아태연구 제32권 제4호 (2025) https://doi.org/10.18107/japs.2020.27.4.004

# 사이버-AI 넥서스와 미국의 동맹외교:
## 바이든 행정부와 트럼프 행정부를 중심으로*

신승휴**

| 목 차 |



| 논문요약 |

인공지능(AI)의 발전으로 인해 사이버 위협이 빠르게 심화하는 상황에도 불구하고 사이버 안보와 AI 분야 미국의 전략은 배타적 국익 중심의 단편적이고 거래적인 국제협력을 선호하는 방향으로 점차 나아가고 있다. 이에 주목하여 이 글은 '사이버-AI 넥서스'에 대한 미국의 대응 역시 가치 중심의 동맹에 기초한 포괄적·통합적 협력에서 점점 더 멀어지고 있음을 지적한다. 이러한 시각을 뒷받침하기 위해 이 글은 사이버 안보와 AI를 위한 미국의 국제전략이 바이든 행정부를 거쳐 트럼프 2기 행정부에 이르는 시기에 어떻게 추진되어왔는가를 살펴본다. 구체적으로 사이버 안보 전략과 AI 전략에 담긴 국제협력의 기조, 이니셔티브, 플랫폼 그리고 추진체계의 내용을 검토하여 그 안에서 발견되는 시기별 특징을 이해하고자 한다. 이렇게 변화하는 미국의 동맹외교가 사이버-AI 넥서스로 인해 발생하는 다양한 문제들에 어떻게 접근하고 있는지 그 추이를 포착하는 것을 목적으로 한다.

▪ 주제어: 사이버 안보, 인공지능, 동맹, 바이든, 트럼프

* 본 논문은 한국사이버안보학회의 연구용역과제(과제명 : '사이버 복합 넥서스: 최신 동향 파악과 대응 전략 모색', 수행기간 : 2025.04~2025.11) 결과물을 바탕으로 수정·보완한 것입니다.
** 서울대학교 정치외교학부 외교학 박사수료

# Ⅰ. 서론

인공지능(AI)의 급격한 발전과 확산은 사이버 안보 분야에서 그간 주목해 온 다양한 초국적 위협을 한층 더 심화시키는 요인이 되고 있다. 사이버 안보를 둘러싼 국제정치의 구조와 동학이 AI 기술의 개입으로 인해 변화하고 있음은 물론이다. 이처럼 사이버와 AI의 결합을 의미하는 '사이버-AI 넥서스(cyber-AI nexus)'는 국가가 해결해야 할 사이버 위협의 양적·질적 변화를 초래하여 그 파급력을 키우고(Lohn 2025), 사이버 안보와 여타 안보 이슈 간 연계 가능성을 확대하며, 디지털 환경에서 발생하는 기술 차원의 문제가 지정학적 갈등과 경쟁으로 이어지게끔 하는(김상배 2025, 101-132), 그야말로 '신흥안보(emerging security)'의 문제로 부상하고 있다.

그동안 사이버와 AI의 결합을 둘러싼 학계의 논의는 주로 AI의 발전이 사이버 작전의 효과성, 사이버 억제와 위기관리 역량, 정보전에서의 공수균형, 그리고 핵무기나 자율무기체계의 취약성 등에 어떠한 변화를 가져오는지에 초점을 두어 전개되어왔다(Johnson 2019; Khan, Khurshid & Cifuentes-Faura 2024). 그러나 오늘날 사이버-AI 넥서스는 군사 영역과 관련한 전통안보의 문제에만 국한되지 않는다. 국가를 지탱하는 핵심 인프라 전반에서 AI가 범용기술로 활용되는 가운데 AI 기반 시스템이 사이버 공격의 대상이 되면서 발생하는 정치적·사회적 문제 역시 AI 기반 사이버 작전(AI-enabled cyber operations)과 그로 인한 전략 환경의 변화만큼이나 중요한 주제로 주목받고 있다. 온라인상 악의적 콘텐츠를 탐지·차단·예방하는 수단으로 AI가 도입됨에 따라 발생하는 윤리적 문제와 주권 침해도 관찰된다.

이렇듯 AI가 사이버 위협을 심화함과 동시에 그 위협의 표적이 되고, 또 사이버 공격을 차단하는 효과적인 수단으로도 활용되는 상황에서 사이버-AI 넥서스에 대한 국가적 대응은 총체적이고 유기적이며 초국적인 접근을 요구하고 있다. 그중에서도 특히 공통의 위협인식과 가치를 공유하는 동맹국 및 우방국들과의 협력은 사이버-AI 넥서스 대응의 가장 중요한 부분을 차지한다. AI의 기반이 되는 데이터와 알고리즘을 체계적으로 관리하는 일부터, AI 기반 사이버 공격이 국가안보 위협으로 이어지지 않도록 그 연결고리를 차단하는 문제에 이르기까지, 모든 단계에서 국제협력이 필수적이기 때문이다. 이는 초

강대국 미국에도 예외 없이 적용되는 조건이다.

바이든 행정부 출범 이후로 지금까지 미국은 사이버 안보와 AI를 위한 국가 전략을 구분 지어 수립하고 그 안에서 국제협력을 모색하는 노력을 기울여왔다. 바이든 행정부는 사이버 위협 대응을 위한 글로벌 공조체계를 구축하고, 기술 표준화를 선도하며, 디지털 환경에서 핵심 가치를 보호하기 위해 '민주주의 동맹' 기반의 국제협력을 중시하는 모습을 보였다. 그와 마찬가지로 AI 분야에서도 기술의 윤리적 개발과 활용을 촉진하는 일련의 규칙과 표준을 마련함과 동시에 AI를 악용한 권위주의 국가의 위협을 차단하려는 목적에서 동맹국과의 연대를 우선하였다. 그에 따라 이 시기 미국의 사이버 안보 전략과 AI 전략은 민주주의와 규칙기반 질서(rules-based order) 그리고 다중이해당사자주의(multistakeholderism)를 표방하는 다양한 (소)다자협력 네트워크를 플랫폼으로 삼아 사이버 위협과 AI의 잠재적 위험, 더 나아가 기술지정학적 위기에 공동으로 대응하는 '동맹외교(alliance diplomacy)'의 요소를 포함하였다(신승휴 2025, 6-7).

그러나 2025년 초 트럼프 2기 행정부가 출범하면서 이러한 전략 기조는 점차 변화하는 양상을 보이고 있다. 트럼프 행정부는 출범 직후 미국에 대한 사이버 위협 가해국을 명확히 지목하면서도 또 한편으로는 사이버 안보를 군사안보의 맥락에서만 범주화하는 이중적 접근을 취하고 있다. 그에 따라 국제협력은 공유된 가치 기반의 포괄적 협력이 아닌 사안별 이익을 위한 단편적 협력으로 귀결되는 결과가 발생하고 있다. AI 분야에서도 역시 동맹국들과 협력하여 글로벌 차원에서 합의된 원칙과 규범에 근거한 질서를 만들어가는 일보다, 기술 혁신과 견제를 통해 글로벌 AI 경쟁의 무대에서 전략적 우위를 확고히 하는 데 더 높은 이해관계를 표출하고 있다. 물론 여전히 동맹국 및 유사입장 국가들과의 협력이 중요하다는 원칙을 표방하고는 있지만, 미국우선주의(America First) 기조로의 회귀가 기정사실화된 가운데 AI를 위한 국제협력은 배타적 국익을 극대화하는 것을 목표로 거래적인 맥락에서 이루어져야 한다는 논리에 지배되고 있는 실정이다.

AI의 발전으로 인해 사이버 위협이 빠르게 심화하는 상황에도 불구하고 사이버 안보와 AI 분야 미국의 전략이 이익 중심의 단편적이고 거래적인 협력을 선호하는 방향으로 나아가고 있음에 주목하여, 이 글은 사이버-AI 넥

서스에 대한 미국의 대응 역시 가치 중심의 동맹외교에서 점점 더 멀어지고 있음을 주장한다. 이러한 시각을 뒷받침하기 위해 이 글은 사이버 안보와 AI에 대한 미국의 전략이 바이든 행정부를 거쳐 트럼프 2기 행정부에 이르는 과정에서 국제협력에 어떻게 접근해왔는지 살펴보았다. 구체적으로 사이버 안보 전략과 AI 전략에 담긴 국제협력의 기조, 이니셔티브, 플랫폼 그리고 추진체계의 내용을 검토하여 그 안에서 발견되는 시기별 특징을 이해하고 그 변화의 추이를 포착하였다. 이를 토대로 AI에 의한 사이버 작전의 양·질적 변화, AI 생성 허위정보를 토대로 이루어지는 영향력 공작, AI 기반 콘텐츠 검열에 따른 데이터 안보와 주권 침해 등 사이버-AI 넥서스 차원에서 최근 주목받고 있는 문제들에 트럼프 행정부가 어떻게 접근하고 있으며, 그러한 접근이 미국의 동맹외교에 미치는 영향은 무엇인지 분석하였다.

따라서 이 글은 크게 세 부분으로 구성되었다. 바이든 행정부와 트럼프 2기 행정부를 분석 대상으로 하여 이어지는 Ⅱ장에서는 미국의 사이버 안보 국제전략이 시기에 따라 기조, 이니셔티브, 플랫폼, 추진체계 측면에서 변화해온 양상을 추적하였다. Ⅲ장에서는 미국의 AI 국제전략을 동일한 분석 시기와 대상을 기준으로 검토하여 행정부별 특징과 변화의 추이를 조명하였다. 끝으로 Ⅳ장에서는 미국이 다양한 영역에서 발생하는 사이버-AI 넥서스 문제들에 접근하는 방식과 그러한 방식이 미국의 동맹외교에 미치게 될 영향을 살펴보았다.

## Ⅱ. 미국의 사이버 안보 국제전략

바이든 행정부 시기 사이버 안보를 위한 미국의 전략은 초국적 사이버 위협을 관리할 수 있는 글로벌 거버넌스를 구축하고 디지털 기술 표준화를 선도함으로써 사이버 공간에서 민주주의, 자유, 인권, 규칙기반 질서 등 핵심 가치를 보호하는 것을 목표로 하였다. 당시 미국은 '동맹의 복원과 다자주의'를 표방한 대외정책을 추진하였으며, 그와 같은 맥락에서 사이버 안보 전략 역시 민주주의 가치 중심의 동맹외교를 통해 자국의 리더십에 기초한 연대를 형성하고 이를 기반으로 패권의 회복을 도모하는 데에 집중되었다

(Fontaine, 2025/01/20). 특히 2023년 3월 수립된 『국가사이버안보전략』은 "공동의 목표를 추구하기 위한 국제 파트너십 구축"을 5대 목표 중 하나로 설정하고 위협 대응 연합 구축, 파트너 역량 강화, 신속한 지원 체계 마련, 글로벌 규범 확립, 공급망 안보 확보 등을 세부 전략과제로 제시하였다. 또한 2024년 국무부를 통해 수립된 『국제 사이버·디지털 전략』에서도 동맹국 및 파트너국과의 상호 지원과 역량 강화 그리고 규범 정립을 모색함으로써 '디지털 연대(digital solidarity)'를 구축하고, 이를 토대로 안전하고 혁신적이며 기본 권리를 보장하는 디지털 생태계를 만들겠다는 강한 의지를 내비쳤다(U.S. Department of State 2024).

