트럼프 대통령의

미국을 위한 사이버 전략 (번역본)

President Trump's

CYBER STRATEGY

for America

MARCH 2026

업비트 투자자보호센터

미국 백악관은 2026.3.6. '트럼프 대통령의 미국 사이버 전략'(President Trump's Cyber Strategy for America)을 발표했습니다. 이번 사이버 전략은 사이버 공간에서 미국의 안보와 기술 우위를 유지하기 위한 새로운 정책 방향을 제시하는 것으로, 사이버 위협 대응을 넘어 인공지능(AI), 양자-내성 암호화(PQC) 등 차세대 기술 경쟁과 미국의 핵심 인프라 보호를 포함하는 포괄적인 국가 전략에 해당합니다. 앞으로 추진할 정책 방향을 '6대 정책 기조'(Six Policy Pillars)로 요약해 제시하고 있습니다.

- 적대 세력의 사이버 활동 억제
- 사이버 규제의 합리화
- 연방 정보 시스템의 현대화 및 보안성 강화
- 국가 핵심 인프라 보호
- 핵심 신기술 부문의 우위 유지
- 사이버 인재와 역량 구축

미국의 사이버 전략은 우리나라의 국가 안보 전략 구상뿐만 아니라, 공공과 민간 부문 간의 협력 체계(민관 파트너십) 구축에도 시사하는 바가 적지 않을 것으로 보여, 디지털자산 사업자를 비롯한 민간사업자들도 그 내용을 참조할 수 있도록 시사점을 정리하고 그 본문을 번역해 참고 자료로 제공해 드리게 되었습니다. 감사합니다. (정리/번역: 투자자보호센터장).

트럼프 대통령의 미국 사이버 전략

I. 주요 내용

□ 미국 백악관은 2026년 3월 6일, **「트럼프 대통령의 미국 사이버 전략」(President Trump's Cyber Strategy for America)**을 발표하고 사이버 공간에서 미국의 안보와 기술 우위를 유지하기 위한 새로운 정책 방향을 제시함

○ 이번 전략은 사이버 위협 대응을 넘어 인공지능(AI), 양자-컴퓨팅 등 차세대 기술 경쟁에서 우위를 유지하고, 평시와 전시에 국가 핵심 인프라를 보호하려는 포괄적인 국가 전략으로 평가됨

□ 트럼프 대통령이 서명한 **전문**에서는, 미국이 비교할 수 없을 만큼 가장 강력하고, 고도화되고, 기술적으로 진보된 군대를 보유하고 있으며, 여기에는 압도적인 재래식 군사력뿐 아니라, 타의 추종을 불허하는 **비-물리적 억지력(non-kinetic powers)**[1]도 포함된다고 하면서

○ 이번 국가 사이버 전략(National Cyber Strategy)은 미국이 사이버 공간에서 독보적 지위를 유지하게 하려는 트럼프 대통령의 **정책 우선순위를 개괄**하는 것이며,

○ 최고의 기술에 투자하고 혁신을 지속하면서, 공세적/방어적 임무 부문에서 사이버 역량을 최대한 활용하기 위해 미국 **정부와 민간 부문 간의 전례 없는 협력**을 천명하는 것이라고 밝힘

□ 사이버 전략 **본문**에서는, "사이버 공간은 미국에서 탄생했고, 미국의 인재와 혁신 연구 역량, 정부의 강력한 역량이 결합해 디지털 세계를 만들어 냈다"는 점을 강조하면서,

○ 트럼프 행정부는 나날이 증가하는 사이버 위협의 심각성을 방치하는 미봉책과 모호한 전략에 머무르지 않고, **신속하고 단호하게**, 그리고 **선제적으로** 행동하면서 사이버 공간의 위협을 바로잡고 무력화하기 위해 **정면 대응**에 나설 것이며, 대응 범위를 '사이버' 영역에만 한정하지 않을 것이라고 밝힘

○ 곧 국익 보호를 위해 최고 수준의 사이버 역량을 신속하고 효과적으로 사용하고, 필요하면 방어적 대응을 넘어 적대적 네트워크와 인프라를 무력화하는 **공격적 사이버 작전**도 불사하겠다는 전략임

---

1) "non-kinetic powers"는 폭격 등 물리적 타격이나 파괴 없이 적의 시스템을 무력화하거나 마비시키는 사이버 공격, 전자전 등을 뜻하며, '비-물리적 억지력'으로 번역함.

□ 향후 추진 방향 부분에서는, **적대 세력의 사이버 캠페인 무력화, 자국 네트워크의 방어 태세와 복원력 강화, 혁신의 촉발과 경제 성장 가속화, 미국의 기술 패권 확보**를 강조하면서

ㅇ 비효율적 규제를 제거해 산업계가 첨단기술 분야에서 빠르게 혁신할 수 있게 하고, 보안성을 갖춘 혁신을 발판으로 연방 시스템, 핵심 기반 시설, 공급망을 방어하고, 민간 부문의 재능과 독창성을 활용하는 **새로운 차원의 공공-민간 부문 간의 관계**를 정립해 나가겠다고 밝힘

□ 구체적인 정책 실행 방안으로 **6대 정책 실행 기조(Six Policy Pillars)**를 적시함

❶ 적대 세력의 사이버 활동 억제

- 미국민, 기업, 우방국이 사이버 공간에서 활동하는 적대 세력을 홀로 상대하도록 하지 않고, 미국의 **모든 방어적/공세적 사이버 작전 역량을 동원**하고, **민간 부문에도 인센티브**를 제공

- 적대 세력의 네트워크 및 시스템 침입 시도를 탐지, 대응, 격퇴하고; 세계 경제에 최대 위협이 되는 사이버범죄와 지식재산권 탈취 등 **범죄 인프라**를 뿌리 뽑고, **자금의 탈출구와 피난처**를 봉쇄

- 사이버 공간 방어와 자유 수호를 위한 **집단적 노력**에 따르는 **비용과 책임**은 미국과 민주적 가치를 공유하는 우방국 간에 **공정하게 배분**되어야 할 것임

❷ 사이버 규제의 합리화

- 사이버 방어가 고비용 체크리스트로 전락하지 않도록 규제 준수 부담을 줄이고, 책임 관계를 명확히 하며, 규제당국과 산업계가 보조를 맞춰나가도록 **사이버 규제를 간소화**

- 민간 부문이 빠르게 진화하는 위협을 따라잡을 민첩성을 갖추도록 **데이터와 사이버 보안 관련 규제를 정비**하고, 미국민에 관계되는 **데이터의 프라이버시 권리**를 강조해 나갈 것임

