국가전략연구위원회 이슈브리핑 37호 (발간일: 2025. 8. 29.)

트럼프 행정부 하 미국 디지털 기업의 동향과 사이버 안보 정책에의 영향

유인태 (단국대)

I. 서론

사이버안보 정책에 영향력을 갖는 행위자로서 디지털 기업을 꼽을 수 있다. 기업들의 정부 정책으로부터의 자율성을 가정하면, 기업들의 이니셔티브를 통해 정부 정책에 영향을 미치는 과정을 생각해볼 수 있다. 흔히, 자유주의 이론틀에서는 정부를 블랙박스로 보고, 사회적 행위자들의 선호가 정책으로 산출되는 과정을 잡아내고자 한다.

기업들의 자율성을 가정하고 미국의 사이버안보 정책에의 영향력을 볼 수 있지만, 다른 한편으론 정책형성과정에 있어 정부의 영향력으로부터 완전히 자유로울 수 없다. 정부는 행위, 제도 그리고 규제를 통해 기업 행위자들의 행동에 제약을 가하거나 특정 행위로 유인하기도 한다. 즉, 기업이 행동하는 범위와 방향성에 대해 정부가 영향을 미칠 수 있다. 그리고 그러한 기업의 행동이 정부에 다시 영향을 미치며, 되먹임순환(feedback loop)을 통해 정책에 영향을 미칠 수 있다. 때로는 기업에 또 때로는 정부에 이니셔티브가 있다고 볼 수 있다.

II. 트럼프 정부의 사이버 안보 정책 선호

미국의 사이버안보에 대한 일반적인 경향성은 대체로 지속될 것으로 볼 수 있다. 우선 미국의 사이버안보에 대한 초당적 지지가 존재하기 때문이다. 다만, 최소한의 변화를 짐작케 하는데, 이는 트럼프 정부에 의한 정부 역할 축소라는 기조 때문이다. 규제나 허위정보와의 싸움에 있어서 정부의 역할은 줄어드는 벡터가 보인다. 그리고 일반적인 사이버범죄의 경향이나 사이버공격에 있어서의 세련됨/고도화(sophistication) 경향성은 트럼프 정부의 출범과 상관 없이 지속될 것이다. 적대적 경쟁국가들의 경우도 미국에 대한 사이버공간에서의 행위에 있어 큰 변화가 없거나, 긴장 관계가 더 심해질 경우 심지어 빈도와 정도를 더할 수도 있다. 가령, 중국과 같은 경우, 사이버에스피오나지, 허위정보 그리고 주요 기반시설 침투 등과 같은 행위의 빈도와 정도를 더할 수 있다. 러시아 또한 우크라이나 그리고 유럽 국가들과의 대립 속에서 사이버 상의 악의적 행태가 더해질 수 있으며, 미국에게도 영향을 미칠 수 있다. 극적인 국제 관계의 전환이 없는 한 이란과 북한도 악의적인 사이버 행태를 지속할 것이며, 친러시아나 친무슬림 핵티비스트 그룹들도 미국과 서방을 향한 공격을 지속해 나갈 것이다. 이러한 위협 상황에 대한 큰 변화가 없거나, 지정학적 국제정세의 심화나 인공지능과 같은 신기술의 개발로 사이버 위협상황이 더 악화될 가능성이 존재하는 가운데, 트럼프 2.0 정부의 사이버안보 정책은 다음과 같은 경로를 예상해 볼 수 있다.

주의해야 할 점은, 비록 트럼프 정부의 정책 선호는 탈규제로 볼 수 있지만, 이러한 정책 선호가 결코 중국이나 러시아의 APT 그룹에 의한 점증하는 사이버위협에 대한 대처가 소홀해지거나 감소된다고 섣불리 예단할 수 없다. 대신 행위자의 중점이 주정부나 민간으로 이동하는 경향이 있다. 2025년 3월 19에 나온 행정명령("국가 및 지역 준비성을 통한 효율성 달성하기(Achieving Efficiency Through Stte and Local Preparedness)")에 따르면 주정부와 개인의 역할의 중요성을 재조명하고 있다.[1] 연방정부 차원의 변화를 위해서는 National Security Affairs(APNSA)가 90일 내로 "National Resilience Strategy"를 고안하도록 할 것과 해당 문서가 매4년마다 점검되고 업데이트 될 것을 정하고 있다.

