Jeju Peace Institute 제주평화연구원

JPI PeaceNet

트럼프 2기 미국의 사이버 안보 전략: '사이버 복합 넥서스'의 시각

김 상 배

서울대학교 정치외교학부 교수

[기획자 註] 제4차 산업혁명(4th Industrial Revolution)은 정치·경제·사회 등 모든 분야에 정보통신 기술(ICT)이 융합될 것으로 전망되고 있다. 이에 따라, 세계 각국은 사이버 공간(cyber space) 및 빅데이터를 적대적인 국가 혹은 세력으로부터 보호하기 위해 정책적·기술적 노력을 경쟁적으로 강화하고 있다. 이러한 흐름 속에서, 본고는 트럼프 2기 행정부 출범 이후 미국의 사이버 안보 전략을 분석 및 전망해보고 이에 따른 변화를 살펴보고자 한다 [기획: 강영훈 원장(yhkang@jpi.or.kr)].

* 이 글에 포함된 의견은 저자 개인의 견해로 제주평화연구원의 공식입장과는 무관합니다.

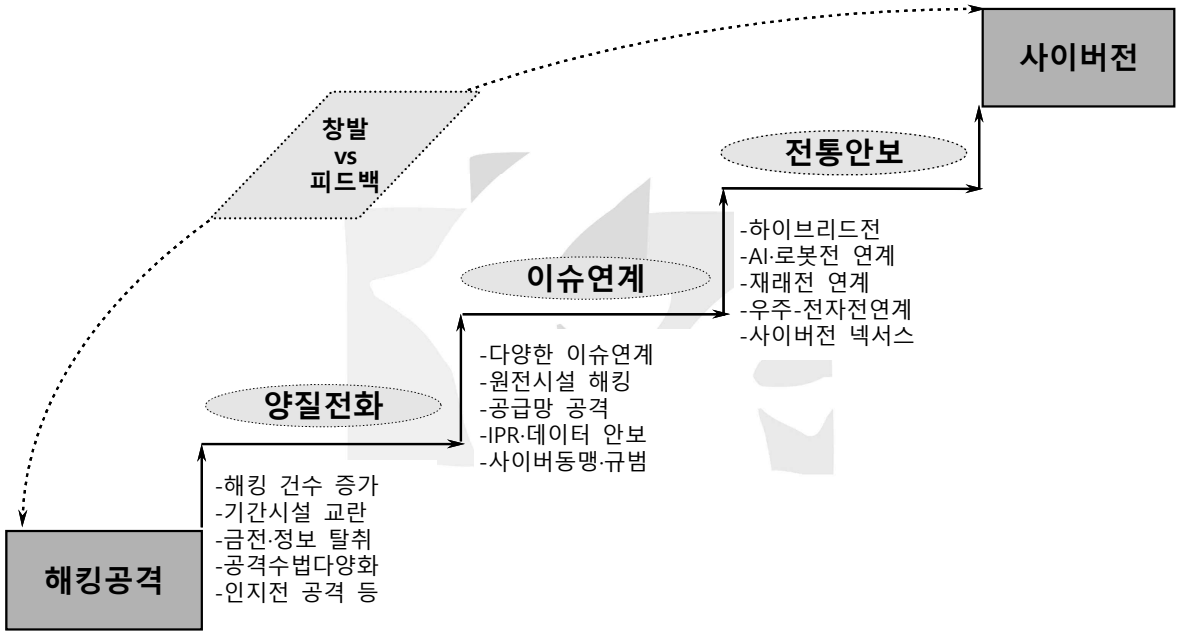
요약

2025년 1월 20일 출범한 제2기 트럼프 행정부가 펼칠 사이버 안보 전략은, 미중 패권경쟁의 맥락에서 중국의 해킹에 대응한다는 차원에서는 이전 바이든 행정부에서 수행한 정책적 연속성을 이어받을 것으로 보인다. 다만 사이버 안보와 여타 다양한 이슈들이 연계되는 맥락을 정치·외교·경제적으로 활용하려는 트럼프의 전략적 의도에 따라서 다양한 변화가 예견된다. 미국이 추구할 새로운 사이버 안보 전략의 방향과 내용을 파악하는 것은, 한국과 같은 중견국에는 매우 중요한 정책적 논제가 아닐 수 없다. 이 글은 트럼프 2기 미국의 사이버 안보 전략에서 나타나는 전반적인 기조 변화를 검토하고, 이를 바탕으로 여러 세부 분야에서 드러날 구체적인 변화의 양상을 전망해 보고자 한다.