❸ 연방 정부 네트워크의 현대화와 보안성 강화

- 연방 **정보 시스템의 현대화, 방어력, 복원력 강화** 속도를 높이기 위해 사이버 보안 모범 사례, 양자-내성 암호(PQC), 제로 트러스트 아키텍처, 클라우드 전환 등 이행

- 정부 지도층과 기업 이사회 내에서 **사이버의 중요성 인식 수준**을 높이고, 최고의 기술과 팀을 활용하여 연방 네트워크들을 **지속적으로 테스트**하고 악성 행위자들을 추적

- 군사, 정보, 민간 기업들을 뒷받침하는 **국가 안보 시스템의 보안성과 복원성**을 최우선에 두고, 연방 네트워크들에 대한 방어와 대규모 침입 탐지를 위해 **AI-기반 사이버 보안 솔루션**을 채택을 가속화

- 정부가 **최고의 기술을 구매하여 사용**할 수 있도록 장벽을 제거하고, 경쟁적 프로세스를 조성

❹ 핵심 인프라 보호

- **우선 식별된 핵심 인프라를** 견고하게 구축하고, **공급망들을 안전하게 보호**

  * 정보 기술과 운영 기술 공급망들의 안전한 보호; 전력망, 금융/통신 시스템, 데이터 센터, 수자원 시설, 병원 등 국가의 핵심 인프라, 민간 회사, 네트워크, 서비스 등에 대한 방어를 포함

- **미국산 기술의 촉진과 활용**을 통해 적대적인 공급자와 제품 의존도를 줄이고, 적대 세력들의 초기 접근을 부정해 나갈 것

❺ 핵심 첨단기술 부문의 우위 유지

- 안전한 혁신과 **국가적인 지적 우위 보호가 최우선**인 만큼 인공지능, 양자 컴퓨팅, 블록체인 등 차세대 기술 부문에서 **미국의 기술 경쟁 우위 유지**를 전략의 한 축으로 제시

- 설계와 배포에 이르기까지 **사용자 프라이버시를 보호**하는 안전한 기술과 공급망을 구축하되, **암호화폐와 블록체인 기술의 보안성 지원을 포함**하고, 양자-내성 암호화 채택의 촉진 및 안전한 양자 컴퓨팅 확보

- AI 보안 부문 혁신을 촉진해 데이터 센터를 비롯한 **AI 기술 스택**을 안전하게 보호하고, 위협 행위자를 탐지, 유인, 기만하기 위해 **AI-기반 사이버 도구**들을 신속하게 도입

- **에이전틱 AI의 빠른 채택**을 장려해 네트워크 방어와 적대 세력 무력화 수준을 안전하게 확장하고, 생성형 AI와 에이전틱 AI 등 AI가 혁신과 글로벌 안정을 가져오도록 **사이버 외교**를 추진

- 미국의 AI 부문 리더십을 뒷받침하는 데이터, 인프라, 모델들을 안전하게 보호하고; 사용자들을 검열, 감시, 오도하는 **외국산 AI 플랫폼**들을 폭로하고 그 확산을 저지(Anti- Censorship & Surveillance)

❻ 사이버 인재와 역량 구축

- 그 투자 가치가 크고 국가 번영과 안보에 필요한 **전략 자산인 사이버 인재**를 개발, 공유하는 실용적이며 접근성이 보강된 **파이프라인** 구축

* 학계, 직업 기술 학교, 기업 등 **기존 경로를 조율**해 이점을 활용하면서 **사이버 인력의 교육과 훈련 프로그램을 강화**하고, 정교한 사이버 기술과 솔루션을 설계하고 구현할 **차세대 인력을 충원**

- 산업계, 학계, 정부, 군이 인센티브를 조율하고 **숙련된 사이버 인력**을 구축할 수 있도록 장애물을 제거하고, 기존의 자원, 권한, 인재와 독창성을 활용해 나갈 방침

II. 우리나라에 주는 시사점

1. 국가 안보 전략 차원

□ 미국 사이버 전략의 핵심 기조는 압도적인 '비-물리적 전력'과 민간 첨단기술의 전략적 통합과 활용을 통한 '공세적 억지력'을 강조하는 것으로, 우리의 국가 사이버안보 전략에도 여러 시사점을 주고 있음

○ **(민생 직결형 안보)** 미국은 사이버 공격과 위협의 대상을 '가족, 농민, 환자' 등 일반 시민으로 정의하고 있는바, 이는 사이버안보가 국가적인 기밀 보호를 넘어 '국민의 일상과 물가' 등을 지켜내는 민생 안보임을 강조하는 논리로 전환될 필요가 있음을 시사

○ **(공세적 대응으로의 전환)** 미국은 적대적인 사이버 위협에 대해 방어에 그치지 않고 가혹한 대가를 동반하는 사이버 공격 등 직접적인 타격을 가하겠다는 의지를 분명히 하고, 단순히 보안에 쓰는 수준을 넘어 스스로 목표를 설정하고 실행하는 '에이전틱'(agentic) AI를 통한 공격과 방어 확장을 명시

- 사람이 일일이 대응하지 않고, AI 군단이 실시간으로 위협자를 기만, 역공격하는 '자동화된 사이버 전쟁' 시대로의 진입을 선포하는 대목으로, 수동적 방어를 넘어 사이버 공격에 대해 경제적/물리적 타격을 줄 강력하고 실질적인 '사이버 억지' 수단 확보와 능동형 사이버 대응체계 개발의 필요성을 시사

○ **(기술 패권주의)** 미국은 초격차 역량을 바탕으로 미국 우선주의(America first)를 강조하며 기술 격차 유지를 사이버안보 전략의 핵심으로 삼고, AI 서비스뿐 아니라, 이를 구동하는 하드웨어, 데이터 센터, 데이터, 알고리즘 모델 전체 즉, AI 기술 스택을 국가 안보 자산으로 보호하겠다는 의지를 천명

- 이는 반도체, AI 등 핵심 기술 보호가 국가 안보와 직결될 수 있음을 재확인시켜 주는 부분으로, 데이터 센터에 대한 사이버/물리적 보안 요구 수준도 '국가 중요 시설급'으로 격상되고, 클라우드/데이터 센터 사업자들에 대해서도 미국 수준의 보안 표준 요구가 거세질 수 있을 것으로 보임

