국가전략연구위원회 이슈브리핑 38호 (발간일: 2025. 8. 29.)

트럼프 행정부 하 국방정책 변동과 사이버 안보 정책 변화

박동휘 (육군3사관학교)

1. 서론

2025년 1월 20일 도널드 트럼프 대통령은 대통령 행정명령-14148『Initial Rescissions of Harmful Executive Orders and Actions』에 서명함으로써 미국의 제47대 대통령이자 자신의 제2기 행정부의 시작을 알렸다. 본 행정명령의 핵심은 전임 대통령인 조 바이든의 행정명령 다수의 철회였다. 이는 1기 트럼프 행정부였던 제45대 대통령 취임 후 버락 오바마 행정부의 정책 철회를 넘어서는 조치였다. 이는 미국 우선주의의 재강조를 넘어 트럼프 1기 행정부의 정책 복원, 그리고 그 이상을 위한 신호탄이었다.

트럼프 2기 행정부는 국방정책에도 큰 변화를 시도하고 있으며, 이러한 변화는 사이버 안보 정책에서도 나타나고 있다. 트럼프 2기 국방부의 사이버 안보 정책의 기조는 2025년 3월 캐서린 서튼(Katherine E. Sutton)의 사이버 정책 국방부 차관보(assistant secretary of defense for cyber policy) 지명을 통해서 엿볼 수 있다.[1] 미국 사이버 사령부에서 사령관 겸 국방부 작전 책임자의 최고 기술 고문을 맡은 서튼은 지명 이후 같은 해 5월 출석한 상원 군사위원회에서 트럼프 1기 때 발표된 '국가안보대통령각서 13호(National Security Presidential Memorandum 13)'를 구체적으로 언급했다.[2] 이 각서는 사이버 무기 사용에 대

1) https://www.congress.gov/nomination/119th-congress/55/41?s=1&r=10
2) Mark Pomerleau, Trump nominates former congressional staffer for top Pentagon, DefenseScoop, Mar. 25, 2025. https://defensescoop.com/2025/03/25/katie-sutton-assistant-secretary-defense-cyber-policy-trump-nominee/ (Accessed on May 3, 2025)

한 규정의 완화와 당시 디지털 작전을 "전통적인 군사 활동"으로 규정한 국방 정책 법률의 완화를 지시한 것이다. 또한, 서튼은 중국 등 국외 적대 세력의 빠른 사이버 역량 강화 속도가 주된 위협임을 강조했다. 즉, 서튼이 상원 군사위원회에서 한 발언은 트럼프 2기 국방부가 중국 등의 적대세력의 사이버 위협에 대응하기 위해 이전보다 더 공격적인 사이버 전략을 추구할 것을 암시하는 것이었다.

본 연구는 이러한 트럼프 2기 행정부의 국방 사이버 안보 정책을 분석할 것이다. 트럼프 2기 행정부의 정책은 1기 때의 정책으로 회기 또는 그 이상을 의미하는 것으로 예측되고 있다. 따라서, 분석의 시기는 트럼프 1기 행정부와 조 바이든 행정부, 그리고 트럼프 2기 행정부이다. 분석 대상은 『국가안보전략서(NSS, National Security Strategy)』, 『국방전략서(National Defense Strategy)』, 『국가사이버전략(National Cyber Strategy)』, 그리고 『국방 사이버 전략(DoD Cyber Strategy)』, 또는 이에 준하는 전략서이다. 국방 사이버 안보 정책은 통상적으로 앞서 언급된 전략서 등에 기초하기 때문이다.

2. 트럼프 1기의 국방 사이버 안보 정책

미 국방부는 새로운 대통령 취임 후 발간되는 『국가안보전략서』를 기반으로 『국방전략서』를 작성한다. 『국방전략서』는 『국가안보전략서』의 내용을 국방 차원에서 구체화하여 국방전략과 목표, 전쟁수행 개념, 전력구조, 예산계획 등을 담고 있다. 부시 행정부는 2008년 『국방전략서』를 한 차례 발간한 바 있으며, 오바마 행정부에서는 2014년 이와 유사한 기능을 담당하는 『4년 주기 국방검토보고서(QDR, Quadrennial Defense Review)』와 2016년 『국방태세검토서(Defense Posture Review)』를 발간했다. 바이든 행정부의 경우 2022년 『국가안보전략서』를 발간했다.

트럼프 1기 국방부 장관인 짐 매티스가 2018년 1월 직접 발표한 『국방전략서 요약본』은 '미국 우선주의'를 반영하고 있다. 2018 『국방전략서 요약본』은 "경쟁하고 억제하며 승리"하려는 것을 핵심으로 삼고 있다. 이러한 전략수립은 미국이 전략적 위축의 시기 속에서 그들의 군사적 우위와 경쟁력이 쇠퇴하고 있는 심각한 상황을 반영하고 있다. 따라서, 미국은 군사력의 경쟁력 우위 복원과 '강한 미군의 재건'을 통하여 '힘을 통한 평화'를 적극적으로 구현할 것을 본 전략서를 통해 밝힌 것이다.[3)]

