ISSUE BRIEF

이슈브리프 827호
(2026. 3.27)

<트럼프 대통령의 사이버 전략>: 특징과 시사점

제827호

오일석 nusl2006@inss.re.kr

국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

2026년 3월 6일 백악관은 <미국을 위한 트럼프 대통령의 사이버 전략(President Trump's CYBER STRATEGY for America)>을 발표하였다. 이 사이버 전략은 ①적대 세력의 행동 형성, ②상식적인 규제 촉진, ③연방 정부 네트워크 현대화 및 보안 강화, ④핵심 인프라 보안 강화, ⑤핵심 및 신기술 분야 우위 유지, ⑥인재 및 역량 육성 등을 6대 기둥으로 제시하고 있다. 이 전략은 2025년 12월 4일 발표된 <국가안보전략(National Security Strategy)>의 주요 내용을 사이버 부문에서 구체화하고 있는 것으로 보인다. 이 사이버 전략은 공세적 사이버 작전의 강화를 위하여 필요한 비용을 동맹과 민간에게 전가하는 것을 핵심으로 제시하고 있다. 따라서 사이버안보 비용에 대한 민간 전가가 확대될 것으로 전망되므로, 미국 증시에 상장된 우리 기업들은 이에 대비할 필요가 있다. 특히 미국 정부가 추진하는 공세적 사이버 작전에 참여하도록 요청받는 상황에 대비할 필요가 있다. 한편 우리 정부는 사이버안보 비용의 동맹 전가 상황에도 대비하여야 한다. 이 경우 우리는 사이버공간에서의 방어적 작전에 대한 지원을 강화하여야 할 것이다. 즉, 사이버공간의 취약성 관련 정보를 공유하고, 발생한 침해사고에 대해 공동으로 조사하며, 핵심 인프라에 대한 방어적 훈련에 보다 집중하여야 할 것이다.

주제어 : 트럼프 대통령의 사이버 전략, 국가안보전략, 공세적 사이버 작전, 안보 비용의 전가, 취약성

사이버 전략의 기조와 방향

이란 전쟁이 발발한 지 일주일이 채 지나지 않은 2026년 3월 6일, 백악관은 〈미국을 위한 트럼프 대통령의 사이버 전략(President Trump's CYBER STRATEGY for America)〉을 발표하였다. 이 사이버 전략은 서문과 방향성을 제외하고 실질적인 내용이 고작 4쪽에 불과할 정도로 매우 간단하다. 이는 바이든 정부가 2023년 3월 발표한 〈국가 사이버안보 전략(National Cybersecurity Strategy)〉의 약 7분의 1 수준에 불과하다. 션 케언크로스(Sean Cairncross) 국가사이버국장은 이 사이버 전략에 관하여 향후 실행 계획이 뒤따를 예정인 최고위 정책 선언문이라고 하였다.

그럼에도 불구하고 이 전략은 미국의 이익을 지키기 위하여 사이버 공간에서 보다 공세적으로 행동할 것임을 천명하였다. 사이버 공격 역량 사용에 대해 명확한 입장을 표명하지 않았던 기존 정부들과는 달리, 트럼프 정부는 이 전략에서 공세적 사이버 작전(offensive cyber operation)을 강조하였다. 즉, 미국을 겨냥한 사이버 위협을 무력화하기 위해 신속하고 신중하며 선제적으로 행동할 것이라고 하였다. 동 전략이 베네수엘라 침공의 성공에 따른 자신감에 기초하여 이란에 대한 전격적인 공격을 감행한 지 일주일도 안 되는 시점에 발표되었다는 점에서, 이 전략에는 트럼프 정부의 공세적 사이버 역량 사용에 대한 자신감이 내재되어 있다고 할 것이다. 이는 동 전략이 사이버공간에서 미국의 이익을 방어할 것이라는 분명한 메시지를 전달하면서, 사이버 작전이 이란의 핵 인프라를 파괴하기 위한 작전을 지원하고, 베네수엘라의 니콜라스 마드로(Nicolas Maduro) 대통령 체포 과정에서 적들을 눈멀게 하고 혼란에 빠뜨렸다고 서술한 것을 통하여도 알 수 있다. 동 전략은 미국이 세계 최고 수준의 사이버 툴과 사이버 작전 수행자들을 통해 적들을 교란하고 혼란에 빠뜨림으로써 미국을 방어할 것