이처럼 바이든 행정부는 집권기 동안 기술지정학적 위기와 권위주의 국가의 위협에 대응하는 기제로서 민주주의 가치와 제도를 공유하는 국가들과의 연대를 지속해서 강조하는 모습을 보였다(The White House 2023a, 29-30). 그리고 이러한 전략 기조는 사이버 대응 역량 강화, 사이버 범죄 정보공유, 법집행 협력 메커니즘 확립, 사이버 사고 대응 원조, 규범적 국가행위 촉구, ICT 및 OT 제품·서비스 공급망 보호 등 다양한 영역에서 미국이 동맹 중심의 국제협력 이니셔티브를 추진하는 결과로 이어졌다(The White House 2024a, 56-64). 일례로 2021년 10월 백악관을 통해 개최한 국제 랜섬웨어 정상회의를 계기로 '랜섬웨어 대응 이니셔티브(CRI)'를 발족하여 사이버 범죄 수사와 사고 대응을 위한 협력을 추진하였으며, 같은 해 4월에는 솔라윈즈(SolarWinds) 공격에 대응하여 동맹국과의 긴밀한 공조 아래 러시아 정보기관과 연계된 악의적 행위자들을 제재하는 조치를 시행하기도 하였다(The White House 2022).

미국의 국제협력 이니셔티브는 다양한 동맹 네트워크를 플랫폼으로 삼아 시행되었는데, 특히 파이브 아이즈(Five Eyes)나 북대서양조약기구(NATO)와 같은 전통적인 다자 동맹 관계를 활용한 협력이 활발히 이루어졌다. 대표적으로 파이브 아이즈는 러시아와 중국 등 권위주의 국가들의 사이버 공격에 공동대응하거나 이들 국가의 악의적 사이버 활동을 한 목소리로 규탄하는 통로로 사용되었으며(신승휴 2025, 23), NATO를 통한 협력은 집단방위를 사이버 안보 분야로 확장함과 동시에 사이버 사고 대응을 위한 상호 지원을 확대하는 형태로 추진되었다(The White House 2023b). 그 밖에도

쿼드(Quad)와 푸른태평양동반자(PBP) 등 인도-태평양 지역을 무대로 한 안보 협의체에서 역내 사이버 복원력 증진을 위한 공조체계를 구축하거나, '통합적 억지(Integrated Deterrence)' 전략의 일부로 미일동맹과 한미동맹을 사이버 동맹으로 격상하려는 움직임도 포착되었다(김상배 2023, 51-88). 가장 최근에는 영국·호주와 AUKUS 안보 협의체를 결성하고 그 안에서 사이버, AI를 포함한 첨단기술 분야 연구 및 개발 협력을 모색하기 시작하였다.

이렇듯 사이버 안보를 위한 가치 동맹 중심의 국제협력이 활성화됨에 따라 전략의 추진체계는 다양한 정부부처와 기관이 협력의 주체로 참여하는 범정부 통합 거버넌스의 구조를 띠게 되었다. 대통령실 산하 국가사이버실(ONCD)이 컨트롤타워에 위치하는 가운데 국토안보부와 그 산하의 사이버·인프라보안국(CISA), 국무부와 그 산하의 사이버공간·디지털정책국(CDP), 국립표준기술연구소(NIST), 법무부, 재무부, 상무부, 국방부 등 다양한 부처가 대외 부문 협력에 참여하였으며, 국가안보국(NSA), 중앙정보국(CIA), 연방수사국(FBI) 등 정보기관 역시 동맹국과의 공조에서 중요한 역할을 담당하였다. 그중에서도 국무부의 CDP는 국제사이버공간안보, 국제정보통신정책, 디지털자유를 각기 담당하는 부서를 통해 사이버 공간과 디지털 기술에 대한 대외정책을 민주주의 가치에 부합하는 방향으로 추진하였다(신승휴 2025, 14-15).

그러나 2025년 1월 트럼프 행정부가 재출범에 성공하면서 미국의 사이버 안보 국제전략은 빠르게 변화하기 시작하였다. 아직 사이버 안보를 위한 새로운 국가전략이 수립되진 않았으나, 2025년 6월 6일 트럼프 대통령은 사이버 안보 우선순위를 재설정하는 것을 목표로 「행정명령 제14306호(국가 사이버보안 강화를 위한 선별된 노력 유지)」를 발표하였다. 「행정명령 제14306호」는 사이버 안보를 위해 오바마 행정부가 2015년 발표한 「행정명령 제13694호(중대한 악의적 사이버 행위에 관여하는 특정인의 재산 차단)」과 바이든 행정부가 집권 말기인 2025년 1월 마련한 「행정명령 제14144호(국가 사이버보안 강화 및 혁신 촉진)」을 일부 수정·철회하여 위협 대상 명확화, 차세대 디지털 기술 도입 가속화, 정부 규제 완화 등을 목표로 하는 것으로 알려졌다. 특히 중국에만 국한되었던 사이버 위협국의 범위를 러시아, 이란, 북한 등으로 확대하는 조치와 더불어 사이버 보안을 위한 정

부의 규제보다 기업의 자체적인 대응을 독려하는 조치가 주된 변화로 평가된다(The White House 2025b).

그러나 트럼프 행정부는 정작 사이버 안보의 범위를 군사안보와 직결된 이슈들에만 주로 한정함으로써 사이버 안보 국제협력이 사안별 이익에 집중된 단편적 협력으로 이어지는 결과를 초래하고 있다. 그에 따라 바이든 행정부 시기에 추진되던 포괄적이고 통합적인 협력 이니셔티브들이 지속되기 어려울 것이라는 전망도 제기되는 상황이다. 무엇보다 러시아에 대한 선제적인 사이버 작전이 중단되었다는 의혹이 확산하면서 그동안 미국이 주도해 온 민주주의 가치 기반의 디지털 연대나 사이버 안보협력의 네트워크가 더는 효과적으로 작동하기 어려울 것을 우려하는 목소리가 작지 않다(Magee 2025/04/15). 당장 「행정명령 제14306호」가 선거개입 위협과 같은 사회안보 이슈와 사이버 안보 간 상관성을 사실상 축소 해석하는 원칙을 담아냄에 따라 민주주의 동맹국과의 공조를 바탕으로 허위정보 확산과 영향력 공작에 능동적으로 대응하는 사이버 작전의 영역도 축소될 가능성이 거론되고 있다(Ortega 2025/04/09).

전략의 기조와 이니셔티브에서 발견되는 이 같은 변화의 조짐은 미국이 중심이 되어 운영해온 국제협력의 플랫폼 자체를 약화하는 요인이 되고 있다. 이는 비단 사이버 안보에 대한 미국의 접근이 변화하였기 때문만은 아니다. 동맹 중심의 국제협력에 대한 미국의 접근이 가치보다는 배타적 국익을 우선하는 단편적이고 거래적인 방식을 선호하게 되면서 나타나는 현상으로 볼 수 있다. 대표적으로 파이브 아이즈의 공조체계가 흔들리는 사례를 예로 들 수 있다. 미국과 캐나다의 외교적 갈등은 차치하더라도 트럼프 행정부가 사이버 안보 국제협력을 위한 이니셔티브에 소극적인 모습을 보이면서 중국과 러시아의 사이버 위협에 공동으로 대응해온 파이브 아이즈 차원의 협력도 약화하고 있는 것으로 파악된다(Miller & Roussi 2025/02/12). 바이든 행정부의 대외정책에서 핵심적인 부분을 담당하던 AUKUS 협정 역시 트럼프 대통령의 외교적 협상 카드로 여겨지면서 사이버 및 첨단기술 부문 3국 협력이 장기간 지속될 수 있을지 장담하기 어려운 상황이다(Roughead et al 2025/09/02).

전략의 추진체계에서 발견되는 변화에도 주목할 필요가 있다. 트럼프 행정

부는 출범과 동시에 그동안 국무부와 함께 국제협력을 추동해온 CISA의 권한을 재검토하는 등 추진체계를 새롭게 정비하기 시작하였다(Cassidy 2025/03/11). 트럼프 대통령은 당선 이전부터 CISA의 폐지를 논할 만큼 그 기능과 역할에 강한 회의를 드러냈으며, 당선 이후 곧바로 CISA에 대한 인력 감축과 예산 삭감을 단행하였다(Rundle 2025/06/02). 또한 국무부의 CDP도 구조적으로 분할·재편됨에 따라 사실상 일원화된 사이버 외교 전담지원기관의 기능을 상실하게 되었다. 허위정보 확산과 내정간섭 위협 대응을 전담해온 국무부 산하의 해외정보조작·간섭대응허브(R-FIMI)[1]를 폐쇄하는 조치 역시 주목할 만하다. R-FIMI의 폐쇄는 트럼프 행정부가 언론을 감시하는 정부의 과도한 권한을 축소하려는 목적에서 내린 결정으로 알려졌지만(Gegeon 2025/04/16), 해당 조치가 사이버상 영향력 공작을 목적으로 하는 악의적 활동에 대한 미국의 자체적인 대응 역량과 동맹 협력의 실효성을 약화하는 결과로 이어지고 있다는 비판도 제기되고 있다(Psaledakis 2025/04/17).

물론 최근 트럼프 대통령은 CISA를 이끌 신임 국장에 사이버 보안 전문가를 지명하였고, 이에 대한 민간 부문의 긍정적 평가가 이어지면서 기존에 제기되던 CISA 폐지론은 사실상 수그러들었다. 미국의 통신망과 핵심 인프라의 사이버 보안을 책임져온 기관이 예산 삭감과 인력 감축의 위기에서 부침을 겪고 있는 상황을 공화당과 민주당이 모두 우려함에 따라 앞으로도 미국의 사이버 안보 전략에서 CISA의 역할은 중요할 것으로 전망된다(Ribeiro 2025/07/28). 실제로 2025년 5월 CISA는 NSA와 FBI 그리고 파이브 아이즈 동맹국 관련 기관들과 합동으로 새로운 'AI 데이터 보안 모범 사례 가이드'를 내놓는 등 사이버 안보와 AI가 융합되는 지점에서 발생하는 문제들에 대응을 이어오고 있다(CISA 2025/05/22). 그러나 동맹 협력 부문에서 CISA의 역할은 바이든 행정부 집권기 수준을 유지하긴 어려울 것으로 보이는데, 이는 트럼프 행정부와 공화당이 CISA의 역할을 대내적 사이버 보안과 민관협력에 국한하려는 모습을 보이고 있기 때문이다. 이렇듯 트럼프 행정부는 사이버 안보를 위한 국제협력에서 중요한 역할을 담당했던 기관들의 권한과 역할을 축소하거나 거두어들이고 있다는 점에서 바이든 행정

1) R-FIMI는 2016년 설립된 글로벌관여센터(GEC: Global Engagement Center)가 2024년 12월 명칭을 변경하면서 출범하였다가 2025년 4월 공식적으로 폐쇄되었다.