미 국방부는 강대국 간 전략적 경쟁을 국가안보의 최우선적 중점 사안으로 설정하고 중국 및 러시아와의 장기적 전략적 경쟁에 적극적으로 대응하겠다는 의지를 표명했다. 미국 우선주의답게 "적 공격으로부터의 본토 방어"를 포함한 11대 국방전략목표를 설정했다. 국방전략목표 달성을 위한 세부 추진전략으로 "보다 치명적인 합동군의 건설, 동맹 강화 및 파트너십 확대, 성과 및 재정 능력 향상을 위한 국방부 개혁" 등이 제시되었다. 더욱이, 미 국방부는 인도-태평양 지역을 지리 및 전략적 중심으로 설정했고, 전쟁수행 전략을 강대국과의 전쟁으로 전환했다.[4)]

3) U.S. DoD, Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, January 2018.

2018『국방전략서 요약본』은 '우주와 사이버공간은 전투 영역(Space and cyberspace as warfighting domains)'이며, "우리는 사이버 방어, 복원력, 그리고 모든 군사 작전에 사이버 역량을 지속적으로 통합하는 데에도 투자할 것(We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations)"이라고 사이버 안보의 중요성도 언급했다.[5)]

트럼프 1기 국방부의 사이버 안보 정책의 근간은 2018년 9월 발간된『국방 사이버 전략, DoD Cyber Strategy』이다. 이는 앞서 설명한『국가안보전략서』를 근간으로 한『국방전략서』와 같은 달에 발간된 트럼프 행정부의『국가사이버전략(National Cyber Strategy)』에 기초하여 작성되었다.

2018년 9월 발표된 트럼프 행정부의『국가사이버전략』은 부시 행정부 시절인 2003년 이후 15년 만에 나온 미국의 포괄적인 사이버 안보 전략이다. 본 전략서의 핵심은 사이버공간에서 미국의 확고한 리더십 확보이고, '힘을 통한 평화'라는 기조를 사이버공간에 적용하려는 것이었다. 미국은 자국민, 본토, 그리고 자신의 생활 방식을 보호하며, 사이버공간에서 자국의 이익을 확보하고 증진하는 것을 최우선 과제로 설정했다. 이는 점증하는 사이버 위협에 대해 보다 '공세적'이고 주도적인 대응 태세를 갖추겠다는 의지의 반영이었다.

구체적인 미국의 4가지 사이버 전략은 다음과 같았다. 첫 번째 핵심 전략 축은 '미국인, 국토, 그리고 미국의 생활 방식 보호(Protect the American People, the Homeland, and the American Way of Life)'였다. 이를 실현하기 위해 연방 정부의 네트워크 및 시스템의 보안을 강화하고, 에너지, 금융, 통신 등 국가 핵심 기반시설의 사이버 복원력을 높이는 데 중점을 두었다. 또한, 사이버 범죄 퇴치, 사이버 공격 발생 시 신속한 대응 및 피해 복구 능력 향상, 그리고 국민의 사이버 보안 인식 제고를 위한 노력도 강조되었다.

두 번째 핵심 전략 축은 '미국의 번영 증진(Promote American Prosperity)'으로, 안전하고 활기찬 디지털 경제 환경의 조성이었다. 특히 그들은 국가적인 경쟁력의 핵심인 미국의 지식재산권과 기업의 혁신 기술을 국가 차원의 해킹으로부터 보호하고자 했다. 더불어, 전 세계적으로 안전하고 신뢰할 수 있는 인터넷 인프라를 촉진하고, 신기술의 안전한 개발과 활용을 지원하는 방안도 강조했다.

세 번째 핵심 전략 축인 '힘을 통한 평화 보전(Preserve Peace through Strength)'은 가장 적극적이고 '공세적'인 측면을 강조했다. 이 전략은 미국과 동맹국에 해를 끼치는 악의적인 사이버 활동을 식별, 교란, 약화시키고 궁극적으로 억제하는 것을 목표로 했다. 이를 위해 사이버 공격의 배후를 명확히 규명하고, 사이버공간에서 미국의 적대 세력에게 비용을 부과하며, 필요시 미국의 사이버 역량을 활용해 대응하는 등 적극적인 조치를 취할 것임을 명시했다. 이는 트럼프 행정부의 가장 핵심적인 공세적 사이버 전략인 소위 '지속적 관여(persistent engagement)' 및 '전방 방어(defend forward)' 개념과 연결되었다.

마지막 네 번째 핵심 전략 축은 '미국의 영향력 증진(Advance American Influence)'으로, 개방적이고 상호운용 가능하며 신뢰할 수 있고 안전한 인터넷 환경을 전 세계적으로 확

4) *Ibid.*
5) *Ibid.*

산시키는 데 기여하는 것이다. 이를 위해 미국은 국제 파트너십과 동맹을 강화하여 사이버 안보 역량을 함께 구축하고, 책임 있는 국가 행동 규범을 정립하는 데 주력하고자 했다. 이 전략은 범정부 차원의 협력, 민관 파트너십 강화, 사이버 보안 인력 양성 등 다각적인 접근을 통해 사이버공간에서 미국의 지속적인 우위를 확보하고 미래의 도전에 효과적으로 대응하는 것이었다.