○ **(규제 합리화를 통한 안보 강화)** 미국은 '비효율적 규제 제거'(상식적인 규제)를 혁신의 열쇠로 보고 규제

간소화를 추진하고 있는바, 보안이 혁신의 걸림돌이 아닌 기반이 되도록 규제를 합리화하되, 국가 안보 자산의 현대화와 경쟁력 확보 관점에서 실질 성과를 강조하는 방향으로 접근해야 함을 시사

○ **(가치 기반의 기술 경쟁)** 미국은 적대적 국가의 저가형 장비나 소프트웨어에 내재된 '감시 및 편향성'을 정면으로 비판하며, 그러한 AI 모델의 확산을 '정보 오염'이나 '안보 위협'을 규정함

- 이는 기술 패권 전쟁이 하드웨어를 넘어 AI 모델과 알고리즘이라는 '소프트파워의 안보화'로 확장되고, 글로벌 AI 시장이 '신뢰할 수 있는 AI'와 '신뢰할 수 없는 AI'로 양분될 수 있음을 의미하므로, 공급망 안보에서 가격 논리보다 '민주적 가치와 신뢰성'을 최우선 기준으로 삼을 필요가 있음을 시사

○ **(비용과 책임의 분담)** 적대 세력의 사이버 활동 억제는 사이버 공간을 방어하고 자유를 수호하려는 집단적 노력이고, 그 비용과 책임은 미국 및 민주적 가치를 공유하는 우방국 간에 공정하게 배분되어야 한다고 강조하고 있는 부분도 참고할 대목

2. 디지털자산 사업자 등 민간 부문에 주는 시사점

□ 트럼프 대통령의 미국 사이버 전략에는 사이버 위협 세력에 대한 공세적 대응 전환 등 **불법 금융**에 대한 단호한 대처뿐 아니라, **암호화폐와 블록체인 기술의 보안성 지원** 및 사용자 프라이버시 보호, **양자-내성 암호화 채택**의 촉진 등도 포함되어 있음

□ 특히, 불법 금융 대응과 사이버보안 부분은 지난해 7월 발표된, **트럼프 대통령 직속의 디지털자산 시장 워킹그룹 보고서(PWG Crypto Report)**[2]에서도 강조되면서 **'공공-민간 협력 체계'의 확대**도 권고되고 있는 부분이므로, 디지털자산 사업자 등 민간 부문에도 직접적인 영향을 미칠 수 있을 것임

○ **(자금세탁 및 탈취에 대한 무관용)** 트럼프 대통령의 미국 사이버 전략에는 불법 자금 "탈출 경로와 피난처 부인"(denying financial exit and safe haven) 등의 표현이 들어있으므로, 국내외 디지털자산 거래소들에도 그 시사하는 바가 큼

- 150억 달러에 이르는 천문학적 규모의 자산 몰수는 미국이 디지털자산 거래소를 통해 흐르는 불법 자금에 대해, 그리고 북한 등 해킹 세력의 탈취 자금의 세탁 경로가 되는 디지털자산 거래소나 믹서(Mixer) 서비스에 대해 언제든 직접적으로, 강력한 사이버/물리적 개입과 제재를 할 수 있음을 뜻함

---

[2] President's Working Group on Digital Asset Markets(2025.7.30.), "Strengthening American Leadership in Digital Financial Technology"(디지털 금융 기술 부문의 미국 리더십 강화). 번역본은 업비트 투자자보호센터 홈페이지 게시물 참조: https://upbitcare.com/academy/research/1026

- 또한, "네트워크 해체"와 "외국 해킹 업체 제재"는 자산 탈취와 연루된 거래소나 프로토콜이 미국의 직접적인 작전 대상이 될 수 있다는 점에서, 디지털자산 거래소들은 자산의 흐름뿐 아니라, 소프트웨어 공급망 전체에 대한 안보 검토를 수행하고, '국가 안보를 위협하는 자금의 통로'가 되지 않도록 금융 사고 방지를 넘어서는 실시간 차단 역량까지 갖춰나갈 필요가 있을 것임

- 적대 세력의 자금줄 차단이 '미국 우선주의'의 핵심이라 할 만큼, PWG Report에서도 디지털자산 부문 내 악성 행위자들에 대한 지속적 억제의 필요성과 효과적인 AML/CFT 체계가 강조되고 있는 만큼, 디지털자산 거래소들이 이를 방조하게 되면 미국의 '세계 최고 수준의 사이버 도구'에 의한 직접적인 타격 대상이 될 수도 있다는 강력한 경고로 해석될 수 있음

○ **(보안 기준의 상향 평준화)** 미국 사이버 전략에서 강조하고 있는 민-관 협력 체계하에서는, 디지털자산 거래소들의 안보 책임이 강화되고 미국이 요구하는 수준의 사이버 보안 체계를 갖출 필요성이 커질 것임

- 사이버 공간의 패권을 강조하는 미국의 전략하에서는, 미국민에 관계되는 디지털자산 거래 데이터 역시 국가 안보 정보로서의 가치를 지니게 될 것이므로, 디지털자산 거래소들은 더욱 엄격한 고객 확인과 실시간 모니터링 등 효과적인 AML/CFT 체계를 구축하고 실행해야 할 것임

- 미국은 사이버 전략에서 "평시와 전시를 아우르는 새로운 차원의 민관 협력 관계"를 강조하고 있는 바, 이는 정부가 필요시 디지털자산 거래소를 상대로 데이터나 인프라 측면의 강력한 협조를 요구할 수 있음을 뜻하므로, 안보 차원의 사이버 위협 정보 공유 체계로 편입되는 디지털자산 거래소들도 단순한 보고를 넘어 '국가 사이버 방위 체계의 일원'이라는 역할을 요구받게 될 것임

- PWG Report에서도 디지털자산 부문의 사이버 보안 위험이 국가적 안보 우려로 이어지고 있음을 고려, **사이버 보안 표준**의 채택과 위협 정보의 자동 전파 체계 등 **공공-민간 부문 간 협력 체계** 확대를 강조한 바 있고, 미국에서는 **Blockchain Alliance**와 **Crypto-ISAC**을 중심으로 디지털자산 부문에서 실질적으로 작동하는 민관 협력 체계[3]가 존재함

