FOCUS 2

AI-사이버 우위 확보를 위한 미국의 정책 동향과 시사점

· **이경복** | 한국국방연구원 국방인공지능정책연구실 연구위원 | kblee@kida.re.kr

· **박태현** | 한국국방연구원 미래전략실 선임연구원 | tpark@kida.re.kr

글로벌 기술패권 경쟁과 국가안보 관점의 AI-사이버 융합 이슈 부상

오늘날 첨단과학기술을 둘러싼 기술패권 경쟁은 단순 산업 성장이나 기술 우위를 넘어 국가안보의 임계치를 결정짓는 이른바 '기술 내셔널리즘(Tech-Nationalism)'의 시대를 앞당기고 있다. 초기 기술패권 경쟁은 글로벌 표준 선점 등 국제안보의 주도권 다툼이었다. 하지만 이제는 반도체 공급망과 데이터 주권을 무기화하는 경제안보 이슈로 자리 잡았고, 더 나아가 전쟁의 승패를 가르는 군사안보로 급격히 확장되고 있다. 사실 기술패권 경쟁의 군사적 확장과 충돌은 최근의 이슈가 아니다. 2022년 시작된 러시아-우크라이나 전쟁에서 등장한 위성통신 방해, 드론 활용, 정밀 타격을 위한 AI 분석 등 첨단기술 활용은 기술패권의 군사적 영향력을 이미 확인시켰다. 2024년 발생한 이란-이스라엘 분쟁도 첨단기술이 정보 우위를 넘어서 전장의 양상을 규정하는 실질적 억지력으로 작동함을 보여주었다.[1][1] 지난 2월, 미국과 이스라엘이 이란에 공습을 단행한 '에픽 퓨리 작전(Operation Epic Fury)'은 AI가 군사작전을 돕는 보조적인 기술이 아니라 군사작전 계획과 작전 수행을 주도하는 핵심 능력임을 입증하였다.[2][2]

이처럼 안보의 경계가 기술 중심으로 재편되는 가운데, 기술패권 경쟁의 상징이자 사회를 혁신하는 게임체인저인 AI는 국가 및 군사안보를 위협하는 새로운 무기로 부상하고 있다. AI는 디지털화된 사이버공간에서 주로 동작하기에 사이버보안 분야에 손쉽게 적용되었고, 사이버보안 기술의 자동화, 지능화, 실시간성을 향상시키는 혁신적인 수단으로 각광 받았다. 하지만 AI는 그 자체가 사이버 공격의 대상이 되거나 사이버 공격에 악용될 수 있는 복합적인 위험을 내포하며, 이러한 위험은 최근 들어 실제 위협으로 실현되고 있다. 2014년 시작된 미 방위고등연구계획국(DARPA)의 Cyber Grand Challenge는 AI가 사이버 공격과 방어에 활용 가능함을 증명하였다. 그리고[3] 이후 진행된 AI Cyber Challenge('23~'25)는 대규모 코드에서 AI가 취약점을 자동으로 찾아 안전한 코드를 작성하고 보안패치를 즉시 생성하는 능력을 실증하였다. 가장 최근인 지난 4월, Anthropic 社가 발표한 첨단 AI 모델 'Claude Mythos Preview'는 보안 취약점 분석과 공격경로 생성 등에 기존 AI 모델 대비 압도적인 성능을 보유함이 밝혀 지기도 했다.[4] 이와 같이 AI는 사이버보안 분야의 게임체인저로 기술적인 양면성을 극명하게 드러나고 있는 상황이다.

다시 말하자면, AI는 사이버보안의 수단이자 위협의 진원지로 사이버 공격과 방어의 양상 모두를 근본적으로 뒤흔들고 있으며, 기술 간의 높은 상호 영향에 따라 앞으로의 미래 기술패권 경쟁은 두 기술이 융합된

1 이란은 이스라엘을 대상으로 150여 발의 미사일과 170여 대의 드론을 발사하는 공습을 펼쳤다. 이스라엘은 미국과 함께 AI 기반 방공통제 시스템과 다중타격분석체계, 미사일 항법 방해·교란 기술 등을 활용한 '아이언실드 작전(Operation Iron Shield)'을 통해 미사일/드론 요격률을 99% 이상으로 끌어올려 이란의 공습을 성공적으로 방어하였다.