2018년 9월 미 국방부가 발표한 『국방사이버전략』은 『국가사이버전략』과 연계하여 같은 해 초에 나온 『국방전략서』의 기조를 사이버공간에 적용한 군사 중심의 핵심 문서였다. 중국과 러시아를 장기적인 전략적 경쟁자로 규정한 2018 『국방 사이버 전략』은 앞선 두 국가로부터 발생하는 사이버 위협에 대응하여 미국의 핵심 이익을 수호하는 것을 최우선 목표로 삼았다. 본 전략은 과거의 방어적, 수동적 대응 전략을 벗어나, 위협의 근원에서부터 적극적으로 대처하는 '사전 방어(proactive defense)' 기조로의 전환을 명확히 밝혔다. 이는 사이버공간을 단순한 지원 영역이 아닌 독자적인 작전 영역으로 인식하고, 이곳에서의 경쟁우위를 확보하겠다는 국방부의 의지를 확고하게 반영했다.

이 전략의 가장 중요한 개념은 '전방 방어'와 '지속적 관여'였다. 국방부 문서는 '전방 방어'를 통해 미국의 네트워크 내부가 아닌 위협이 발생하는 외부의 지점에 더 가까운 곳에서 작전을 수행하여 위협이 미국 본토에 도달하기 전에 이를 무력화하거나 교란하겠다는 의지를 밝혔다. 이를 위해 미 국방부는 '지속적 관여'를 통해 적의 활동을 지속적으로 관찰하고, 그들의 의도를 사전에 파악하며, 필요시 비용을 부과함으로써 사이버공간에서의 우위를 확보하고자 한 것이다.

국방부의 사이버 전략은 다음과 같은 핵심 목표를 제시했다. 첫째는 사이버공간에서의 군사력 우위를 확보하고 '치명성(lethality)'을 강화하여 적을 압도하는 것이었다. 둘째는 전략적 경쟁자들과의 장기적인 경쟁에서 승리하고, 그들의 악의적인 사이버 활동을 억제하는 것이었다. 셋째는 동맹국 및 파트너 국가와의 협력을 강화하여 공동으로 사이버 위협에 대응하는 체계를 구축하는 것이었다.

본 전략은 사이버 작전을 육상, 해상, 공중, 우주 등 다른 작전 영역과 통합하여 시너지를 창출하는 '다영역 작전(Multi-Domain Operations)' 개념을 강조했습니다. 이를 위해 국방부는 우수한 사이버 인재를 확보하고 양성하며, 민간 부문과의 기술 협력을 강화하고, 필요한 예산과 자원을 확보하는 것의 중요성 강조했다.

2018년 발간된 트럼프 행정부의 『국방사이버전략』은 미국의 사이버 안보 정책에 있어 중요한 전환점이었다. 미 국방부가 이전의 소극적 방어에서 벗어나 적극적이고 공세적인 자세를 취함으로써 사이버공간에서의 주도권을 확보하겠다는 의지를 분명히 했기 때문이었다. 다만, 많은 전문가는 본 전략서의 핵심 개념인 '전방 방어'와 '지속적 관여'가 국제법 및 규범과 충돌하거나, 사이버 공격의 오판 및 확전 위험을 높일 수 있다는 비판적 시각을 제시했다. 그런데도, 이 전략은 이후 미군의 사이버 작전 개념과 능력 발전에 지속적인 영향을 미치며, 특히 후술할 트럼프 행정부 2기의 국방 사이버 안보 정책의 핵심과도 연결되고 있다.

3. 바이든 행정부의 국방 사이버 안보 정책

조 바이든 행정부의 국방부 장관인 로이드 오스틴 역시 2022년 10월 12월 발표된『국가안보전략서』의 기조에 따라, 같은 해 10월 27일 2022『국방전략서』를 발표했다. 주목할 점은『미사일 방어 검토보고서(Missile Defense Review)』와『핵태세 검토보고서(Nuclear Posture Review)』를『국방전략서』에 포함해 함께 발표한 것이다.

2022『국방전략서』는 점점 더 복잡해지는 도전적인 글로벌 안보환경을 극복하기 위한 미 국방부의 로드맵을 제시했다. 미 국방부는 중국을 국가안보의 가장 포괄적이며 심각한 장기적 위협으로 보고 있으며, 러시아 역시 심각한 위협으로 규정하고 있다. 또한, 본 전략서는 북한, 이란, 극단주의 단체로부터의 위협에 대하여 미국의 억지력 유지, 그리고 기후변화와 팬데믹 등의 초국가적 위협에 대한 대처 역시도 포함하고 있다.

구체적으로 2022『국방전략서』는 급변하는 국제 안보 환경 속에서 미국의 국방 목표와 우선순위를 제시하고 있다. 이 전략서는 중국을 미국의 가장 중대한 '추격하는 도전(pacing challenge)'으로 명확히 규정하며, 국제 질서를 자국에 유리하게 재편하려는 중국의 의도와 그들의 군사력 현대화에 대하여 심각한 우려를 표명했다. 동시에, 바이든 행정부는 우크라이나 침공 등으로 국제 규범을 명백히 위반한 러시아를 '현존 위협(acute threat)'으로 지정했다. 즉, 미 국방부는 두 국가가 제기하는 다층적인 안보 도전에 대응하는 것을 국방전략의 최우선 과제로 삼았다.