그리고 이러한 접근은 빅테크기업들(Big Tech firms)에게 유인을 주고자 취해졌다. 구글, 마이크로소프트, 아마존, 메타와 같은 기업들이 신속하게 혁신할 수 있도록 하고자 했으며, 동시에 정부 기관들과의 협력을 촉진하고자 한다. 민관 협력을 통해 위협으로부터 방어하고자 했으며, 특히 중국이나 러시아와 같은 국가 행위자들로부터 사이버안보를 확보하고자 했다.[2]

방점이 찍히는 행위자와 그 역할이 변화하는 것과 동반되어, 국가적 사이버안보 관련 사안의 주안점이 변화하고 있다. 예를 들어, 적어도 주요 기반시설의 보안과 복원력에 대해

1)https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/

2) https://quointelligence.eu/2024/11/trump-second-term-what-it-means-cybersecurity-threats/; https://sprinto.com/blog/trumps-approach-to-cybersecurity-policies/

서는 지속하거나 강화할 것이다. 다만, 사이버안보 영역에서도 정부의 직접적 감독과 같은 개입적 정부 행동을 줄이고자 하는 한편, 민관협력(ppublic-private partnerships, PPP)의 증진을 통해 사이버안보를 강화하고자 한다. 다른 한편, 허위정보와 관련한 정부 개입은 줄어들 것으로 예상할 수 있다. 그렇다고 해서 미국의 허위정보 관련 사이버보안 정도가 전반적으로 낮아질 것이라는 예단은 너무 성급하다. 대신, 민간의 역할이 더 크게 부각될 것이라고 볼 수 있다. 다만, 민간이 특히 빅테크가 얼만큼 허위정보에 대해 규제를 시도할 것인지는 검토해 볼 필요가 있다. 여기서는 일단 정부의 정책 선호 방향성을 이와 같이 상정하고, 이하에서 디지털 기업과의 관계에서 다시 다룬다.

1. 주요 기반시설

주요 기반시설의 사이버안보와 관련해서 가장 중요한 정부기관이라고 한다면, '사이버안보 및 인프라 보안국(CISA: Cybersecurity and Infrastructure Security Agency)'를 들 수 있다. CISA는 미국의 사이버안보 협력에서 민관협력의 상징이라고 볼 수 있는데,[3] 미국 정부가 사이버안보 정책 개발과 이행에 있어 민간과 어떻게 협력하는지를 잘 보여준다.[4] 주요 기반시설의 사이버안보와 관련해서 CISA의 역할이 중요했던 것은 민간과의 주요 기반시설의 상당부분을 민간이 담당하고 있기 때문이기도 하다.

2. 허위정보

허위정보에 대한 트럼프 2기 행정부의 입장은 CISA의 위상과 역할 변화를 통해서도 볼 수 있다. 그간 CISA의 임무가 선거보안 관련 허위정보 대응으로 확장하였는데, 트럼프는 이를 정치적 임무로 비판하며 축소할 것을 강조한 바 있다. 이미 트럼프 새정부 들어서 CISA내 선거 관련된 사이버안보 기구들에 대한 지원이 끊겼다.[5]