서론: '사이버 복합 넥서스'의 시각

최근 사이버 공격은 그 양이 급격히 늘어나서 질적인 변화를 초래하는 '양질전화(量質轉化)'의 양상을 보이고 있다. 게다가 양적으로만 늘어나는 게 아니라 복합적인 '이슈연계(issue linkage)'의 과정을 거치면서 새로운 패턴을 드러내고 있다. 이러한 과정을 거쳐서 '전통안보'의 임계점을 넘어 사이버 안보 이슈가 지정학적 문제로 부상하는 현상이 나타나고 있다(<그림-1> 참조). 실제로 최근 사이버 안보 문제는 좁은 의미의 시스템 해킹이나 악성코드 공격 등의 경계를 넘어서 다양한 신흥안보(emerging security)의 이슈로 창발(emergence) 및 피드백(feedback)의 과정을 겪고 있다.[1)]

<그림-1> 사이버 안보의 창발·피드백과 복합 넥서스



이러한 사이버 안보의 진화 과정과 구조를 최근 학계에서는 '사이버 복합 넥서스(Cyber Complex Nexus)'로 개념화하고 있다.[2)] 사이버 안보 이슈가 다양한 이슈들과 복잡하게 연계되는 현상을 의미하는 '사이버 복합 넥서스'에 대한 논의는 현재 진화하고 있는 사이버 안보 문제를 보는 새로운 시각을 제시한다. 이러한 넥서스의 개념은 사이버 안보의 지정학이 단순한 단계적 부상이 아니라 양질전화-이슈연계-전통안보의 세 단계가 모두 복잡하게 얽히면서 부상하는 입체적 창발 과정이라는 점을 드러낸다. 이 글은 사이버 복합 넥서스의 시각을 원용하여 향후 트럼프 2기 미국의 사이버 안보 전략의 행보를 살펴보고자 한다.

1) 김상배. 2016. "신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해." 『한국정치학회보』 50(1), pp.75-102.
2) 김상배. 편. 2024. 『사이버 안보의 국제정치학』, 사회평론.

사이버 안보 전략의 전반적 기조

바이든 행정부와 비교하여 트럼프 2기의 사이버 안보 전략은 상당한 부분에서 연속성을 유지할 것으로 예상된다. 미국의 사이버 안보 정책이 공화당과 민주당을 막론하고 초당적으로 추진되어 온 역사를 돌아볼 때 그러한 전망은 설득력이 있다. 그럼에도 트럼프 2기 사이버 안보 전략은 몇 가지 핵심적인 분야에서 변화를 보일 것으로 예상된다. 사이버 안보 전략의 전반적 기조에서 드러나고 있는 변화의 조짐은 다음과 같은 네 가지 차원에서 발견된다.

사이버 안보 전략의 연속성

첫째, 트럼프 2기 미국이 바이든 행정부의 사이버 안보 전략의 기조를 어느 정도 이어받을지, 아니면 '바이든 그림자 지우기'에 나설지가 관건이다. 미중 사이버 안보 갈등이 지속되거나 아니면 새로운 국면에 접어들 것으로 전망되는 가운데, 바이든 행정부 말기 중국 해커들의 통신사 해킹, 재무부 해킹 등과 같은 사건의 발생으로 인해서 미국의 대중국 사이버 안보 대응 태세와 제재 수위는 갈수록 강화되는 추세이다. 특히 바이든 대통령은 임기 종료 4일 전인 2025년 1월 16일 사이버 안보 관련 행정명령을 발표하고 나섰다. 미국 정부와 거래하는 소프트웨어 기업들에 새로운 보안 기준을 부과하였는데, 이 행정명령의 핵심은 소프트웨어 공급망 보안을 강화하는 차원에서 소프트웨어 구성표(Software Bill of Materials, SBOM) 제도를 도입했다.[3)]