이러한 도전을 극복하기 위해 2022『국방전략서』는 '통합 억제(integrated deterrence)'라는 핵심 개념을 전면에 내세웠다. 이는 전통적인 군사력뿐만 아니라 외교, 정보, 경제, 기술 등 국가 권력의 모든 요소를 동원하고, 동맹국 및 파트너 국가들과 긴밀히 협력하여 시너지를 극대화하는 포괄적인 억제 전략을 의미했다. 통합 억제는 잠재적 적국이 어떠한 형태의 침략이나 강압 행위도 성공할 수 없으며, 그 대가가 감당할 수 없을 만큼 클 것이라는 인식을 심어줌으로써 분쟁을 사전에 방지하는 것을 목표로 했던 것이다. 이는 또한 핵 억제력의 현대화와 함께 재래식 전력, 사이버 및 우주 능력 등 모든 영역에서의 억제력 강화를 포함했다.

2022『국방전략서』는 통합 억제를 구체적으로 실행하기 위한 두 가지 주요 축으로 '캠페이닝(campaigning)'과 '지속적인 우위 구축(building enduring advantages)'을 제시했다. '캠페이닝'은 평시에도 경쟁국들의 악의적인 활동과 회색지대 전략에 적극적으로 대응하고, 미국의 군사적 준비태세를 강화하며, 동맹 및 파트너 국가들과의 연합 작전 능력을 향상시키는 일련의 군사 활동을 의미했다. 이는 경쟁 환경을 미국에 유리하게 조성하고, 위기 발생 시 신속하고 효과적으로 대응할 수 있는 능력을 유지하기 위한 지속적인 노력이었다.

'지속적인 우위 구축'은 장기적인 관점에서 미국의 국방력을 강화하기 위한 노력을 포괄했다. 여기에는 국방 인력에 대한 투자, 첨단 기술 연구개발 및 도입을 통한 군사력 현대화, 국방 산업 기반 강화, 그리고 공급망의 회복력 증대 등이 포함되었다. 또한, 기후 변화와 같은 안보 환경 변화 요인에 대한 적응력 강화와 함께, 국방부의 혁신을 가속화하여 미래의 위협에 선제적으로 대비할 수 있는 역량을 키우는 것을 목표로 했다. 이는 단순히 현재의

위협에 대응하는 것을 넘어 미래의 경쟁에서도 우위를 확보하기 위한 근본적인 체질 개선 노력이었다.

마지막으로, 2022『국방전략서』는 동맹국 및 파트너 국가들과의 협력을 미국의 가장 큰 비대칭적 우위로 강조하며, 이들과의 관계를 더욱 강화하고 확대해 나갈 것을 분명히 했다. 이러한 협력은 공동의 안보 위협에 대한 부담을 분담하고, 집단적 억제력을 강화하며, 자유롭고 개방된 국제 질서를 수호하는 데 핵심적인 역할을 하는 것이었다. 이 부분은 이전의 트럼프 1기 행정부와 다른 점이기도 했다. 또한, 2022『국방전략서』는 처음으로『핵태세 검토보고서』및『미사일 방어 검토보고서』와 통합되어 발표됨으로써, 미국의 국방전략과 핵 및 미사일 방어 정책 간의 일관성과 시너지를 높이려는 의도를 보여주었다.

2023년 3월 2일 바이든 행정부는『국가사이버안보전략(National Cybersecurity Strategy)』을 발표했다. 이 전략의 핵심 목표는 미국의 디지털 생태계를 안전하고 회복력 있게 만들고, 모든 미국인이 디지털 환경의 혜택을 안전하게 누릴 수 있도록 하는 것이었다. 이를 위해 미 정부와 민간 부문 간의 긴밀한 협력, 그리고 사이버공간에서의 역할과 책임, 자원의 재배분이 강조되었다.[6)]

바이든 행정부의『국가사이버안보전략』은 두 가지 근본적인 패러다임 전환을 제시했다. 첫 번째는 사이버 안보 책임의 중심을 개인, 소규모 기업, 지방정부, 인프라 운영자에서 대규모 인프라 소유주, 소프트웨어 공급업체 등 더 큰 역량과 자원을 가진 조직으로 옮기는 것이었다. 둘째는 단기적 위협 대응과 동시에 장기적 회복력 확보를 위한 투자를 유도하는 인센티브 구조의 재설정이었다.[7)]

이는 다음과 같은 5개의 구체적 전략으로 세분되었다. (1) 중요한 인프라 방어, (2) 위협 행위자 교란 및 해체, (3) 시장 메커니즘을 통한 보안 및 회복력 강화, (4) 회복력 있는 미래를 위한 투자, 그리고 (5) 국제 파트너십 구축이 그것이었다. 그리고 각각은 IoT 보안 강화, 양자 내성 시스템 투자, 사이버 인력 양성, NIST 프레임워크를 기반으로 하는 보안 관행 도입 등과 같은 세부 실행과제를 포함했다.

