대한정치학회보 34집 1호
The Korean Journal of Political Science
2026년 2월 : 79~108
http://doi.org/10.34221/KJPS.2026.34.1.4
ISSN 1229-5469(Print)
ISSN 2671-5384(Online)

미국의 AI 안보화 담론과 AI 안보 거버넌스의 재구성

윤 정 현*

•요 약•

미국은 AI를 국가안보와 직결된 핵심 전략기술로 인식해왔으며, 미·중 기술 경쟁의 심화 속에서 AI 기술 우위의 유지를 국가안보의 핵심 과제로 설정해 왔다. 그러나 앞서의 연구들은 이러한 AI 안보화를 주로 위기 담론의 형성이나 규제 정책의 기조 변화를 중심으로 분석해 왔으며, 어떠한 대내외적 정책수단의 조합과 집행 구조로 조직·전환되는지에 대한 설명은 충분히 제시하지 못하였다. 이에 본고는 미국의 AI 안보화가 규제 강화나 탈규제의 이분법으로 설명될 수 없으며, AI를 국가 역량으로 조직하기 위한 거버넌스 전환의 과정으로 이해되어야 함을 보여주고자 하였다. 이를 위해 미국의 AI 안보화 담론을 전략자산화 기반의 제도화, 대내외 정책수단-집행체계-확산으로 이어지는 연속적·구조적 과정으로 이해하고, 트럼프 2기 행정부 시기에 적용하여 살펴보았다. 분석 결과, 미국의 AI 안보화는 규제의 총량을 확대하거나 국가의 직접 통제를 강화하는 단순한 방식으로 전개되지 않았으며 AI 생태계의 요소들을 관리 가능한 국가 전략자산의 집합체로 인식하고 조정 중심의 구조 속에서 차등적 개입과 선택적 통제를 결합하는 방식으로 운영하고 있음을 확인하였다. 실제로 군사·안보적 파급력이 높은 영역에서는 연방 차원의 직접 개입과 통제가 강화되는 반면, 민간 혁신과 산업 경쟁력과 직결된 영역에서는 규제 완화와 자율성이 확대된다. 동시에 이러한 거버넌스는 국내 집행에 그치지 않고 민간 기업과 주정부, 학계로의 내부 확산과 더불어, 동맹과의 정책 정합성 확보·표준 수립·수출 통제 등을 통한 대외적 확산으로 연결되고 있다.

주제어 : 인공지능(AI), AI 안보화, AI 거버넌스, AI 행동계획, 제네시스 구상

* 국가안보전략연구원 연구위원 (AI안보연구센터장). 이 논문은 서울대학교 통일·평화연구원에서 운영하는 2025년 서울대학교 통일·평화기반구축사업의 지원을 받아 수행한 연구의 결과물임(2025-IPUS-0009).

Ⅰ. 서론

미국은 일찍이 인공지능(AI)을 국가안보와 경제, 혁신 경쟁의 종합 국력 강화와 직결된 핵심기술로 인식해왔다. 특히, 바이든-트럼프 2기의 정권 교체기에도 AI를 '시대를 정의하는 기술'로 규정하였으며[1], AI를 단순한 산업 경쟁력의 원천이 아니라 국가 역량 전반에 영향을 미치는 전략적 변수로 인식해야 한다는 관점은 정책 전반에 일관되게 반영되어 왔다. 이러한 인식 하에서 미국은 AI를 책임감 있게 활용함으로써 글로벌 리더십을 강화해야 한다는 기조를 확립해왔으며, AI를 둘러싼 정책은 과학기술 정책의 범주를 넘어 국가안보 전략의 핵심 요소로 자리잡아 왔다.[2] 실제로 중국과 러시아 등 야심찬 군사·기술 강대국들의 도전이 격화되는 상황에서, 미국은 AI 분야의 압도적인 기술적 우위를 유지하는 것이 국가안보의 최우선 과제라는 점을 일관되게 강조하고 있다. 이러한 문제의식은 2024년 10월 발표된 "AI 국가안보각서(AI National Security Memorandum, AI NSM)"에 집약적으로 드러난다. 동 각서는 핵보유국과 비보유국 간의 전략적 불균형에 비유하며, AI 기술 보유 여부와 발전 수준이 국가 간 역량 격차를 결정짓는 핵심 요인이 될 수 있음을 지적한 바 있다. 나아가 AI 기술적 우위의 상실은 국가안보는 물론 외교 전략의 목표까지 훼손할 수 있음을 명시적으로 경고하고 있다.[3]

특히 미국은 AI를 국가안보에 직접적인 영향을 미치는 전략기술로 일관되게 간주해왔으며, 경쟁국에 대한 기술적 우위의 유지가 곧 안보 유지라는 인식을 전제로 AI 안보 거버넌스 체계를 구축해왔다. 지금까지 발표된 각종 지침과 법안, 대통령 행정명령들은 AI의 범정부적·복합적 속성에 주목함으로써, AI를 개별 기술 품목이 아닌 연산 자원, 반도체, 데이터, 인재, 연구 인프라를 포괄하는 국가 역량의 집합체로 관리·조정하려는 접근을 반영한다. 또한 미국은 대통령 권한을 적극적으로 활용하여 AI 혁신과 안보를 결합하는 종합 실행체계로서 행정명령을 빈번히 활용해왔는데, 이는 신속성과 집행력을 중시하는 미국식 기술안보 거버넌스의 특징을 잘 보여준다.

그러나 이러한 AI 안보 인식과 거버넌스의 기본 틀은 행정부 교체에 따라 동일한 방식

1) Sarokhanian, Nicholas A. and Lyric D. Menges. 2025. "A Look at U.S. Government's Changed Approach to Artificial Intelligence Development and Investments." *The National Law Review* (Feb 10, 2025). https://natlawreview.com/article/look-us-governments-changed-approach-artificial-intelligence-development-and

2) The White House. (July 2025). "Winning the Race: AMERICA'S AI ACTION PLAN"

3) CSET. (October 24, 2024). The National Security Memorandum on Artificial Intelligence: CSET Experts React, https://cset.georgetown.edu/article/the-national-security-memorandum- on-artificial-intelligence-cset-experts-react/ (검색일: 2025.8.22.).

으로 유지되지는 않았다. 바이든 행정부 시기에는 '안전(safety)'과 '신뢰성(trustworthy)'을 강조하는 규범적 접근이 AI 안보 담론의 중심에 위치했던 반면, 트럼프 2기 행정부 출범 이후에는 규제 완화와 민간 혁신 가속화를 통해 AI 기술 우위를 확보하려는 보다 실리적인 안보 접근이 전면에 부상하였다. 트럼프 2기 행정부는 기존의 안전 중심 행정명령을 폐기하거나 조정하는 한편, AI 인프라 확충, 연산자원과 반도체 공급망 통제, 동맹국 대상 AI 기술 풀스택 확산 등을 핵심 축으로 하는 'AI 행동계획(AI Action Plan)'을 발표한 바 있다.[4] 이러한 변화는 AI 안보화가 약화되었음을 의미하지 않는다. 오히려 미국의 AI 안보화 담론은 규제 중심의 관리 방식에서 민간 주도의 혁신 역량과 국가 차원의 전략적 통제 수단을 결합하여 국가 역량을 조직·배치하는 방식으로 재구성되고 있기 때문이다. 다시 말해, 트럼프 2기 행정부의 AI 정책은 '탈안보화'라기보다는, 안보화의 강도나 목표가 아니라 안보화가 작동하는 거버넌스의 방식과 수단이 전환되는 과정으로 이해할 필요가 있다.

그럼에도 불구하고 기존 연구들은 미국의 AI 정책을 개별 행정부의 정책 성향이나 특정 법·제도의 변화 중심으로 분석하는데 머물러 있다. 즉, 트럼프 2기 행정부에서 나타난 AI 안보 담론과 거버넌스 변화가 갖는 구조적 의미, 즉 AI 안보화가 어떠한 방식으로 재조직되고 있는지에 대한 분석은 충분히 이루어지지 못하였다. 본 논문은 이러한 문제의식에서 출발하여, 트럼프 2기 행정부 시기를 중심으로 미국의 AI 안보화 담론과 거버넌스가 어떠한 방향으로 재구성되고 있는지를 분석한다. 특히, AI 안보화 담론을 기술안보 거버넌스의 관점에서 재해석하고, 미국의 AI 정책 문서와 제도적 변화를 토대로 안보화의 작동 방식과 거버넌스 구조의 변화를 면밀히 조명하고자 한다.

이를 위해 Ⅱ장에서는 AI가 핵심적인 안보 변수로 부상한 2019년 이후, 미국의 AI 안보 거버넌스 체계의 형성과 전개 과정을 이론적으로 정리한다. AI 안보화 담론에 관한 선행연구 검토에 이어, AI NSM, 국방수권법(National Defense Authorization Act, NDAA), AI 위험관리 프레임워크, 대통령 행정명령 등 핵심 정책 문건들을 중심으로 AI 안보 거버넌스가 어떠한 논리와 메커니즘을 통해 군사·경제·기술 안보를 관통하는 전략적 프레임으로 재구성되어 왔는지를 설명하기 위한 이론적 분석틀을 제시한다. Ⅲ장에서는 제시한 분석틀을 적용하여, 트럼프 2기 행정부를 중심으로 미국의 AI 안보 거버넌스에서 나타난 핵심 축과 작동 방식을 도출한다. 이 과정에서 '혁신역량', '안보·통제 및 책임성', '인재·인프라 기반 및 생태계', '국제규범·동맹 협력과 글로벌 거버넌스'의 네 가지 측면에서 각 축이 어떠한 방식으로 강화·조정·재배치되고 있는지를 분석하고, 그 대외적

4) The White House. (July 2025).

파급 효과를 함께 검토한다. 이를 토대로 Ⅳ장에서는 트럼프 2기 행정부 이후 미국 AI 안보 거버넌스의 주요 특징을 종합적으로 정리하고 미국의 외교·안보 기조 및 글로벌 기술 질서에 어떠한 전략적 함의를 갖는지를 분석한다. 마지막 결론에서는 한국적 맥락의 시사점과 함께 AI 중견국으로서 한국에 요구되는 AI 안보 거버넌스의 설계 방향과 정책 방향을 제언하고자 한다.