부와는 뚜렷한 차이를 드러낸다.

**[표 1] 미국의 사이버 안보 국제전략**

| | 바이든 행정부 | 트럼프 행정부 |
|---|---|---|
| **기조** | 글로벌 거버넌스와 규칙기반 질서 강화<br>→ 민주주의 가치 기반 동맹 협력을 중시 | 사이버 안보의 군사화, 규제 완화 및 기업 자율 대응 강조<br>→ 사안별 이익 중심의 단편적 협력 선호 |
| **이니셔티브** | 랜섬웨어 대응 이니셔티브(CRI), 국제 사이버·디지털 전략, 파트너 역량 강화, 규범 확립 | 사이버 안보와 선거위협 분리 조치 |
| **협력 플랫폼** | 파이브아이즈/NATO/쿼드/AUKUS /PBP 등 양자·다자 동맹 네트워크 활용 | 기존 협력 네트워크 약화, 파이브 아이즈 공조 약화, AUKUS 지속가능성 감소 |
| **추진체계** | 컨트롤타워에 ONCD 지정, 국토안보부(산하 CISA)/국무부(산하 CDP)/NIST/ 법무부/재무부/상무부/국방부/정보기관(NSA·CIA·FBI) 등 다부처 역할 강조<br>→ 범정부 통합 거버넌스 채택 | ONCD의 컨트롤타워 역할 유지, CISA 권한 축소·예산 삭감, CDP 구조 분할, R-FIMI 폐쇄<br>→ 범정부 통합 거버넌스 약화 |

▪ 출처: 저자 작성

# Ⅲ. 미국의 인공지능 국제전략

바이든 행정부 시기 AI에 대한 미국의 전략은 신기술의 안전성 확보와 위험성 관리를 위한 규범을 마련하는 것을 목표로 하였다. 따라서 AI 분야 국제협력을 모색하는 노력 역시 AI의 윤리적 개발과 활용을 촉진하는 일련의 규칙과 표준을 마련하고, 나아가 AI를 악용한 권위주의 국가의 위협을 차단하는 데에 집중되었다. 2023년 11월 30일 바이든 행정부는 AI의 안전성·보안성·신뢰성 확보를 위해 「행정명령 제14110호(안전하고 신뢰할 수 있는 인공지능 개발 및 활용)」을 발표함으로써 AI 안전 및 보안에 대한 새로운 기준을 수립하였다. 이는 일차적으로 정부의 기술 규제를 강화하기 위해 마

련된 조치였지만, 대외적 차원에서는 동맹국을 포함한 유사입장 국가들과 협력하여 글로벌 AI 규제 거버넌스 구축을 주도하고, AI 표준의 개발과 구현을 촉진하며, 안전한 AI 시스템의 확산을 도모하는 것을 목표로 하였다(The White House 2023c). 즉 바이든 대통령은 신기술의 무분별한 개발보다 적절한 안전장치(guardrails)와 규범을 도입하여 그 안정성을 확보하는 것이 우선이라는 판단에서 이상의 조치를 시행하였다. 레이먼도(Gina Raimondo) 당시 상무부 장관 역시 이러한 시각에서 "AI를 발전시키는 것은 옳은 일이지만, 결과를 생각하지 않고 가능한 한 빨리 발전시키는 것은 현명한 일이 아니다"는 뜻을 밝히기도 하였다(Pillay 2024/11/21).

물론 바이든 행정부가 AI에 대한 윤리와 규제의 원칙을 마련하는 국제적 노력을 주도하고자 한 것은 기술의 잠재적 위험성에 대한 경각심 때문만은 아니었다. 다른 한편으로는 미국에 "유리한 국제기술질서(a favorable international technology order)"를 확립하여 핵심 가치를 보호하고 더 나아가 패권을 강화하고자 하는 이해관계도 강하게 작용하였다(NSCAI 2021, 13). 2024년 10월 바이든 대통령은 백악관을 통해 미국 최초의 'AI국가안보메모랜덤(AI NSM)'을 발표하여 자국의 글로벌 리더십, 국가안보, 민주주의 가치와 인권 보호를 위해 AI를 개발하고 활용할 계획을 내놓았는데, 이 역시 신기술의 개발과 활용이 미국과 그 핵심 가치를 위협하지 않는 방향으로 이루어져야 한다는 인식을 반영한 것이었다(The White House 2024b).

이 같은 기조 속에서 바이든 행정부의 AI 분야 국제협력은 2021년 1월 트럼프 1기 행정부 말기에 공식적으로 시행된 '국가AI이니셔티브(NAII)'와 맞물려 이루어졌다. NAII는 미국이 AI의 안전성·신뢰성·설명가능성·책임성을 확보하는 국제적 노력을 주도하여 안보와 경제 그리고 과학기술 분야에서 리더십을 공고히 하는 것을 목표로 다양한 정책 과제를 제시하였고, 국제협력의 방향성 역시 이에 맞춰졌다. 그리고 2023년 미국은 영국과 AI안전연구소(AISI)[2]를 동시 설립하여 양자 협력을 추진하였으며, 2024년 11월에는 AI 안전성 연구·평가·정보공유를 위한 동맹 중심의 협력을 증진하려는 목적에서 '국제 AI안전연구소 네트워크(International Network of AI Safety

2) 2023년 11월 AI안전연구소(AI Safety Institute)로 최초 설립되어 2025년 6월 표준혁신센터(CAISI)로 개편되었다.

Institutes)'를 결성하였다. 동 네트워크에는 영국을 비롯하여 호주, 캐나다, 유럽연합(EU), 일본, 한국, 싱가포르 등 핵심 동맹국 및 파트너국들이 참여하였고, 샌프란시스코에서 개최된 제1차 회의에서 AI 합성 콘텐츠의 위험 관리, AI 기반 모델 테스트, 첨단 AI 시스템 위험 평가 수행 등을 위한 협력 방안이 논의되었다(NIST 2024/11/20).

AI안전연구소 중심의 협력 외에도 바이든 행정부 집권기 미국이 AI 국제협력을 위해 활용한 플랫폼은 다양한데, 대표적으로 G7, 경제협력개발기구(OECD), 글로벌AI파트너십(GPAI), 국제표준화기구(ISO) 등 서구권 중심의 다자협의체 및 국제기구에서 리더십을 행사하며 안전한 AI의 개발 및 활용을 위한 규범 형성을 주도하고자 하였다(Allen & Adamson 2024). EU와는 2023년 기후변화, 자연재해, 의료, 에너지, 농업 관련 초국적 과제를 해결하여 공익을 증진하는 것을 목표로 AI에 관한 행정협약을 체결하였으며(Smalley 2023/01/28), 2024년에는 인권, 민주주의, 법치주의 등 공유된 가치에 기초한 AI 규범을 마련하고자 유럽평의회(CoE) 차원에서 마련된 'AI 기본협약(Framework Convention on AI)'에 서명하기도 하였다(Murgia & Espinoza 2024/09/05).

또한 사이버 안보 분야에서와 마찬가지로 파이브 아이즈, NATO, 쿼드 등 동맹 및 소다자 안보협력 네트워크를 적극적으로 활용하는 행보를 보였다. 2021년 바이든 행정부는 NATO가 군사 용도의 AI를 책임감 있는 방향으로 도입·활용하고자 최초의 AI 전략을 수립하는 과정에 적극적으로 관여하였고, 같은 해 쿼드 차원에서는 '기술의 설계·개발·거버넌스·사용에 관한 원칙'을 발표한 바 있다(The White House 2021). 2023년 11월 미 하원에서는 파이브 아이즈 국가 간 AI 이니셔티브를 개발하고 조정하도록 요구하는 「5개국 AI 법안(Five AIs Act)」이 발의되기도 하였다(Freedberg 2023/11/22).

이 시기 미국의 AI 전략은 대통령실 산하의 과학기술정책실(OSTP)과 그 아래 설치된 국가AI이니셔티브실(NAIIO)이 컨트롤타워 기능을 담당하는 가운데, 상무부 및 NIST, 국무부, 에너지부, 국토안보부, 국방부 및 그 산하의 국방정보국(DIA), 국립과학재단(NSF), 국가정보장실(ODNI), NSA, CIA 등 다양한 연방정부 조직을 국제협력에 참여시키는 방향으로 추진되었다. 특히 상무부의 NIST는 AI의 안전성 평가와 위험성 관리에 관한 미국 주도

의 글로벌 표준화를 추진하고자 2023년 그 산하에 AISI를 설립하였다. 국무부 산하에는 첨단기술 전반에 걸쳐 미국의 글로벌 경쟁력과 리더십을 강화하기 위해 핵심신기술특사실(S/TECH)이 운영되었고, S/TECH는 국가안보 우선순위에 따라 '통합된 기술외교전략'을 수립함으로써 미국이 5G/6G, AI, 양자컴퓨팅, 반도체 등 첨단기술 분야에서 동맹 중심의 기술산업 공급망과 생태계를 보호하고 규제 거버넌스를 구축할 수 있도록 지원하였다(Kelley 2023/01/04).

바이든 행정부와 마찬가지로 트럼프 행정부도 1차 집권기인 2019년 백악관 산하에 'AI국가안보위원회(NSCAI)'를 설립하고 퇴임 직전인 2021년 1월 「국가AI이니셔티브법 2020」을 제정하는 등 일찍이 AI가 미국의 안보와 경제에 미치는 영향에 대해 높은 관심을 드러냈다. 그러나 2차 집권 시작과 동시에 「행정명령 제14148호(위험 행정명령과 조치에 대한 1차 취소)」를 발효하여 바이든 행정부의 「행정명령 제14110호」를 폐지함과 동시에 「행정명령 제14179호(미국 인공지능 주도에 대한 장벽 제거)」에 서명함으로써 AI 전략의 초점을 규제보다는 혁신과 성장에 맞추는 방향으로 수정하였다. 「행정명령 제14179호」는 미국의 AI 혁신을 저해하거나 제약한다고 판단되는 기존의 규정을 철회하는 것을 목적으로 하며, 규범보다는 혁신을 통해 글로벌 AI 경쟁 구조에서 미국의 주도권을 공고히 하려는 의도를 반영한다(The White House 2025/01/23). AI에 대한 트럼프 행정부의 전략도 큰 틀에서는 다중이해당사자주의 접근을 취하고 있지만, 민간 부문 행위자들에게 윤리적이고 책임 있는 참여를 유도한 바이든 행정부와 달리 트럼프 행정부는 민간 주도 성장을 강조하는 차원에서 미국 기업에 확대된 권한과 역할을 부과한다는 점에서 뚜렷한 차이를 보인다.