3. 공급망

앞서 언급한 2025년 3월 19일의 행정명령에는, 주요 행위자의 변화나 주요 사안에서의 변화가 보인다는 점을 지적했다. APNSA에게 사이버안보를 포함한 국가안보 전반의 복원력에 대해 점검할 것을 명령하였는데, 그중에는 위에서 언급한 주요 기반시설 뿐 아니라, 공급망 복원력과 관련한 행정명령들의 재점검을 명령하고 있다. 이에는 2021년 2월 24일에 나온 '미국의 공급망'에 관한 행정명령14017에 재점검도 포함된다.[6] 행정명령14017은 주요 부문(critical sectors), 정보통신기술에 대한 감독을 포함하고 있을 뿐 아니라, ICT 소프트웨어, 데이터, 관련 서비스 등의 개발과 관련한 산업 기반도 아우른다. 2025년 3월 19일의 행

3) https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity
4) https://www.cisa.gov/news-events/news/cisa-through-years-policy-and-impact
5) 트럼프 대통령은 CISA 국장 크리스토퍼 크렙스(Christopher Krebs)를 해고하였는데, 2020년 부정 선거를 주장할 당시, 해당 국장은 선거가 조작으로부터 안전함을 강조한 바 있기 때문이다.
6) https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

정명령에 포함된 공급망과 관련한 또 다른 이전 행정명령에는 2024년 6월 14일에 나온, '공급망 복원력에 관한 백악관 위원회'라는, 행정명령14123도 포함되어 있다.[7)]

미국의 공급망 사이버 안보 사건하면, 2020년 12월에 불거진 솔라윈즈(SolarWinds) 사건을 들 수 있다. 러시아 FIS(Foreign Intelligence Service)가 솔라윈즈의 오리온 소프트웨어를 겨냥하여 행한 사이버공격으로 '포츈(Fortune)500'의 수많은 기업들의 데이터, 네트워크 그리고 시스템뿐 아니라, 국토안보부, 재무부 그리고 유럽 의회와 같은 여러 정부 기관들도 피해르 입었다. 이러한 사건은 '미국 IT에 있어서의 진주만 사건(the Pearl Harbor of American IT)'라 불리울 정도로 충격적인 사건이었다.

트럼프 정부 1기에서는 공급망 안보는 국가안보와 밀접히 연결되었다. 코로나19로 인한 물자 수송과 관련하거나, 핵심 광물 자원 등도 공급망 안보에 대한 경각심을 일으켰지만, 무엇보다 적성국가에 의한 미국의 민감한 기술들에 대한 접근이 큰 이유가 되었다. 이어서 바이든 정부에서의 100일 재점검 행정명령은 반도체, 대량 배터리, 핵심 광물, 의약 재료와 같은 핵심 영역에서의 취약점을 밝히는 것이었다. 이러한 과정을 통해, 국내적으로는 '반도체법(CHIPS and Science Act)'이나 국제적으로는 인도태평양경제프레임워크(IPEF: Indo Pacific Economic Framework)의 공급망 위원회(Supply Chain Council)이 도입되기도 했다.

공급망안보와 관련한 트럼프 2기 초기는 아직까지 바이든 정부의 정책을 폐지하지 않고 유지하고 있다. 공급망의 사이버안보와 관련해서 '신뢰하지 않고 항상 검증하라(never turst, always verify)'라는 '제로트러스트(Zero Trust)' 사이버보안 프레임워크가 채택되어 기업들이 도입하였다. 공급망 안보의 붕괴·중단(disruption)을 막기 위함이다. 이에 따라 추적가능성(traceability)에 대한 민간과 공공의 수요도 늘었다. 공급망 보안을 지키면서도 생산성을 향상시키기 위한 AI 기술들도 발전하고 있다.[8)]

이러한 시도는 데이터 이동에 관한 규제와 맞닿아 있다. 데이터 국지화나 데이터 이전에 관한 파편화된 규제 지평은 디지털 고속도로에 장애가 되고 있으며, 변칙(anomalies)적 데이터 이동을 탐지하기 위한 거대한 데이터의 수집 노력에 파열을 일으키기도 한다. 거대 데이터의 수집은 금융지불사기(payment fraud)와 같은 범죄행위의 추적에 도움이 된다.