2 미군은 Palantir 社의 AI 표적화 플랫폼 Maven Smart System을 활용하여 24시간 이내에 이란 내 1,000개 이상 표적을 처리, 타격 우선순위를 결정하는 등 대규모 공습을 빠르게 수행하였고, 이스라엘은 하마스와의 분쟁 간 개발·검증된 Gospel, Lavender, Where's Daddy?와 같은 독자 개발 AI 체계를 미군 기술과 통합 운용하였다.

양상으로 전개될 것이다. 그리고 AI를 많이 활용하는 국가일수록 그 모델과 시스템을 둘러싼 사이버 보안이 매우 중요하게 될 것이며, 이로 인해 이른바 'AI-사이버 융합[3]'은 새로운 국가 안보 전략의 핵심 과제로 자리 잡을 것이다. 지난 3월 미국의 Trump 2기 행정부가 발표한 미국의 새로운 『국가 사이버 전략』(President Trump's CYBER STRATEGY for America)[5]은 Agentic AI를 사이버작전의 핵심 실행 도구로 명시하는데, 이는 AI-사이버의 융합을 본격 추진하려는 시도로 보인다. 이러한 관점에서 본고는 동 전략의 발표를 촉발점으로 삼아, 사이버보안과 AI 분야 모두에서 기술과 정책을 선도하는 미국이 'AI-사이버'의 융합을 어떻게 접근하고 있는지 Trump 2기 행정부의 주요 정책을 중심으로 살펴보고, 미국의 정책 동향과 방향을 바탕으로 우리가 취해야 할 AI-사이버 융합에 관한 국가 전략의 방향성을 논의하도록 한다.

AI-사이버 융합에 관한 미국의 정책 동향

美 국가 사이버안보 전략의 정책 발전과 AI에 대한 인식 전환

사이버보안에 관한 국가 정책이 본격화된 Obama 행정부부터 현재까지 미국의 국가 사이버안보 전략의 흐름을 살펴보면([표 1] 참고), 행정부에 따라 일부 변화가 있었지만 사이버위협 고도화에 따라 '수동적 방어'로부터 '능동적·선제적 억제', '회복탄력성과 책임'에 중점을 두고 '공세적 사이버보안'을 강화하는 방향으로 정책 기조를 발전시켜왔고,[6] 이번 Trump 2기 행정부의 『국가 사이버 전략』은 이러한 정책 기조를 더욱 강화한 '공세적 사이버작전'을 강조하고 있다.[7]

이러한 정책 기조 발전은 기술패권 경쟁의 격화에 따른 것이며, 이에 맞춰 사이버안보 전략에서 AI를 바라보는 관점 역시 '단순한 보호 대상'에서 '구조적 회복탄력성의 기반'으로 변화했고, Trump 2기 행정부에서는 '적극적 공격 수단(무기화)'으로 진화하고 있다.

3 본고에서 'AI-사이버 융합'은 AI 기술과 사이버보안 기술이 긴밀히 결합되어 AI가 사이버보안 역량을 혁신하면서, 동시에 사이버보안이 AI를 보호하는 상호의존적으로 융합된 관계의 상태를 지칭한다.