이렇게 변화된 전략 기조를 바탕으로 미국은 2025년 7월 새로운 『미국의 AI 행동계획』을 수립하여 세부적인 목표와 정책 과제 및 실행 방안을 소개하였다(The White House 2025c). 여기서도 트럼프 행정부는 'AI 경쟁(AI Race)'에서의 승리가 혁신의 가속화, 인프라 구축, 국제 리더십 확보에 달려 있음을 명확히 하였다. 책임 있는 AI 개발 원칙에 근거한 국제협력이 세부적인 목표로 언급되긴 하였으나, 전략의 무게중심과 초점은 혁신에 맞춰졌다. 그에 따라 현재 미국이 AI 분야에서 추진하는 국제협력의 이니셔티브는

공유된 가치나 규범보다는 배타적 국익 증진을 위한 거래적 협력을 선호하는 방향으로 계획·시행되고 있다. 당장 2025년 7월 시행된 「행정명령 제14320호(미국 AI 기술 수출 촉진)」만 보더라도 미국은 자국 AI 기술을 패키지화하여 수출함으로써 미국산 AI에 대한 동맹국 및 파트너국의 도입을 더욱 적극적으로 유도하는 것을 목표로 한다. 또한 『미국의 AI 행동계획』 역시 동맹국 및 파트너국에 대한 미국산 AI 수출 촉진, AI 관련 기술의 해외 유출 통제 등 보호주의적이고 일방적인 대외 조치를 다수 포함하고 있다. AI 규범과 표준을 확립하기 위한 협력마저도 공유된 가치보다는 중국이 관련 국제기구나 다자협의체 안에서 영향력을 더 키우지 못하도록 견제하는 데 초점을 맞추고 있다(Mok 2025/08/08).

물론 바이든 행정부도 2022년 이른바 'CHIPS법'으로 알려진 「반도체칩과 과학법」을 도입하여 대중국 견제를 위한 기술 수출 통제를 강화하는 한편, 반도체 공급망의 안정성을 확보하고자 일본·한국·대만과의 협력을 모색하는 '칩4동맹' 구상을 내놓은 바 있지만, 트럼프 행정부는 여기서 한발 더 나아가 동맹국에 미국산 AI 도입을 강요하는 행보를 보인다는 점에서 차이를 가진다. 따라서 협력의 플랫폼도 이전보다 그 활기를 잃게 될 가능성이 커졌다. 일차적으로 미국이 AI 규제 거버넌스 구축을 위한 다자협의체나 국제기구에 적극적으로 참여할 동기가 줄어들면서 G7, OECD, GPAI, CoE 등을 통해 이루어지던 규범 협력이 부침을 겪게 될 여지가 있다. 미국의 빅테크 기업이 유럽에서 규제법을 두고 역내 정부들과 갈등하는 국면에서 트럼프 행정부의 AI 전략이 기업의 혁신 활동에 힘을 실어주면서 안전한 AI 개발 및 확산을 위한 미국과 EU 간 협력에도 비상등이 커졌다는 평가가 나온다(Kroet 2025/05/08). 한편 AUKUS가 트럼프 행정부의 외교적 협상 카드로 활용되는 가운데 AI를 포함한 첨단기술 부문 AUKUS 필러-2 협력도 현재는 표류하고 있다. 물론 미 의회를 중심으로 AUKUS에 대한 긍정적인 여론이 점차 커지는 상황에서 2025년 10월 트럼프 대통령 역시 AUKUS를 통한 잠수함 협상 추진을 약속하였지만, 트럼프 행정부가 거래적 협력 기조를 유지하는 한 그 지속가능성을 확신하기는 어렵다는 분석도 제기된다(Motwani 2025/09/03).

이와 더불어 전략 추진체계에서 나타나는 변화 역시 눈길을 끈다. 미국의

관심이 AI에 대한 규제보다는 혁신과 성장으로 옮겨감에 따라 정부 내부적으로 국제협력에 참여하는 주체도 자연스럽게 제한되는 경향을 보인다. 이는 바이든 행정부 집권기에 AI의 윤리원칙과 규범을 확립하기 위해 국제협력에 적극적으로 참여했던 정부부처와 기관의 기능이 약화하는 현상을 통해 가장 명확히 드러난다. 가장 대표적인 예로 국무부의 역할이 축소된 것을 들 수 있다. 2025년 7월 국무부는 CDP 안에서 사이버, AI, 양자컴퓨팅 등 첨단기술 관련 업무에 종사하던 인력을 대폭 감축하는 개편을 단행하였고, 그 중에서도 디지털자유를 전담하던 부서는 아예 해체되기에 이르렀다. 이로 인해 국무부의 기술 전문성이 크게 훼손되었다는 지적과 함께 미국의 AI 분야 기술외교가 가치 중심에서 국익 중심으로 완전히 돌아섰다는 평가가 잇따랐다(Miller 2025/07/17). 상무부의 NIST와 그 산하의 CAISI도 상황은 비슷하다. NIST는 AI 위험관리를 위한 자율적 프레임워크(AI RMF)를 통해 AI 생성 허위정보 대응을 위한 국제협력에 참여해왔지만, 트럼프 행정부의 결정에 따라 AI RMF에서 “허위정보(misinformation)”라는 표현이 삭제되면서 해당 이슈 분야의 국제협력도 미온해질 가능성이 커졌다. 그보다 더 큰 변화는 CAISI와 관련한 것인데, 트럼프 행정부는 AI 안정성 증진을 위한 국제협력에 큰 관심을 드러내지 않고 있을뿐더러 2025년 2월 파리 ‘AI 안정성 정상회의’에 참석한 미국 대표단에 CAISI 관계자가 포함되지 않았다는 점에서 해당 기관의 활동도 더욱 제한될 것으로 보인다(Dastin 2025/02/07).

[표 2] 미국의 인공지능 국제전략

| | 바이든 행정부 | 트럼프 행정부 |
|---|---|---|
| **기조** | 규범·윤리 기반, 안전·보안·신뢰성 확보 강조<br>→ 가치 동맹 협력을 통한 AI 거버넌스 구축 | 규제 철폐, 혁신·성장 우선,<br>자국 기업 중심 민간 주도 혁신 강조<br>→ 국익 우선의 거래적 동맹 협력 선호 |
| **이니셔티브** | 국가AI이니셔티브(NAII)/국제 AI안전연구소 네트워크/<br>AI NSM/EU·CoE 등을 통한 협력 | 「AI 행동계획(2025)」,<br>「행정명령 14179호(장벽 제거)」,<br>「행정명령 14320호(AI 수출 촉진)」<br>→ 보호주의·일방주의 협력 |
| **협력 플랫폼** | G7/OECD/GPAI/ISO/EU·CoE/NATO/쿼드/파이브아이즈 등에 적극 참여<br>→ 양자·다자협력 네트워크 활용 | 다자협의체 및 규범협력에 소극적,<br>AUKUS AI 협력 표류,<br>G7/OECD/EU·CoE 참여 약화 |
| **추진체계** | 컨트롤타워에 OSTP/NAIIO 지정,<br>상무부(산하 NIST·AISI)/<br>국무부(산하 S/TECH·CDP)/<br>에너지부/국토안보부/국방부(산하 DIA)/NSF/ODNI/NSA/CIA 등 국제협력에 참여<br>→ 범정부 통합 거버넌스 채택 | OSTP/NAIIO의 컨트롤타워 역할 유지,<br>그러나 국무부의 기술 전문성 축소,<br>NIST/CAISI 역할 약화, 허위정보 대응 축소<br>→ 범정부 통합 거버넌스 약화 |

▪ 출처: 저자 작성

# Ⅳ. 사이버-AI 넥서스와 미국의 동맹외교

이상에서 살펴본 바와 같이, 트럼프 행정부 재출범 이후로 사이버 안보와 AI를 위한 미국의 전략은 각각 '사안별 이익 중심의 단편적 협력'과 '배타적 국익 우선의 거래적 협력'을 선호하는 방향으로 나아가고 있다. 그렇다면 사이버-AI 넥서스 시대에 미국의 사이버 안보 전략과 AI 전략은 어떠한 내용의 국제협력을 모색하게 될까? 사이버-AI 넥서스가 초래하는 다양한 안보 문제를 바라보는 트럼프 행정부의 시각은 바이든 행정부의 그것과 어떠한 차이를 가지는가? 좀 더 구체적으로, 트럼프 행정부는 사이버 위협이 AI로 인해 날로 진화하는 상황을 어떻게 인지하고 있는가? 또는 AI 시스템에 대

한 사이버 공격을 효과적으로 탐지하고 예방하기 위해 트럼프 행정부가 추진하고자 하는 동맹외교는 무엇인가?

물론 '사이버-AI 넥서스'를 위한 별도의 전략이 마련되지 않은 상태에서 이상의 질문에 대한 답을 찾기 위해서는 최근 트럼프 행정부가 사이버 안보와 AI가 융합되는 지점에서 발생하는 문제들에 어떻게 대응하고 있는가를 좀 더 자세히 들여다볼 필요가 있다. 따라서 이 글은 다음의 세 가지 사이버-AI 넥서스 문제에 주목하였다. 첫째, AI가 사이버 작전에 활용됨으로써 증폭되는 위협과 그러한 위협에 대응하는 방법을 모색하는 '군사·정보' 영역의 문제이다. 둘째, AI를 통해 생성되는 허위정보 및 오정보가 선거개입이나 내정간섭으로 이어지는 '정치·사회' 영역의 문제이다. 셋째, 온라인상 악의적 콘텐츠를 탐지·차단하는 수단으로 AI가 도입됨에 따라 발생하는 '데이터·주권' 영역의 문제이다. 이 세 가지 영역의 안보 문제는 트럼프 행정부의 사이버 안보 전략과 AI 전략이 규제에서 멀어져감에 따라 그 심각성을 더해갈 것으로 예상되는 사이버-AI 넥서스 차원의 위협이라 할 수 있다.