이와 같이 공급망 안보는 여전히 현실이기보다는 실현해 내야 할 간극이 존재하는 영역이다. 이러한 영역에 'AI 샌드박스'를 양자적으로 또는 지역적으로 도입을 할 수 있다. '신뢰할 수 있는 공급자 프로그램(Trusted Supplier Program)'의 운영과 국제적 협약을 도입할 수 있다. 이를 통해, 대기업이나 금융권 회사들이 SMEs와 협력하여 역량 강화를 도모할 수 있다. 협력이나 지불 관련 로지스틱스나 문서의 전자화를 통해, 거래(과정)에서의 투명성을 높이고, 세관에서의 흐름을 신속히 할 수 있을 것이다. 6G 무선 통신 시스템의 연구와 개발

7)https://www.federalregister.gov/documents/2024/06/21/2024-13810/white-house-council-on-supply-chain-resilience

8) 물론 이러한 발전과 함께 한계도 노정한다. 공급망 상에서 여전시 가시성이 결여된 구간, 자원의 부족 그리고 증대하는 사이버 위협 등이 존재한다. 많은 소규모 사업체들은 그들의 공급망 추적가능성을 높이기 위한 데이터 수집의 초기 단계에 머물고 있다.

에 박차를 가해 공급망 안보를 강화할 수 있다. 그리고 미국의 CPTPP에 가입을 통해, 'IPEF 공급망 협정'과의 연계를 도모하여 사이버안보, 데이터, 디지털 규칙 등을 강화할 수 있을 것이다. 물론, 바이든 행정부가 추진한 다자간 (공급망) 협력 자체에 대한 미국의 노력이 축소될 수 있다.

4. 데이터안보

트럼프 2기 정부는 바이든 행정부가 추진했던 AI 정책과는 다른 방향으로 향하고 있다. 바이든 행정부가 AI의 안전과 신뢰성에 중점을 두었다면, 트럼프 2기는 AI와 데이터의 광범위한 활용을 통한 행정 효율화와 혁신에 방점을 두고 있다. 미국 연방총무청은 공공 대화형 AI 챗봇 'GSAi'를 개발 및 배포하여, 이메일 등 단순 업무에 적용부터 시작사여, 정부 데이터베이스와 연계한 서비스로 고도화할 계획이다. 이러한 미 정부 AI 서비스 개발을 주도하는 행위자는 정부효율부(Department of Government Efficiency, DOGE)를 이끄는 일론 머스크(Elon Musk), 테슬러 최고경영자(CEO)와 테슬러 출신 기술진 다수가 포진된 연방총무청 기술혁신서비스팀(TTS)이다.

이러한 AI 정책은 데이터안보 정책의 변화와 긴밀히 연계되며 추진되고 있다. AI의 도입은 데이터의 적극적 또는 공격적 활용과 연결된다. 즉, AI 활용을 통한 데이터 분석, 자동화, 서비스 고도화가 공공·국방 등 전방위적으로 확장되고 있다. 이에는 핵심 정부 시스템에 대한 광범위한 데이터 접근권을 허용하고, AI를 활용한 데이터 분석과 자동화를 적극 추진하고자 하는 정책도 포함된다. 또한 AI를 통해서는 정부 규제 간소화, 인원 감축뿐 아니라 국방 분야에서의 활용도 적극적으로 이행 또는 모색되고 있는데, 예를 들어 오픈소스 라마 3.3 기반 군사용 AI 프로토타입 서비스 '카모GPT'를 개발을 들 수 있다.[9] 즉, 기존의 데이터 보호 규제를 통한 데이터안보 보다는 데이터의 경제적, 행정적, 군사적 가치의 극대화에 초점을 맞추고 있다고도 볼 수 있다. 이러한 공공 데이터에 대한 개방은 이해충돌 논쟁을 낳기도 한다. 일론 머스크의 국방이나 항공우주국 관련 데이터 접근 시도는 대표적인 예이다.[10]

