveraineté numérique européenne à Berlin.” November 18. https://www.elysee.fr/emmanuel-macron/2025/11/18/sommet-sur-la-souverainete-numerique-europeenne-a-berlin.

Présidence de la République. 2026. “Visite d’État de Lee Jae Myung, Président de la République de Corée.” September 8. https://www.elysee.fr/emmanuel-macron/2026/09/08/visite-detat-de-lee-jae-myung-president-de-la-republique-de-coree.

République française. 2024. “Décret n° 2024-376 du 23 avril 2024 relatif au service à compétence nationale dénommé « agence ministérielle pour l’intelligence artificielle de défense ».” *Journal officiel de la République française*, 0097, texte 25. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049467967.

République française. 2026. “Loi n° 2026-791 du 16 août 2026 actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.” *Journal officiel de la République française*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054694832.

Sénat. 2026. “Projet de loi actualisant la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense.” La loi en clair. https://www.senat.fr/travaux-parlementaires/textes-legislatifs/la-loi-en-clair/projet-de-loi-actualisant-la-programmation-militaire-pour-les-annees-2024-a-2030-et-portant-diverses-dispositions-interessant-la-defense.html.

ⓒ EAI 2025

U.S. Department of Justice. 2026. “Ukrainian National Sentenced for Laptop Farm Scheme That Generated Income for North Korean IT Workers.” Press release. February 19. https://www.justice.gov/usao-dc/pr/ukrainian-national-sentenced-laptop-farm-scheme-generated-income-north-korean-it-workers.

United Nations. 2025. “General Assembly Adopts More Than 60 Resolutions, Decisions of Its First Committee (Disarmament and International Security) (GA/12736).” Press release. https://press.un.org/en/2025/ga12736.doc.htm.

United Nations General Assembly. 2024. “Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security (A/RES/79/239).” December 24. https://digitallibrary.un.org/record/4070018.

Virkkunen, Henna. 2026. “Opening Words by Executive Vice-President Virkkunen at the Special Meeting of the AI Scientific Panel (SPEECH/26/2148).” European Commission. October 9. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_26_2148/SPEECH_26_2148_EN.pdf.

ⓒ EAI 2025

■ 조은정_국가안보전략연구원 지정학센터장

■ 담당 및 편집: **임재현**_EAI 연구원

문의: 02-2277-0746 (ext. 209) jhim@eai.or.kr

인용할 때에는 반드시 출처를 밝혀주시기 바랍니다.
EAI는 어떠한 정파적 이해와도 무관한 독립 연구기관입니다.
EAI가 발행하는 보고서와 저널 및 단행본에 실린 주장과 의견은 EAI와는 무관하며 오로지 저자 개인의 견해임을 밝힙니다.

발행일 2026년 11월 06일
“” 979-11-7584-176-5 95340

재단법인 동아시아연구원
03028 서울특별시 종로구 사직로7길 1
Tel. 82 2 2277 1683 Fax 82 2 2277 1684

Email eai@eai.or.kr Website www.eai.or.kr

ⓒ EAI 2025