---

3) 미국에는 FinCEN, 법무부(DoJ) 등 법 집행을 담당하는 공공 부문과 민간 부문의 협력 체계가 구축되어 있음. 그 예로 **Blockchain Alliance**와 **Crypto-ISAC**을 들 수 있는데, 전자는 디지털자산에 대한 부정적 인식을 해소하고 거래소 법무팀과 수사기관 관계자가 교류하며 교육과 협의하는 포럼 성격의 '**사람 중심 네트워크**'로 2015년경 구성되었고, 후자는 국가 배후의 정교화된 지속적 해킹 공격이 늘어나면서 단순히 대화만으로는 대응이 어려운 '사이버 전쟁' 양태가 되고 있다는 상황 인식을 바탕으로, 디지털자산이 본격적으로 제도화된 시기인 2024년에 설립된 '**시스템 중심의 네트워크**'로서, 사람이 만나서 회의하는 게 아니라 API를 통해 해커의 지갑 주소, 악성코드 패턴 등을 기계적으로 실시간 공유하는 역할을 함. Blockchain Alliance가 평소 수사기관과 신뢰를 쌓고, 법적인 절차를 매끄럽게 만드는 역할을 한다면, Crypto-ISAC은 해킹이 발생하게 되면 기술적으로 즉각 대응하는 역할을 하는

* 국내의 경우, 대표적인 디지털자산 거래소인 업비트는 AI-기반 이상거래탐지 시스템(FDS)과 온체인 추적 시스템(OTS, On-chain Tracing System)을 갖춰 높은 수준의 기술 역량을 바탕으로 민관 협력 체계의 작동에 기여하고 있음

○ **(디지털자산 보안 확보)** 미국 사이버 전략은 "**암호화폐 및 블록체인 기술의 보안 지원 포함**"도 명시하고 있는바, 안보 체계로 수용되는 디지털자산의 보안 표준은 미국이 주도하겠다는 의지로 볼 수 있음

- 향후 미국이 주도하는 PQC(효과성 검증을 전제) 적용 등 보안 표준을 맞추지 못하게 되는 국내외 디지털자산 프로토콜이나 디지털자산 거래소들이 글로벌 시장에서 고립될 수도 있음을 시사

○ **(AI 기반 솔루션 고도화)** 미국이 '에이전틱 AI'를 도입하게 되면서, 자금세탁이나 해킹 자금에 대한 추적 속도가 비약적으로 빨라질 것이므로, 디지털자산 거래소들의 AI-기반 솔루션 도입은 현실적 과제임

- 디지털자산 거래소들도 수동적 모니터링을 넘어 AI-기반의 이상거래탐지 체계(FDS) 등 불법 자금을 AI 에이전트가 실시간으로 추적·동결하는 시스템을 구축하라는 압박을 받게 될 것이며,

- 거래소가 사용하는 예측 모델이나 보안 AI 자체가 적대적 해킹을 당해 국가 안보 사고로 이어지지 않도록, AI 모델에 대한 취약점 점검(AI security)도 보안 프로세스의 필수적 요소가 되어야 할 것임

상호 보완적 관계라고 할 수 있음. FBI 등 정부 당국은 제재, 기소라는 법적 권한은 있으나 실시간 추적 등 기술적 민첩성이 부족하지만, 민간의 Crypto-ISAC과 SEAL 911은 권한은 없으나 속도에 앞선다는 점에서, 이 둘이 결합한 릴레이 형태 즉, **"민간의 선제 대응→ 정부 당국의 법적 확정 → 민간의 봉쇄"**로 이어지는 협력 체계를 구축하고 있음. 코인베이스, 크라켄 같은 메이저 거래소들은 Blockchain Alliance와 Crypto-ISAC이라는 민관 파트너십 모두에 가입되어 있음. **화이트 해커 그룹인 SEAL 911**도 당국과는 MOU를 맺지 않은 '비공식 핫라인'으로 민관 협력 체계를 지원함. SEAL 911은 해커의 것으로 의심되는 IP, 특정 패턴을 식별해 중개자 역할을 하는 체이널리시스나 TRM랩스 같은 블록체인 분석 기업을 통해 FBI 사이버수사대 등에 전달하고, 수사기관은 서버 압수 수색 영장을 청구하는 방식으로 작동함.

트럼프 대통령의 미국 사이버 전략

President Trump's Cyber Strategy for America

【전문】

THE WHITE HOUSE

지난 수년간, 미합중국은 우리가 지구상에서 가장 강력하며, 고도화되고, 기술적으로 진보된 군대를 보유하고 있음을 전 세계에 보여주었으며—이는 비교하기도 불가능한 수준이다. 여기에는 우리의 압도적인 재래식 군사력뿐 아니라, 타의 추종을 불허하는 비-물리적 억지력(non-kinetic powers)[4]도 포함된다.

본 국가 사이버 전략(National Cyber Strategy)은 미국이 사이버 공간(cyberspace)에서 독보적 지위를 유지하도록 하고자 본인이 우선순위를 두는 정책 기조를 개괄하는 것이다. 본 전략은 최고의 기술에 투자하고 세계 수준의 혁신을 지속하기 위해, 그리고 공세적 임무와 방어적 임무라는 두 부문에서 미국의 사이버 역량을 최대한 활용하기 위해 정부와 민간 부문 간의 전례 없는 협력을 천명하는 것이다.

우리의 사이버 도구와 운용자들 수준은 세계 최고이며—우리는 이들 역량이 우리의 적대 세력들을 와해시키며 교란하고, 그 어떤 피난처도 그들에게 허용하지 않음으로써 미국을 방어하도록 이들 역량에 강력한 권한을 부여하는 바이다. 미국은 전 세계 다른 국가들이 이제 막 상상하기 시작할 만한 수준의 역량을 보유하고 있다. 그 누구든 미국에 해를 끼치려는 자라면 가장 가혹하고 가장 끔찍한 대가를 치르도록 우리의 사이버 공간 전사들이 매일 정진하고 있다.

본 전략은 미국 국민의 안전, 안보, 그리고 번영을 수호하도록 하려는 것이다. 미국 독립 250주년을 앞둔 지금, 이 문서에 적시된 전략은 미국이 세계 역사상, 미래에도 오랫동안, 가장 강력하며, 가장 자유롭고, 가장 위대한 국가로 남을 수 있도록 해줄 것이다. 이제 사이버 공간에서도 미국의 힘(American Power)은 당당히 바로 서게 될 것이다.

트럼프 대통령 서명

---

[4] [참고] "비물리적 전력"(non-kinetic powers)이란 폭격 등 물리적 타격 없이 적의 시스템을 마비시키거나 무력화하는 사이버 공격, 전자전 등을 뜻하며, 현대전의 핵심 변수로 떠오르고 있음.