조 바이든 행정부의 국방부는 앞서 설명한 2022『국방전략서』와『국가사이버안보전략』을 기반으로 2023년 9월 12일『국방사이버전략 요약본』을 발표했다. 이는 2018년 트럼프 1기 국방부의 전략을 기반으로 하되, 러시아-우크라이나 전쟁에서 관찰된 사이버 작전의 실전 경험을 반영했다. 본 전략은 2022년『국가안보전략』과『국방전략서』, 2023년『국가사이버안보전략』의 우선순위를 구체화하며, '전진 방어' 개념을 통해 적의 악성 행위를 사전 차단하는 적극적 방어를 강조했다. 특히, 조 바이든의 국방부는 중국과 러시아의 사이버 위협을 핵심적인 도전요인으로 규정하는 동시에, 전통적 군사력의 균형을 무력화하려는 그들의 시도를 저지하는 데 초점을 맞췄다.

이를 달성하기 위해 제시된 핵심 전략은 (1) 중요 인프라 보호 및 사이버 공격 사전 차단을 목표로 하는 '국가 방어', (2) 전투 영역에서의 사이버 작전 통합 및 사이버 회복력 강화를 의미하는 '전쟁 수행 준비'; (3) 헌트 포워드(Hunt Forward) 작전 확대를 통한 기술

6) https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/
7) *Ibid.*

협력 및 국제 규범 준수 촉진하기 위한 '동맹국·파트너와의 협력', 그리고 (4) 제로 트러스트 아키텍처 도입, 암호화 기술 현대화, 사이버 인력 양성을 추구하는 '지속적 경쟁우위 확보'였다. 지속적 경쟁우위 확보는 기존의 억제(deterrence) 중심 접근에서 '지속적 관여'로의 패러다임 전환을 반영하며, 위협의 사전 차단을 통한 전략적 주도권을 확보하려는 것이었다.

2023년 미 국방부의 『국방사이버전략 요약본』은 러시아-우크라이나 전쟁에서의 사이버전 요소가 반영되었다. 전쟁에서의 사이버전은 국가 차원의 사이버 공격과 비국가적 해커 집단의 활동이 병행되며, 민간 인프라가 군사적 표적으로 활용되는 양상을 보였다. 그에 따라 도출된 대응방안은 민간-군사 협력 체계 강화, 실시간 위협 인텔리전스 공유, 동맹국과의 연합 사이버 훈련 확대 등이었다. 군사전략적 관점의 핵심은 적의 사이버 능력을 지속적으로 약화시키는 '캠페이닝(campaigning)' 개념의 적용이며, 이는 단일 공격이 아닌 지속적 압박을 통한 적의 전략적 의지 약화에 주안을 두는 것이었다.

본 전략서 요약본은 국방 사이버 안보 분야에서의 기술적 혁신과 제도개선 방향도 제시했다. 전략서는 양자 내성 암호화(PQC) 기술 개발, 인공지능(AI) 기반 위협 탐지 시스템 구축, 클라우드 보안 아키텍처 표준화 등을 핵심 투자 분야로 지정했다. 특히, 제로 트러스트 원칙을 DODIN(국방부 정보네트워크) 전반에 적용해 내부 위협을 최소화하고, 무기체계의 사이버 취약점을 주기적으로 진단하는 프로세스를 강화하고자 했다.

바이든의 국방 사이버 안보 정책은 사이버 안보 위협의 중요성 인식하에 동맹과 함께 연대하여 국가 사이버 방위 목표 달성 및 지속적인 미국의 이익 구축이었다. 특히, 당시의 전략은 '사이버공간에서의 권력 투영' 개념을 군사학적으로 확장시켰다는 점에서 의미가 있다. 하지만, 동맹국 간 기술 표준 불일치, 사이버 작전의 법적·윤리적 경계의 모호성, 그리고 민간 기업의 보안 투자 유인 부족 등이 국방부 전략을 구현하는데 잠재적 장애 요인으로 평가되었다.

4. 트럼프 2기 행정부 하 국방정책 변동과 사이버 안보 정책 변화

트럼프의 재집권은 트럼프 1기 행정부의 국방정책과 사이버 안보 정책으로의 변화를 의미하는 것으로 평가되고 있다. 이를 이해하기 위해서는 앞서 나열한 트럼프 1기 행정부와 바이든 행정부의 국방정책 변화 속에서 사이버 정책의 핵심 내용을 비교할 필요가 있다.

첫 번째는 상황의 인식이다. 2018년 『국방사이버전략』은 강대국 간 경쟁의 귀환을 강조했다. 미국은 중국과 러시아를 자국의 안정과 번영을 약화시키려는 지속적이고 진화하는 사이버 위협으로 인식했다. 따라서, 트럼프 1기 국방부는 미국의 군사적 우위와 중요 기반시설을 목표로 하는 점점 더 복잡하고 정교해지는 사이버 공격에 대처하는 것을 목표로 했다.