Ⅱ. 이론적 논의와 분석틀

1. AI 안보화 담론에 대한 선행연구 검토

코펜하겐 학파를 중심으로 한 '안보화(securitization)' 이론은 안보를 객관적 위협의 존재 여부가 아니라, 특정 사안이 정치 행위자에 의해 '존재적 위협'으로 구성되는 담론적 과정으로 설명하는 접근이라 할 수 있다.[5] 해당 이론은 냉전 종식 이후 안보 개념이 군사 영역을 넘어 정치·경제·사회 전반으로 확장되는 과정을 고찰하는 유용한 틀로 기능해 왔으며 특히, 안보를 고정된 상태가 아닌 사회적으로 구성되는 정치적 행위의 결과로 이해하는데 기여했다.[6] 일부 연구자들은 안보화가 특정 시점의 선언을 통해 급격히 이루어지기보다는, 제도와 정책, 행정 관행을 통해 점진적으로 축적되는 과정임을 강조하며 '일상적 안보화' 또는 '제도적 안보화' 개념을 제시하기도 하였다.[7] 이러한 논의는 안보화가 위기 시에만 작동하는 예외적 메커니즘이라기 보다는 평시의 정책 설계와 거버넌스 구조 속에서도 지속적으로 재생산될 수 있음을 보여준다.[8]

AI를 둘러싼 안보화 논의 역시 초기에는 군사안보 중심으로 전개되었다. 자율무기체계(LAWS), AI 기반 지휘통제 및 정보·감시·정찰(ISR) 능력의 발전은 전통적인 전략적 안정성과 억지 이론에 중대한 도전을 제기하는 요소로 간주되었다. 특히, Scharre(2018)와

5) Buzan, Barry Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*, (Boulder: Lynne Rienner Publishers, 1998); Wæver, Ole. 1995. "Securitization and Desecuritization," in Ronnie D. Lipschutz ed., *On Security*, (New York: Columbia University Press, 1995).

6) McDonald, Matt. 2008. "Securitization and the Construction of Security," *European Journal of International Relations*, Vol. 14, No. 4.

7) Bigo, Didier. 2002. "Security and Immigration: Toward a Critique of the Governmentality of Unease," *Alternatives: Global, Local, Political*, Vol. 27; Floyd, Rita. 2019. *The Morality of Security: A Theory of Just Securitization*, (Cambridge: Cambridge University Press).

8) Hansen, Lene. 2000. "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School," *Millennium: Journal of International Studies*, Vol. 29, No. 2.

Horowitz(2018)은 AI가 의사결정 속도를 급격히 단축시키면서 오판과 비의도적 확전의 위험을 증폭시킬 수 있다는 점은 집중적으로 강조한 바 있다.[9] 그러나, 최근에는 AI 안보화의 적용 범위를 군사 영역에 한정하지 않고, 금융, 에너지, 사이버, 기술 등 비군사적 영역으로 확장해 볼 필요성이 제기되고 있으며, 명시적인 위협 담론보다는 수출통제와 보호, 투자, 표준 설정과 같은 제도적 수단을 통해 구현될 수 있다는 점이 강조되는 추세이다.[10] 실제로 최근의 연구들은 AI 안보화를 기술안보 및 경제안보의 시각에서 재해석하고 있으며, 첨단 기술 경쟁이 군사 영역을 넘어 산업 정책, 공급망 통제, 표준 경쟁, 연산자원과 인재 확보를 둘러싼 구조적 경쟁으로 확장되고 있음에 주목한다.[11] 특히, 기술의 상호의존성이 국가 간 권력 투사와 통제의 수단으로 활용될 수 있다는 분석들은 최근의 AI 안보화 흐름을 이해하는데 중요한 이론적 토대를 제공하고 있다.[12] 대표적으로, Farrell & Newman(2023)와 Bradford(2023), Suleyman & Bhaskar(2024) 등은 기술경쟁과 경제안보의 맥락에서 미국이 공급망·표준·수출통제·동맹 네트워크를 활용해 전략을 투사하는 과정을 면밀히 보여준 바 있다.[13] Miller(2022) 등, 반도체·제조 기반과 지정학을 다룬 연구 또한 AI 경쟁을 가능하게 하는 '하부 구조'인 칩·제조·공급망의 중요성을 부각함으로써 AI 안보가 물리적 기반과 분리될 수 없다는 점을 강조하였다.[14]

반면, AI 안보화 논의에 대한 기존 연구에는 몇 가지 한계가 내재해 있다. 첫째, 개별 정책 수단이나 주요 법안을 중심으로 특정 행정부의 AI 안보화 기조를 단순화하여 설명하는 경향이 강하다.[15] 투자와 보조금, 수출 통제, 연구안보, 동맹 중심의 기술 협력 등 다양한 정책 수단이 결합된 종합적 패키지로서 안보화가 작동함에도, 이를 단일 규제 프레임이나 개별 법제 중심으로 환원하는 접근이 대표적이다. 그러나 AI 안보화는 단일 규

9) Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War*, (New York: W. W. Norton & Company, 2018); Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review*, Vol. 1, No. 3.

10) CSET (Center for Security and Emerging Technology), 2022. "AI and National Power", (Washington, DC: Georgetown University); OECD, 2023. "Economic Security and Critical Technologies: Policy Toolkit" (Paris: OECD Publishing).

11) Farrell, Henry and Abraham L. Newman. 2024. *Underground Empire: How America Weaponized the World Economy*, (Princeton: Princeton University Press, 2023); OECD, "AI, Data and Economic Security", (Paris: OECD Publishing).

12) Ciuriak Dan and Patricia Goff. 2021. "Technology and Economic Security: Conceptual Foundations and Policy Implications," (CIGI, Waterloo: 2021).

13) Farrell & Newman(2023).

14) Miller, Chris. 2022. *Chip War: The Fight for the World's Most Critical Technology*, (Scribner).

15) Brown, Mark B. 2009. *Science in Democracy: Expertise, Institutions, and Representation*, (Cambridge, MA: MIT Press); Chowdhury, Rumman. 2024. "Dictators, disinformation, disputed outcomes and more," *Nature*, (October), Vol. 634.

제의 강화·약화로 환원되기보다, 투자·보조금(산업정책)-인프라(연산·데이터센터·에너지)-표준·평가-연구안보-수출통제-동맹 연계가 결합된 정책 조합이 어떻게 설계·동원되는가의 문제로 재정의될 필요가 있다.[16] 특히 트럼프 2기 이후 나타나는 국내 규제·가드레일의 완화와 같은 혁신 가속 기조와 대외 통제·정합성 강화 등 수출통제·동맹 결속이 동시에 추진되고 있는 정책 간 조합은, '규제 강화=안보화', '규제 완화=탈안보화'라는 기존의 이분법적 접근으로는 그 복합적 의미를 포착하기 어렵다.

둘째, 기존 연구는 AI 안보화가 산업정책, 수출통제, 표준 경쟁, 연산자원 및 인프라 구축과 같은 기술안보 거버넌스 수단을 통해 어떻게 집행되고 제도화되는지를 충분히 설명하지 못했다. 개별 문건이나 단일 정책 영역에 대한 분석은 축적되어 왔으나, 이들 수단이 상호 결합되며 '풀스택(연산-데이터-모델-응용)' 차원의 거버넌스 체계로 재구성되는 과정을 종합적으로 추적한 연구는 부족한 것이 특징이다.[17] 특히, AI 안보화 담론이 동맹 및 파트너 국가와의 규범 정렬, 공급망 연계, 기술 이전과 통제를 통해 대외적으로 '확산과 통제의 병행 전략'으로 작동하는 과정에서 담론의 정당화와 거버넌스의 집행 메커니즘 사이의 결합 구조를 정교화히 살펴본 연구는 제한적이다. 즉, 국내 차원의 혁신 가속과 대외 차원의 통제라는 이중적 결합을 AI 안보화 메커니즘으로 재구성하지 못한 한계가 있다.[18] 또한, 규범과 가치 또는 구조와 네트워크에 치우쳐, 인허가·조달·표준화·패키지 수출과 같은 안보화 구현의 현실적 집행 장치들로 구현되는지를 충분히 설명하지 못하였다.

이에 본고는 AI 안보화를 규제의 강화·완화 여부로 환원하지 않고, 기술안보 거버넌스의 재구성 과정으로 개념화하고자 한다. 이를 위해 첫째, AI를 '전략자산화'하는 담론이 어떤 정책수단 조합을 정당화하는지, 둘째, 그 조합이 국내(혁신 가속·규제 혁파·인프라 확장)와 대외(수출통제·표준·동맹 연계)에서 어떻게 상이한 강도로 배치되는지, 셋째, 미국식 AI 질서가 '민간 주도-국가 안전판'이라는 다층적 구조로 어떻게 제도화되는지를 추적할 수 있도록, 담론-수단-집행체계-대외확산을 연결하는 분석틀을 제시하고자 한다. 따라서 최근 미국의 AI 안보화를 이해하기 위해서는 규제의 총량이 아닌, 거버넌스의 배치 방식, 즉, '무엇을 국내에서 완화하고, 무엇을 대외적으로 규제하며, 어떤 수단을 결합해

16) OECD. 2025; Schaake, Marietje. 2024. *The Tech Coup: How to Save Democracy from Silicon Valley*, (Princeton Uiversity Press).

17) Miller. 2022; Triolo, Paul. 2024. "The Great Widening: America's New Strategy to Counter Chinese Tech," *American Affairs*.

18) Farrell & Newman. 2023; Silvad, Elise, Nari Johnson, Ravit Dotan, Motahhare Eslami, Hoda Heidari and Beth Schwanke. 2025. "Procuring Public Sector AI Guidance for Local Governments," (Pittsburgh, Pittsburgh University Press).

실행력을 확보함으로써 정책효과를 확장하는가'를 중심으로 논의를 전개할 것이다. 나아가 AI 안보화를 특정 문건의 성격 규정이 아니라 기술안보 거버넌스의 재구성 과정인 정책수단 패키지의 재배열·재결합의 메커니즘으로 이해하고, 트럼프 2기에서 두드러진 '혁신 가속화-통제 강화'의 이중적 논리를 대안적인 'AI 안보화 담론-수단/집행-확산의 분석틀'을 통해 설명하고자 한다.

2. 미국의 AI 안보화 담론-수단/집행-확산의 분석틀

기존 안보화 이론이 특정 사안이 '안보 문제'로 치환되고 정당화되는 담론적 과정에 주목해 왔다면, 본고는 더 나아가 그러한 담론이 특정한 정책수단의 조합을 강화하고, 어떻게 제도적·운영적 구조로 종합되는지에 초점을 맞춘다. 이러한 측면에서, AI 안보화는 위기 인식의 확산이나 규제 강화 여부 자체가 아니라, 기술 생태계를 관리·조정하기 위한 거버넌스 수단들이 재배치·재결합되는 과정으로 이해될 필요가 있다.[19] 이를 위해 본고는 AI 안보화를 네 개의 상호연결된 분석 차원—① 담론(discourse), ② 정책수단(policy instruments), ③ 집행체계(implementation architecture) 및 확산(external projection)—으로 구성된 단계적·연쇄적 구조로 접근하고자 한다. 이는 AI 안보화를 규제의 강화 여부가 아니라, 전략적 인식이 정책수단의 조합과 집행 방식으로 구체화되는 거버넌스 재구성 과정으로 파악하기 위함이다.

첫째, 담론 차원에서는 AI가 '경제 성장의 수단'이나 '산업 혁신의 도구'를 넘어, 국가 경쟁력과 전략적 우위를 좌우하는 자산, 즉 '전략자산(strategic asset)'으로 재정의되는 과정을 포착한다. 이 단계에서 AI 우위 상실은 국가안보의 구조적 취약성으로 연결되며, 기술, 인재, 연구개발 환경을 포함한 광범위한 AI 생태계의 하나하나가 '국가 전략자산'으로 간주되어야한다는 논거를 제공한다. 이는 AI 경쟁력을 위해 국가가 개입하고 적극적으로 관리해야 한다는 정당성을 부여하는 기능을 수행하게 된다.