[표 1] 미국 국가 사이버(안보) 전략의 변화

구분	Obama	Trump (1기)	Biden	Trump (2기)
정책 기조	연방 인프라의 현대화와 사이버보안 기반 조성	힘을 통한 평화와 사이버안보의 군사안보화	사이버보안의 책임 재분배와 회복탄력성 (resilience) 구축	미국 우선주의 하 압도적 힘의 과시
거버넌스	백악관 중심 중앙집권적 구조	국토안보부 중심 분권적 구조	백악관 중심 중앙집권적 구조	분권적 구조
규제 인식	자율적 규제	규제 최소화, 민간의 자발적 보안 관행 장려, 연방 부처 책임성 강화	정부 개입 확대, 민간(기업)의 법적 책임 강화(liability shift)	상식적 규제 (과도한 규제 완화 및 철폐)
전략 중점	민-관 정보 공유 및 NIST 사이버보안 프레임워크 기반 민간 자율 보안	선제방어(defend forward), 지속관여(persistent engagement)를 통한 적대세력 인프라 무력화	사이버 대응을 위한 통합억제, SW 기업 책임 강화, 공급망보안 고도화	공세적 사이버 작전 강화, 적대국 대상 독자적 제재 능력 확보
국제·외교	적대행위 억제를 위한 국제규범 형성과 국제협력	미국 주도 다자 국제규범 수립, 사이버위협의 공개 귀속(attribution)을 통한 억제	미국 주도 동맹과의 협력적 방어 및 글로벌 가치 연대 구축	동맹국의 역할 강화 및 비용 분담(전가) (burden shift)
위협 인식	지식재산권 유출 및 규범 위반	기술 도용에 따른 경제적 위협 및 선거 개입으로 인한 주권 침해	SW 공급망 취약점, 랜섬웨어 등에 따른 사회 기반시설 위협	적대세력의 AI 우위 확보와 이를 통한 자율적 사이버공격

Obama 행정부 시기('09~'17)의 사이버 정책은 AI를 직접 다루지 않았다. 하지만 AI를 미래 경제·사회·기술의 혁신을 이끌 동력으로 인식하고, 관련 연구개발 지원과 함께 중국 등 경쟁국의 지식재산권 탈취 방지를 전략 과제로 추진하였다. Trump 1기 행정부('17~'21)는 AI를 미국의 기술 리더십 유지를 위한 신흥 기술(emerging technology)로 인식하고, 기술패권 경쟁의 시작으로 볼 수 있는 적대국의 지식재산권 탈취와 스파이 활동 방어에 중점을 둔 사이버보안을 강조하였다. 또한, 사이버방어 역량을 실질적으로 높이는 중요한 수단으로 AI와 자동화 기술을 언급하는 등 Trump 1기 행정부 시기 AI에 대한 인식은 사이버방어를 위한 기반 역량으로 발전하였다.

AI 논의가 본격화된 Biden 행정부('21~'25)는 연방 네트워크 방어를 위한 도구로 AI를 인식함과 동시에 AI를 복잡성과 리스크를 높이는 위험 유발 요인으로 인식하고, 안전·책임·신뢰를 위한 규제의 대상으로 AI를 다루었다.[8] Biden 행정부의 국가 사이버안보 전략은 광범위한 AI 도입이 시스템 복잡성을 가중시키고 예상치 못한 위험을 높일 수 있음을 지적하고, AI의 보안성과 회복탄력성을 높이는 연구개발 투자를 지시함과 동시에, 연방 네트워크 방어를 위한 도구로 AI 기반 솔루션 도입을 장려하였다. 그리고 국방 사이버 전략 측면에서 자율형 및 AI 주도 사이버역량의 군사적 적용을 연구하되, '책임 있는 AI(Responsible AI)' 원칙에 따른 윤리적이고 신중한 AI 도입을 강조하였다.

Trump 2기 행정부는 국가의 기술적 우위(Technological Superiority) 유지를 위한 공세적 수단으로 AI를 재정의하였다. 이는 기술패권 경쟁에서 압도적인 우위를 차지하는 것을 넘어 힘으로 경쟁국을 굴복시키겠다는 '기술 지배(Technology Dominance)'에 대한 미국 우선주의 인식이 포함된다. Trump 2기 행정부의 이번 『국가 사이버 전략』은 위협 행위자의 선제적 탐지와 기만, 자율적·대규모 네트워크 방어 및 교란 작전 수행이 가능한 Agentic AI의 신속한 채택, 외산 AI 플랫폼 확산 저지, 미국 AI 기술 스택에 대한 안보 차원의 강력한 보호, 혁신과 글로벌 안정을 통해 미국의 압도적인 기술 지배력을 지키기 위한 도구로 생성형 AI와 Agentic AI의 외교적 활용 등을 제시하고 있다.