## 1. 군사·정보 영역

군사·정보 영역에서 최근 미국이 예의주시하고 있는 사이버-AI 넥서스 문제는 AI가 사이버 작전에 활용됨으로써 증폭되는 사이버 위협과 그러한 위협에 대응하는 방법을 모색하는 일이다. 자동화된 사이버 공격을 대규모로 수행하는 작전이나 정보전의 효율성을 높이기 위해 봇(bot) 계정과 텍스트·이미지·영상을 활용하는 과정에서 AI가 사용되는 사례가 증가하고 있다. 특히 미국과 전략적 경쟁 구도에 있는 중국의 경우, '군민융합(軍民融合)' 전략 아래 무인 시스템, 전장 상황 인식, 다영역 작전 등에 AI를 점진적으로 적용하고 있는 것으로 파악된다. 중국이 AI를 타깃 네트워크에 대한 사전 침투(pre-positioning)의 도구로 이용하고 있다는 분석도 있다. 즉 AI 기술을 통해 특정 네트워크에 대한 지속적이고 일상적인 자동화 접속을 수행함으로써 네트워크 방어자가 접속자를 특정하거나 비정상적 활동을 쉽게 식별하지 못하게끔 하는 전략을 수행하고 있음을 뜻한다. 이러한 공격은 단기적 차원의 성과를 위한 것이라기보다 중장기적인 차원에서 서서히 공격 대상

네트워크에 침투·잠입하여 적당한 때에 막대한 피해를 초래한다는 점에서 더욱 위협적인 것으로 평가된다(Lesser 2025/06/12).

AI를 기반으로 한 중국의 사이버 작전은 그 공격 주체를 식별하기 어렵다는 점에서 미국에 큰 위기로 다가온다. 현재 중국은 민간 부문 기업과 대학 등 '비전통 방산기관'들의 사이버·AI 자원을 군이나 정보기관의 활동과 연계함으로써 제로데이 공격과 같은 침투형 사이버 작전을 활성화하고 있다. 2017년 중국 정부가 도입한 「국가정보법(中華人民共和國國家情報法)」 등 국내법에 따라 중국 기업은 정보기관의 요청이 있을 시 사실상 협력을 거부할 수 없는 위치에 있다. 이로 인해 ICT 및 AI 관련 기업과 플랫폼들이 잠재적 트로이 목마가 될 수 있다는 경고가 지속해서 제기되고 있는 것이다. 특히 최근에는 딥시크(DeepSeek)의 데이터와 알고리즘이 중국 정부의 선전 도구로 활용되고 있다는 지적도 나오고 있는데, 사용자 로그를 정부에 제공하거나 소프트웨어에 백도어를 숨기는 방식, 또는 중국 정부의 이익을 위해 AI 생성 정보를 필터링하도록 강제되고 있는 것으로 추정된다(Grealy 2025).

현재 트럼프 행정부는 군사작전의 맥락에서 사이버와 AI가 결합되는 현상에 다소 이중적인 시각을 내비치고 있다. 2025년 7월 트럼프 행정부는 「AI 행동계획」을 통해 AI가 사이버 공격과 방어 양쪽에서 그 역할을 확대해가고 있다고 경고하며, 미국을 대상으로 이루어지는 적대적 사이버 작전과 AI 기술 간 연관성을 강조하였다. 그러나 또 한편으로는 대러시아 관계와 국내정치적 갈등 상황을 고려하여 사이버 안보를 영향력 공작, 선거개입, 내정간섭 등 정치안보 문제와 분리함으로써 그 범위를 군사안보 영역에 제한하려는 의도 역시 내비치고 있다. 사이버 안보 전략에서 핵심적인 역할을 담당했던 기관들의 기능을 대폭 축소한 결정은 이러한 의도에서 비롯된 것이다. AI를 매개로 중국의 기업과 대학들이 제로데이 공격과 같은 정보기관의 침투형 사이버 작전을 지원하는 상황에서 사이버 안보의 이슈 범위를 축소하는 이 같은 행보는 국제협력의 지평을 좁히는 결과로 이어질 수 있다는 점에서 우려를 낳는다(Chin 2025/09/03).

물론 최근 미국은 군사 분야에서 핵심 동맹국들과 사이버 안보 및 AI 관련 협력을 지속하는 움직임을 보이고 있기는 하다. 대표적으로 AUKUS 첨단기술 부문에서 영국, 호주와 사이버 및 AI를 위한 동맹 협력이 여전히 유

지되고 있다. AUKUS는 트럼프 행정부의 재검토 대상 중 하나로 지목되는 등 외교적 협상 카드로 활용되는 측면이 있어 그 지속가능성을 장담하긴 어렵지만, 당장은 2025년 10월 미호 정상회담을 통해 트럼프 대통령의 지지 의사가 확인됨으로써 당분간은 협력이 지속될 것으로 전망되고 있다(Caisley 2025/10/21). 또한 미국은 최근 능동적 사이버 방어체계를 구축하기 위해 「사이버대응능력강화법(サイバー對處能力强化法)」을 도입한 일본과도 협력을 증진하는 한편 공동연구를 통해 AI 기반 사이버 공격을 차단하는 방법을 함께 모색해나갈 계획임을 밝히기도 하였다. 이는 동맹국 간 정보공유, 전장 인식 및 기타 작전에 사용되는 AI 시스템을 공동으로 개발하고 또 도입함으로써 빠르게 디지털화되고 있는 지휘통제통신 체계의 상호운용성을 끌어올리려는 의도를 반영한다.

다만, 이 같은 협력은 어디까지나 미국의 배타적 이익을 극대화하는 조건 아래에서만 지속되고 있으며, 그 결과 공유된 가치 기반의 협력은 점차 그 동력을 잃어가고 있다. 이는 '공세적 사이버 작전(OCO: Offensive Cyber Operations)'을 둘러싼 미국의 접근을 통해 명확히 드러난다. 2025년 7월 트럼프 행정부는 「하나의 크고 아름다운 법(One Big Beautiful Bill Act)」을 발효하였으며, 그 일부로 OCO 역량 강화를 위해 향후 4년간 10억 달러 규모의 예산을 투입할 계획을 발표하였다(Brewster 2025/7/15). 아직은 능동적 위협 차단을 위한 사이버 작전에 AI를 적용하여 그 효율성을 끌어올릴지 명확히 밝혀진 바 없지만, 진화하는 사이버 위협을 고려할 때 트럼프 행정부는 앞으로 AI를 OCO에 적극적으로 활용해나갈 것으로 전망된다. 실제로 국방 분야에서는 사이버 작전 교육 및 훈련(시뮬레이션)을 위해 AI가 이미 도입되고 있는 것으로 알려지기도 하였다.

OCO의 개발과 활용에 대한 트럼프 대통령의 이해관계는 1차 집권기에 이미 명확히 드러난 바 있는데, 당시 트럼프 행정부는 적대 세력의 사이버 공격을 원천적으로 차단하기 위해 역으로 OCO를 수행할 필요가 있음을 줄곧 강조하였다. 그 과정에서 사이버 방어의 개념을 적의 사이버 공격을 사전에 탐지하고 차단하는 '선제적 방어(defend forward)'와 '지속적 개입(persistent engagement)' 능력으로 확대하는 등 OCO의 제도적·전략적 기반을 마련한 것으로도 평가된다(김소정 2025). 트럼프 1기 행정부의 OCO

정책은 바이든 행정부 시기에도 지속되었는데, 바이든 행정부는 특히 파이브 아이즈 동맹국들과 협력하여 OCO가 국제법의 울타리 안에서 이루어질 수 있다는 인식을 대외적으로 확산시킴으로써 그 당위성을 마련해가고자 노력하였다.

문제는 현재 OCO에 대한 트럼프 2기 행정부의 접근이 그 적용 대상과 범위 측면에서 명확하지 않다는 데 있다. 앞서 언급한 것처럼, 트럼프 행정부는 정치적 이해관계에 따라 사이버 안보의 이슈연계 가능성을 의도적으로 외면하거나, 사이버 안보를 군사안보 문제로 축소하여 접근하려는 경향을 보인다. 특히 OCO의 주된 대상이 되어야 할 러시아발 사이버 공격에 대해 모호한 해석을 내놓고 있다. 그에 따라 사이버 안보 협력 역시 사안별 이익 중심의 단편적 협력의 형태로만 이루어지고 있어 동맹국과의 긴밀하고 장기적인 공조를 보장하기 어려운 상황이다. AI로 인해 사이버 위협이 양적·질적으로 심화하는 가운데 미국이 보이는 이 같은 행보는 오히려 OCO를 둘러싼 가치 동맹 중심의 협력이 제대로 이루어지지 못하게끔 하는 요인으로 작용할 수 있다. 무엇보다 중국, 러시아 등 권위주의 국가들의 사이버 위협을 염두에 두고 그동안 파이브 아이즈 동맹 차원에서 추진되어온 OCO 공조의 역할 분담, 기술협력, 규범화 담론 등이 점차 동력을 상실할 가능성도 배제하기 어렵다.

## 2. 정치·사회 영역

정치·사회 영역에서 미국의 안보를 위협하는 사이버-AI 넥서스는 AI 생성 허위정보를 통해 이루어지는 영향력 공작의 형태로 나타난다(Mchangama & White 2024/02/26). AI 기반 영향력 공작은 자유로운 인터넷 환경을 지향하는 민주주의 국가들의 내재적 취약점을 효과적으로 공격하여 정부에 대한 불신과 사회적 불안정을 단기간 내에 초래할 수 있다. 특히 AI 학습에 사용되는 데이터를 악의적으로 조작하는 데이터 오염(data poisoning)과 AI 모델에 대한 탈옥(jail-break) 공격이 이러한 정치·사회안보적 위협을 심화하는 원인이 되고 있다. 실제로 중국이 상업용 AI를 정보원 포섭 전략의 도구로 활용하고 있다는 분석도 제기된 바 있다. 그동안 중국은 소셜미디어 플랫폼을 활용하여

외국의 정부 관계자, 군인, 학자 등을 정보원으로 포섭하는 전략을 취해왔는데, 상업용 AI 모델이 이러한 작전의 속도와 규모 그리고 성공 가능성을 높이는 데에 도움을 제공하고 있는 것으로 알려져 있다. 이러한 전략은 정보수집(intelligence gathering)과 지식공유(knowledge sharing) 사이의 모호한 경계를 착취하는 방식으로 이루어진다는 점에서 대응이 더욱 어려운 것으로 평가된다.