둘째, 정책수단 차원에서는 이러한 담론이 어떤 정책 도구의 결합을 정당화하는지에 주목한다. 본고가 주목하는 핵심은 규제 강화 또는 완화라는 단선적 선택이 아니라, 투자·보조금, 규제 혁파, 인프라 확장과 같은 국내 혁신 가속 수단과 수출통제, 표준 설정, 동맹 연계와 같은 대외 통제 수단이 하나의 '정책 조합'으로 결합되는 방식이다. 이 과정에서 안보화는 규제의 총량을 늘리는 방식이 아니라, 수단의 기능적 분화와 차등 배치를

19) Balzacq, Thierry. 2011. *Securitization Theory: How Security Problems Emerge and Dissolve*, (London: Routledge).

통해 제도화된다.[20]

셋째, 집행체계 차원은 이러한 정책수단 조합이 실제로 작동하도록 만드는 제도적·조직적 메커니즘에 초점을 둔다. 연산자원과 데이터센터의 인허가 및 전력 연계, 정부 조달과 표준·평가 요건, 연구안보 체계와 인재 이동 관리, 부처 간 역할 분담과 조정 메커니즘 등은 AI 안보화가 선언적 구호에 그치지 않고 지속적이고 반복적으로 작동하도록 만드는 핵심 수단으로 기능한다. 특히 대통령 행정명령과 국가안보 전략 문건을 중심으로 한 집행 구조는 정책 조합을 신속히 제도화하는 미국식 기술안보 거버넌스의 특징을 보여준다. 본고는 이러한 집행 장치들이 개별적으로가 아니라 상호 연동된 구조로 설계된다는 점에 주목하며, 이를 통해 '민간 주도-국가 안전판'이라는 미국식 AI 거버넌스 구조로 체계화되는 과정을 조명하고자 한다.[21]

출처: 저자 작성

〈그림 1〉 미국 AI 안보화의 '담론-수단-집행/확산' 추진 모델

특히, 미국의 AI 안보 거버넌스가 동맹 및 파트너 국가와 연계 및 정책 공조의 차원에서 나타나는 규범 정렬, 기술 협력, 조건부 접근 권한 부여 등 정책 집행의 확장·구현 과정을 분석한다. 실제로 최근의 미국의 AI 안보화 담론은 대통령 행정명령과 국가전략서(National Security Strategy, NSS), NSM 등의 형태로 대내외 AI전략 기조에 투영되고 있으며 최근의 AI 행동계획의 경우, AI 풀스택을 단위로 한 확산과 통제의 병행 전략을 통해 글로벌 기술 질서의 규칙과 경로를 재구성하는 수단으로 작동한다. 이러한 대외 확

20) Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*, (Oxford: Oxford University Press); OECD(2023).

21) O'Keefe et al., Cullen. 2024. "Governing Computing Power for Artificial Intelligence," Institute for Law & AI; The White House. (October 24, 2024). "Memorandum on Advancing the United States' Leadership in Artificial Intelligence."

산은 통제와 협력을 병행하는 형태로 나타나며, 미국이 AI 질서의 중심 노드를 유지하려는 전략과 밀접하게 연결되기 때문이다. 즉, 미국의 AI 안보화 담론은 국내 정책에 머무르지 않고, 글로벌 기술 질서의 규칙과 경로를 재구성하는 수단으로 작동한다. 이어지는 Ⅲ장에서는 AI 안보화를 제시한 담론-수단-집행-확산의 분석틀로 고찰함으로써 '규제 강화 vs 규제 완화'라는 이분법적 시각이나 단일 정책수단 중심의 접근이 포착하지 못한 정책 조합의 논리와 작동 메커니즘을 설명하고자 한다. 특히, 본 연구에서 '안보화'는 단순한 위기 담론의 형성이 아니라, 특정 기술이 국가 전략자산으로 재정의됨으로써 정책수단의 조합과 집행 구조를 재배열하는 기제로 개념화된다. 이에 기반하여 본고는 AI 담론이 정책 조합과 제도적 배치를 실질적으로 전환시켰는지의 여부를 기준으로 구분하여 살펴보기로 한다.

Ⅲ. 미국 AI 안보화 담론의 전환

1. AI의 안보화 담론 기반 전략자산화

미국은 이미 트럼프 1기에서부터 AI를 단순한 첨단 기술을 넘어 국가의 생존과 기술 패권에 직결된 핵심 안보 문제로 격상시켜 왔다. 바이든 행정부와 트럼프 2기에 접어들어서도 미국의 AI 안보화 인식은 보다 강화되었으며, 특히 중국과의 전략경쟁 심화와 AI의 광범위한 이중 용도적 특성에 대한 우려가 결합하면서 이를 적극적으로 육성·보호하기 위한 민관 파트너십 결속으로까지 이어지고 있는 추세이다.

그 안보화의 실천은 AI의 '전략적 자산화'이다. 사실, '전략 자산'이라는 용어를 군사적으로 특화하여 빈번하게 사용하는 한국과 달리, 미국 국방부 및 정부 기관에서는 이에 조응하는 'strategic assets'이라는 용어를 공식적으로 통용하고 있지 않다. 미국 국방부 공식 용어집(Joint Publication)에 등재된 '전략군(strategic forces)', '전략 능력(strategic capabilities)', '전략적 억지(strategic deterrent)' 등과 달리 '전략 자산(strategic assets)'은 정의된 군사용어로 보기 어려운 것이 사실이다.[22] 다만, 미국에서도 고위력·장거리 타격 무기체계나 전략적 가치가 높은 인프라 및 시스템 지칭 시, 비공식적으로 'strategic assets' 라는 표현을 언론 발표문이나 정책적 언어로 사용하고 있다.

22) '전략자산(strategic assets)'은 경제·경영 분야 용어로, 기업이나 국가의 장기 경쟁우위를 제공하는 핵심 자원 및 능력(capabilities)을 의미하며 지식재산(IP), 연구개발(R&D) 능력, 인재 풀, 브랜드 가치, 첨단기술 역량 등이 대표적이며, 전략경영 이론에서 사용되고 있다.

그러나 AI NSM 원문 '3절(Section 3),「미국의 기초 AI 역량 증진 및 확보」를 살펴보면, 'AI', 'AI 반도체', '인재', '데이터', '컴퓨팅 인프라' 등에 대해 직접적으로 'strategic assets'으로 표현하지는 않으나, '전략적 경쟁력(strategic advantage)', '안보 우선순위(national security priority)', '전략적 기습 방지(preventing strategic surprise)'등, 사실상 이에 준하는 전략적 기능을 수행하는 중요 자산으로서 의미를 담고 있음에 주목해야 한다.[23] 또한, 군사적 맥락뿐만 아니라 데이터와 같은 비물질적 자산과 반도체, 컴퓨팅 자원 등을 포함한 광범위한 의미로 사용되고 있다.[24]

이러한 사실상의 전략자산으로서 AI 안보화 담론은 트럼프 2기 행정부 출범 이후 보다 노골적이고 실행중심적인 정책 언어로 확장되었다. 2025년 1월 발표된「스타게이트 프로젝트(Stargate Project)」는 AI를 단순한 연구개발 대상이 아니라, 미국의 국가 생존과 전략적 우위를 지탱하는 '핵심 인프라(infrastructure of strategic competition)'로 규정하며, 대규모 데이터센터, 에너지 공급망, 고성능 연산 자원을 하나의 국가 전략 패키지로 통합하였다. 동 프로젝트에서 AI 컴퓨팅 인프라는 민간 투자 유치의 대상인 동시에 국가안보 차원의 보호·관리 대상물로 다뤄지며, AI 연산 역량 자체가 장기적 전략 경쟁에서의 우위를 좌우하는 결정적 요소임을 전제한 바 있다.[25]

이어 2025년 7월 발표된「미국의 AI 경쟁에서의 승리를 위한 행동계획(Winning the Race: America's AI Action Plan)」은 이러한 인식을 정책 전반으로 확장하였다. 동 계획은 AI를 '현 시대를 규정하는 기술(the defining technology of our era)'로 간주하고 AI 반도체, 컴퓨팅 파워, 인재, 데이터, 모델 개발 역량 등을 개별 기술 요소가 아닌 미국의 전략적 경쟁력을 구성하는 '상호의존적 전략 자산(interdependent strategic assets)'로 정의한다. 특히 행동계획은 국내적으로는 규제 완화와 인프라 확충을 통한 혁신 가속을, 대외적으로는 수출통제, 동맹과의 정책간 정합성 추구(alliance alignment), 표준 확산을 통해 접근을 차등화하는 이중 전략을 제시함으로써, AI를 사실상 전략자산과 동일한 방식으로 관리·배치하고 있음을 보여준다.[26]

비교적 최근인 2025년 11월 발표된「제네시스 구상 행정명령(Launching the Genesis Mission: A Long-Term Strategy for an American-Led Artificial Intelligence Ecosystem)」

23) https://strategy.data.gov/assets/docs/federal-data-strategy-practices.pdf?utm

24) 다음의 내용이 대표적이다. "AI 반도체와 컴퓨팅 자원(computing resources)은 미국의 AI 리더십 유지의 '핵심 역량(critical enablers)'이며(Section 3.1(b)), 인재 확보 실패는 미국의 전략적 우위(strategic advantage) 상실을 의미한다(Section 1(f), Section 3.1(b))" CSET(Oct. 24, 2024).

25) The White House(January 2025).

26) The White House(July 2025).

은 AI 전략자산화 담론을 단기 기술 경쟁 차원을 넘어 장기 국가전략 설계의 문제로 더욱 확장하였다. 동 전략서는 AI를 차세대 국가책략(statecraft), 안보, 산업 질서의 기반 기술로 규정하며, 반복적으로 '통합 AI 플랫폼(integrated AI platform)', '인프라(infrastructure)', '연산 기반(computational foundation)'으로 규정하고 있다. 이는 AI를 국가 역량을 구성·증폭시키는 '기반적 역량(foundational capability)'으로 해석할 수 있는 근거를 제공하는 한편, AI를 특정 무기체계나 단일 기술을 넘어, 국가 역량을 지속적으로 증폭시키는 '전략적 기반 자산(strategic foundational capability)'으로서의 위상을 부여함을 보여준다.[27]

이처럼 바이든에서 트럼프 2기 행정부의 핵심 AI 전략서 및 행정명령들은 전략자산이라는 용어를 공식적으로 채택하지 않으면서도, AI와 이를 가능하게 하는 반도체, 연산 인프라, 인재, 데이터 체계를 국가안보의 최상위 우선순위로 배치하고 있다. 이는 미국의 AI 안보화가 개념적 명명보다는 정책 설계와 자원 배분 방식을 통해 실질적으로 구현되고 있음을 보여주며, 안보화의 담론적·제도적 전환 동력으로 기능하고 있음을 시사한다.