이라고 하였다. 나아가 미국의 사이버 전사들은 사이버공간에서 미국을 해하려는 어떠한 적에 대해서도 가장 가혹하고 치명적인 대가를 치르게 할 것이라고 하였다.

이러한 자신감에 기초하여 동 전략은 미국의 공세적 대응이 사이버 영역에만 국한되지 않을 것이라고 하였다. 미국은, 네트워크를 해체하고, 해커와 스파이를 추적하며, 법을 무시하는 외국 해킹 기업들에게 제재를 가할 것이라고 하였다. 또한 온라인 간첩 활동(online espionage), 파괴적인 선전선동(destructive propaganda) 및 영향력 공작(influence operations), 그리고 문화적 전복 행위(cultural subversion) 등의 실체를 밝혀낼 것이라고 하였다.

이와 더불어 미국은 적들의 사이버 공격을 저지하고 미국 네트워크의 방어력과 회복탄력성을 강화함으로써, 혁신을 촉진하고 경제 성장을 가속화하며 미국의 기술 우위를 공고히 할 것이라고 하였다. 또한 보안을 혁신의 토대로 삼아 연방 시스템, 핵심 인프라, 공급망을 방어할 것이라고 하였다.

이를 위하여 동 전략은 민간 부문의 적극적인 역할을 주문하고 있다. 즉, 민간 부문의 파트너들이 미국 경제의 지속성을 보장하기 위해 신속하게 대응하고 복구할 수 있어야 한다는 것이다. 아울러 미 정부가 민간 부문 연구개발의 재능과 독창성을 활용할 것이라고 강조하였다. 나아가 평시는 물론 전시에도, 미국을 방어하기 위해, 공공 부문과 민간 부문 간의 관계를 새로운 차원으로 발전시킬 것이라고 하였다.

주요 내용

〈트럼프 대통령의 사이버 전략〉은 ①적대 세력의 행동 형성,

②상식적인 규제 촉진, ③연방 정부 네트워크 현대화 및 보안 강화, ④핵심 인프라 보안 강화, ⑤핵심 및 신기술 분야 우위 유지, ⑥인재 및 역량 육성 등을 6대 기둥으로 제시하고 있다.

먼저 '적대 세력의 행동 형성' 부분에서는 공세적 사이버 작전(offensive cyber operations)과 이에 대한 민간 부문의 적극적 역할 강화라는 동 전략의 기조와 방향을 다시 확인하고 있다. 우선 동 전략은 미국 시민과 기업, 그리고 동맹국들이 사이버 공간에서 정교한 군사·정보·범죄 세력들의 공격에 노출되어있다고 지적하였다. 이에 미국 정부는 모든 방어 및 공세적 사이버 작전 수단을 총동원할 것이라고 하였다. 아울러 민간 부문이 적의 네트워크 취약성을 식별하고 교란함은 물론 국가적 역량을 확대할 수 있도록 인센티브를 제공함으로써, 민간 부문의 역량을 최대한 발휘하게 할 것이라고 하였다.

여기에 동맹국의 역할 강화와 비용 분담을 강조하고 있다. 즉 동 전략은 사이버공간을 방어하고 자유를 수호하기 위해서는 민주적 가치를 공유하는 미국과 동맹국들의 공동 노력이 필요하다고 하면서도, 이를 위한 비용과 책임의 분담은 공정해야 한다고 강조하고 있다.