【본문】

사이버 공간은 미국에서 탄생하였다. 미국의 인재, 혁신, 연구, 그리고 정부의 강력한 역량이 결합하여 모든 미국인이 정보와 경제적 기회를 얻고, 우리 삶의 기본적인 방식을 위해 의존하게 된 역동적이며, 번창하는, 디지털 세계를 만들어냈다. 실제로, 사이버 영역(cyber domain)은 미국이 금융 부문, 혁신과 신흥 기술 부문, 군사력과 제조업 부문에서 세계를 선도할 수 있게 하려는 트럼프 대통령이 취한 여러 조치의 핵심 부분이다.

그러나, 사이버 공간에서의 자유와 안전이 당연하게 주어지는 건 아니다. 적대 세력들과 사이버 범죄자들은 권위주의를 심화시키고, 민주주의를 억압하며, 우리의 국가 안보와 경제 안보를 훼손하기 위해 사이버 공간을 악용하고 있다.

과거 행정부와 달리, 트럼프 행정부는 나날이 증가하는 사이버 위협의 수위와 심각성을 방치하는 부분에 그치는 조치나 모호한 전략으로 주변에만 머무르지 않을 것이다. 트럼프 대통령은 사이버 공간에서의 위협을 바로잡기 위해 계속해서 정면 대응해 나갈 것이다.

미국은 기술과 경제 부문의 독보적인 혁신, 필적할 바 없는 군사력, 그리고 자유롭고 개방된 표현에 헌신하는 사회를 향유하고 있다. 모든 미국인은 사이버 공간에서 그들 자신과 가족을 보호하기 위해 실질적인 조치를 할 수 있어야 하지만, 미국의 시민들이 홀로 대처하도록 해서는 아니 된다. 트럼프 대통령은 우리의 모든 비교 우위를 활용하여 미국민들이 안전하고 번영하도록 만들겠다는 의지를 거듭해서 보여주었다. 이 전략은 트럼프 대통령이 취한 여러 조치의 연장선이며, 사이버 공간에서도 미국을 우선함으로써(putting America first in cyberspace) 국가 안보 전략(National Security Strategy)을 직접적으로 뒷받침하는 것이다.

사이버 공간에서 우리의 적대 세력들과 사이버 범죄자들은 우리의 가족, 이웃, 중소기업, 농민, 응급 구조대원, 환자, 그리고 노년층을 표적으로 삼고 있다. 그들은 의료, 은행 서비스, 식량 공급, 수자원 처리 등 핵심 서비스들을 교란하면서, 우리 경제에 막대한 비용을 전가하고 일상 용품의 가격을 감당하기 어렵게 만들고 있다.

그러나, 트럼프 대통령이 취한 여러 조치는 명확한 메시지를 보내고 있다: 사이버 공간에서 우리 이익을 지켜내기 위해 우리는 행동할 것이다. 온라인 사기 조직의 네트워크를 파괴하고 이들이

훔쳐낸 150억 달러의 장물을 압수한 것이나, 이란의 핵 기반 시설을 궤멸시키기 위한 전 지구적 작전을 지원한 것이나, 혹은 국제적인 마약 테러리스트인 니콜라스 마두로를 법의 심판대에 세우려는 완벽한 군사 작전을 수행하는 동안 우리의 적대 세력들의 눈을 가리고 무력하게 만들었던 사례들에서 보듯, 적대 세력들은 미국의 사이버 요원과 도구들이 세계 최고이며 미국의 이익을 방어하기 위해 신속하고 효과적으로 동원될 수 있다는 사실을 분명히 인지하게 되었다.

미국민은 미국 우선주의를 실현하도록 트럼프 대통령을 재선시켰다. 본 전략은 미국의 국민에게, 의회에, 우리의 산업 부문 파트너들에게, 전 세계 우방국에—그리고 적대 세력들에게도 트럼프 행정부의 사이버 비전과 접근법을 전달하는 것이다. 본 전략은 행정부의 우선순위를 설명하는 것으로, 요약된 6대 정책 기조(six policy pillars)는 후속 정책 수단들을 통해 실행과 자원의 배분을 이끌 지침이 될 것이다. 이 전략은 트럼프 대통령이 지금까지 취해온 여러 조치를 바탕으로 수립되었고, 사이버 위협에 대응해 이전에 동원된 적이 없는 수준의 조정과 관여, 그리고 정치적 의지를 요구하는 것이다. 트럼프 대통령의 리더십이 사이버 공간에서 새 시대를 열고 있다.

향후 추진 방향 (Moving Forward)

우리의 결의는 확고하다. 미국에 대한 사이버 위협을 무력화하기 위해 신속하고 단호하게, 그리고 선제적으로 행동할 것이다. 우리의 대응 범위를 "사이버" 영역에만 한정하지 않을 것이다. 미국 정부 전반에 걸쳐 조율된 지속적인 방식으로 작동하는 전례 없는 노력을 기울이게 될 것이고, 전 세계 우방국들과 협력하면서, 미합중국의 이익과 안보를 증진해 나갈 것이다. 우리는 표현의 자유를 위축시키는 행위에 맞서 싸울 것이다. 검열과 감시 기능이 내장되고, 이념적 편향성을 동반하는 "저가형"와 디지털 기술들을 판매하는 적대 세력들과 경쟁에서 앞설 것이다. 우리는 우리가 직면한 위협에 걸맞은 속도와 규모로, 그리고 우리의 가치에 부합하는 방식으로 산업계 및 학계와 긴밀히 협력해 나갈 것이다.

트럼프 대통령은 미국인들을 표적으로 삼는 건 위험천만한 일이 되도록 만들었다. 우리의 적대 세력들은 이미 자신들의 행위에 따른 대가를 치르고 있고, 앞으로도 점점 그 대가를 느끼게 될 것이며; 우리는 네트워크들을 해체하고, 해커와 첩자들을 추적하며, 법질서를 무시하는 해외

해킹 회사들을 제재해 나갈 것이다. 우리는 온라인 첩보 활동, 파괴적인 선전과 영향력 행사 작전, 그리고 문화적 전복 기도를 밝혀내고 그들에게 수치심을 안겨줄 것이다.