〈표 1〉 미국 AI 안보화 담론·거버넌스의 정권별 특징

구분	트럼프 1기	바이든 행정부	트럼프 2기
안보화 담론 방향	대중 전략경쟁 하에서의 AI의 국가경쟁력·안보 우위 요소 확보	'안전·신뢰' 중심의 규범·가드레일을 통해 안보와 혁신의 균형성 추구	'혁신 가속 + 전략적 통제' 결합: 국내 연방정부 차원 규제 장벽 제거·인프라 확장, 대외 통제·진영 내 정책 정합성 확보
거버넌스 작동 방식	연방 차원의 방향 제시 + 부처별 추진 (분절적 축적)	연방 표준·요건을 통해 민간·기관 운영 관행에 내재화 시도	정책수단 패키지 재배열: 차등개입(국방·인프라=강, 상업 혁신=완화) + 확산(민간·주·동맹)
핵심 전환적 의미	경쟁 프레임의 전환을 촉발한 제도적 토대	위험관리·책임성의 제도화(가드레일)	규제 총량이 아닌 '배치 방식' 전환 (조정-차등-선별-확산)

출처: The White House. 2023. Executive Order 14110; Memorandum on AI (Oct. 24, 2024); The White House. 2025. "Winning the Race: America's AI Action Plan"; NDAA FY2025; U.S. Congress 자료를 토대로 저자 재구성.

27) "The Order repeatedly characterizes AI as an "integrated AI platform," "infrastructure," and "computational foundation," supporting an interpretation of AI as a foundational capability for national power"(Sections 1 and 3). The White House, "Launching the Genesis Mission: A Long-Term Strategy for an American-Led Artificial Intelligence Ecosystem" (November 24, 2025).

2. 전략자산 담론의 제도화: 군사·외교·경제 안보의 결합

앞서 살펴본 바와 같이, 미국의 AI 안보화 담론은 AI를 단순한 기술 혁신 수단이 아닌 국가 경쟁력과 안보 우위를 좌우하는 전략적 자산으로 재정의하는 데에서 출발한다. 그러나 이러한 담론은 선언적 차원에 머무르지 않고, 구체적인 제도와 정책 수단을 통해 군사안보, 외교안보, 경제안보 영역을 관통하는 통합적 거버넌스 구조로 제도화되어 왔다는 점에서 그 특징이 보다 분명하게 드러난다. 즉, 미국의 AI 전략은 개별 안보 영역의 병렬적 대응이 아니라, AI를 매개로 한 안보 영역 간 결합으로 작동하고 있다.

첫째, 군사안보 차원에서의 제도화는 트럼프 2기 행정부의 AI 전략자산 담론을 구체적 실행 정책으로 전환하는 핵심 영역으로 나타난다. 2025 회계연도 국방수권법(National Defense Authorization Act, NDAA for FY2025)은 이전 NDAA에 비해 AI 기술의 실전 운용성과 통합성을 강조함으로써 AI를 단순한 연구개발이나 보조 시스템이 아니라, 전력과 전투 체계 전반을 재편하는 통합적 전투역량의 요소로 제도화 되었다. 특히 개정된 NDAA 2025의 AI 및 자동화 전력화 관련 조항(Sec. 4201-4210)은 AI 기반 다영역 작전능력(Multi-Domain Operations) 강화, △지휘·통제·통신·컴퓨터·정보·감시·정찰(C4ISR) 체계의 AI 통합, △자율 무인 시스템 전력화, △AI 기반 전장 의사결정 지원 시스템과 △AI 기반 사이버·전자전 역량 확보 등을 명시하며, AI 기술을 개별 장비나 센서 수준이 아니라 시스템·전력 체계 전체의 전략적 구성 요소(strategic component)로 재구성하고 있는 것이 특징이다.[28] 또한, AI 기반 전력의 법적·윤리적 활용을 위한 제도 구축 및 가이드라인 수립이 NDAA 입법 과정을 통해 병행되고 있어, AI가 군사 전략적 자산으로 간주되고, 그 활용 체계와 책임 범위가 제도화 단계로 진입하고 있음을 보여준다. 트럼프 2기 행정부는 이러한 법제화 흐름을 기반으로, 미 국방부(DOD)와 에너지부(DOE) 간의 연방 부처 간 연구·운용 협력을 강화하고 있다. 이는 전장 AI 체계가 단일 부처의 기술 도입을 넘어 국가 전체의 전력 생산·통합·운용 역량으로 확장되어야 한다는 전략자산 담론과 맞닿아 있다. 결과적으로 2025년 NDAA는 AI가 군사 안보의 보조적 역할을 넘어, 전력 구조 자체를 재편하는 전략적 핵심 구성 요소(strategic foundational capability)로 제도화되는 결정적 전환점으로 평가된다.[29]

둘째, 경제안보 측면에서는 AI를 기술·경제적 혁신 가치 창출을 위한 원동력이라는 인식 하에 기술 경쟁력 확보를 위한 다수의 법안과 행정명령이 공포되었고, 트럼프 행정부

28) U.S. Congress, 2025. “National Defense Authorization Act for Fiscal Year 2025” (Washington, DC: U.S. Government Publishing Office).
29) The White House(July 2025).

2기 이후 더욱 강화되었다. '미국의 AI 리더십에 대한 장애물 제거 행정명령(EO 14179, 2025)', '스타게이트 프로젝트(2025)' 및 'AI 행동계획(2025)'에 나타난 주요 정책 축은 공통적으로 AI에 기반한 미국 경제·안보 경쟁력 증진, AI 인프라와 에너지 자립, AI 산업 일자리 증대, AI 연구개발 및 혁신기반 조성 등의 실천 내용을 담고 있다. 특히, 경쟁국의 기술적 추격을 차단하는 정책 수단의 결합에 초점을 두고 있으며, 반도체 및 고성능 연산자원에 대한 수출 통제, 외국인 투자 심사 강화, 연구안보 제도, 데이터 접근 및 관리 기준은 모두 AI 전략자산화를 뒷받침하는 경제안보적 장치로 기능한다. 연산 인프라, 데이터, 인재를 하나의 풀스택 차원에서 관리하려는 접근은, AI 경쟁을 개별 산업 경쟁이 아닌 국가 차원의 총력적 경쟁 구도로 인식하고 있음을 보여준다.[30] 실제로 트럼프 2기 행정부에서는 AI 기술, 사회, 제도의 전주기 공급망을 국내 뿐만 아니라 동맹과 우호국에도 적용함으로써 미국이 주도하는 AI 공급망에 대한 안정적 관리 목표를 달성하고자 하고 있다.

셋째, 외교안보 측면에서의 제도화는 AI 전략자산화 담론이 동맹 및 파트너 국가와의 정책 공조를 통해 대외적으로 확장되는 방식으로 나타난다. AI 행동계획은 AI를 외교·안보·통상 정책을 관통하는 핵심 전략 기술로 규정하고, 동맹국들과의 주요 정책에 있어 '정합성(coherence)'을 확보하는 방향으로 AI 거버넌스를 설계하고 있다. 이 과정에서 AI 협력은 단순한 기술 교류 차원을 넘어, 연산자원 접근, 반도체 공급망, 표준 및 안전성 평가 체계 수용을 포함하는 '조건부 접근 구조(conditional access architecture)'로 제도화된다. 이는 AI 기술의 확산과 통제를 병행함으로써, 동맹국을 미국 주도의 기술 생태계에 구조적으로 편입시키려는 외교안보 전략의 일환으로 이해할 수 있다.[31] 특히, Pillar Ⅲ에 나타난 'AI 국제외교 및 안보 선도'를 위한 실천방안과 미국식 풀스택을 확산수용시키기 위한 관세부과 등의 조항에서 볼 수 있듯이 동맹국과 우호국, 나아가 전략적 수출통제를 위한 단합 등 글로벌 차원에서의 미국 안보 논리의 확장성을 고려한 매우 적극적인 조치들을 망라하고 있다.

대외적으로는 국무부·상무부(표준·수출통제), NIST(측정·표준·평가), 국방부·정보공동체(국가안보 적용), DHS(핵심기반시설), 에너지부(전력·연산 인프라)가 역할을 분담하며, 유엔·G7·OECD·NATO·TTC·IPEF 등 다자틀에서 '미국 기준의 글로벌 보호조치'와의 정합성을 모색하고 있다. 이를 통해 민주주의 진영이 함께 권위주의 규범의 글로벌 확산을 억제한다는 구상을 전개하고 있다. 특히 2025년 「AI 행동계획」은 동맹국 대상의 미국

30) Miller(2022); OECD, AI, Data and Economic Security (Paris: OECD Publishing, 2024).
31) The White House(July, 2025).

산 AI 기술체계 풀스택 수출(하드웨어-모델-표준)과, 고성능 연산자원·반도체에 대한 집행력 있는 수출통제를 동시에 추진하며, UN·ITU 등 거버넌스 기구 내 중국 영향력에 대한 공동대응에 나설 것을 명시하고 있다. G7 히로시마 'AI 행동강령'의 OECD 관리, NATO의 군사용 AI 원칙, 한국-네덜란드의 '군사분야의 책임있는 AI(REAIM)' 등은 미국 주도의 규범 아키텍처를 글로벌 차원의 표준으로 제도화하려는 시도를 과정을 보여준다.[32]

이처럼 AI를 '전략적 기반 역량'으로 규정하는 담론의 변화는 연산 자원, 반도체, 인재, 데이터와 같은 AI 생태계의 요소들을 단순한 산업 경쟁 자원이 아니라 국가안보 우선순위에 편입되어야 할 관리 대상으로 재정의한다. 그리고 이러한 재정의는 위험 인식의 확산에 머무르지 않고, 예산 배분 구조의 재조정, 연방 차원의 전략 조정 권한 강화, 수출통제 및 인프라 통합과 같은 제도적 장치의 설계로 이어진다. 특히 NDAA 개정, 고성능 반도체에 대한 통제 강화, 연산 인프라의 연방 통합 관리와 같은 조치는 기술 경쟁의 연속선상에 있는 산업정책과 달리, AI 생태계 전체를 국가 전략자산의 묶음으로 관리하려는 거버넌스적 전환을 보여준다 할 수 있다. 즉, 미국의 AI 안보화 담론은 상징적 선언을 넘어 정책수단의 조합과 집행 구조를 재배열하는 정당화 기제로 기능하게 되는 것이다.

특히, 미국의 AI 전략자산 담론은 군사·외교·경제 안보 영역에서 각각 분절적으로 제도화되는 것이 아니라, 상호 연계된 정책 조합의 형태로 작동한다. 군사 영역에서는 전력화와 작전 통합을 통해, 외교 영역에서는 동맹과의 정합성을 통해, 경제 영역에서는 공급망과 인프라 통제를 통해 AI의 전략적 가치를 제도적으로 고정시키는 것이다. 이러한 결합 구조는 AI 안보화가 단순히 규제의 강화나 완화의 문제가 아니라, 국가 역량을 조직하고 배치하는 거버넌스 방식의 재구성 차원에서 추진되고 있음을 보여준다 할 수 있다.[33]

Ⅳ. 미국의 AI 안보 거버넌스의 재구성

1. AI 안보화 담론의 거버넌스화: 연방 전략 통제의 체계화

미국 AI 안보 거버넌스의 출발은 2022년 「AI 권리장전(Blueprint for an AI Bill of

32) The White House(July 2025).