바이든의 2023년 『국방사이버전략 요약본』은 트럼프 1기의 국방 사이버 전략을 대체하는 것이었다. 주목할 점은 미 국방부가 수년간의 사이버 작전 수행을 통해 쌓은 경험과 러시아-우크라이나 전쟁과 같은 분쟁에서의 사이버 활동을 관찰해서 얻은 교훈을 통합적으로 반영했다. 중국과 러시아는 여전히 미 국방부의 주요 사이버 위협이었다. 다만, 2023년 『국방사이버전략』은 중국과 러시아의 위협 차이를 구체화하여 명시했다는 점이다. 또한, 이

는 러시아-우크라이나 전쟁 경험에서 얻은 회복력, 동맹 협력, 그리고 예방의 중요성과 같은 교훈을 포함한 것이다.

두 번째 비교는 주요 전략적 개념 및 접근 방식의 차이다. 2018『국방사이버전략』의 핵심 개념은 '전방 방어'였다. 이는 악의적인 활동이 미국 네트워크에 도달하기 전에 이를 방해하거나 중단시키기 위하여 사이버 위협의 근원지에서 적극적으로 대응하는 전략개념이다. 이를 위해 미국의 군사적 우위를 위협하는 사이버 공격에 대응하기 위해 일상적인 경쟁에서 '지속적인 관여'가 강조되었던 것이다.

2023『국방사이버전략』은 '전방 방어'를 핵심 원칙으로 남겨 두었지만, '통합 억제(Integrated Deterrence)' 전략을 더 강조했다. 이는 갈등을 억제하기 위해 다른 국가와 함께 사이버 작전을 하는 것을 강조한 것이다. 동맹국 및 파트너의 사이버 역량에 상당한 투자를 통해 '집단적 사이버 회복력(Collective Cyber Resilience)' 구축에 대한 약속 역시도 이러한 맥락 선상에 있었다.

세 번째인 동맹국 및 파트너에 대한 인식 차이는 앞선 내용의 연장선이다. 2018년 미 국방부 사이버 전략은 동맹국, 산업계 및 정부 기관 간 파트너와의 파트너십의 중요성을 인식하고 협력 및 정보 공유 확대를 강조했습니다. 2023『국방사이버전략』은 2018년보다 한 발 더 나아갔다. 새로운 전략서에서 동맹국 및 파트너의 역할은 더 격상되었다. 미 국방부는 전방 방어, 기술 협력 및 사이버 보안 인프라에 대한 접근 확대 등 다양한 수단을 통해 이들의 사이버 역량과 능력을 구축시키고자 했다. 이는 사이버공간의 상호 연결된 특성과 집단 방어의 필요성에 대한 더 깊은 이해를 반영했던 것으로 볼 수 있다.

요약해보면, 이전의 두 국방 사이버 전략서는 사이버공간에서 미국의 이익을 보호한다는 근본적인 목표는 유지했지만, 2018년 전략서의 경우 공세적인 대응에 큰 방점을 두었고, 2023년 전략서의 경우 진화하는 위협 환경, 집단적 사이버 회복력 달성에 있어 동맹국 및 파트너의 중요한 역할, 그리고 악의적인 사이버 활동을 억제하고 대응하기 위한 예방적이고 통합적인 접근 방식의 필요성을 강조했던 것이다.

한편, 2025년 1월 20일 도널드 트럼프 대통령은 대통령 행정명령-14148『Initial Rescissions of Harmful Executive Orders and Actions』에 서명함으로써 미국의 제47대 대통령이자 자신의 제2기 행정부의 시작으로 알렸다. 본 행정명령의 핵심은 전임 대통령인 조 바이든의 행정명령 다수의 철회였다. 이는 1기 트럼프 행정부였던 제45대 대통령 취임 후 버락 오바마 행정부의 정책 철회를 넘어서는 조치였다. 이는 트럼프 대통령이 미국 우선주의의 재강조하는 동시에 트럼프 1기 행정부 당시의 정책 복원을 넘어 더 강화하기 위한 신호탄이었다.

트럼프 2기의 국방정책과 사이버 안보 정책 역시도 이러한 기조에 따라 변화할 것으로 예상되고 있다. 2025년 5월 1일 피트 헤그세스(Pete Hegseth) 국방부 장관은 엘브리지 콜비(Elbridge Colby) 정책 담당 차관에게 2025『국방전략서』2025년 8월 31일 이전까지 작성할 것을 주문했다. 미 국방부는 본 전략이 트럼프 대통령이 주창하는 '미국 우선주의'와 '힘에 의한 평화'를 실현할 구체적이고 분명한 방향성을 제공할 것이라고 밝혔다.[8)]

8) U.S. DoD, Statement on the Development of the 2025 National Defense Strategy, 2025.5.2.

헤그세스 국방부 장관은 새로운『국방전략서』작성을 지시하며, 2025년 3월 국방 내에 전파된 '임시 국가 방어 전략 지침'을 기반으로 할 것을 명시했다.[9] '임시 국가 방어 전략 지침'은 2025년 3월 29일 자 『워싱턴포스트』의 'Secret Pentagon memo on China, homeland has Heritage fingerprints'란 제목의 기사를 통해 처음 일반 대중에게 알려졌다.[10] 이는 기밀 정책 문서로,『국방전략서』가 확정될 때까지 미국 국방전략의 임시적 틀을 제공하는 역할을 담당한다. 알려진 바에 따르면, 이 지침은 트럼프 행정부 하에서 국방부의 우선순위에 중대한 변화를 예고하며, 미국 본토 방위와 중국, 특히 대만 및 인도-태평양 지역에서의 억지력을 미국 군사 전략의 최우선 과제로 명확히 제시했다.