트럼프 2기 행정부가 안보보다 상업적 이익 테크기업들의 이익에 더 중점을 보여주는 사례가 있다. 동시에 이 사례는 해당 정부가 IT 업계의 요구에 민감하게 반응하고 있는 것을 보여주기도 한다. 트럼프 2기 행정부의 틱톡 유예 결정이다. 틱톡금지는 애당초 데이터 안보에 대한 우려에서 도입되었다. 트럼프 행정부 1기에서는 2020년 틱톡 금지를 주장했었다. 그런데 트럼프 행정부 2기 출범의 1월 20일에 내려진 행정명령에서는 틱톡 금지법 시행을 75일 유예한다. 그러한 이유는 여러 가지이다. 사회적 반발을 완화하고 젊은 층의 지지를 위한 것이기도 하다. 틱톡 규제 유예는 시장의 충격을 완화하고, 데이터 보호 방안 등의 기술적 법적 문제를 충분히 검토하고 정당성을 확보하기 위함도 있다. 그리고 규제 유예를

9) 한국지능정보사회진흥원(NIA) 2025
10) https://news.mt.co.kr/mtview.php?no=2024121813571429162

통해 메타나 유튜브 등 미국 IT 기업에게 시장 점유율을 확보할 시간을 주기 위한 것도 있다. 유예 기간은 바이트댄스가 틱톡의 미국 사업권을 미국 기업에 매각하도록 압박하는 시간이 되기도 한다.

III. 디지털 기업들의 정책 선호

정부의 사이버안보 정책에 디지털 기업들의 영향력이 있었는지 여부를 판단하기 위해서는 해당 기업들의 정책적 선호를 파악할 필요가 있다. 디지털 기업들이 정부의 사이버안보 정책에 영향을 미쳤는지를 판단하기 위해서는, 우선적으로 정부의 정책이 디지털 기업들의 선호에 부합되는 방향으로 바뀌었는지를 살펴볼 필요가 있다.

디지털 기업들의 사이버 안보 정책 선호

디지털 기업들은 사이버안보, 데이터안보 등에 대한 정책적 선호를 가지고 있었는데, 비록 체계적인 문서가 공개되지 않았다고 하더라도, 그들의 정책적 선호가 공식적 발언이나 행동에서 보이기도 하였다. 예를 들어, 메타(Meta)의 최고 경영자 마크 저커버그(Mark Zuckerberg)는 자사 소셜미디어 플랫폼의 오정보(misinformation)를 검열하는 '제3자 팩트체크(the third-party fact-checking) 프로그램'을 2025년 1월 초 종료하며, 트럼프의 오/허위정보에 대한 정책 선호와 같은 입장을 보이기도 했다. EU의 규제에 대해서도 규제 정책이 일관성이 없으며 오픈 소스 AI 발전에 저해가 된다는 의견을 표하기도 했다.[11] EU 규제에 대한 비판은 직접적으로는 AI 기업을 규제하는 프레임이 이달부터 발효한 AI 법(AI Act) 외에도 디지털시장법(DMA)와 디지털서비스법(DSA), GDPR까지 겹쳐 있다는 규제 거버넌스 때문이다. 다른 한편으로, 비판의 이면에는 메타의 광고 사업에 상당한 지장이 발생할 수 있는 EU 집행위의 조치 때문이다. EU 집행위는 '페이스북이나 인스타그램에서 소비자가 원한다면 맞춤형 광고를 안 볼 수 있도록 무료 사용자에게도 선택권을 줘야 한다'는 취지로 결정을 내리고 디지털시장법(Digital Market Act) 근거하여 메타에 벌금과 함께 준수 명령을 내릴 것으로 예상되고 있다.[12]