33) Farrell and Abraham(2023); Schaake, Marietje. 2024. *The Tech Coup: How to Save Democracy from Silicon Valley* (Princeton, NJ: Princeton University Press).

Rights)」에서 제시된 원칙들에 기반하였으며, 2023년 10월, 바이든 행정부의 안전하고 신뢰할 수 있는 AI 활용 촉진을 위한 행정명령을 기점으로 본격화되었다. 여기에는 AI 관련 표준을 마련하고 위험을 보고하며, 연방 운영 전반에 거버넌스를 적용하는 동시에, 특히 강력한 AI 시스템을 개발하는 민간 기업들에게 명확한 기대와 책임을 부여하는 것을 포함한다. 관련 원칙에는 안전성, 효과성, 차별 방지, 데이터 프라이버시, 투명성, 인간 감독 등이 제시된 바 있으며 AI가 공익에 기여하면서 위험을 최소화하는 방향으로 발전을 유도해왔다.[34]

그러나 넓은 의미에서 미국의 AI 안보 거버넌스는 「AI 권리장전」이나 바이든 행정부의 안전 AI 행정명령에만 국한되지 않는다. 이는 2019년 이후 제정된 「국방수권법(National Defense Authorization Act)」, AI 관련 국가안보 각서, 그리고 여러 행정명령들까지 포괄하는 확장된 정책 체계로 이해될 수 있다. 그 이유는 첫째, AI가 군사·안보적 차원에서 잠재하는 위협과 기회를 동시에 내포하기 때문에, 국방 차원에서의 예산 편성과 법률적 뒷받침이 필수적이었기 때문이다. 둘째, AI는 단순히 기술 혁신이 아니라 사이버 보안, 핵심 인프라 보호, 전략적 경쟁 등 국가안보 전반에 직결되는 요소로 인식되었고, 따라서 백악관과 국가안보회의(NSC)를 중심으로 한 안보 각서가 이를 제도화해왔다. 셋째, AI 기술이 빠르게 진화함에 따라 기존 법·제도 틀만으로는 대응이 어려웠기 때문에, 대통령 행정명령을 통한 신속한 정책 수립과 조정이 지속적으로 이루어졌다. 이러한 이유로 미국 AI 안보 거버넌스는 특정 문서나 단일 정책이 아니라, 법률·각서·행정명령 등 다층적 정책수단이 복합적으로 작동하는 총체적 구조로 자리 잡아왔다.

트럼프 2기 행정부에서 AI 안보 거버넌스가 본격적으로 형성된 과정은 단일한 규제 법안이나 중앙집중형 통제기관의 출현을 통해 이루어지기보다는, 행정명령-전략 문서-입법 조치가 동일한 통치 기능을 수행하도록 수직화되는 과정을 통해 가시화되었다. 이 과정에서 AI는 개별 정책 영역에서 분절적으로 관리되는 대상이 아니라, 연방 차원의 전략적 조정 대상으로 재구성되었다는 점에서 기존의 기술 거버넌스 접근과 구별된다.[35]

우선, AI 행동계획과 제네시스 구상 행정명령은 형식상 산업·과학·연구개발 정책 문서의 외형을 띠고 있으나, 그 내용에서는 AI를 특정 응용 기술이나 산업 분야에 한정하지 않고, 연산 자원, 데이터, 모델, 인재, 연구 인프라를 포괄하는 조정 대상으로 설정하고

34) The White House, (October 2022). "BLUEPRINT FOR AN AI BILL OF RIGHTS: Making Autonomous Systems Work for the American People" https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (검색일: 2025.5.23.).

35) Balzacq, Thierry. 2011. *Securitization Theory: How Security Problems Emerge and Dissolve*, (London: Routledge).

있다. 다시 말해, 이들 문서는 AI 정책의 실행 세부를 규정하기보다는, 이후 입법과 집행 단계에서 AI를 어떻게 묶고 관리할 것인가에 대한 기준점을 설정하는 역할을 담당한다. 이러한 기준점은 NDAA 2025를 통해 제도적으로 고정되었는데, 동 회계문서는 AI를 개별 무기체계나 연구개발 프로그램 단위로 규율하지 않고, AI가 통합된 전력 구조 전체를 연방 안보 우선순위에 따라 배치·조정하도록 규정한다. 특히 AI 기반 지휘·통제·통신·컴퓨터·정보·감시·정찰(C4ISR), 자율 무인체계, 사이버·전자전 역량은 개별 사업 항목이 아니라, 상호 연동된 전력 묶음으로 관리되며, 이 과정에서 AI는 특정 부처의 기술 도입 과제가 아니라 연방 정부가 배분하고 조정해야 할 이른바 '전략적 역량 묶음(capability bundle)'으로 재정의된다.[36] 이는 AI 안보 거버넌스가 단순한 규제 강화 기조가 아닌 국가의 우선순위 설정과 자원 배분의 구조를 통해 구현되고 있음을 보여준다.

이러한 통합적 관리 체계는 집행 단계에서도 확인된다. 제네시스 구상은 에너지부(DOE)를 중심으로 고성능 연산 자원, 연방 데이터 자산, 연구 인프라를 통합하는 '미국 과학·안보 플랫폼(American Science and Security Platform)' 구축을 명시함으로써, AI를 연방 차원의 집행 인프라로 구체화하고 있다. 동시에 백악관 OSTP와 NSTC는 부처 간 조정 메커니즘을 통해 AI 관련 예산, 연구 과제, 인력 프로그램의 중복을 조정하고 상호 운용성 또한 확보하고 있다.[37] 이는 AI 거버넌스가 단일 규제기관의 파편적 통제보다는, 전략 문서-입법-집행 체계가 기능적으로 결합된 구조로 설계되고 있음을 보여준다. 결과적으로 트럼프 2기 행정부에서의 AI 안보화는 새로운 규제 틀의 도입보다는, AI를 조정 가능한 국가 역량으로 형성하는 거버넌스 구조의 출현이라는 방식으로 전개되고 있다. 즉, AI를 '통제해야 할 위험'으로만 다루는 접근과 달리, AI를 연방 차원의 전략적 자원으로 조직·배치하는 통치 방식의 전환을 의미한다.[38]

2. 연방 AI 안보 거버넌스의 조정·차등·선택적 개입 메커니즘

앞서 살펴본 바와 같이 트럼프 2기 행정부의 AI 안보 거버넌스는 안보 담론의 제도화-입법-집행 체계의 결합을 통해 체계화되었다. 그러나 이러한 거버넌스의 핵심은 단순히 통제 주체가 명확해졌다는 데에 있지 않다. 주목해야 할 점은, AI를 둘러싼 다양한 정책 수단들이 동일한 규율 방식으로 관리되지 않고, 위험 수준과 전략적 중요도에 따라 차등

36) U.S. Congress, 2025. National Defense Authorization Act for Fiscal Year 2025 (Washington, DC: U.S. Government Publishing Office).

37) The White House(Nov. 24, 2025),

38) Farrell and Newman(2023).

적으로 배치·운영되고 있다는 점이다. 이는 미국의 AI 안보 거버넌스가 일괄적 규제 모델이 아니라, 조정과 차등, 선택적 개입을 결합한 작동 논리를 갖고 있음을 시사한다.

우선, 트럼프 2기 행정부의 AI 안보 거버넌스는 단일 규제기관이나 포괄적 기본법을 중심으로 구축되지 않았다. 대신 백악관 OSTP와 NSTC를 중심으로 국방부(DOD), 에너지부(DOE), 상무부(DOC) 등 기존 부처들의 기능을 재배치하고 상호 연동시키는 조정 중심 구조를 채택하였다. AI 행동계획과과 제네시스 구상은 이러한 조정의 기준점을 제공하는 전략 지침으로 기능하며, 예산·연구개발·인프라·인력 정책을 단일한 연방 전략 논리 하에 결합시키고 있다. 이를 통해AI는 개별 정책 영역의 대상이 아니라, 연방 차원에서 배분·관리되는 역량의 집합체로 관리되는 것이다.

둘째, 이러한 조정 구조는 규제의 차등 적용이라는 방식으로 구체화된다. 트럼프 2기 행정부의 AI 안보 거버넌스는 모든 AI 시스템에 동일한 규제 강도를 적용하지 않으며, 군사·안보적 파급력이 클수록 연방 차원의 직접 개입과 통제가 강화되는 반면, 민간 혁신과 산업 경쟁력과 직결되는 영역에서는 규제 완화와 자율성이 확대되고 있다. 국방·정보·핵심 인프라와 연계된 AI 시스템은 NDAA와 국가안보 각서를 통해 엄격히 관리되는 반면, 상업적 AI 연구개발과 응용 영역에서는 규제 장벽 제거, 인프라 투자, 인재 유입 촉진이 강조된다. 이는 AI 안보화가 규제의 총량을 확대하는 방식이 아니라, 안보적 중요도에 따라 개입 강도를 재배치하는 방식으로 작동하고 있음을 보여준다.[39]

셋째, 이러한 차등적 거버넌스는 국내와 대외 영역에서 서로 다른 방식으로 작동하는 선택적 개입 논리로 확장된다. 국내적으로는 연산 인프라 확충과 데이터 접근성 제고를 통해 민간 주도의 혁신을 가속하는 한편, 대외적으로는 수출통제, 표준 설정, '동맹과의 정책적 정합성(coherence with allies)'을 통해 접근을 제한하는 구조가 병행된다. 특히, 동맹과의 정책 정합성은 단순한 협력 담론이 아니라, 미국이 설정한 기준을 수용하는 국가에 한해 AI 풀스택 접근을 허용하는 '조건부 개방(conditional access)'의 메커니즘으로 기능한다. 이로써 AI 거버넌스는 국내에서는 촉진 장치로, 대외적으로는 통제 장치로 상이하게 배치된다.[40]

이러한 작동 논리는 최근 트럼프 2기 행정부의 대중국 반도체 정책에서 더욱 선명하게 드러난다. 2025년 12월, 트럼프 대통령은 엔비디아의 AI 가속칩 H200(이전 세대의 준플래그쉽 AI 칩)을 정부 승인 고객에 한해 조건부로 중국에 수출하는 정책 전환을 발표하였고, 이후 미 상무부 산업안보국(BIS)은 해당 조치를 '거부 추정' 방식(presumption of

39) U.S. Congress(2025).
40) The White House(July 2025).

denial: 원칙적으로는 불허하지만, 예외적으로만 허가를 검토·승인하는 방식)에서 개별 심사 체계로 전환하였다.[41] 이 같은 조치는 최첨단 'Blackwell' 계열 칩은 계속 봉쇄하면서도, 한 세대 이전의 연산 자원은 전략적 조건 하에 접근을 허용함으로써 중국 내 미국 기술 의존도를 유지하려는 계산된 선택으로 해석된다. 즉, 봉쇄와 개방을 병행하며 경쟁국의 기술 종속의 경로를 관리하려는 전략적 개입이 구체적 정책 사례로 구현된 것이다.[42]

결과적으로 트럼프 2기 행정부의 AI 안보 거버넌스는 규제 강화와 규제 완화라는 이분법으로 설명되기 어렵다. 오히려 이는 AI를 국가 역량으로 조직하고 배치하기 위해 조정과 차등, 선별을 결합한 정교한 거버넌스로 메커니즘으로 이해되어야 한다. 이러한 거버넌스 방식은 AI를 통제해야 할 위험으로만 다루는 접근을 넘어, AI를 통해 국가 경쟁력과 전략적 우위를 지속적으로 증폭시키려는 안보화의 정교한 구현을 보여주는 핵심적 특징이라 할 수 있다.[43]

3. 집행과 확산의 다층화: 연방 조정에서 국내·외 규범 전이로

트럼프 2기 행정부의 AI 안보 거버넌스는 특정 규제 기관의 권한 집중이나 단일한 규율 모델을 통해 구현되기보다는, 집행과 확산이 결합된 다층적 메커니즘을 통해 실행력을 확보하고 있다. 이러한 집행 구조는 우선 국내적 확산을 통해 민간 기업, 주정부, 학계와 연구기관으로 파급된다. 실제로 연방 차원의 포괄적 AI 기본법이 부재한 상황에서, 미국의 AI 안보 거버넌스는 정부 조달 기준, 연구 보안 요건, 연방 자금 지원 조건, 보안 가이드라인과 같은 간접적 수단을 통해 민간 부문과 연구 생태계에 영향을 미치고 있다. 이는 민간의 혁신 역량을 억제하기보다는, 연방이 설정한 최소한의 안전·보안 기준을 운영 관행의 형태로 내재화시키는 방식인 것이다.