『AI 실행계획』 상의 AI-사이버 융합 요소와 특징

2025년 7월 발표된 『AI 실행계획』(America's AI Action Plan)[9]은 AI에 대한 Trump 행정부의 정책 방향을 제시한다. 사이버 분야와 유사하게 행정부별로 차이가 있었지만, 미국은 전반적으로 기술패권 경쟁 대응의 관점에서 AI 정책을 발전시켜왔다.[10] Obama 행정부는 AI를 통한 기술 혁신과 미래 사회에 대한 정책 방향을 최초 제시하였고, Trump 1기 행정부는 이를 발전시켜 국가안보와 경제 전략의 핵심 기술로 AI를 명시하고 행정명령 등 제도적 기반을 마련하였다. Biden 행정부는 Trump 행정부가 취한 AI 경쟁력 확보의 정책 기조를 계승하되 안전성과 윤리적 개발을 강조하는 방향의 AI 정책을 추진하였다. 이후 Trump 2기 행정부는 그동안의 민간 주도 기술 개발을 넘어 국가 주도의 전략적인 관점으로 AI를 접근하며, 이를 구체화한 정책이 바로 『AI 실행계획』이다. 인류의 지속 가능한 번영, 경제적 경쟁력 강화, 국가안보 증진을 통해 미국의 글로벌 AI 패권을 지속·강화하는 것을 정책 목표로 수립된 『AI 실행계획』에서 AI-사이버 융합과 관련된 정책 권고사항을 분석하면 다음의 [표 2]와 같다.