또한 저커버그는 EU가 지난 20년간 미국 기술 기업들에게 300억 달러 이상의 벌금을 부과했다고 지적하며. 이러한 벌금이 미국 기업에 대한 "사실상의 관세"와 같다고 주장한 바 있다.[13] 그와 같은 맥락에서 그는 미국 정부가 자국 기업을 방어해야 한다고 강조했으며, 유럽의 규제에 대해서 보복 관세가 필요하다는 의견을 표하기도 했다.[14]

---

11)https://www.aitimes.com/news/articleView.html?idxno=162783
12)https://www.yna.co.kr/view/AKR20250401133500009
13)https://www.happyscribe.com/public/the-joe-rogan-experience/2255-mark-zuckerberg?utm_source=chatgpt.com
14)https://www.theverge.com/news/640368/mark-zuckerberg-meta-eu-fine-trump?utm_source=chatgpt.com

이에 대해 2025년 2월 트럼프 대통령은 미국 기업과 기술을 "해외의 갈취(overseas extortion)"로부터 보호하겠다며, EU의 디지털시장법(DMA), 디지털서비스법(DSA), 디지털세 등 미국 빅테크를 겨냥한 규제와 과세에 대해 관세 등 보복 조치를 검토하라는 각서에 서명하였다. EU 등 외국 정부가 미국 기업에 부과하는 디지털세, 벌금, 규제 정책을 "일방적이고 반경쟁적"이라고 규정하며, 이에 대한 대응으로 관세 부과를 공식적으로 고려한다고 밝혔다.[15] 특히 EU의 디지털 규제(DMA, DSA)가 미국 기업의 시장 진입과 운영을 어렵게 하고 있다고 보고, 미국 행정부 차원에서 EU와 영국 등 주요국의 정책을 면밀히 조사하고 관세 등 무역 보복 조치를 준비하겠다고 공식화한다.

디지털 기업과 트럼프 2기 행정부 간의 관계를 보여주듯, 미국 디지털 기업에 의한 백악관에의 로비는 직접적으로 그리고 대담하게 이루어지고 있다. 월스트리트저널에 따르면 메타 관계자들이 미국 도널드 트럼프 행정부의 통상 담당 공무원들에게 곧 단행될 것으로 관측되는 유럽연합(EU) 집행위원회의 규제 움직임에 맞서 줄 것을 요구했다고 보도된 바 있다.[16] 미국과 EU 간의 갈등 심화에, 규제의 차이, 상업적 이유, 디지털 기업의 이윤추구 행위가 작동하는 것을 볼 수 있다.

정부와 기업 간의 정책적 연결 채널

트럼프 2기 행정부에서는 기업의 목소리를 더욱 반영할 가능성이 더 높아졌다. 첫째, 트럼프 대통령 개인의 탈규제 그리고 친시장적 정책 선호이다. 이는 정부의 일반적 정책 기조에도 잘 나타나 있으며, 사이버안보 관련 정책에도 반영되고 있다.

둘째, 트럼프 내각에서의 디지털 기업 행위자의 참여이다. 상기한 바와 같이 테슬러 최고경영자인 일론 머스크는 정부효율부를 이끌고 있으며, 미 정부의 AI 서비스 개발을 주도하는 연방총무청 기술혁신서비스팀(TTS)에는 테슬러 출신 기술진 다수가 포진되어 있다. 데이비드 삭스(David Sacks)는 전 페이팔 COO 그리고 야머(Yammer) 창립자이자 벤처캐피털리스트인데, 백악관 인공지능 및 암호화폐 특별보좌관('AI·Crypto Czar')으로 임명되었다. 인공지능 및 디지털 자산 정책을 총괄하며, '디지털 자산 시장 실무그룹'과 '암호화폐 위원회' 주재하고 있다.[17] 마이클 크라치오스(Michael Kratsios)는 전 트럼프 1기 행정부 CTO이자, Scale AI(AI 인프라 기업) 대표를 역임했으며, 2기에서는 백악관 과학기술정책실(OSTP) 실장 겸 대통령 과학기술보좌관으로 지명되었고, 과학기술 정책 개발 및 PCAST(대통령 과학기술자문위원회) 공동위원장을 맡고 있다. 스리람 크리슈난 (Sriram Krishnan)은, 마이크로소프트, 페이스북, 트위터 등에서 근무하였으며 안데르센 호로위츠(Andreessen Horowitz)의 파트너이자, 트럼프 2기에서는 OSTP 내 인공지능 선임 정책 보좌관으로 임명되어, 미국의 AI 주도권 확보 및 정책 조율 담당하고 있다. 그레고리 바르바치아 (Gregory Barbaccia)는 전 팔란티어 및 Elementus 출신으로, 해당 내각에서는 연방예산관리국(OMB) CIO로 임명되어, 연방