바이든 행정부 시기 최대 쟁점이었던 '소프트웨어 공급망 안보' 문제는 지속될 가능성이 있다. 취임 후 트럼프 대통령이, 바이든 정부의 여타 많은 행정명령을 폐기했는데도 불구하고 사이버 안보 관련 행정명령은 그대로 유지한 것에 주목할 필요가 있다. 오히려 트럼프 대통령은 2025년 3월 19일 미국내 사이버 안보 정책에 대한 행정명령을 발표하여 사이버 복원력(cyber resilience)을 강조하였다. 이 행정명령에는 연방정부의 역할은 최소화하고, 지방과 민간의 자율성은 확대하는 등과 관련된 트럼프 행정부의 정책적 기조를 주 내용으로 담았다. 이러한 양상은 사이버 안보 전략과 관련해서는 미국내에서 공화당과 민주당 간의 초당적 공감대가 존재하고 있음을 보여준다,[4)]

3) White House, 2025. "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity," January 16. 소프트웨어 구성표(SBOM) 제도는 공공조달 과정에서 소프트웨어의 구성요소, 개발 및 취득 과정, 그리고 운영에 대한 정보를 공개하도록 하는 정책으로, 바이든 행정부가 2021년 5월 12일에 발표한 행정명령 14028호("Improving the Nation's Cybersecurity")에서 처음 도입되었으며, 이번 행정명령은 이를 보다 강화하여 적용하는 내용을 담고 있다.

4) White House. 2025. "Executive Order on Achieving Efficiency Through State and Local Preparedness." March 18.

사이버 안보 전략 추진체계의 변화

둘째, 트럼프 행정부에서 단행한 사이버 안보 추진체계의 변화, 특히 '사이버 보안 및 인프라 보안국(CISA)'의 권한 및 활동 범위를 축소한 조치에 주목할 필요가 있다. 이는 사이버 안보 업무에서 정부의 개입을 줄이고 민간 부문의 자율성을 높이려는 의도가 반영된 것으로 해석된다. 그런데 CISA의 축소에 대한 논의의 이면에는 미국의 정치적 상황도 작용한 것으로 보인다. 2020년 대선 당시 CISA의 수장이었던 크리스 크렙스(Chris Krebs) 국장이 트럼프 행정부의 부정선거 주장을 반박하면서 보수 진영을 비판하여 정치적 논란에 휘말린 바 있다. 당시 CISA의 임무가 선거보안 관련 허위조작정보 대응으로 확장되었는데, 트럼프는 이를 정치적 임무로 비판하며 축소할 것을 주장했다. 트럼프는 '진보세력'이 CISA를 장악하여 언론의 자유를 억압하는 것으로 묘사하기도 했다.

트럼프 정부 출범 이후 이러한 논란은 CISA의 활동 범위 축소에 영향을 미쳤는데, CISA의 사이버 안보 업무에서 허위조작정보 관련 업무가 분리되는 것으로 나타났다. 유사한 맥락에서 2025년 1월 22일 CISA가 관리하던 자문기구인 사이버 안전 검토위원회(CSRB) 위원 전원을 해임하였는데, 그 위원 중에 크리스 크렙스 전 국장도 포함되어 있었다. 2025년 5월에는 CISA의 2026년도 예산을 약 5억 달러 감축할 것을 제안했으며, 1,300명을 감원하는 계획의 추진을 밝히기도 했다.

사이버 안보 분야 규제완화와 민관협력

셋째, 트럼프 행정부의 정책 기조는 규제 완화를 통한 시장 활성화에 초점을 맞추고 있는데, 사이버 안보 분야에서도 정책의 권한과 책임을 분산시키고, 규제를 완화하는 정책을 도입할 것으로 보인다. 앞서 언급한 2025년 3월 19일 행정명령은 사이버 안보 정책 추진과 관련하여 연방정부의 역할을 최소화하고, 주정부의 자율성을 확대하며, 사이버 안보에 대한 민간 기업의 책임 완화를 강조하고 있다. 구글, MS, 아마존, 메타 등 빅테크 기업들의 신속한 혁신 유도를 강조하되, 기업의 자율적인 보안 책임을 더욱 강조하고 있다. 이 과정에서 민간 기업과 정부 기관과의 협력을 촉진하고 연방정부의 직접적 감독과 같은 개입은 최소화하려 한다.