입법부인 의회에서는 행정부의 규제 완화 기조와는 별개로 적대국의 AI 기술 협력 방지에 초점을 맞춘 법안 발의가 지속되었다. 대표적으로, '적대국 간 불법 협력 차단법(Defending International Security by Restricting Unlawful Partnerships and Tactics Act: DISRUPT Act)'은 국무부, 국방부, 상무부 등 다수의 연방 기관들이 중국, 러시아 등 적대국 간의 AI 기술 제휴 및 전술을 집단적으로 방해하고 저지하기 위한 태스크 포

41) U.S. Department of Commerce, (December 2025). Bureau of Industry and Security, "Export Licensing Policy Update on Advanced AI Chips"

42) 최재필, "트럼프가 중국의 엔비디아 칩 판매를 허용하면서 중국을 지배하는 방법" 「Infoloop」, (2025. 12. 27). https://infoloop.co.kr/opinion/article/56397/ (검색일: 2025.12.30.).

43) Farrell and Newman(2025).

스 및 전략을 수립하도록 의무화하고 있다. 이는 AI 기술이 군사적 능력에 미치는 영향을 평가하고, AI 안보를 전통적인 국방 및 정보 영역에서 명시적인 법제적 과제로 포괄한다. 전반적으로 트럼프 2기 행정부 이후 미국의 AI 안보는 기술 개발의 자유를 최대한 보장하면서도, 동시에 국가 간의 기술 패권 경쟁이라는 관점에서 수출 통제, 국제 표준화, 국방 AI 역량 강화라는 세 가지 법제적 방어선을 구축하는 방향으로 전개되고 있다.

이 같은 기조에서 추진된 세부 법안으로는 지난 2025년 6월 미국의 AI 시스템을 외국의 사이버 위협으로부터 보호하기 위해 발의된 「첨단 AI 보안 대비법안(Advanced AI Security Readiness Act, H.R.3919)」('25.6.11.)이 있다.[44] 이는 중국의 딥시크 모델(Deepseek R1)이 오픈 AI의 챗GPT 기술을 도용했다는 지적이 제기됨에 따라 미국 내에서 적대국의 AI 기술 탈취 우려에 대한 초당적 공감대가 형성되었기 때문이다. 동 법안은 국가안보국으로 하여금 '23년 9월 신설된 국가안보국 산하의 AI 보안센터(Artificial Intelligence Security Center, AISC)에 'AI 보안 플레이북(AI Security Playbook)' 개발 의무를 부과하여 연방기관 뿐만 아니라 민간 부문에서도 활용할 수 있는 위협 탐지 및 대응 지침을 제공한 바 있다.[45] 즉, 미국은 AI 리더십을 단순한 기술 경쟁력이 아닌 국가 안보 자산으로 취급하고 있다는 점이 재확인되었으며, 동 법안을 통해 미국이 소유한 AI 기술 및 인프라 등에 대한 글로벌 공급망 관리가 강화될 것으로 예상되고 있다.

연방 차원의 규제 완화 기조와 주 차원의 안전 규제 강화는 표면적으로는 '규제 충돌'처럼 보일 수 있다. 실제로 AI 규제의 연방 주도를 둘러싼 논쟁은 각각의 권한의 경계를 불안정하게 만들며, 기업 입장에서도 규제 파편화에 따른 비용을 증가시킬 수 있다. 그러나 중요한 것은 이러한 이질성이 곧바로 거버넌스의 충돌로 이어지지 않는다는 점이다. 트럼프 2기 행정부의 혁신 장려 기조가 연방 차원에서 시장·인프라·투자·인재에 대한 촉진 장치를 강화하는 동안, 주정부는 고위험 영역을 중심으로 제한적 규범을 실험·정착시키는 방식으로 위험 관리 기능을 분담해왔다.[46] 즉, 규제의 완화와 강화의 동시성은 단순한 충돌이라기보다, 위험 수준과 정책 목적에 따라 규율 강도를 분화시키는 다층 거버

44) The Select Committee on the CCP, "Defending American AI: Moolenaar, Bipartisan Group Introduce Advanced AI Security Readiness Act" (June 12, 2025), https://selectcommitteeontheccp.house.gov/media/press-releases/defending-american-ai-moolenaar-bipartisan-group-introduce-advanced-ai (검색일: 2025.10.3.).

45) 한국인터넷진흥원. 2025. "해외입법동향: 미국 하원, 「첨단 AI 보안 대비법안」 발의(2025.6.11.)" (2025년 7월).

46) House Judiciary Democrats. (Sep. 18, 2025). "At Hearing on Federal Preemption of State AI Laws, Subcommittee Democrats Underscore Need for Guardrails to Protect Americans While Promoting Innovation"

넌스의 귀결로 이해될 필요가 있다. 이러한 관점에서 주정부의 고위험 AI 규제는 연방 차원의 포괄 규제 부재를 보완하는 동시에, 향후 연방 조달·표준·기업 준수 체계에 적용될 수 있는 '최소 기준'의 고려사항으로도 기능한다. 즉, RAISE 법안은 연방-주 간 규율의 '대체재'라기보다, 고위험 영역부터 규범을 정교화하여 적용시키는 보완적 근거가 되는 것이다.

또한, 주정부 차원에서도 AI 모델의 안전과 보안 체계에 대한 투명성, 위험관리 의무를 부과한 법안이 통과된 사례가 존재한다. 뉴욕주 의회는 2025년 6월 13일 「RAISE (Responsible Artificial Intelligence Safety and Education」 법안을 가결하였는데, 해당 법안은 100명 이상 인명 피해 또는 10억 달러 이상의 재산 피해를 초래할 수 있는 AI 위험에 대하여 법적 안전장치를 마련해야 함을 명시하고 있다. 즉, 일정 규모 이상의 AI 모델 개발사로 하여금 안전 및 보안 체계에 대한 투명성 보고, 위험 발생 시 즉각 보고 등을 의무로 정한 것이다.[47] 개발사는 모델 배포 전 안전 및 보안 프로토콜을 구현하고 게시할 의무를 지니며, 치명적 위해 위험 발생 시 72시간 이내에 법무장관 및 국토안보국에 의무 보고해야 한다. 이는 AI의 잠재적 재앙적 위험을 국가 안보의 시각에서 다루려는 시도로 해석된다. 다만, 논란이 컸던 '킬 스위치(kill switch)' 의무를 삭제하고 적용 대상을 최상위 모델로 한정하여, 기술 혁신을 저해한다는 빅테크 기업의 반발을 최소화하는 다소 유연한 안보 규제 모델을 제시한 것이 특징이다.[48] 또한, 고위험 AI 모델을 대상으로한 주 단위 규제는 연방 차원의 규제 공백을 보완하는 동시에, 위험 수준이 높은 영역부터 선별적으로 규범을 정착시키는 실험적 상향 규율의 성격을 갖는다. 이는 AI 안보 거버넌스가 연방에서 일괄적으로 하달되는 구조가 아니라, 연방-주-민간 행위자 간 상호작용 속에서 점진적으로 확산되고 있음을 시사한다.[49]

또한, 미 의회 및 주 차원의 AI 관련 입법 흐름을 보면, 통과된 법안과 계류·미통과 법안 사이에 나타나는 차이를 발견할 수 있다. 예를들어, NDAA FY2025와 같이 기존 국가 안보 및 예산 체계에 AI 조항을 흡수하는 방식은 비교적 안정적으로 법제화되고 있다.[50]

47) 법률신문. 2025. "미국 RAISE 법안 분석: AI 안전 규제의 확산 가능성과 기업 대응 전략" (2025.6.26). https://www.lawtimes.co.kr/LawFirm-NewsLetter/209219 (검색일: 2025.10.12.).

48) The New York State Senate. 2025. "Assembly Bill A6453A, 'Relates to the training and use of artificial intelligence frontier models' (March 5, 2025), https://www.nysenate.gov/ legislation/bills/2025/A6453 /amendment/A (검색일: 2025.10.18.).

49) 뉴욕주 의회에서 2025년 통과된 고위험 AI 모델 규제 법안인 RAISE Act'는 초거대 AI 프론티어 모델을 대상으로 안전 및 보안 체계 구축, 위험 관리 프로토콜 공개, 중대한 위해 발생 시 72시간 이내 주정부 보고 의무 등을 규정하고 있다. The New York State Senate, Assembly Bill A6453A, "Relates to the training and use of artificial intelligence frontier models" (March 5, 2025),

50) U.S. Congress, National Defense Authorization Act for Fiscal Year 2025 (Public Law P.L. 118-159),

이는 AI 안보화 담론이 '상시적 운영 규칙'의 형태로 제도권에 고정되고 있음을 보여준다. 반면, 연방 차원의 포괄적 AI 규제 법안, 예컨대 「첨단 AI 보안 대비법안(Advanced AI Security Readiness Act, H.R.3919)」과 같은 입법안은 하원 발의 이후에도 연방정부와 주정부 간 규제의 우선 문제, '프론티어·고위험 AI' 범위 설정, 기업 책임과 보고의무 수준, 집행기관 권한 배분 등을 둘러싼 쟁점으로 인해 계류되는 경향이 있다.[51] 흥미로운 점은, 연방 차원에서의 교착과 달리 뉴욕주의 「RAISE Act」와 같이 고위험 AI를 대상으로 한 주 단위 규제는 비교적 실험적·선별적 방식으로 도입되고 있다는 점이다. 이는 연방의 포괄 규제 공백을 주 차원에서 부분적으로 보완하는 동시에, 위험이 높은 영역부터 상향 규율을 정착시키는 경로를 보다 빈번히 형성할 것임을 시사한다.