바이든 행정부 집권기 미국은 AI 영향력 공작이 군사·기술·사회·경제 분야에서 국가안보 위기를 심화하고 있으며, 특히 권위주의 국가들이 AI를 악용해 생성하는 허위정보가 민주주의 기반을 위협한다고 보았다. 일례로 ODNI가 2023년 발간한 『연례위협평가』 보고서는 머신러닝과 (빅)데이터 분석 기술이 급격히 발달하면서 미국 정부와 기업 그리고 국민의 중요 데이터가 정치적 담론을 형성하는 전략 자원으로 악용되고 있다고 밝혔다. 2024년도 보고서 역시 AI를 활용한 중국과 러시아의 영향력 공작 활동이 미국의 선거를 위협하고 민주주의를 훼손할 수 있음을 경고하였다(ODNI 2024). 그러나, 재차 강조하듯, 현재 트럼프 행정부는 선거에 대한 위협을 사이버 안보와 분리하여 인식하는 경향을 보이고 있으며, 이는 AI 기반 영향력 공작 위협을 의도치 않게 '탈안보화(de-securitisation)'하는 결과로 이어지고 있다.

물론 2025년 3월 ODNI가 발간한 『연례위협평가』 보고서에도 중국과 러시아의 AI 기반 사이버 공격과 영향력 공작에 대한 위협인식이 담겼지만, 트럼프 행정부의 정책은 그러한 인식과는 일치하지 않는 방향으로 나아가고 있다. 트럼프 대통령은 당선 직후 CISA의 영향력 공작 및 선거 안보 관련 활동을 중단시키는 한편 ODNI 산하에 설치된 해외악성영향센터(FMIC: Foreign Malign Influence Center)의 해체 및 기능 통합을 예고하였다(Madhani, Tucker & Swenson 2025/08/21). FBI의 해외위협 전담팀 역시 해체 절차를 밟게 되었다. 이들 기관은 바이든 행정부 집권기에 영향력 공작에 대한 범정부 대응을 총괄하거나 지원하는 기관이었다는 점에서 안보적 공백을 경고하는 목소리가 작지 않다(Itkowitz, et al 2025/02/08). 이에 더하여 트럼프 대통령이 러시아에 대한 OCO 수행을 중단하도록 지시하면서 AI 기반 영향력 공작 대응을 위한 동맹 차원의 협력도 약화될 것이라는 우려 섞인 전망도 제기된다(Nakashima & Menn 2025/03/01).

한편 NIST가 AI 시스템의 설계·개발·도입·활용 과정에서 발생할 수 있는 위험을 관리하기 위해 공공기관, 기업, 연구기관 등에 제공한 AI RMF에서 “허위정보” 항목이 빠지게 된 것 역시 사이버-AI 넥서스 대응을 위한 국제 협력에 부정적인 영향을 미칠 우려가 있다. 바이든 행정부 시기 NIST는 EU, 일본 등 파트너국들과 AI 규제 표준 및 지침의 호환성을 높이기 위해 AI RMF를 지속해서 조율하고 맞춰나갈 계획을 내놓은 바 있다. 하지만 AI를 활용한 영향력 공작 위협이 심화하는 상황에서 트럼프 행정부 재출범과 동시에 미국이 허위정보 문제를 안보 위협이 아닌 정치적 쟁점으로 간주하게 되면서(Knight 2025/03/14), AI 생성 허위정보를 여전히 중대한 위험으로 받아들이는 동맹국 및 파트너국들과의 협력 범위가 축소될 가능성이 커지고 있다. G7의 ‘히로시마 AI 프로세스’, EU의 「AI법」, OECD의 「AI 권고안」 등이 AI 생성 허위정보·오정보·딥페이크에 공동으로 대응할 필요성을 강조한다는 점에서 미국의 동맹외교가 전개될 공간이 줄어들 수 있음을 의미한다.

정치·사회 영역에서 발생하는 또 다른 사이버-AI 넥서스는 AI 학습 데이터가 오염되거나 AI 모델에 대한 탈옥 공격이 이루어지면서 유해하고 악의적인 결과물이 생성되는 문제이다. 이는 앞서 조명한 AI 기반 영향력 공작과도 밀접한 관련이 있는데, AI 시스템이 학습하는 데이터를 의도적으로 오염시켜 정치적·문화적 편향성을 키우거나, AI 안전장치를 우회하여 윤리적으로 적절하지 않은 악의적 허위정보를 생성·확산함으로써 선거개입, 내정간섭, 사회분열 등을 초래할 수 있기 때문이다. 데이터 오염과 AI 탈옥 공격은 최근 트럼프 행정부가 AI 전략의 초점을 혁신과 성장에 맞춤에 따라 더욱 심화할 가능성이 크다. 트럼프 대통령은 경제 성장에 대한 자신감의 원천으로 자신의 행정부와 기업 간 긴밀한 관계를 강조하며, 기업 친화적이고 시장 주도적인 기술 정책을 선호하고 있다. 크라치오스(Michael Kratsios) OSTP 실장 역시 “바이든 행정부는 (AI) 기술이 국가에 가져올 수 있는 피해를 분석하고 예측하는 등 약속보다는 두려움의 정신으로 이끌었다”고 비판하며, AI 규제 완화와 시장 주도 혁신을 지향하는 트럼프 행정부의 접근을 치켜세웠다(Moynihan 2025/05/08). 정부의 규제에 부담을 느끼는 산업계도 이러한 변화를 긍정적으로 평가한다(Zakrzewski & Natanson 2025/07/24).

이 같은 상황은 데이터 오염과 AI 탈옥에 대한 미국의 대응이 효과적으로 이루어지기 어려운 환경적 조건이 될 수 있다. 기업에 대한 규제를 완화하는 조치가 데이터 품질 관리 규제의 약화로 이어질 가능성을 배제하기 어렵기 때문이다. 신속한 기술 개발과 상용화에 높은 이해관계를 가지는 기업이 AI 탈옥 방어를 위한 메커니즘을 충분히 검증하지 않은 채로 기술을 제공할 위험도 크다. 탈옥은 미시적인 차원에서 반복적으로 이루어지는 기술 안전의 문제라는 점에서 이를 관리하기 위해서는 그 개발 주체인 기업의 역할이 특히 중요한데, 기업은 정부와 달리 공익을 추구할 의무가 없으므로 상황에 따라 안정성 검증에 소극적일 수 있기 때문이다.

더 큰 문제는 미국과 동맹국 간 AI 시스템과 데이터의 신뢰성·안전성·책임성에 대한 정합성이 감소하여 데이터 오염과 AI 탈옥에 대한 공동대응이 원활히 이루어지지 못하는 상황이 발생하는 것이다. 트럼프 행정부의 AI 전략은 기본적으로 미국의 배타적 국익을 극대화하는 거래적 협력만을 고집하는 경향을 보인다는 점에서, 자국에 대한 직접적인 경제적 손실이나 안보적 피해가 발생하지 않는 이상 AI 시스템과 데이터 품질을 관리·규제하는 국제협력에 적극적으로 나서지 않을 가능성이 작지 않다. 이는 결국 AI 규제 거버넌스에 대한 미국의 리더십이 동맹국들의 지지를 확보하는 데 실패하게 될 위험으로 이어지며, 종국에는 다중이해당사자주의와 민주주의 등 핵심 가치에 기초한 글로벌 AI 거버넌스 구축을 저해하는 결과를 초래할 수도 있다.

## 3. 데이터·주권 영역

끝으로, 콘텐츠를 검열하는 기술로서 AI가 도입됨에 따라 발생하게 되는 데이터 안보 문제도 미국이 당면한 사이버-AI 넥서스 차원의 위협이다 (Goldstein & DiResta 2023). AI 기반 검열은 AI 산업 진흥과 치안 강화의 측면에서 분명 혜택을 제공하지만, 그와 동시에 사회적 분열과 국제적 갈등을 초래하는 양날의 검이 될 수 있다. AI는 그 기술적 특성으로 인해 내재적인 편향과 환각(hallucination)에서 자유롭지 않기 때문에 콘텐츠 검열 수단으로 AI가 활용될 경우 방대한 데이터를 수집하는 과정에서 프라이버시 침해와 표현의 자유 억압 등이 발생할 수 있다. 더 큰 문제는 AI의 자동화된

데이터 수집 활동이 국경을 넘어 이루어지게 되면서 타국의 '데이터 주권(data sovereignty)'을 위협하는 문제로 이어질 수 있다는 점이다. 물론 데이터 부문에서 선두를 달리는 미국의 입장에서는 이러한 문제가 언뜻 보기에 심각하지 않은 것으로 비칠 여지가 있다. 하지만 미국 정부나 기업의 AI 기반 데이터 수집과 콘텐츠 검열 활동이 동맹국 및 파트너국을 대상으로 이루어질 경우, 이는 데이터 주권 침해나 디지털 식민주의(digital colonialism) 위협으로 인식되면서 데이터의 자유로운 이동을 옹호하는 미국 주도의 담론과 연대에 부정적인 영향을 미칠 가능성이 크다. 데이터 안보 분야 미국의 리더십이 심각하게 훼손될 수 있음은 물론이다.

이미 미국은 사이버 위협 탐지와 콘텐츠 검열을 위해 AI를 활용하고 있는데, 2025년 1월 바이든 행정부는 사이버 안보에 대한 마지막 조치로 백악관을 통해 「행정명령 제14144호」를 발표하여 사이버 공격자에 대한 제재의 실효성 강화와 사이버 범죄 대응을 위해 AI를 활용할 필요성을 강조한 바 있다. 그리고 트럼프 행정부도 「행정명령 제14306호」에서 AI가 "사이버 취약점을 신속하게 식별하고, 위협 탐지 기술의 규모를 늘리며, 방어를 자동화함으로써 사이버 방어를 혁신할 수 있는 잠재력을 가지고 있다"고 명시하였다. 더 나아가 2025년 5월에는 플랫폼 기업에 딥페이크 콘텐츠 삭제를 요구하는 「테이크잇다운법(Take It Down Act)」이 발효되기도 하였다. 일각에서는 동 법률의 조치가 종단간 암호화(E2EE) 해제를 강요할 여지가 있으며, 동시에 공정한 논평부터 뉴스 보도에 이르기까지 합법적인 콘텐츠도 삭제 대상으로 인식하는 자동화 필터링 기술에 의존한다는 점에서 표현의 자유를 억압할 위험이 크다고 경고하고 있다(Ortutay 2025/05/21).