'상식적인 규제의 촉진'과 관련하여 동 전략은 사이버 규제를 간소화하여 규제 준수에 따른 부담을 감소시키고, 책임 문제를 해결함은 물론, 전 세계적으로 규제 당국과 산업계의 조화를 도모할 것이라고 하였다. 또한 데이터 및 사이버 보안 규제를 간소화함으로써, 민간 부문이 진화하는 위협에 대응할 수 있는 유연성을 확보하도록 할 것이라고 하였다.

'연방 정부 네트워크의 현대화 및 보안 강화'와 관련하여 동 전략은 사이버 보안 모범 사례, 포스트-양자 컴퓨팅 암호화 기술, 제로

트러스트 아키텍처, 클라우드 전환을 도입하여, 연방 정보 시스템의 현대화와 방어 능력 및 회복력을 가속화할 것이라고 밝혔다. 또한 첨단 기술과 전문 인력을 활용하여 연방 네트워크에 대한 악의적인 행위자들을 지속적으로 탐지하고 추적할 것이라고 하였다. 국가 안보시스템의 보안과 회복 탄력성을 최우선과제로 하고, 연방 네트워크를 방어하고 대규모 침입을 억제하기 위해, AI 기반 사이버 보안 솔루션을 도입할 것이라고 하였다.

'주요 인프라 보호'와 관련하여 미국의 핵심 인프라를 식별하고 우선순위를 정하여 보안을 강화할 것이라고 하였다. 특히, 에너지 전력망, 금융 및 통신 시스템, 데이터 센터, 상수도 시설, 병원 등 핵심 인프라와 관련된 공급업체, 민간 기업, 네트워크, 서비스 등을 보호할 것이라고 하였다.

'핵심 및 신기술 분야의 우위 유지'와 관련하여 동 전략은 미국의 혁신을 보장하고 국가의 지적 우위를 보호하는 것이 최우선 과제라고 천명하였다. 또한 암호화폐 및 블록체인 기술의 보안을 지원함은 물론, 설계에서부터 유통단계까지 프라이버시 보호를 위한 안전한 기술과 공급망을 구축할 것이라고 하였다. 아울러 포스트-양자 컴퓨팅 암호 기술과 안전한 양자 컴퓨팅의 도입을 촉진할 것이라고 하였다.

또한 데이터 센터를 포함한 AI 기술 스택(stack)을 보호하고 AI 보안 분야의 혁신을 촉진할 것이라고 하였다. 사이버 위협 행위자를 탐지, 회피, 기만하기 위한 AI 기반 사이버 툴을 신속하게 도입할 것이라고 하였다.

'인재 및 역량 육성'과 관련하여 트럼프 대통령은 미국의 사이버 인력을 미국 국민과 영토, 그리고 미국의 생활 방식을 보호하는

전략 자산(strategic asset)이라고 하였다. 사이버 인력은 막대한 투자가 필요한 자산일 뿐만 아니라, 미국의 경제적 번영과 안보에 필수적인 요소이므로 사이버 인력을 양성하고 공유할 수 있는 체계가 필요하다고 강조하였다.

평가

이번에 발표한 〈트럼프 대통령의 사이버 전략〉은 2025년 12월 4일 발표된 〈국가안보전략(National Security Strategy)〉의 주요 내용을 사이버 부문에서 구체화하고 있는 것으로 보인다. 〈국가안보전략〉은, 적성국이나 경쟁국으로부터의 신안보 위협을 강조하기 보다는, 경제적 안정과 전략적 우위 유지를 위하여 신안보 분야를 활용하는 방안에 중점을 두었다.[1] 아울러 지역 전략과 동맹국 협력을 추진함에 있어 신안보 분야를 연계 또는 활용하고자 하였다. 이러한 기조의 연장선에서 동 전략은 △외국 혹은 국외로부터의 영향력 공작 대응과 미국의 영향력 증대, △에너지 분야의 경쟁력 강화, △주요 기반시설 보호, △신기술 개발과 투자 등을 중점적으로 강조하였다.[2]