이와 같은 집행 및 확산의 다층적 구조는 〈그림 1〉에 제시된 트럼프 2기 행정부의 AI 안보 거버넌스 추진체계에서 종합적으로 확인된다. 상단의 연방 법·정책 프레임워크(Federal Legal & Policy Framework)는 NDAA 기반 군사·안보 법제, 상무부(BIS)의 수출통제, 국무부의 국제 표준 및 동맹 협력, 에너지부의 안전한 AI 연구 인프라, 백악관과 OSTP의 정책 조정 기능을 통해 AI를 연방 차원의 전략적 관리 대상으로 묶어내는 중앙 조정 축을 형성한다. 중간 층위의 주(州) 차원의 규제 대응은 고위험 AI 모델을 중심으로 한 주정부 입법을 통해, 연방 기준이 국내적으로 확산되는 경로를 보여준다. 하단의 모니터링 및 통제 메커니즘은 모델 감사, 접근 통제, 위협 탐지, 보안 자동화와 같은 집행 기술을 통해 이러한 기준이 실제 운영 단계에서 작동하도록 만드는 장치다. 이들 메커니즘은 대외 통제 수단이기 이전에, 연방 기준이 민간 기업과 연구기관, 주정부 시스템으로 전이되는 공통 운영 규칙으로 기능한다.

종합하면, 트럼프 2기 행정부의 AI 안보 거버넌스는 집행과 확산을 통해 연방 조정–국내 확산–대외 투사가 순환적으로 결합된 구조를 형성하고 있다. 이는 AI 안보화가 규제의 강화나 완화라는 단선적 선택의 문제가 아니라, 위험과 혁신을 분리 관리하면서 국가 역량을 조직·배치하는 거버넌스 기술로의 전환임을 보여준다. 이러한 구조적 특징은 미국식 AI 안보 거버넌스가 향후 글로벌 기술 질서에서 지속적인 영향력을 행사할 수 있는 핵심 기반으로 작동할 가능성을 시사한다.

2024/2025.

51) 한국인터넷진흥원, "해외입법동향: 미국 하원, 「첨단 AI 보안 대비법안(Advanced AI Security Readiness Act, H.R.3919)」 발의(2025.6.11.)" (2025년 7월).

출처: 저자 작성

〈그림 2〉 트럼프 2기 행정부의 AI 안보 거버넌스 추진체계

4. AI 안보화의 법제화를 통한 거버넌스 구조의 기능적 확립

전술한 AI 거버넌스가 일시적 정책 조합에 그치지 않고 지속성을 갖기 위해서는, 정책 조정과 집행을 가능하게 하는 법제적 기반이 필수적이다. 이 점에서 미국의 AI 안보화는 새로운 포괄 법률의 제정이나 단일 규제 기관의 설치가 아니라, 기존 국가안보 법·제도 체계 내에 AI를 기능별로 흡수·고정하는 방식의 법제화를 선택하고 있다는 점에서 주목할 필요가 있다.

미국의 AI 안보화 법제는 AI를 독립적인 규율 대상으로 설정하기보다는, 국가안보시스템(NSS)이 이미 규정하고 있는 임무·권한·지휘 체계에 이를 연계시키는 방식으로 전개된다. 다시 말해, AI는 법령 이전에 군사 지휘통제, 정보 수집·분석, 사이버 방어, 핵심 인프라 보호, 외교·동맹 관리 등 기존 NSS 기능을 수행하는 과정에서 보유·활용되어야할 요소로 간주되고 있다. 이러한 접근은 미국의 AI 안보화가 단순한 규제적 수단으로서가 아니라 국가안보 기능 체계 내에서 재구성되고 있음을 명확히 보여주고 있다.

〈표 2〉는 이러한 법제화 방식의 핵심적 특징을 잘 보여준다. 표에 제시된 바와 같이, 국방부는 AI를 지휘통제(C2), 전장관리, ISR, 무기체계 연계망의 핵심 구성 요소로 흡수하고 있으며, 정보공동체는 대외·군사 정보수집과 분석, 위성·지리정보 네트워크의 효율성을 증폭시키는 수단으로 활용하고 있다. 법무부와 국토안보부는 테러·사이버 위협 대응과 핵심 기반시설 보호 과정에서 AI를 위험 탐지 및 분류 체계에 통합하고 있으며, 에

너지부는 핵 관련 시설과 ICS/SCADA 체계의 통신·제어 영역에서 AI를 핵심 보조 역량으로 배치하고 있다. 국무부 역시 외교 분류망과 동맹국 간 위기 대응 채널에서 AI 활용 가능성을 제도적으로 열어두고 있다.

이러한 기능별 배치는 AI가 단일한 '안보 기술'로 통제되는 것이 아니라, NSS 전반에 걸쳐 분산적으로 내재화되고 있음을 의미한다. 다시 말해, 미국의 AI 안보화는 〈표 2〉와 같이 기존 안보 법·제도와 조직의 임무 체계 속에 AI의 활용 역량 요소를 내재화함으로써 각 기능이 스스로 AI를 운용·통제하도록 만드는 구조를 취하고 있다. 이는 AI 안보 거버넌스가 규제 중심 모델로 수렴하기보다, 연결과 조정, 책임 분산을 전제로 한 제도적 고정의 형태로 진화하고 있음을 보여준다.

〈표 2〉 미국 주요 정부기관 별 AI 안보정책 기조 및 법제적 역할

정부기관	주요 AI 안보 법제적 역할		핵심 정책 목표 및 기조
국무부 (DOS)	국제 표준화 주도	AI 안전, 윤리 관련 국제 협약 및 표준 구축 주도	혁신된 AI 기술을 동맹국에 확산하여 지정학적 영향력 확대 및 적대국 견제를 위한 외교적·법제적 기반 마련
	기술 전용 방지	적대국과의 AI 기술 제휴 및 오용을 막기 위한 외교 조치 주도	
상무부 (DOC)	수출 통제 강화 (BIS)	첨단 반도체 및 AI 학습용 소프트웨어 등 이중 용도 기술에 대한 수출 규정 실행 및 강화	기술 유출 방지와 더불어, 혁신 가속화에 중점을 둔 AI 위험 관리 프레임워크(AI RMF)의 재설정(NIST 주도)
	AI 표준 및 평가 (NIST)	AI 위험 관리 프레임워크(AI RMF) 수정 및 워터마크 기술 표준 개발	
국방부 (DOD)	군사 AI 윤리 및 안전성 검증	군사용 AI 시스템의 윤리적 활용 원칙 및 취약성 발견 프로그램 제도화	AI를 활용한 국가 안보 역량 극대화. AI 기반 워 플래닝 도구의 안전한 디지털화 및 배치를 위한 법적 가이드라인 수립
	국방 AI R&D 투자 촉진	국방수권법(NDAA) 등을 통한 AI 연구 개발 총괄 책임자 임명 및 투자 지원	
에너지부 (DOE)	컴퓨팅 인프라 보안 지원	고성능 컴퓨팅(HPC) 인프라의 물리적·사이버 보안 강화 및 AI 연구 활용	국가 중요 인프라 보호 및 AI 연구 개발을 위한 첨단 컴퓨팅 자원 확보 및 안전성 관리
	핵심 인프라 방어	AI를 이용한 에너지 시설 및 전력망에 대한 사이버 위협 탐지 및 방어 규정 수립	

정부기관	주요 AI 안보 법제적 역할		핵심 정책 목표 및 기조
백악관 과학기술정책 국장실 (OSTP)	규제 전수조사 및 폐지 주도	혁신을 저해하는 연방 AI 규제 및 장벽의 개정 또는 폐지 지시	범정부 차원의 '혁신 우선' AI 정책 기조 설정 및 연방/주 정부 간 AI 규제 통일 주도
	AI 정책 가이드 제공	연방 기관의 AI 어플리케이션 규정에 대한 정책 가이드 제공 및 통일된 방향 제시	

출처: The White House (Jul 2025); AI NSM (Oct 24, 2024); Genesis Mission EO (Nov 24, 2025); NDAA FY2025 (P.L.118-159); CRS (R48527); (plus state-level example: NY RAISE Act) 토대로 저자 재구성.

즉, 이러한 AI 안보화의 기능적 구현은 중요 임무조직별 AI의 활용 범위를 확장하는 동시에, 필요 시 국가가 개입할 수 있는 법적 레버리지를 유지하도록 기여한다. AI는 평시에는 각 부처와 민간의 자율적 혁신과 운영에 맡겨지지만, 위기 상황에서는 기존 NSS 법체계에 따라 한시적으로 통합·동원될 수 있는 여지를 갖게되는 것이다. 이는 미국의 AI 안보화가 민간 주도의 분산형 혁신을 원칙으로 하되, 국가안보가 요구될 경우 즉각적으로 작동 가능한 제도적 안전판을 구축하는 방식으로 법제화되고 있음을 의미한다. 즉, AI를 통제하기 위한 새로운 규범 체계 수립에 방점을 두는 것이 아닌, AI를 국가안보 기능 체계 속에서 효과적으로 활용할 수 있는 역량으로 재구성하는데 초점을 두고 있다.

Ⅴ. 결론

본고는 미국의 AI 안보화를 단순히 특정 기술이 '안보 문제'로 규정되는 담론적 과정으로 보지 않고, 그러한 인식이 정책수단의 조합과 집행 구조를 어떻게 재배치·재구성하는지 초점을 맞추어 분석하였다. 이를 위해 AI 안보화를 담론-정책수단-집행체계-확산이라는 연속 구조로 파악하고, 특히 트럼프 2기 행정부 시기를 중심으로 그 거버넌스적 성격을 규명하였다. 살펴본 결과, 미국의 AI 안보화는 규제 강화 여부나 위험 인식의 고조 그 자체에 있지 않았다. 오히려 핵심은 관리 가능한 국가 역량으로 조직하기 위한 통치 방식의 전환에 있었다. AI는 더 이상 개별 산업 정책이나 기술 규제의 대상이 아니라, 연산 자원, 반도체, 데이터, 인재, 연구 인프라를 포괄하는 국가 역량의 집합체로 인식되었고, 이에 따라 정책수단 역시 단일 규율 방식이 아닌 조합적·차등적 방식으로 배치되었다.

특히 트럼프 2기 행정부에서 이러한 경향은 더욱 분명해졌다. AI 행동계획과 제네시스 구상은 AI를 '통합 플랫폼', '인프라', '연산 기반'으로 규정함으로써, AI를 특정 기술이나 응용 분야가 아닌 국가 역량을 증폭시키는 기반적 요소로 재정의 하였다. 이러한 전략 문서들은 이후 입법과 집행 단계에서 AI를 연방 차원의 전략적 조정 대상으로 다루는 기준점으로 기능하였으며, 그 결과 AI 안보화는 새로운 규제의 도입보다는 기존 제도와 자원 배분 구조를 재조정하는 방식으로 구현되고 있다. 요컨대, 미국의 AI 안보화는 '안보화된 기술에 대한 통제 강화'라기보다는, 국가가 기술 생태계를 조정·배치하는 거버넌스적 전환으로 이해되어야 한다는 것을 시사한다.