적대 세력들의 사이버 캠페인을 무력화하고 우리의 네트워크들의 방어 태세와 복원력을 더욱 강화함으로써, 우리는 혁신을 촉발하고 경제 성장을 가속하며 미국의 기술 패권을 확보해 나갈 것이다. 우리는 부담스럽고 비효율적인 규제들을 제거함으로써 우리의 산업계 파트너들이 신흥 기술 분야에서 빠르게 혁신할 수 있도록 해 나갈 것이다. 민간 부문에 있는 파트너들은 미국 경제의 연속성이 확보될 수 있도록 빠르게 대응하고 회복할 수 있어야 한다. 우리는 혁신의 토대에 보안성을 갖춤으로써 우리의 연방 시스템, 핵심 기반 시설, 그리고 공급망을 방어해 나갈 것이다. 우리는 낡은 인프라가 혁신을 가로막지 않도록 우리의 정보 시스템들을 현대화해 나갈 것이다. 국제적으로 우리는 외교, 통상과 작전을 통해 제반 규범과 표준에 우리의 가치가 반영되도록 해 나갈 것이다. 우리는 우리의 민간 부문 연구 기반이 가진 엄청난 재능과 독창성을 활용해 나갈 것이며, 평시와 전시에 미국을 방어하기 위해 공공과 민간 부문 간에 새로운 차원의 관계를 정립해 나갈 것이다.

정책 실행 기조 (Pillars of Action)

6대 정책 기조는 본 전략을 뒷받침하면서 그 이행과 성공 여부를 가늠하는 척도가 될 것이다.

1. 적대 세력의 사이버 활동 억제 (Shape Adversary Behavior)

미국의 시민들, 기업들, 그리고 우리 우방국들이 사이버 공간에서 활동하는 정교한 군사, 첩보, 그리고 범죄 세력들을 홀로 상대하도록 해서는 아니 된다. 우리는 미합중국 정부의 모든 방어적이며 공세적인 사이버 작전 역량을 동원할 것이다. 우리는 적대적인 네트워크들을 식별해 분쇄하고 우리의 국가적 역량을 확장하도록 민간 부문에 유인을 제공하면서 독려해 나갈 것이다. 우리는 적대 세력들이 우리의 네트워크와 시스템에 침입하기 전에 이들을 탐지, 대응하고 격퇴해야 한다. 우리는 그들의 지위와 역량을 약화하고, 공격해 오는 그들의 비용이 높아지도록 국력의 모든 수단을 사용할 것이다. 우리는 시민들을 감시하고 억압하는 감시 국가와 권위주의적 기술

들의 확산을 저지할 것이다. 사이버범죄와 지식재산권 탈취는 세계 경제에 대한 최대의 위협이다. 우리는 범죄 인프라를 뿌리 뽑고, 자금의 탈출구와 피난처(financial exit and safe heaven)를 부정해 나갈 것이다. 사이버 공간을 방어하고 자유를 안전하게 지키는 일은 집단적 노력이 되어야 한다—그 비용과 책임의 배분은 미합중국 그리고 우리의 민주적 가치를 공유하는 우방국들 사이에 공정해야만 한다. 우리는 우리를 해치려는 적대 세력들에게 실제의 위험이 만들어지도록 서로 협력하고, 우리를 상대로 그렇게 하는 자들에게 대가를 부과할 것이다.

2. 사이버 규제의 합리화 (Promote Common Sense Regulation)

사이버 방어가 준비 태세, 조치와 대응을 늦추는 고비용 체크리스트(costly checklist)로 전락해서는 아니 된다. 우리는 규제 준수 부담을 줄이고, 책임 관계를 명확히 다루며, 전 세계적으로 규제 당국자들과 산업계가 보조를 더 잘 맞춰나가도록 사이버 규제를 간소화해 나갈 것이다. 우리는 민간 부문이 급속히 진화하는 위협을 따라잡는 데 필요한 민첩성을 갖추도록 데이터와 사이버 보안 관련 규제를 정비해 나갈 것이다. 우리는 미국민들과 미국민에 관계되는 데이터의 프라이버시 권리를 강조해 나갈 것이다.

3. 연방 정부 네트워크의 현대화와 보안성 강화 (Modernize and Secure Federal Government Networks)

우리는 제반 사이버 보안 모범 사례, 양자-내성 암호(PQC), 제로 트러스트 아키텍처, 클라우드 전환을 이행함으로써 연방 정보 시스템의 현대화, 방어력, 그리고 복원력 강화 속도를 높여나갈 것이다. 우리는 정부의 지도층과 기업 이사회 내에서 사이버의 중요성 인식이 높아지도록 노력할 것이다. 우리는 연방 네트워크들에서 지속적으로 테스트하고 악성 행위자들을 추적하기 위해 최고의 기술과 팀을 활용해 나갈 것이다. 우리는 우리의 군사, 정보 및 민간 기업들을 뒷받침하는 국가 안보 시스템(National Security Systems)의 보안성과 복원성을 최우선에 둘 것이며, 연방 네트워크들을 방어하고 대규모 침입을 탐지해 내기 위해 AI-역량을 기반으로 하는 사이버 보안 솔루션들을 채택하는 노력을 기울일 것이다. 정부 전반에 걸쳐 자금 조달 절차를 현대화하고 경쟁적 프로세스가 만들어지도록 협력하면서, 우리는 정부가 최고의 기술을 구매하고 사용할 수 있도록 장벽들을 제거해 나갈 것이다.

4. 핵심 인프라 보호 (Secure Critical Infrastructure)

우리는 미국의 핵심 인프라를 식별하여, 우선에 두고, 공고히 해 나가고, 그 공급망들을 안전하게 보호해 나갈 것인바, 여기에는 정보 기술과 운영 기술 공급망들을 안전하게 보호하면서 에너지망, 금융과 통신 시스템, 데이터 센터, 수자원 시설, 병원들 같은 핵심 인프라와 근린 편의시설, 민간 회사, 네트워크들 및 서비스 등에 대한 방어가 포함될 것이다. 우리는 미국산 기술들을 촉진하고 활용하면서, 적대적인 공급자들과 제품에서 벗어나야 한다. 우리는 우리 적대 세력들의 초기 접근을 부정해 나갈 것이며, 그리고 사고가 발생하게 되면, 빠르게 복구할 수 있어야 한다. 우리는 우리의 국가적인 사이버 보안 노력을 대체하는 것은 아니지만, 그 보완책으로 주와 지역, 부족(Tribal), 속령을 관장하는 당국들의 역할을 활성화해 나갈 것이다.

5. 핵심 신기술 부문의 우위 유지 (Sustain Superiority in Critical and Emerging Technologies)

미국의 혁신을 안전하게 하고 우리의 국가적인 지적 우위를 보호하는 일이 최우선의 과제가 될 것이다. 우리는 암호화폐와 블록체인 기술의 보안성에 대한 지원을 포함하여, 설계 단계에서 가동에 이르기까지 사용자 프라이버시를 보호하는 안전한 기술과 공급망을 구축해 나갈 것이다. 우리는 양자-내성 암호화 채택을 촉진하고 양자 컴퓨팅의 안전성을 확보해 나갈 것이다.