[표 2] 『AI 실행계획』의 AI-사이버 융합 관련 주요 내용

전략 축	실행과제	정책 권고사항
I AI 혁신 가속화	AI 해석, 제어, 견고성 혁신의 투자	**설명 가능성 부족으로 고위험 분야에서 AI 활용이 제약받는 문제를 해결하기 위해, 내부 작동 원리와 결과 도출 과정의 근본적 이해를 위한 연구에 투자** • AI 해석 가능성, 제어시스템, 적대적 견고성* 기술 개발 프로그램 추진 * Adversarial robustness: AI가 적대적 공격, 입력 조작에도 정확성과 안정성을 유지하는 능력 • 학계 최고 AI 인재들이 모이는 AI 해커톤 이니셔티브를 구성, AI 시스템의 투명성, 효과성, 사용 제어, 보안 취약성에 대한 테스트 추진
	상용 및 공공 AI 혁신 보호	**AI 리더십 유지를 목표로 첨단 AI 기술 확산과 국가안보 간 균형을 도모, 정부-산업계 협력을 통해 기업, 인재, 지식재산, 보안 위협에 효과적으로 대응** • 민간 부문이 악성사이버행위자, 내부자 위협 등을 포함한 다양한 보안 위험으로부터 AI 혁신을 적극적으로 보호할 수 있도록 미국 주요 AI 개발업체와 협력
II 미국 AI 인프라 구축	고보안 데이터센터 구축	**원시정보 데이터 처리에 적합한 AI 시스템의 활용 확장을 위한 고도화된 사이버 공격도 방어할 수 있는 군사·정보기관용 데이터센터 구축** • 고보안 AI 데이터센터를 위한 새로운 기술 표준 수립, 산업계와 협력
	핵심기반시설 사이버보안 강화	**AI 기반 사이버방어 도구 도입으로 새로운 위협의 선제적 대응 역량 강화 및 설계 단계부터 보안 내재화, 변화 탐지, 데이터오염/적대적공격 경보 역량 확보** • 미국 내 핵심기반시설 간 AI 보안위협 정·첩보 공유를 위한 AI 정보 공유 및 분석센터(AI-ISAC) 설립 • AI 관련 취약점 및 대응지침을 수립, 민간 부문에 제공 • 기존 사이버 취약점 공유체계를 활용, 연방기관 내 확인된 AI 취약점을 민간과 공유
	AI 보안내재화 (Secure by Design) 촉진	**국가안보 용도의 AI 시스템을 적대적 공격으로부터 보호하기 위한 AI 보증(AI Assurance) 분야 발전 및 회복탄력성 있고 안전한 AI 개발·배포 촉진** • 국방부의 책임 있는 AI 및 생성형 AI 프레임워크, 로드맵, 툴킷 개선 지속 • 『AI에 관한 정보공동체(IC) 지시 505』* 하 AI 보증에 대한 IC 표준 발표 * 미 정보공동체(IC)에서 AI 개발·도입·운용과 관련된 관리·거버넌스 체계를 규정하는 정책
	AI 사고 대응의 연방 역량 강화	**AI 시스템 장애 시 핵심 서비스·기반시설 피해 최소화를 위한 연방정부 차원 대응 능력을 강화(기존 사고 대응 지침과 모범사례 AI 관련 사고 대응 절차 포함)** • CISA의 「Cybersecurity Incident & Vulnerability Response Playbook」에 AI 시스템 고려사항을 통합, CISO-CAIO 협업 의무화를 포함하도록 개정 • 『대통령 행정명령-14306』* 이행의 일환으로 AI 취약점 정보의 책임 있는 공유 장려 * 국가 사이버보안 역량 강화 지속 및 기존 행정명령(제13694호 및 제14144호) 개정
III 국제 AI 외교 및 안보 주도	글로벌 보호 조치 조정	**민감 기술 수출에 대한 통제를 강화하며 불이행 시 외국산직접생산규칙(FDPR), 보복관세 등의 수단을 통해 동맹국 및 파트너국의 준수 유도** • 동맹국이 미국이 수출통제하는 기술을 적대국에 공급하지 않도록 AI 글로벌 동맹을 위한 기술 외교 전략을 수립, 정부 전반의 정책 수단을 조정, 주요 동맹국들이 공급망 전반에 보완적인 AI 보호 시스템과 수출통제 도입을 유도 • 동맹국들의 미국 수출통제 채택과 공동의 통제 조치 개발 추진, 적성국의 동맹국 방산 산업 공급 및 공급업체에 대한 지배권 확보 차단
	미국 주도의 프런티어 AI 모델 위험 평가	**미국 주도로 화학·생물·방사능·핵·폭발물(CBRNE) 및 사이버보안 분야에서 최첨단 AI 모델이 초래할 수 있는 위험을 선제적으로 파악·평가하는 체계 구축** • 분야별 전문기관(사이버위험 포함)과 AI 개발자 협력 하 최첨단 AI 시스템의 국가안보 위험의 평가 공동 수행 • 국가안보 관련 AI 평가체계 수립, 운영, 갱신 • 잠재적 보안 취약점 및 악의적 외국 세력 개입 가능성의 평가 및 분석 • AI 시스템의 첨단 평가 및 분석의 지속 수행 보장을 위한 연방 기관 내 AI 선도 연구자 우선 채용

[표 2]의 정책 권고사항을 종합하면, 미국의 'AI-사이버'의 융합은 크게 두 가지 방향성으로 압축된다. 첫 번째는 AI가 사이버보안을 혁신하는 방향(AI for Cybersecurity)이다. AI로 인해 새롭게 등장·진화하는 사이버위협 대응에 AI를 활용하는, AI 기반 사이버보안 역량을 확보하는 것을 의미한다. 『AI 실행계획』은 전략 축 Ⅱ의 '핵심기반시설 사이버보안 강화'에서 'AI 기반 사이버방어 도구 도입'을 명시하여 이러한 방향을 강조하고 있다. 두 번째는 AI 혁신을 위해 AI의 사이버보안을 강화하는 방향(Cybersecurity for AI)이다. AI 자체가 사이버 공격과 위협의 표적이 되기에, AI 모델·시스템·데이터 등에 대한 사이버보안을 강화하는 것을 의미한다. 이를 위해 『AI 실행계획』은 전략 축 Ⅰ에서 AI 해커톤(보안 취약성 테스트)과, AI 혁신 보호를 위한 민간 협력을, 전략 축 Ⅱ에서 고보안 데이터센터 구축, AI 보안 내재화를 위한 AI 보증 표준 수립, AI의 사이버 사고·취약점 대응·정보 공유를, 전략 축 Ⅲ에서 최첨단 AI 모델의 사이버위험 평가를 제시하고 있다.