이 지침에 따라, 국방부는 자원과 작전 계획을 중국의 침략, 특히 대만 침공 가능성 억지와 미 본토에 대한 미사일·드론 공격 등 다양한 위협에 대한 방어 강화에 집중할 것으로 예상된다. 이를 위해 미군은 중동과 유럽 등 다른 지역에서의 위험 감수를 전제로, 군사 자산을 재배치하고 해당 지역에서의 미국의 영향력이나 주둔 규모를 줄이더라도 동아시아 억지력을 유지하는 데 중점을 둘 것으로 보인다.

또한, 본 임시 지침은 트럼프 행정부의 '힘에 의한 평화' 철학을 반영하여, 군사력이 평화와 안보의 핵심 보장 수단임을 강조했다. 아울러 유럽과 아시아 동맹국들의 방위 분담 확대를 요구하며, 특히 한국과 일본 등은 북한과 중국의 위협에 대해 자국 방위에 더 큰 책임을 져야 한다는 입장을 분명하게 나타내고 있다. 이 문서는 또한 펜타닐 등 마약이 미-멕시코 국경을 통해 유입되는 문제와 같은 비전통적 안보 위협도 국가 안보의 범주에 포함시키며, 국방 정책의 범위를 기존 군사 위협을 넘어 확장시키고 있다. 헤그세스의 임시 지침은 중국과의 강대국 경쟁과 본토 안보를 중심으로 하는 보다 좁고 위험을 감수하는 미국 방위 전략의 방향성을 분명히 보여주고 있다.

트럼프 2기 국방부의 사이버 안보 정책의 기조는 2025년 3월 캐서린 서튼의 사이버 정책 국방부 차관보 지명을 통해서 엿볼 수 있다.[11] 본 직책은 미국 사회와 군대 내에서 사이버 위협이 심각해지자, 많은 의원이 국방부 내 차관보급에서 사이버 정책을 총괄해야 한다는 목소리가 높아져 만들어진 것이다. 사이버 정책 국방부 차관보는 백악관의 사이버 정책 및 지침을 바탕으로 국방부의 사이버공간 정책 및 전략을 수립하고 감독하는 역할을 한다. 구체적으로, 본 직책은 해외 사이버와 관련된 위협, 국제 협력, 해외 파트너 및 국제기구와의 협력을 책임질 뿐만 아니라 국방부의 사이버 역량, 인력, 활용과 관련된 모든 활동에 대한 지침과 감독을 제공할 의무를 지닌다.[12]

---

https://www.defense.gov/News/Releases/Release/Article/4172735/statement-on-the-development-of-the-2025-national-defense-strategy/

9) Secretary of Defense, Memorandum for All Department of Defense Personnel, Subject: National Defense Strategy, 2025.5.1. https://media.defense.gov/2025/May/02/2003703230/-1/-1/1/MEMORANDUM-DIRECTING-THE-DEVELOPMENT-OF-THE-2025-NATIONAL-DEFENSE-STRATEGY.PDF

10) Alex Horton and Hannah Natanson, Secret Pentagon memo on China, homeland has Heritage fingerprints, Washington Post, March 29, 2025. (Accessed on May 15, 2025) https://www.washingtonpost.com/national-security/2025/03/29/secret-pentagon-memo-hegseth-heritage-foundation-china/

11) https://www.congress.gov/nomination/119th-congress/55/41?s=1&r=10

12) https://policy.defense.gov/OUSDP-Offices/ASD-for-Cyber-Policy/

트럼프 2기에서 처음으로 사이버 정책 국방부 차관보에 지명된 서튼은 미국 사이버 사령부에서 사령관 겸 국방부 작전 책임자의 최고 기술 고문을 맡고 있다.[13] 그녀는 차관보 지명 후 2025년 5월 상원 군사위원회에 출석하여 "사이버 공격의 속도가 점점 빨라지는 데 대응할 수 있는 태세를 갖추고 AI의 영향에 대처할 수 있어야"한다고 했다.[14]

양당의 상원의원과 서튼 지명자 간의 질의응답은 트럼프 2기 국방부의 사이버 안보 정책 방향을 간접적으로 시사했다. 먼저, 의원들은 중국과 같은 국외 적대 세력의 디지털 공격 억제를 위한 미국의 대응이 충분한가에 대하여 질문했다. 서튼은 국외 빠르게 향상되고 있는 적대 세력의 사이버 능력에 의한 공격 가능성 증대에 대해 우려를 표했다. 더욱이 서튼은 트럼프 정부가 가장 큰 위협으로 보고 있는 중국을 중심으로 대답을 했다. 중국이 지원한다고 알려진 해커 그룹인 볼트 타이푼과 솔트 타이푼이 미국의 중요 인프라에 침투해 각각 최소 9개의 통신 회사 네트워크에 침투하여 미국의 안보를 심각하게 위협하고 있는 상황이기 때문이다. 그녀는 미국이 여전히 모든 면에서 선두를 달리고 최고인 인재를 보유하고 있으나, 중국의 엄청난 사이버 능력 향상과 공격적인 AI 기술 등의 도입을 지적했다.[15]