그리고 우리는 우리의 데이터 센터들을 포함하는, AI 기술 스택(AI technology stack)을 안전하게 보호하고, AI 보안 부문에서 혁신을 촉진해 나갈 것이다. 우리는 위협 행위자들을 탐지해 내고, 유인하며, 기만하기 위해 AI-기반의 사이버 도구들을 신속하게 시행해 나갈 것이다. 우리는 네트워크 방어와 적대 세력 무력화 수준을 안전하게 확장하는 방식으로 에이전틱 AI(agentic AI)를 빠르게 채택하고 장려해 나갈 것이다. 사이버 외교를 통해서는, 특히 생성형 AI 및 에이전틱 AI 등 AI가 혁신과 글로벌 안정을 증진하도록 해 나갈 것이다. 우리는 AI 부문에서 미국의 리더십을 뒷받침하는 데이터, 인프라, 모델들을 안전하게 보호할 것이며, 그 사용자들을 검열, 감시하고 오도하는 외국산 AI 플랫폼들을 폭로하고 그 확산을 저지해 나갈 것이다.

6. 사이버 인재와 역량 구축 (Build Talent and Capacity)

트럼프 대통령은 사이버 인력을 "미국민, 조국, 그리고 미국민의 생활 방식을 보호하는" 전략 자산이라고 지칭해 왔다. 사이버 인력은 투자 가치가 매우 큰 자산이며 국가의 번영과 안보에 필수적인 자산이다. 우리에겐 인재를 개발하고 공유하는 파이프라인이 필요하다. 여러 산업계와 직종에 걸쳐 우리의 기존 사이버 인력을 교육하고 훈련하고, 정교한 사이버 기술과 솔루션들을 설계하고 구현하도록 차세대 인력을 충원하는 일은 실용적이면서도 접근성이 확보되는 방향이 되어야 하며—학계, 직업 기술 학교, 기업들, 그리고 벤처 캐피털 기회 내에 존재하는 기존의 경로들을 조율하고 그 이점을 활용하는 것이어야 한다. 우리는 산업계, 학계, 정부와 군이 인센티브를 조율하고 고도로 숙련된 사이버 인력을 구축하지 못하게 가로막고 있는 장애물들을 제거해 나갈 것이며, 미국을 위대하게 만들어 주는 기존의 자원, 권한들, 인재들과 독창성을 활용해 나갈 것이다.

결어 (Conclusion)

본 전략은 트럼프 대통령이 사이버 공간에서 추구해 왔던 경로와 향후 미합중국 정부가 영향력을 높이면서 추구해 나갈 방향을 명확히 제시하는 것이다. 트럼프 대통령은 미국인들, 특히 미래 세대가 안전하게 보호받는 강한 국가, 그리고 개인의 자유, 경제적 번영 및 기회로 정의되는 미래를 갖도록 하려고 행동해 왔다. 트럼프 대통령은 사이버 공간에서 우리의 이익을 해치고 우리의 가치를 공격하는 자들은 스스로가 위험에 빠져들고 있다는 점을 계속해서 보여주게 될 것이다.

President Trump's

CYBER STRATEGY

for America

MARCH 2026

THE WHITE HOUSE

WASHINGTON

Over the past year, the United States has shown the entire world that we have the most powerful, sophisticated, and technologically advanced military on earth—and it is not even close. This includes not only our overwhelming conventional military strength, but also our unparalleled non-kinetic powers.

The National Cyber Strategy outlines my priorities for ensuring that America remains unrivaled in cyberspace. It calls for unprecedented coordination across government and the private sector to invest in the best technologies and continue world-class innovation, and to make the most of America's cyber capabilities for both offensive and defensive missions.

Our cyber tools and operators are the best in the world—and we are empowering them to defend America by disrupting and disorienting our adversaries, and denying them a safe haven. The United States has capabilities that the rest of the world can only begin to imagine. Our warriors in cyberspace are working everyday to ensure that anyone who would seek to harm America will pay the steepest and most terrible price.

This strategy is about defending the safety, security, and prosperity of the American People. As we approach the 250th anniversary of American Independence, the strategy laid out in this document will help ensure that America remains the strongest, freest, and greatest country in the history of the world, long into the future. American Power will finally stand up in cyberspace.

Cyberspace was born in America. American talent, innovation, research, and powerful government capabilities combined to create a dynamic, thriving, digital world that every American relies on for information, economic opportunity, and our basic way of life. Indeed, the cyber domain is key to President Trump's actions to ensure America leads the world in finance, innovation and emerging technology, military power, and manufacturing.

Freedom and safety in cyberspace, however, cannot be taken for granted. Adversaries and cybercriminals exploit cyberspace to advance authoritarianism, suppress democracy, and undermine our national and economic security.

Unlike other Administrations, the Trump Administration will not tinker at the edges and apply partial measures and ambiguous strategies that neglect the growing number and severity of cyber threats. President Trump will continue to address threats in cyberspace directly.

America enjoys unrivalled technological and economic innovation, unmatched military power, and a society devoted to free and open expression. Every American should take practical steps to protect themselves and their families in cyberspace, but America's citizens do not stand alone. President Trump has demonstrated time and again that he is determined to make Americans secure and prosperous by harnessing all of our comparative advantages. This strategy is a continuation of President Trump's actions, and directly supports the National Security Strategy by putting America first in cyberspace.

Our adversaries and cyber criminals target our families, neighbors, small businesses, farmers, first responders, patients, and senior citizens in cyberspace. They disrupt critical services like healthcare, banking, food supply, and water treatment. They impose tremendous costs on our economy and make everyday goods less affordable.

President Trump's actions, however, send a clear message: we will act to defend our interests in cyberspace. Whether destroying online scammers' networks and seizing $15 billion of their stolen money, supporting a globe-spanning operation to obliterate Iran's nuclear infrastructure, or leaving our adversaries blind and uncomprehending during a flawless military operation to bring international narco-terrorist Nicolas Maduro to justice, adversaries are on notice that America's cyber operators and tools are the best in the world and can be swiftly and effectively deployed to defend America's interests.

Americans re-elected President Trump to put America first. This strategy communicates the Trump Administration's cyber vision and approach to the American people, to Congress, to our partners in industry and allies across the globe—and also to adversaries. It explains the Administration's priorities, summarized in six policy pillars, which will guide action and resourcing through the follow-on policy vehicles. This strategy builds on President Trump's actions to date, and requires a level of coordination, commitment, and political will never before marshalled against cyber threats. President Trump's leadership has created a new era in cyberspace.