이러한 'AI-사이버' 융합의 두 가지 방향성은 근본적으로 AI와 사이버보안 분야의 기술이 가지는 상호보완적인 관계의 특성에 기인한다. AI와 사이버보안의 기술 융합은 AI 자체를 공격하거나 악용하는 새로운 사이버위협의 발생과 AI가 기존 사이버위협을 가속화하여 위협 자체를 진화시키는 새로운 위협 환경을 발생시키는데, 이에 대응하기 위해 AI와 사이버보안 간 서로를 도구로 삼는 동시에 서로를 보호해야 하는 상호의존적인 관계가 요구된다. 특히, 이러한 관계는 일회성으로 끝나는 정적인 관계가 아닌, 적응적인 과정이 지속 반복되는 동적인 관계로 형성되는 점은 주목할 필요가 있다.

미국이 추구하는 AI-사이버 융합의 핵심 요소와 전략적 방향

미국의 『AI 실행계획』('25)과 『국가 사이버 전략』('26)은 'AI-사이버 융합'에 대한 전반적인 정책 방향을 제시하고, 국가 전략적 수준에서 정책 이행을 위한 핵심 요소를 구체화한다. 이러한 관점에서 미국이 추구하는 AI-사이버 융합의 전략 방향을 구성하는 보완적 관계로 두 정책에 제시된 '사이버-AI 융합'의 연계성을 분석하면 다음 [표 3]과 같다.

[표 3]의 내용을 바탕으로 미국이 추구하는 AI-사이버 융합의 핵심 요소를 도출하면, 첫 번째는 AI를 사이버 방어와 공격의 실무적 도구로 채택하여 대응 속도를 극대화하는 데 중점을 두는 'AI 기반의 사이버작전 역량 고도화'이다. 두 번째는 AI 자체에 대한 공격에 대응하여 AI의 신뢰성, 안전성, 강건성을 확보하고자 하는 'AI 기술 스택의 보호'이며, 세 번째는 제도적 측면에서 이미 구현된 사이버보안의 체계에 AI를 통합하는 '제도·거버넌스 통합'이다.

[표 3] 미국 국가정책 상 'AI-사이버 융합'의 핵심 요소 간 연계성

핵심 요소	「AI 실행계획」(2025)		「국가 사이버 전략」(2026)	
	전략 축	주요 정책 내용	전략 축	주요 정책 내용
① AI 기반 사이버 작전 역량 고도화	II (미국 AI 인프라 구축)	• AI 기반 사이버방어 도구(AI-enabled cyberdefensive tools)를 통한 위협 선제 대응 및 방어태세 유지	3 (연방 정부 네트워크 현대화·보호)	• 연방 네트워크 보호와 대규모 침입 억제를 위한 AI 강화 사이버보안 솔루션(AI-powered cybersecurity solutions) 채택
			5 (핵심·신흥 기술 우위 유지)	• 위협 행위자 탐지·유도·기만을 위한 AI 기반 사이버도구 (AI-enabled cyber tools)의 신속한 구현 • 네트워크 방어·교란을 위한 Agentic AI의 적극 채택
② AI 기술 스택의 보호	I (AI 혁신 가속화)	• 국가안보 영역의 AI 활용을 위한 적대적 견고성 기술 개발	5 (핵심·신흥 기술 우위 유지)	• AI 기술 스택(데이터센터 포함) 보호 • AI 보안 혁신 촉진
	II (미국 AI 인프라 구축)	• AI 시스템 내 보안 내재화, 견고성, 회복탄력성 확보 - 데이터오염, 적대적 공격 등의 위협에 노출된 핵심기반시설의 AI를 보호		
③ 제도·거버넌스 통합	II (미국 AI 인프라 구축)	• 핵심기반시설 간 AI 보안 위협 (AI-security threat) 정보 공유를 위한 AI-ISAC 설립 • CISA의 Cybersecurity Incident & Vulnerability Response Playbook에 AI 시스템 고려사항을 통합 • 사고 대응 시 CISO-CAIO 협의 의무화	1 (적대세력 행동 구체화)	• 정부의 공세적·방어적 사이버작전 역량을 통합 • 적대세력의 네트워크 침해 전 탐지·대응·격퇴 및 적 능력 약화를 위한 국가의 모든 수단 동원 • 적 네트워크 식별·교란을 위한 민간 참여 인센티브 확대 • 동맹과의 집단적 사이버안보를 위한 비용 분담
	III (국제 AI 외교·안보 주도)	• 첨단 AI 프런티어 모델에 대한 사이버공격 위험 평가 • 적대국 AI의 보안 취약성 조사 등		