물론 「테이크잇다운법」처럼 AI 생성 악의적 콘텐츠의 확산을 저지하는 조치는 EU의 「AI법」이나 영국·호주의 「온라인안전법(Online Safety Act)」과 마찬가지로 딥페이크 규제를 강화하는 한편 소셜미디어와 플랫폼 기업의 윤리적·법적 책임을 강조한다는 점에서 글로벌 AI 규범을 선도하는 미국의 위치를 확고히 하는 데 기여하는 바가 분명히 크다. 또한 파이브 아이즈와 같은 동맹 네트워크 차원에서 딥페이크 대응 공조체계를 마련하고 법제적 협력을 추진하는 과정에도 도움이 될 수 있다. 그러나 다른 한편으로 미국 기업이 악의적 콘텐츠 검열 규제를 준수하기 위해 자국 밖에서 생

산·보관되는 데이터까지 감시의 대상으로 삼게 될 경우, 이는 데이터 주권 위협과 같은 의도치 않은 역외적 효과를 낳을 위험이 있다. 더욱이 2018년 트럼프 1기 행정부 시기에 도입된 「클라우드법(CLOUD Act)」이 이미 해외 데이터에 대한 미국 수사기관의 접근을 허용하는 근거가 되고 있다는 점에서 AI 기반 검열과 데이터 주권 침해 간 상관관계를 외면하기 어려운 상황이다(Mellor 2025/03/27). 이러한 우려는 현재 트럼프 행정부의 사이버 안보와 AI 전략이 동맹국의 사정에는 별다른 관심을 보이지 않은 채 미국의 배타적 이익을 우선하는 방향으로만 작동하고 있다는 점을 고려할 때 더욱 무겁게 다가온다.

설상가상으로 최근 중국이 자국의 값싼 AI 모델을 글로벌 사우스 국가들에 수출하며 점차 중국형 데이터 안보 거버넌스 모델을 확산해나가는 추세는 데이터·주권 영역에서 미국의 동맹외교를 한층 더 어렵게 만드는 요인이 되고 있다. 그동안 중국은 개별 국가의 데이터 통제 권리를 강조하는 국가주권 중심의 데이터 안보 거버넌스를 추구하며 서방 세계와 끊임없이 충돌해왔다. 2020년 중국이 발표한 「글로벌 데이터 보안 이니셔티브(全球數据安全倡議)」 역시 표면상 진영을 따지지 않는 협력을 표방하지만, 실제로는 데이터 국지화와 정부 통제를 정당화하는 논리를 담고 있다(Webster & Triolo 2020/09/07). 따라서 중국이 강조하는 데이터 주권 보호 원칙은 자국에만 적용되는 기준일 뿐 중국산 AI 모델을 수용하는 국가들의 데이터 주권을 보호하는 데에는 사실상 적용되지 않는다고 봐야 할 것이다. 앞서 언급한 것처럼, 중국산 AI 모델은 국내 법령에 따라 정부의 요구가 있을 경우 사용자 정보와 데이터를 제공할 수밖에 없기 때문이다. 딥시크의 경우에도 개인정보취급방침에 사용자 데이터를 "중화인민공화국 내 보안서버"에 저장할 수 있다는 조항을 포함하고 있다(장은지 2025/01/30). 그럼에도 불구하고, 당장 프라이버시 침해나 데이터 착취를 돌아볼 여유가 없는 글로벌 사우스 국가들은 값싼 중국산 AI 모델의 실용성만을 고려하여 이를 도입하는 데 거리낌이 없다.

이처럼 중국산 AI 모델의 확산에 힘입어 데이터 주권 담론이 이전보다 더 힘을 얻고 있는 상황은 미국의 AI 기반 데이터 검열 조치가 동맹국 및 우방국의 데이터 주권을 침해할 수 있다는 우려와 맞물리면서 결과적으로 미국에 불리하게 작용할 가능성이 크다. 더 큰 문제는 바이든 행정부 시기 상당

한 수준의 성과를 거둬온 민주주의 기반의 글로벌 데이터 안보협력이 축소되거나 와해될 수 있다는 점이다. 트럼프 행정부는 1차 집권기에 해당하는 2019년 일본 정부와 함께 데이터의 자유로운 흐름과 반(反)국지화(data localisation)를 촉구하는 「오사카 트랙(Osaka Track)」을 발족시켰고, '신뢰할 수 있는 데이터 유통론'을 강조했던 바이든 행정부도 이에 협력적 자세를 유지하였다. 현재 트럼프 2기 행정부 역시 여전히 데이터 국지화에 반대하며 디지털 무역 확대를 위한 자유로운 데이터의 유통을 옹호한다는 점에서 정책적 지속성을 보인다. 그러나 AI 기반 데이터 검열 조치로 인해 미국의 이 같은 데이터 유통론은 데이터 식민주의와 디지털 기술 봉건주의를 위한 수단으로 곡해될 위험에 직면해 있다. 이는 결국 민주주의와 인권 등 공유된 가치에 근거한 데이터 안보 거버넌스를 창출하고자 그동안 미국이 주도해온 국제협력에 걸림돌이 될 수밖에 없다.

# Ⅴ. 결론

이 글은 바이든 행정부와 트럼프 2기 행정부를 중심으로 미국의 사이버 안보 국제전략과 AI 국제전략을 살펴봄으로써 변화의 추이를 조명하고, 사이버 안보와 AI가 교차하는 지점에서 현재 미국의 동맹외교가 당면하고 있는 문제들을 살펴보았다. 바이든 행정부는 민주주의 가치 연대를 강조하며 규범과 제도 형성을 위한 동맹 협력을 추구하였으나, 트럼프 행정부는 규제보다는 혁신과 산업적 이익을 우선함에 따라 단편적이고 거래적인 동맹 협력을 선호하고 있다. 그로 인해 사이버 안보와 AI를 위한 미국의 전략은 국제협력의 이니셔티브와 플랫폼 그리고 추진체계 면에서 빠르게 변화하고 있으며, 그 결과 사이버-AI 넥서스 차원에서 발생하는 문제들에 대응하는 과정에서 동맹외교가 전개될 공간은 점점 줄어들고 있다.

물론 트럼프 행정부가 재출범 이후 첫해를 보내고 있는 지금, 미국의 사이버 안보 전략과 AI 전략은 과도기를 거치고 있다는 점에서 이 글에 담긴 분석과 전망을 기정사실로 여기는 것은 시기상조일 수 있다. 또한 사이버-AI 넥서스에 대한 동맹 중심의 국제협력도 지금보다 더 적극적으로 모색

될 가능성을 완전히 배제하긴 어렵다. 트럼프 대통령의 「행정명령 제14306호」도 악의적 사이버 활동을 수행하는 국가로 중국뿐만 아니라 러시아, 이란, 북한 등 전통적인 적대국들을 지목함으로써 바이든 행정부 집권기 사이버 안보 국제협력을 뒷받침했던 '권위주의에 대항하는 민주주의 연대' 기조가 유지될 여지를 남겨두었기 때문이다. 앞서 소개한 사이버-AI 넥서스의 문제들이 만약 2018년 발발한 이른바 '화웨이 사태'처럼 권위주의 국가가 연관된 특정 이슈를 계기로 쟁점화된다면, 트럼프 행정부도 민주주의 동맹 네트워크를 다시금 적극적으로 활용할 수밖에 없을 것이다. 그러나 사이버-AI 넥서스 대응을 위한 미국 주도의 민주주의 연대와 동맹 협력은 사안별 이익에 집중된 단편적이고 거래적인 협력과는 거리가 멀다는 점에서 당장은 이를 기대하기는 어려울 것이다.

따라서 미국과 동맹 관계에 있는 한국은 앞으로의 변화 양상을 더욱 주시해야만 한다. 사이버-AI 넥서스가 군사·정보, 정치·사회, 데이터·주권 영역에서 초래하는 문제들은 북한과 마주한 한국에게 특히 위협적일 수밖에 없는데, 사이버 안보와 AI에 대한 미국의 접근이 각각 규범보다 국익을, 규제보다 혁신을 우선하는 상황은 한국이 위협 대응을 위한 가치 동맹 차원의 긴밀한 협력을 기대하기 어렵게 만들기 때문이다. 당장 OCO의 개발과 활용을 둘러싼 국제협력은 북한에 대한 공세적 사이버 방어가 절실한 우리에게 가장 중요한 문제이다. 앞서 윤석열 정부 집권기에 한국은 북한 등 외부 세력의 사이버 공격에 대해 공세적인 방어로 맞서는 전략을 수립하였고, 이는 당시 바이든 행정부의 통합적 억지 전략과 맥이 닿으며 한미 간 사이버 안보협력을 강화하는 기제로 작용하였다(신승휴 2023). 그러나 현재 미국이 정치적 이해관계와 사안별 이익에 따라 OCO의 실행 범위와 대상을 모호하게 설정하는 경향을 보인다는 점에서 대북 견제를 위한 한국의 공세적 사이버 방어는 미국의 지원과 협조를 확보하는 데 어려움을 겪게 될 가능성이 있다.

한편 선거개입과 허위정보 문제를 사이버 안보 분야에서 분리하려는 미국의 움직임도 북한의 대남 영향력 공작이 갈수록 심화하는 상황을 고려할 때 한국에게는 여러모로 이롭지 않다. 해킹이나 피싱 등 사이버 공격의 형태로 이루어지는 북한발 선거공작이 AI를 통해 이전보다 훨씬 더 자동화되고, 그와 동시에 우리 정부와 사회의 디지털화가 빠르게 이루어지게 되면서

AI 생성 허위정보를 활용한 사이버 공격은 그 어느 때보다 더 심각한 위협이 되고 있다. 이에 대한 대응은 단연 미국과의 긴밀한 정보공유와 사이버 안보협력을 필요로 한다. 만약 트럼프 행정부의 미국이 사이버 안보와 여타 정치안보 이슈 간 연계 가능성을 지속해서 축소하며 AI 기반 영향력 공작과 선거개입 위협을 사이버 안보와 구분 지어 대응한다면, 한국으로서는 AI 생성 허위정보와 사이버 공격을 통해 이루어지는 북한발 선거공작을 차단하는 과정에서 미국과의 밀도 높은 공조를 기대하기 더욱 어려워질 것이다.

끝으로, 미국의 AI 기반 콘텐츠 검열 조치가 글로벌 플랫폼과 AI 모델을 매개로 데이터 주권을 위협하는 상황도 우리에게 부담스럽긴 마찬가지이다. 이미 한국은 챗GPT와 같은 미국산 AI 모델과 ICT 기술이 소비되는 주요 시장 중 하나이며, 미국이 주도하는 데이터 유통 담론을 지지하는 동맹국이기도 하다. 미중 기술패권 경쟁이 심화하면서부터 디지털 기술 분야에서 한미 간 교류 역시 갈수록 더 증대하고 있다. 이는 달리 말해 한국의 데이터 주권이 미국 기업의 데이터 수집 활동과 미국 정부의 AI 기반 콘텐츠 검열에 따른 위협에 많은 부분 노출되어 있음을 의미한다. 물론 미국을 포함한 강대국의 데이터 착취에 대처하기 위해 최근 우리 정부도 「AI 기본법」을 제정하고 '소버린 AI(sovereign AI)' 개발에 박차를 가하고 있다. 그러나 미국이 앞으로도 자국의 경제적·안보적 이익을 앞세워 동맹국에 기술 수용을 강제하며 데이터 주권을 직간접적으로 위협한다면, 한국은 더욱 곤란한 처지에 놓일 수밖에 없을 것이다. 미국이 배타적 이익을 위한 단편적·거래적 협력이 아닌 공유된 가치를 추구하는 협력으로 나아가길 기대할 수밖에 없는 이유이다. 결국 사이버-AI 넥서스 시대의 불확실성 속에서 한국에게 주어진 과제는 미국의 전략적 변화가 동맹국들에게 전가할 수 있는 비용과 위험을 면밀히 검토하는 일이라 할 수 있다.