15)https://www.euractiv.com/section/tech/news/trump-threatens-to-launch-tariff-attack-on-eu-tech-regulation/;
16)https://www.wsj.com/politics/policy/trump-administration-targets-europes-digital-laws-as-a-threat-to-basic-rights-and-u-s-business-20db1016?utm_source=chatgpt.com
17) https://www.fastcompany.com/91264535/these-tech-leaders-have-jobs-in-the-trump-administration

정부 디지털 혁신 및 정보화를 총괄하고 있다.[18] 이밖에도 트럼프 2기 행정부는 인공지능, 암호화폐, 디지털 자산 등 신기술 분야에서 실리콘밸리와 벤처캐피털 출신 인사들을 전면에 배치하고 있다. 이러한 인사 포진은 트럼프 2기 행정부가 바이든 행정부와 달리, 디지털 혁신·민간 주도·친시장 정책으로의 강한 전환의 가능성을 크게 보이고 있다.

2025년 1월 20일 미국 연방의회 의사당에서 열린 도널드 트럼프 제47대 미국 대통령 취임식 행사에 참석한 주요 정보기술(IT) 기업 총수와 그 배우자들. 오른쪽부터 일론 머스크 테슬라 CEO, 순다르 피차이 알파벳 CEO, 제프 베이조스 아마존 CEO와 그 약혼녀인 로렌 산체스, 마크 저커버그 메타 CEO와 그 부인인 프리실라 챈. (Chip Somodevilla/Pool Photo via AP)

셋째, 최근 2025년 2월 25일 트럼프 대통령은 '미국의 AI 기술 리더십 강화를 위한 행정명령'의 발표를 통해서이다. 해당 행정명령에서 미국의 AI 기술 혁신을 위해 'AI 행동계획(AI Action Plan)'을 개발할 것을 지시했다. 3월 15일까지 미국인들은 '정보요청(Request for Information, RFI)'에 응하여 의견을 제시할 수 있었으며, 디지털 기업들의 의견까지 포함하여 8,755개의 의견이 접수된 것으로 알려졌다.[19] 백악관 과학기술정책실(Office of Science and Technology Policy, OSTP)로부터의 RFI에는 기업과 같은 민간 행위자들도 불필요한 요

18)https://govciomedia.com/tracking-cios-in-trumps-second-term/
19)https://www.insidegovernmentcontracts.com/2025/04/march-2025-ai-developments-under-the-trump-administration/;
https://www.mintz.com/insights-center/viewpoints/2025-03-21-trump-administration-receives-8755-comments-ai-action-plan-ai

구사항 제거를 요청이 다수 있었던 것으로 알려져 있다. 이러한 요청은 2025년 7월 중순에 발표될 'AI 행동계획(AI Action Plan)'에 반영될 예정이다. 예를 들어, OpenAI 출신 연구자들이 설립한 엔트로픽(Anthropic)은 Claude 시리즈를 내놓는 것으로도 알려져 있는데, 그들의 권고 사항에는, 더 강력한 반도체 수출통제, 연구소 보안 강화, 그리고 정부의 AI 도입 가속화 등이 포함되어 있다.[20]

20) https://www.anthropic.com/news/anthropic-s-recommendations-ostp-u-s-ai-action-plan