다만, AI-사이버 융합에 있어, 『AI 실행계획』과 『국가 사이버 전략』은 몇 가지 간극이 확인된다. 첫 번째, Trump 2기 행정부가 강조하는 상식적 규제(규제 완화)와 관련된 혁신 촉진과 보안 강화 사이의 충돌이다. 『AI 실행계획』은 AI의 신뢰성, 안전성 등을 위한 새로운 사이버보안 요구사항을 부과하나(전략 축 II), 『국가 사이버 전략』은 신흥 기술의 신속한 혁신을 위한 규제 제거를 강조한다. 이러한 충돌은 표면적으로 혁신-보안의 균형을 추구하는 것으로 보일 수 있지만, 실제 정책 실행 과정에서 AI의 국제 경쟁력 유지와 국가안보 요건의 균형점을 어떻게 맞출 것인가라는 도전 과제를 발생시킬 것이다. 두 번째, AI 우위 확보와 보안 위협의 긴장이 동시에 발생하는 딜레마이다. 『AI 실행계획』은 최첨단 AI 모델의 위험성이 적대국의 잠재적인 역량이 될 수 있음을 경고하는데, 『국가 사이버 전략』은 공세적 작전을 통한 힘에 의한 우위 달성을 더 강조하고 있다. 다시 말하면, 미국이 추구하는 AI 우위 확보 전략은 군비 경쟁과 같이 오히려 적대국에 의한

AI 위협을 비례적으로 높이는 구조적 딜레마로 작용할 수 있는 위험성이 잠재되어 있다. 세 번째, 글로벌 AI 질서 주도권 강화 등 기술 외교 정책 추진과 동맹·우방국에 요구하는 역할·비용 전가, 그리고 공세적 역량 강화의 정책 기조 간 괴리이다. 『AI 실행계획』은 미국 AI 기술 스택의 수출 강화, 첨단기술 수출통제, 동맹·우방으로의 영향 확장 등을 제시하는데, 『국가 사이버 전략』은 사이버보안에 대한 동맹국의 역할 강화와 비용 분담, 자국의 공세적 역량을 통한 우위 확보를 강력하게 강조하는 모순적인 정책 방향을 제시하고 있다. 이러한 방향은 미국의 단독 역량과 동맹 체계의 공동 대응·억제력 사이의 차이를 발생시킬 것이며, 이는 단기간에 해소될 수 없는 구조적 한계로 남을 가능성이 높다.

시사점: AI-사이버 우위 확보를 위한 AI-사이버 안보 전략의 수립

올해 3월 RAND는 중국 등 미국의 적대국가가 범용인공지능(Artificial General Intelligence)을 활용하여 예기치 못한 시점에 대규모 사이버공격을 감행하는 사이버 급습(cyber surprise)에 관한 연구를 발표하였다.[11] 해당 연구는 AI를 활용한 대규모 사이버 공격을 새로운 전략적 위협으로 가정하고, 위협 시나리오 기반 TTX 훈련을 통해 새로운 위협 대응을 위해 국가안보전략에 반영해야 할 요소를 식별하였다. 이와 같이, AI-사이버 융합의 위협과 이에 대한 국가안보 차원의 대응 논의는 이미 시작되었고, Trump 2기 행정부가 발표한 이번 『국가 사이버 전략』은 이러한 논의를 한층 가속화하는 시발점이 될 것이 분명하다.