이러한 기조의 연장선에서, 이 사이버 전략은 공세적 사이버 작전의 강화를 천명하고 있음에도 불구하고 사이버 위협 환경에 대해서는 거의 언급하지 않고 있다.[3] 사이버 범죄만이 구체적인 위협으로 논의될 뿐, 중국, 러시아, 이란, 북한 등 국가 차원 혹은 국가 배후에 의하여 발생되고 있는 사이버 위협에 대해서는 침묵하고 있다. 이는 〈국가안보전략〉이 적성국이나 경쟁국으로부터의

1) 오일석, "미 국가안보전략: 신안보 분야의 주요 내용과 시사점", 이슈브리프 제772호, 국가안보전략연구원(2025. 12. 12).
2) Ibid.
3) Matthew Ferren, "Trump's Cyber Strategy Falls Short on China, Iran, and the Threats That Matter Most", Council on Foreign Relations(March 16, 2026), https://www.cfr.org/articles/trumps-cyber-strategy-falls-short-on-china-iran-and-the-threats-that-matter-most(Accssed: March 23, 2026).

신안보 위협을 강조하기 보다는 경제적 안정과 전략적 우위 유지를 강조하고 있는 것과 궤를 같이 한다고 볼 수 있다. 특히 미 정보공동체가 〈2025년 연례 위협 평가 보고서(2025 Annual Threat Assessment of the U.S. Intelligence Community)〉에서 중국을 미국 네트워크에 대한 가장 활발하고 지속적인 사이버 위협으로 지목하였음에도 불구하고, 동 사이버 전략이 이에 대해 침묵하고 있는 것은 중국에 대한 사이버 위협을 강조하여 적대성을 확장하기 보다는 경제적 안정과 전략적 우위의 유지가 중요하다는 정책 기조를 반영하고 있다고 할 것이다.

이 사이버 전략은 파괴적인 선전 및 영향력 공작, 그리고 문화적 전복 행위의 실체를 밝힐 것이라고 하고 있는데, 이는 〈국가안보전략〉에서 언급한 △외국 혹은 국외로부터의 영향력 공작 대응과 미국의 영향력 증대와 맥락을 같이 한다고 볼 수 있다. 또한 〈국가안보전략〉에서 천명한 △에너지 분야의 경쟁력 강화와 △주요 기반시설 보호는, 이 사이버 전략에서 '주요 인프라 보호'와 관련하여 미국의 핵심 인프라를 식별하고 우선순위를 정하여 보안을 강화함은 물론 에너지 전력망의 보호를 강화하는 것으로 정리되었다. △신기술 개발과 투자는 사이버 전략의 '핵심 및 신기술 분야의 우위 유지'로 구체화 되었다. 이에 따라 이 사이버 전략은 암호화폐 및 블록체인 기술의 보안 지원, 프라이버시 보호를 위한 안전한 기술과 공급망 구축, 선진 암호화 기술과 안전한 양자 컴퓨팅의 도입, AI 기술 스택 보호, 사이버 위협의 탐지·회피·기만을 위한 AI 기반 사이버 툴의 신속한 도입 등을 강조하였다.

〈트럼프 대통령의 사이버 전략〉은 사이버 위협으로 사이버 범죄를 강조하면서 이에 대한 적극적인 대응을 주문하고 있다. 동 전략은 미국의 적들과 사이버 범죄자들은 사이버공간에서

우리 가족, 이웃, 소상공인, 농민, 응급 구조대원, 환자, 그리고 노인들을 표적으로 삼고 있다고 하였다. 또한, 사이버 범죄자들이 의료, 금융, 식량 공급, 수자원 처리 같은 핵심 서비스를 마비시키고, 미국 경제에 막대한 비용을 부과하며, 생필품의 가격을 상승시키고 있다고 하였다. 이에 따라 동 전략에서는 공세적 사이버 작전을 강조함과 동시에, 같은 날 사이버 범죄 관련 행정명령을 발표하였다.[4] 이는 앞에서 언급한 바와 같이 적대국이나 경쟁국의 사이버 위협을 강조하기 보다는 사이버 전략을 통하여 미국의 경제적 안정과 전략적 우위의 유지에 방점을 두고 있는 것으로 볼 수 있다. 또한 사이버 범죄로 인한 폐해를 강조함으로써 '상식적인 규제의 촉진'과 '연방 정부 네트워크의 현대화 및 보안 강화'라는 이 사이버 전략의 주요 행동 기둥을 실행하고자 하는 것으로 보인다.