Moving Forward

Our resolve is absolute. We will act swiftly, deliberately, and proactively to disable cyber threats to America. We will not confine our responses to the "cyber" realm. We will undertake an unprecedented effort, operating in a coordinated and sustained fashion across the U.S. government. Working with allies across the globe, we will promote U.S. interests and security. We will fight the curtailment of free speech. We will outcompete adversaries who sell "low cost" AI and digital technologies that carry embedded censorship, surveillance, and ideological bias. We will partner closely with industry and academia, at the speed and scale commensurate with the threats we face, and in accordance with our values.

President Trump has made targeting Americans a hazardous business. Our adversaries have and will increasingly feel the consequences of their actions; we will dismantle networks, pursue hackers and spies, and sanction lawless foreign hacking companies. We will unveil and embarrass online espionage, destructive propaganda and influence operations, and cultural subversion.

By disrupting adversaries' cyber campaigns, and making our networks more defensible and resilient, we will unleash innovation, accelerate economic growth, and secure American technology dominance. We will remove burdensome, ineffective regulations so that our industry partners innovate quickly in emerging technologies. Partners in the private sector must be able to respond and recover quickly to ensure continuity of the American economy. We will defend our federal systems, critical infrastructure, and supply chains by putting security at the foundation of innovation. We will modernize our information systems so that old infrastructure does not choke innovation. We will engage internationally through diplomacy, commerce, and operations to ensure norms and standards reflect our values. We will leverage the immense talents and ingenuity of our private sector research base. We will establish a new level of relationship between the public and private sectors to defend America in peace and war.

Pillars of Action

Six Policy Pillars underpin this strategy and will guide implementation and measures for success.

1. *Shape Adversary Behavior*

American citizens, companies, and our allies should not have to fend off sophisticated military, intelligence, and criminal adversaries in cyberspace alone. We will deploy the full suite of U.S. government defensive and offensive cyber operations. We will unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities. We must detect, confront, and defeat cyber adversaries before they breach our networks and systems. We will erode their capacity and capabilities, and use all instruments of national power to raise the costs for their aggression. We will counter the spread of the surveillance state and

authoritarian technologies that monitor and repress citizens. Cybercrime and intellectual property theft are some of the greatest threats to global economies. We will uproot criminal infrastructure and deny financial exit and safe haven. Defending cyberspace and safeguarding freedom is a collective effort—the distribution of cost and responsibility must be fair across the U.S. and allies who share our democratic values. We will work together to create real risk for adversaries who seek to harm us, and impose consequences on those who do act against us.

2. *Promote Common Sense Regulation*

Cyber defense should not be reduced to a costly checklist that delays preparedness, action, and response. We will streamline cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally. We will streamline data and cybersecurity regulations to ensure that the private sector has the agility necessary to keep pace with rapidly evolving threats. We will emphasize the right to privacy for Americans and American data.

3. *Modernize and Secure Federal Government Networks*

We will accelerate the modernization, defensibility, and resilience of federal information systems by implementing cybersecurity best practices, post-quantum cryptography, zero-trust architecture, and cloud transition. We will work to elevate the importance of cyber in government leadership and in the board room. We will use the best technologies and teams to constantly test and hunt for malicious actors on federal networks. We will prioritize the security and resilience of the National Security Systems that underpin our military, intelligence, and civilian enterprises. We will work to adopt AI-powered cybersecurity solutions to defend federal networks and deter intrusions at scale. Working across the government to modernize and create competitive procurement processes, we will remove barriers to entry so that the government can buy and use the best technology.

4. *Secure Critical Infrastructure*

We will identify, prioritize, and harden America's critical infrastructure and secure its supply chains, including defense critical infrastructure and adjacent vendors, private companies, networks, and services—such as the energy grid, financial and telecommunication systems, data centers, water utilities, and hospitals—securing information and operational technology supply chains. We must move away from adversary vendors and products, promoting and employing U.S. technologies. We will deny our adversaries initial access, and in the event of an incident, we must be able to recover quickly. We will galvanize the role of state, local, Tribal, and territorial authorities as a complement to—not a substitute for—our national cybersecurity efforts.

5. *Sustain Superiority in Critical and Emerging Technologies*

Securing American innovation and protecting our national intellectual advantage will be paramount. We will build secure technologies and supply chains that protect user privacy from design to deployment, including supporting the security of cryptocurrencies and blockchain technologies. We will promote the adoption of post-quantum cryptography and secure quantum computing.

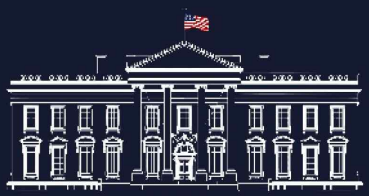
And we will secure the AI technology stack—including our data centers—and promote innovation in AI security. We will swiftly implement AI-enabled cyber tools to detect, divert, and deceive threat actors. We will rapidly adopt and promote agentic AI in ways that securely scale network defense and disruption. Through cyber diplomacy, we will ensure that AI—particularly generative AI and agentic AI—advances innovation and global stability. We will secure the data, infrastructure, and models that underpin U.S. leadership in AI and we will call out and frustrate the spread of foreign AI platforms that censor, surveil, and mislead their users.

6. *Build Talent and Capacity*

President Trump has called America's cyber workforce a strategic asset that "protects the American people, the homeland, and the American way of life." It is an asset worthy of great investment and essential to our nation's economic prosperity and security. We need a pipeline that develops and shares talent. It must be pragmatic and accessible—reconciling and taking advantage of existing avenues within academia, vocational and technical schools, corporations, and venture capital opportunities—to educate and train our existing cyber workforce across industries and occupations, and to recruit the next generation to design and deploy exquisite cyber technologies and solutions. We will eliminate roadblocks that prevent industry, academia, government, and the military from aligning incentives and building a highly skilled cyber workforce. We will harness the existing resources, authorities, talents, and ingenuity that make America great.

Conclusion

This strategy makes clear the course President Trump has pursued in cyberspace, and the direction the U.S. government will pursue with increasing impact. President Trump has acted to ensure that Americans—especially future generations—will have a strong country where they are secure and defended, and a future defined by individual freedom, economic prosperity, and opportunity. President Trump will continue showing those who harm our interests and attack our values in cyberspace place themselves at risk.



THE WHITE HOUSE

WASHINGTON