지난 2월 발표된 『대한민국 AI 행동계획』('26.2)은 AI 기반 사이버보안 체계 구축 등 AI-사이버 융합 측면의 과제를 일부 제시하고 있으나, 전반적으로 AI를 위한 실무를 나열한 내용으로 구성된 한계가 존재한다. 따라서 미국과 같이 '계획'과 연계 하에 국가안보를 위한 AI-사이버 우위 확보의 목표와 방향이 국가 사이버 전략에 포함되어 제시될 필요가 있으며, 이러한 방향은 단순히 AI와 사이버보안 분야의 개별적인 발전에 국한되지 않고 두 기술이 밀접히 상호 보완되고 융합되는 측면으로 지향될 필요가 있다. 또한, 우리 정부의 행동계획 자체가 미국의 『AI 실행계획』을 벤치마킹하는 관점에서 기획되고 추진된 만큼, 전략과 연계되어 발전하는 정책 방향 역시 미국의 추진 동향을 참고할 필요가 있다.

우리 정부가 역시 새로운 국가 사이버 전략을 준비하고 있는 현시점에서, 미국이 AI-사이버 우위 확보를 위해 중점을 둔 3가지 핵심 방향 ① AI 기반 사이버작전 역량 고도화, ② AI 기술 스택의 보호, ③ 제도·거버넌스의 통합은 AI-사이버 융합을 국가 전략적 차원에서 구체화하기 위한 핵심 요소로 반드시 고려할 필요가 있다. 그리고 이러한 사이버-AI 융합의 방향은 단순히 우리나라의 AI-사이버 우위 확보를 넘어, 미국이 요구할 가능성이 높은 사이버안보 비용의 동맹 전가와 미국이 추구하는 기술패권 경쟁에 유연하게 대응하기 위한 국가안보의 전략적인 방향성으로 접근해야 할 것이다.

참고문헌

[1] Josef Federman and Jon Gambrell, "Israel says Iran launched more than 300 drones and missiles, 99% of which were intercepted", The Associated Press, April 14, 2024.

[2] Noor Hammad, "The proliferation of AI-enabled military technology in the Middle East", IISS - Charting Middle East, April 2, 2026.

[3] 이경복, "사이버작전과 인공지능, 미 국방 분야의 추진 동향", 한국국방연구원, 국방논단 제1847호(21-15), 2021년 4월 21일.

[4] Nicholas Carlini, et al., "Assessing Claude Mythos Preview's cybersecurity capabilities", Anthropic's Frontier Red Team, April 7, 2026. https://red.anthropic.com/2026/mythos-preview

[5] The White House, 『President Trump's CYBER STRATEGY for America』, March 2026.

[6] 이경복, 박태현, "트럼프 2기 행정부의 미국 사이버보안 정책방향 전망", SW중심사회, Focus 2, 2025년 3월호.

[7] 오일석, "<트럼프 대통령의 사이버전략>: 특징과 시사점", INSS 이슈브리프, 제827호. 2026년 3월 27일.

[8] Executive Order 14110. "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence".

[9] The White House, 『Winning the Race: AMERICA'S AI ACTION PLAN』, July 2025.

[10] 오연주, 명사은, 윤정영, 이정민, "미국 「AI 실행계획」 주요 내용 및 시사점", 한국지능정보사회진흥원, The LENS, 2025-6호.

[11] Gregory Smith, George Hage, Chad Heitzenrater, Matt Chessen, and Richard S. Girven, "Infinite Potential - Insights from the Cyber Surprise Scenario", RAND Research Report, Mar 9, 2026.