이 사이버 전략은 사이버 분야 동맹 비용 전가를 밝히고 있다. 우선 이 전략은 "모든 미국인은 사이버공간에서 자신과 가족을 보호하기 위해 실질적인 조치를 취하여야 하지만, 미국 시민들은 홀로 서 있는 것이 아닙니다."라고 하면서 모든 비교우위를 활용하여 미국인을 안전하고 번영하게 만들겠다고 하였다. 이는 사이버 공간에 대한 집단 방위 개념의 기반을 조성하기 위한 수사(修辭)적 시도로 보여진다. 이에 기초하여 미국이 공세적 사이버 작전을 강화하고, 군사 작전에 사이버 작전을 통합함에 있어 동맹국의 협력이 필요하다고 강조하고 있다. 그럼에도 불구하고 이 전략은 동맹국의 협력과 관련한 구체적인 활동들에 대해서는 밝히지 않고 있다. 다만 이 전략은 동맹국의 협력과 관련하여 비용과 책임의 분담에 대하여만 기술하고 있을 뿐이다. 이는 사이버공간에서의 동맹 비용 전가라고 할 수 있다. 이 사이버 전략이 "비용과

4) 미국 시민을 대상으로 한 사이버 범죄, 사기 및 악의적인 계획 행위 근절 행정명령(2026년 3월 6일, COMBATING CYBERCRIME, FRAUD, AND PREDATORY SCHEMES AGAINST AMERICAN CITIZENS Executive Orders March 6, 2026), https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/(Accssed: March 23, 2026).

책임의 분담은 민주적 가치를 공유하는 동맹국들과 공정하게 이루어져야 한다."고 명시적으로 밝히고 있기 때문이다.

이 사이버 전략은, 공세적 사이버 작전을 위하여, 동맹국에 대한 비용 전가 뿐만 아니라 민간 부문의 적극적인 가담을 요구하고 있다. 이 전략은 사이버공간에서의 미국의 공세적 작전 강화를 정책 방향으로 제시하면서, 연방 정부가 민간 부문에 대해 적대 세력의 네트워크를 식별하고 교란하도록 인센티브를 제공하는 것으로 정책을 전환할 것이라고 하였다. 다만 민간 기업으로 하여금 적대 세력을 상대로 직접 공세적 사이버 작전을 수행하도록 명시적으로 기술하지는 않았다.[5)]

그럼에도 불구하고 미 정부의 사이버 당국자들은 민간 기업들이 단순히 개별 범죄자나 범죄 집단뿐만 아니라 국가 차원의 사이버 위협 행위자로부터 국가를 방어하는 데도 적극적으로 참여할 것을 기대하고 있는 것으로 보인다. 이는 션 케언크로스 국가사이버국장이 동 사이버 전략의 핵심을 대응적 방어(reactive defense)를 넘어, 적의 행동을 유도하고, 비용과 결과를 부담하도록 하는데 초점을 맞춘 선제적 작전(proactive operations)으로 나아가는 데 있다[6)]고 설명한 것을 통하여도 알 수 있다.

---

5) Aaron R. Cooper, Philip Chertoff and Shoba Pilay, "Trump Admin Cyber Strategy Centers Private Sector in Offensive Cyber Operation", LAWFARE(March 9, 2026), https://www.lawfaremedia.org/article/trump-admin-cyber-strategy-centers-private-sector-in-offensive-cyber-operations(Accssed: March 25, 2026).

6) https://cyberscoop.com/trump-national-cybersecurity-strategy-2025-release/(Accssed: March 23, 2026).