## | 참고문헌 |

### 1. 논문 및 단행본

김상배 (2023). “사이버 억지의 새로운 개념화: '한미 사이버 안보 동맹론'의 성찰적 맥락에서.” 『국제정치논총』. 제63집 제2호, pp. 51-88.

김상배 (2025). “미중 인공지능 패권경쟁과 한국: 국제정치의 전환과 중견국의 국가전략.” 『국가전략』. 제31권 제2호, pp. 101-132.

김소정 (2025). “미국 사이버공간의 선제적 방어 전략과 한국에의 시사점.” 『평화학연구』. 제26권 제2호, pp. 7-30.

신승휴 (2023). “한미 사이버 안보협력의 진화: 복합지정학의 시각.” 『국제정치논총』 제63집 제3호, pp. 95-149.

신승휴 (2025). “파이브 아이즈 국가의 사이버 안보 전략 동조화: 정책지향성과 추진체계를 중심으로.” 『국제지역연구』. 제20권 제2호, pp. 3-36.

Johnson, James (2019). “The AI-cyber nexus: implications for military escalation, deterrence and strategic stability.” *Journal of Cyber Policy.* Vol. 4. No. 3, pp. 442-460.

Khan, Khalid, Khurshid, Adnan, and Cifuentes-Faura, Javier (2024). “Is artificial intelligence a new battleground for cybersecurity?.” *Internet of Things.* Vol. 28, 101428.

### 2. 정부자료

CISA (2025). “AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems.” (May 22).

NIST (2024). “FACT SHEET: U.S. Department of Commerce & U.S. Department of State Launch the International Network of AI Safety Institutes at Inaugural Convening in San Francisco.” (November 20). https://www.nist.gov/news-events/news/2024/11/fact-sheet-us-department-commerce-us-department-state-launch-international

NSCAI (2021). *NSCAI Final Report.* March.

ODNI (2023). *Annual Threat Assessment of the U.S. Intelligence Community.* February 6.

The White House (2021). “Quad Principles on Technology Design, Development,

Governance, and Use." (September 24). https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/

The White House (2022). "FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity." (October 11). https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/

The White House (2023a). *National Cybersecurity Strategy.* March.

The White House (2023b). "A Proclamation on Cybersecurity Awareness Month, 2023." (September 29). https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/09/29/a-proclamation-on-cybersecurity-awareness-month-2023/

The White House (2023c). "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." (October 30). https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

The White House (2024a). *National Cybersecurity Strategy Implementation Plan, Version 2.* May.

The White House (2024b). "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." (October 24). 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/

The White House (2025a). "Removing Barriers to American Leadership in Artificial Intelligence." (January 23). https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence

The White House (2025b). "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order

14144." (June 6). https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

The White House (2025c). *Winning the Race: America's AI Action Plan.* July.

U.S. Department of State. 2024. *United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future.* May 6.

### 3. 보고서

Allen, Gregory and Adamson, Georgia (2024). "The AI Safety Institute International Network: Next Steps and Recommendations." CSIS Report (October).

Goldstein, Josh A. and DiResta, Renee (2023). "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations." Cyber Policy Center Report, Stanford University (January 11).

Grealy, Andrew (2025). "China's AI Surge: New Front in Cyber Warfare." Armis Labs.

Lohn, Andrew (2025). "Anticipating AI's Impact on the Cyber Offense-Defense Balance." Centre for Security and Emerging Technology Policy Brief (May).

### 4. 신문·잡지·인터넷 자료

장은지 ""딥시크, 중국내 서버에 개인정보 저장"…정보유출 우려 제기." 『동아일보』. 2025년 1월 30일.

Brewster, Thomas. "The Wiretap: Trump's $1 Billion Offensive Cyber Budget." *Forbes* (July 15, 2025).

Caisley, Olivia. "Trump ends AUKUS uncertainty with firm backing for Albanese." *ABC News.* October 21, 2025.

Cassidy, Christina. "Trump administration halts funding for two cybersecurity efforts, including one for elections." *AP News.* March 11, 2025.

Chin, Josh. "China Is Using the Private Sector to Advance Military AI." *The Wall Street Journal.* September 3, 2025.

Dastin, Jeffrey. “Exclusive: Trump's Paris AI summit delegation won't include AI Safety Institute staff, sources say.” *Reuters.* February 7, 2025.

Fontaine, Richard. “The Trump-Biden-Trump Foreign Policy: American Strategy's Strange Continuity.” *Foreign Affairs.* January 20, 2025.

Freedberg, Sydney. “AI For Five Eyes? New bill pushes AI collaboration with UK, Australia, Canada, New Zealand.” *Breaking Defense.* November 22, 2023.

Gegeon, Joseph. “Trump administration shutters US office countering foreign disinformation.” *The Guardian.* April 16, 2025.

Itkowitz, Colby, et al. “Trump administration cuts teams that fight foreign election interference.” *The Washington Post.* February 8, 2025.

Kelley, Alexandra. “State Department Creates First Office Devoted to Emerging Technology Diplomacy.” *Nextgov.* January 4, 2023.

Knight, Will. “Under Trump, AI Scientists Are Told to Remove ‘Ideological Bias’ From Powerful Models.” *Wired.* March 14, 2025.

Kroet, Cynthia. “US companies still engaging with AI Code despite Trump, says EU official.” *Euro News.* May 8, 2025.

Lesser, Max. “New Report Shows How China Uses AI to Augment its Online Intelligence Operations.” Foundation for Defense of Democracies. June 12, 2025.

Madhani, Aamer, Tucker, Eric, and Swenson, Ai. “Gabbard slashing intelligence office workforce and cutting budget by over $700 million.” *AP News.* August 21, 2025.

Magee, Tamlin. “Trump cyber cuts put US allies on guard.” *Raconteur.* April 15, 2025.

Mchangama, Jacob and White, Jules. “The Future of Censorship Is AI-Generated.” *Time.* February 26, 2024.

Mellor, Chris. “Data sovereignty in focus as Europe scrutinizes US cloud influence.” *Blocks & Files.* March 27, 2025.

Miller, Maggie. “State Department cyber, tech cuts deeper than previously known.” *Politico.* July 17, 2025.

Miller, Maggie and Roussi, Antoaneta. “Trump's return freezes Western cyber plans to counter Russia, China.” *Politico.* February 12, 2025.

Miller, Maggie and Sakellariadis, John. “Trump executive order takes steps to protect domestic hackers from blowback.” *Politico.* June 6, 2025.

Mok, Charles. “The US Aims to Win the AI Race, But China Wants to Win Friends First.” *Tech Policy.* August 8, 2025.

Moynihan, Lydia. “Michael Kratsios-Trump’s go-to tech policy guy-reveals how the US needs to step up its innovation plan.” *New York Post.* May 8, 2025.

Motwani, Nishank. “America Is Watching: AUKUS Needs More Than Rhetoric From Australia.” *The Diplomat.* September 3, 2025.

Murgia, Madhumita and Espinoza, Javier. “US, Britain and Brussels to sign agreement on AI standards.” *Financial Times.* September 5, 2024.

Nakashima, Ellen and Menn, Joseph. “As Trump warms to Putin, U.S. halts offensive cyber operations against Moscow.” *The Washington Post.* March 1, 2025.

Ortega, Bob. “Trump is dismantling election security networks. State officials are alarmed.” *CNN.* April 9, 2025.

Ortutay, Barbara. “President Trump signs Take It Down Act, addressing nonconsensual deepfakes. What is it?.” *AP News.* May 21, 2025.

Pillay, Tharin. “U.S. Gathers Global Group to Tackle AI Safety Amid Growing National Security Concerns.” *Time.* November 21, 2024.

Psaledakis, Daphne. “US State Department closing office aimed at countering foreign disinformation.” *Reuters.* April 17, 2025.

Ribeiro, Anna. “Sean Plankey pledges to rebuild, refocus CISA as lawmakers warn of weakened cyber defense posture.” *Industrial Cyber.* July 28, 2025.

Roughead, Gary, et al. “Don’t Abandon AUKUS: The Case for Recommitting to-and Revitalizing-the Alliance.” *Foreign Affairs.* September 2, 2025.

Rundle, James. “Top U.S. Cyber Agency Faces Staff and Funding Cuts in New Budget.” *The Wall Street Journal.* June 2, 2025.

Smalley, Suzanne. “U.S. and EU to launch first-of-its-kind AI agreement.” *Reuters.* January 28, 2023.

Webster, Graham and Triolo, Paul. “Translation: China Proposes 'Global Data Security Initiative'.” New America. September 7, 2020.

Zakrzewski, Cat and Natanson, Hannah. “Silicon Valley’s bet on Trump starts to pay off.” *The Washington Post.* July 24, 2025.

| **논문투고일** : 2025년 10월 24일 |
| **논문심사일** : 2025년 11월 17일 |
| **게재확정일** : 2025년 11월 20일 |

| ABSTRACT |

# The Cyber-AI Nexus and the U.S. Alliance Diplomacy:
## From Biden to Trump

Seung Hugh SHIN
(PhD Candidate, Department of Political Science and International Relations, Seoul National University)

This study examines the evolving trajectory of U.S. strategies in cybersecurity and Artificial Intelligence(AI), with particular attention to the shifting patterns of international engagement. Despite the growing imperative for global cooperation under the emerging 'cyber-AI nexus', U.S. approach is increasingly leaning toward fragmented and transactional forms of collaboration, moving away from comprehensive and integrated alliance cooperation grounded in shared values. To substantiate this argument, the study examines how successive administrations-from Biden to Trump's second term-have framed international cooperation and alliance diplomacy in the domains of cybersecurity and AI. The study investigates the guiding principles, initiatives, cooperation platforms, and governance mechanisms embedded in these strategies, to identify distinctive characteristics across periods and capture broader trends of change over time. Based on the analysis, the study traces how the evolving trajectory of U.S. alliance diplomacy has responded to the challenges emerging from the cyber - AI nexus.

▪ Key words Cybersecurity, Artificial Intelligence, Alliance, Biden, Trump