가장 주목할 점은 서튼이 '공세적 전략'을 강조한 것이다. 억제력과 관련하여 그녀는 "우리에게는 강력한 방어가 필요하지만, 방어만으로는 적을 막을 수 없을 것"이라 했다. 서튼은 만약 자신이 인준된다면, 미국이 증대하는 사이버 위협에 대응할 수 있는 필요한 옵션을 갖도록 '공격적 사이버 역량'을 강화하기 위해 노력할 것임을 밝혔다. 또한, 그녀는 다른 나라가 사이버 세계에서 미국에게 할 수 있는 모든 일을 미국도 그들에게 똑같이, 그리고 그보다 더 많이 할 수 있다는 사실을 세상에 알려주는 것이 필요함도 덧붙였다. 즉, 트럼프 2기 행정부가 국방부의 사이버 정책 국방부 차관보에 서튼을 지명한 것은 트럼프 1기 행정부의 국방 사이버 안보 정책으로의 회귀이자 더 강력한 공세적 전략 도입의 시사를 의미하는 것이다.[16]

그 외에도 서튼은 NSA 사이버 협력 센터(NSA Cyber Collaboration Center) 설립과 같은 노력을 언급하며, 사이버 안보를 위하여 민간 산업계와의 정보 공유 노력을 언급하기도 했다. 그럼에도 그녀는 방어의 방식 문화 자체의 변화를 같이 언급하며, 협력적 방어에 있어서도 공격적인 전략의 필요성을 내비쳤다. 한편, 서튼은 미 국방부가 오랫동안 사이버 인력의 모집과 유지에 어려움을 겪고 있음을 언급했다. 트럼프 2기 행정부의 국방부가 단순한 금전적 인센티브를 넘어 자긍심을 향상시키는 방안 또한 강구하여 우수 사이버 인력을 유지하려는 방안을 내놓으려 하고 있다. 트럼프 2기 국방부가 공세적 사이버 전략을 유지할 수 있는 적절한 인력을 수급하고 유지할 수 있을지 지켜볼 필요가 있다.

---

13) Mark Pomerleau, Trump nominates former congressional staffer for top Pentagon, DefenseScoop, Mar. 25, 2025. https://defensescoop.com/2025/03/25/katie-sutton-assistant-secretary-defense-cyber-policy-trump-nominee/ (Accessed on May 3, 2025)
14) https://therecord.media/dod-cyber-policy-nominee-offensive-cyber-operations
15) https://www.armed-services.senate.gov/hearings/to-consider-the-nominations-of-mr-anthony-j-tata-to-be-under-secretary-of-defense-for-personnel-and-readiness-and-ms-katherine-e-sutton-to-be-assistant-secretary-of-defense-for-cyber-policy
16) *Ibid.*

5. 결론

트럼프 2기 행정부 집권 초기라 아직 『국가안보전략서』, 『국방전략서』, 『사이버안보전략서』, 『국방사이버전략서』 등이 발간되지는 않았다. 그럼에도 헤그세스의 '임시 국가 방어 전략 지침'의 주요 내용, 그리고 캐서린 서튼의 국방부 사이버 정책 차관보 지명과 상원 군사위원회에서 한 발언 등은 국방 사이버 안보 정책이 트럼프 1기 때로 돌아갈 것으로 예상된다.

트럼프 2기 국방부는 조 바이든의 국방부 기조였던 동맹국과의 연대를 강조하던 국방 및 사이버안보전략보다는 공격적인 전략을 선택할 것으로 보인다. 특히, 트럼프 2기 국방부는 지역적으로 인도-태평양에 중점을 두고, 중국과 같은 적대 세력에 의한 사이버공간에서의 위협에 대하여 사전 대응 차원의 공세적인 전략을 취해 갈 것이다.

한편, 사이버 안보의 중요성에 대한 계속적인 강조에도 불구하고, 트럼프 2기 국방부의 국방 및 사이버 안보 정책의 변화는 동맹과의 연대를 일부 약화시킬 가능성이 크다. 또한, 정책의 일관성이 훼손되는 문제로 인해, 동맹국들이 사이버 안보 전략에 있어 큰 혼란을 겪을 것으로 예상이 된다.

미 국방정책과 사이버 안보 전략의 변화는 대한민국 국방에 큰 도전적 요인이다. 대한민국은 한미동맹 강화 지속 노력과 함께 다자외교를 통하여 도전과 기회 마련해야 한다. 또한, 약화된 협력 속에서도 대한민국은 자주적 국방 역량 확대, 독자적인 전·평시 사이버 안보 전략과 회복력 구축을 해야 한다. 예측이 어려운 미 국방부의 국방정책과 사이버 안보 전략변화 속에서 대한민국은 어떻게 새로운 국방 사이버 안보 전략을 수립할 것인지 심도 있는 논의를 계속 이어가야 할 것이다.