트럼프 2기 행정부 시기의 AI 안보화 담론은 이전 행정부들과 연속성을 유지하면서도, 몇 가지 차이점들이 보다 분명히 드러나고 있다. 첫째, 경제안보 중심성의 강화이다. AI는 혁신, 성장, 생산성, 글로벌 경쟁력의 핵심 동력으로 규정되었으며, 기술 패권 유지를 위한 혁신 가속이 국가안보의 핵심 과제가 되었다. 이 과정에서 AI 안전이나 윤리 문제는 기술 발전을 저해하지 않는 범위 내에서 관리되어야 할 부차적 고려사항으로 다뤄지고 있다. 둘째, 군사안보와 외교안보의 결합이 심화되고 있다. AI는 군사 영역에서는 전력 구조를 재편하는 핵심 요소로 통합되는 한편, 외교적으로는 동맹과의 정책적 정합성, 기술 표준, 수출 통제와 결합된 전략 자산으로 활용되었다. 이는 AI가 더 이상 군사 기술이나 산업 기술로 분리되어 다뤄지지 않고, 군사·외교·경제 안보를 관통하는 기준점으로 작동하고 있음을 보여준다. 셋째, 바이든 행정부 시기에 강조되었던 시민권, 프라이버시, 차별 방지와 같은 가치 중심 담론은 트럼프 2기 들어 우선순위에서 밀려났으며, 안전과 책임의 문제 역시 혁신을 저해하지 않는 최소한의 관리 대상으로 재배치되었다. 이는 AI 안보화의 중심축이 '위험의 관리'에서 '역량의 증폭'으로 이동했음을 시사한다. 즉, 트럼프 2기 행정부의 AI 안보화 담론은 규범적 균형보다는 전략적 효율과 실리를 중시하는 방향으로 재편되고 있음을 보여준다.

본고에서 살펴본 안보화 담론의 이론적 시각에서 본 미국의 AI 안보 거버넌스의 재구성 과정은 다음과 같은 시사점을 제시한다. 기술 안보화는 단순히 규제 강화 여부로 측정될 수 없으며 정책수단의 조합에 따른 차등적 효과로 구별될 필요가 있다. 또한, 담론과 제도는 병렬적 층위가 아닌, 전략자산화 담론이 정책 패키지의 재배열을 정당화하는 인과 구조를 통해 구현된다. 나아가, AI와 같은 범용 기술의 안보화는 중앙집중적 통제보다 민관의 분산적 조정 모델로 제도화될 수 있음을 확인하였다.

이 같은 미국의 AI 안보 거버넌스 사례는 한국에 단순히 모방 가능한 정책 모델을 제공하기보다는, 정책의 실효적 추진을 위해 필요한 몇 가지 방향성을 암시한다. 그 첫 번

째는, AI 안보를 단일한 규율 방식으로 관리하기보다 영역과 위험 수준에 따라 차등적으로 적용하는 접근이 필요하다는 점이다. 특히, 미국의 선별적 개입 사례는 규제의 총량을 늘리는 방식이 아니라, 국가안보적 중요도가 높은 영역에 선택적으로 개입하고, 나머지 영역에서는 민간 혁신을 최대한 존중하는 방식을 택하고 있음을 보여준다. 둘째, '민간 주도-국가 안전판'이라는 역할 분담 구조의 전략적 의미이다. 미국의 AI 안보화는 국가가 직접 혁신을 주도하기보다는, 민간의 기술 역량과 시장 경쟁력을 최대한 활용하면서도, 수출 통제나 핵심 인프라 보호와 같은 전략적 레드라인은 국가가 명확히 설정하는 방식으로 전개되고 있다. 이는 민간의 자율성과 국가의 안보 책임을 병렬적으로 결합하는 거버넌스 모델로 해석할 수 있다. 셋째, AI 안보를 사이버, 군사, 외교 영역과 연계된 복합 안보 문제로 인식할 필요성이다. AI는 단일 기술 차원을 넘어 국가 전반의 취약성과 역량을 동시에 증폭시키는 특성을 지니고 있으며, 이에 따라 AI 안보 역시 특정 부처나 정책 영역에 한정된 문제가 아니라 범정부적·범분야적 대응이 요구된다.

마지막으로, 미국의 AI 안보 거버넌스 재구성 과정은 우리로 하여금 AI 안보를 '위험 규제'로 바라보는 접근을 넘어 선별적 통제와 촉진·지원 수단을 강화하는 차등적 정책 조합으로 나아가야 함을 일깨워준다. 미국의 '조건부 접근'과 표준·수출통제의 연계 전략은 한국에도 국방 중심의 협의적 안보 개념을 넘어, 조달·표준·보안 인증·핵심 인프라 보호·대외 기술협력까지를 포괄하는 범정부적 안보 개념으로 확장되어야 한다. 민간·지방정부·학계·연구계 등 현장의 상향식 혁신 의제를 정책화할 수 있는 연계성 확보와 최소 가드레일 마련이 필요하다.

참고문헌

법률신문, "미국 RAISE 법안 분석: AI 안전 규제의 확산 가능성과 기업 대응 전략" (2025.6.26). https://www.lawtimes.co.kr/LawFirm-NewsLetter/209219 (검색일: 2025.10.12.).

윤정현, 2025. "'스타게이트 프로젝트'로 본 트럼프 2기의 AI 국가전략" 『ISSUE BRIF』, (2025.2.13), 제657호.

_____, "美 'AI 행동계획' 발표 의미와 한국에 주는 시사점" 『ISSUE BRIF』, (2025.8.18), 제717호.

이주형, 2025.. "행정명령 쏟아진 트럼프 100일… 고밀도 모니터링·대응해야" 『월간 통상』, (2025년 4월). https://tongsangnews.kr/webzine/202504/2025040480113.html (검색일: 2025.7.30.).

한국인터넷진흥원, "해외입법동향: 미국 하원, 「첨단 AI 보안 대비법안」 발의 (2025.6.11.)" (2025년 7월).

한국정보화진흥원, 2024. "미국 AI 국가안보각서(AI NSM) 분석 및 시사점" 『THE AI REPORT 2024-7』, (2024.11.6).

Balzacq, Thierry. 2011. *Securitization Theory: How Security Problems Emerge and Dissolve*. London: Routledge.

Congressional Research Service (CRS). 2025. "National Defense Authorization Act for FY2025: Overview and Selected Issues." CRS Report R48527, May 8, 2025.

CSET, 2024. The National Security Memorandum on Artificial Intelligence: CSET Experts React, CSET (October 24, 2024), https://cset.georgetown.edu/article/the-national-security-memorandum-on-artificial-intelligence-cset-experts-react/ (검색일: 2025.8.22.).

Farrell, Henry and Abraham L. Newman. 2023. *Underground Empire: How America Weaponized the World Economy*. New York: Henry Holt and Company.

House Committee on the Judiciary Democrats, 2025. "At Hearing on Federal Preemption of State AI Laws, Subcommittee Democrats Underscore Need for Guardrails to Protect Americans While Promoting Innovation" https://democrats-judiciary.house.gov/media-center/press-releases/at-hearing-on-federal -preemption-of-state-ai-laws-subcommittee-democrats-underscore-need-for-guardrails-to-protect-americans-while-promoting-innovation (검색일: 2025.9.25.).

Infoloop. 2025. "트럼프가 중국의 엔비디아 칩 판매를 허용하면서 중국을 지배하는 방법: 트럼프의 'AI 맨해튼 프로젝트'." (December 27, 2025).

The New York State Senate, "Assembly Bill A6453A, 'Relates to the training and use of artificial intelligence frontier models' (March 5, 2025)", https://www.nysenate.gov/ legislation/bills/2025/A6453/amendment/A (검색일: 2025.10.18.).

OECD. 2019. "Recommendation of the Council on Artificial Intelligence." Paris: OECD Publishing.

Sarokhanian, Nicholas A. and Lyric D. Menges. 2025. "A Look at U.S. Government's Changed Approach to Artificial Intelligence Development and Investments." *The National Law Review* (Feb 10, 2025). https://natlawreview.com/article/look-us-governments-changed-approach-artificial-intelligence-development-and (검색일: 2025.7.2.).

The Select Committee on the CCP, "Defending American AI: Moolenaar, Bipartisan Group Introduce Advanced AI Security Readiness Act" (June 12, 2025), https://selectcommitteeontheccp.house.gov/media/press-releases/defending-american-ai-moolenaar-bipartisan-group-introduce-advanced-ai (검색일: 2025.10.3.).

U.S. Congress. 2025. National Defense Authorization Act for Fiscal Year 2025. Washington, DC: U.S. Government Publishing Office.

U.S. Department of Commerce, Bureau of Industry and Security (BIS). 2024-2025. Advanced Computing Export Control Guidance (China-related licensing and presumption of denial framework).

The White House, "BLUEPRINT FOR AN AI BILL OF RIGHTS: Making Autonomous Systems Work for the American People" (October 2022) https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (검색일: 2025.5.23.).

_____, 2025. "Genesis Mission: Executive Order on Building the American Science and Security Platform."

_____, 2024. “Memorandum on Advancing the United States’ Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence” (Oct. 24, 2024), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/ (검색일: 2025.2.24.).

_____, 2025. “Winning the Race: AMERICA’S AI ACTION PLAN”, (July 2025).

【Abstract】

From AI Securitization Discourse to the Reconfiguration of AI Security Governance in the United States

Yoon, Junghyun

The United States has long regarded artificial intelligence (AI) as a core strategic technology directly linked to national security, and, amid the intensifying U.S.–China technological competition, has positioned the preservation of AI technological superiority as a central national security objective. Existing studies, however, have largely analyzed AI securitization through the lenses of threat discourse formation or changes in individual policies and legal instruments, offering limited explanations of how AI securitization is organized and transformed through specific combinations of domestic and external policy instruments and implementation structures.

This article argues that U.S. AI securitization cannot be adequately understood through a binary framework of regulatory expansion versus deregulation. Instead, it should be conceptualized as a process of governance transformation aimed at organizing AI as a form of national capability. To this end, the study approaches U.S. AI securitization as a sequential and structural process encompassing the institutionalization of AI as a strategic asset, the configuration of policy instruments, implementation architectures, and mechanisms of diffusion. This analytical framework is applied to the period of the Trump administration's second term.

The analysis shows that U.S. AI securitization has not proceeded through a uniform expansion of regulation or strengthened direct state control. Rather, it operates by treating the elements of the AI ecosystem as a bundle of manageable national strategic assets and by combining coordinative governance with differentiated intervention and selective control. In practice, federal-level intervention and oversight are intensified in areas with high military and security externalities, while regulatory flexibility and autonomy are

expanded in domains closely tied to private-sector innovation and industrial competitiveness. At the same time, this governance model extends beyond domestic implementation, diffusing internally to private firms, state governments, and academic institutions, and externally through alliance alignment, standard-setting, and export controls. Together, these dynamics illustrate how U.S. AI securitization functions as a governance-oriented reconfiguration of state–market relations rather than a simple shift toward greater regulation or deregulation.

Key Words : Artificial Intelligence(AI), AI securitization, AI governance, AI Action Plan, Genesis Mission.

• 논문투고일 : 2026년 2월 02일 / 논문심사완료일 : 2026년 2월 08일 / 게재확정일 : 2026년 2월 14일