시사점

안보비용의 동맹 전가가 트럼프 2기 〈국가안보전략〉의 특징 가운데 하나였다면 〈트럼프 대통령의 사이버 전략〉은 공세적 사이버 작전의 강화를 위하여 필요한 비용을 동맹과 민간에게 전가하는 것을 핵심으로 제시하고 있다. 미국의 사이버공간 안전성 보장을 위해 동맹과 민간 기업에 대하여, 미 정부가 수행하여야 할 역할의 일부를 수행토록 하거나, 관련 비용과 책임을 공정하게 분담하라고 압박하고 있는 것이다. 이는 데이터 센터를 구축함에 있어 필요한 전력 인프라를 해당 데이터 센터 구축 기업으로 하여금 건설하도록 하는 트럼프의 정책과도 그 방향을 같이하는 것이다. 사이버안보 비용의 민간 전가는 안보라는 공공재 창출에 대한 국가의 역할을 축소하는 것이라고 할 수 있다. 특히 사이버 안보 분야는 시장실패에 있으므로 민간의 자발적 안보 활동을 기대하는 데에는 한계가 있다.

따라서 트럼프 정부는 비록 패권의 수축이 진행되더라도 사이버 공간의 안전성 확보를 위해 미 정부의 역량과 재원을 보다 확대하여야 한다. 이를 통해, 국내적으로는 자국의 인프라 보호를 강화하고 대외적으로는 사이버공간에서의 항행의 자유에 대한 신뢰를 회복할 수 있을 것이다. 이러한 조치에 따른 비용은 디지털 경제의 활력을 통해 미국의 경제적 번영을 지속시키고, 미국의 이익 증대로 환원될 것이기 때문이다.

〈트럼프 대통령의 사이버 전략〉으로 사이버안보 비용에 대한 민간 전가가 확대될 것으로 전망되므로, 미국 증시에 상장된 우리 기업들은 이에 대비할 필요가 있다. 특히 미국 정부가 추진하는 공세적 사이버 작전에 참여하도록 요청받는 상황에 대비할 필요가 있다. 공세적 사이버 작전의 모호한 개념과 성격은 물론

해당 작전에 대한 참여가 승인되는 경우라 하더라도 예측 불가능한 상황으로 인하여 책임을 부담할 가능성이 크기 때문이다. 공세적 사이버 작전을 수행하면서 그 대상인 사이버 위협 행위자나 그가 사용하는 장비와 인프라를 잘못 식별하여 해당 작전을 수행함으로써 무고한 사람이나 기업에 대해 심각한 피해를 야기할 수 있다. 이러한 피해를 야기하는 경우 미국 법원에 불법행위로 인한 손해배상 소송을 당하거나 징벌적 손해배상 책임을 부담하거나 혹은 형사 기소까지 당할 수 있기 때문이다. 나아가, 미국 이외의 국가에 대한 피해를 야기하는 경우 외교적 문제로 비화됨은 물론 해당국으로부터 민사 소송 및 기소 위험에 노출될 수 있다.

한편 우리 정부는 사이버안보 비용의 동맹 전가 상황에도 대비하여야 한다. 우리 정부는 이미 미국으로부터 한미 방위비 분담의 증액을 요구받고 있으며. 호르무즈 해협 봉쇄 해제를 위한 군사적 조치 또한 요구받고 있다. 이러한 상황 하에서 미국은 공세적 사이버 작전에 대한 참여와 비용 분담 강화를 요구할 수 있다. 이러한 요구가 있는 경우, 우리는 사이버공간에서의 방어적 작전에 대한 지원을 강화하여야 할 것이다. 즉, 사이버공간의 취약성 관련 정보를 공유하고, 발생한 침해사고에 대해 공동으로 조사하며, 핵심 인프라에 대한 방어적 훈련에 보다 집중하여야 할 것이다. 또한 사이버안보 관련 기술 개발과 인력양성 및 민간 생태계 지원을 더욱 강화하여야 할 것이다.

//끝//