2024년 4월 미 사이버사령부가 발표한 「사이버 공간 우위 달성 및 유지」(Achieve and Maintain Cyberspace Superiority)라는 새로운 비전에서도 민간 부문과의 파트너십 강화 의지를 드러냈다. 이러한 상황 전개는 한국 기업들이 미국 시장에서 활동하거나 미국 기업들과 협력할 때, 사이버 위협 정보를 공유하고 공동 대응하는 데 있어 더욱 적극적인 역할을 요구받을 수 있음을 예견케 한다. 다시 말해 한국 기업들에 혁신의 기회와 강력한 자체 보안 역량 확보라는 도전을 동시에 안겨줄 가능성이 있다.

대중국 견제의 기조 유지

끝으로, 트럼프 2기의 사이버 안보 전략은 미중 디지털 패권경쟁의 전개에 대해 적극 대응하는 방향으로 전개될 것으로 예상된다. 중국과의 경쟁에서 승리하기 위한 기술혁신과 규제완화, 국가안보 목표를 중심으로 사이버 안보 전략의 강화도 지속될 것으로 보인다. 대중국 사이버 전략의 초점은 기술적·물리적 인프라 보호에 맞춰질 가능성이 있다. 미중 첨단기술 경쟁에서의 우위를 확보하기 위한 기술통제 목적의 사이버 안보 담론 개발 및 관련 대응책 강화에 주력할 것으로 보인다.

한편, 미국이 중국에 집중하면서 러시아 등의 사이버 안보 위협에 대한 대응은 상대적으로 약화되는 양상이 나타나고 있다. 2025년 3월 3일, 피트 헤그세스(Pete Hegseth) 미 국방장관은 러시아에 대한 사이버 공격 작전 중단을 명령했다. 마이클 왈츠(Michael Waltz) 전 미 국가안보보좌관도 사이버 위협국으로 러시아는 언급하지 않고, 중국과 이란만 언급했음에 주목할 필요가 있다.

이러한 과정에서 미국의 자국 우선주의 기조 아래 자국 빅테크 기업들 중심의 사이버 안보 전략을 노골적으로 추구하는 양상이 전개될 것으로 예견된다. 이러한 사이버 안보 분야의 행보는 트럼프의 기술·경제 노선이 취하고 있는 경향을 반영하는 것으로 평가할 수 있다.

'사이버 복합 넥서스'의 전개

트럼프 2기 미국은 자국의 경제적 영향력 유지라고 하는 큰 목표 아래 사이버 안보 수단을 적극 활용하리라는 점에서 이전의 바이든 행정부와의 연속성이 발견된다. 그러나 트럼프 2기의 전략은 좁은 의미의 사이버 안보를 넘어서 다양한 이슈들이 연계되어 넥서스를 이루는 맥락에서 여러 가지 차이를 드러낼 것으로 전망된다. 이러한 과정에서 좁은 의미의 사이버 안보와 확장된 사이버 안보 넥서스를 연계하는, 이른바 '성동격서(聲東擊西)'를 연상케 하는 트럼프 대통령의 현란한 전략 구사가 불확실한 변수로 등장할 가능성이 있다. 구체적으로 주목해야 할 '사이버 복합 넥서스'의 사례로서 다음과 같은 여덟 가지 이슈를 제시하고자 한다.

사이버 안보와 인지전

첫째, '사이버 복합 넥서스' 중에서 트럼프 2기를 맞아 제일 많이 주목받을 이슈 중의 하나는 '사이버-AI-인지전 넥서스'일 듯하다. 생성형 AI를 활용한 사이버 공격에 대한 논의가 큰 쟁점이고, AI가 수행하는 사이버 영향력 공작 또는 인지전(cognitive warfare)도 논란거리이다. 특히 거대언어모델(LLM)의 활용 문제가 부상했는데, 최근 발생한 중국발 '딥시크 쇼크'로 인해서 생성형 AI가 데이터 유출, 인지전 위협 등 사이버 안보 문제에 미치는 영향이 정책

적 차원에서 큰 관심거리가 될 것으로 보인다. 이미 미국을 포함한 해외 정부들이 이 문제에 대한 우려를 제기했고, 최근에는 개인정보 유출과 인지전 위협을 우려해서 미국 텍사스주 등에서 딥시크에 대한 금지 조치를 내리고 있다. 트럼프 2기에도 딥시크 등 중국산 AI 모델의 사이버·데이터 안보 문제에 대한 논란이 더 커질 것으로 보인다.

그런데 취임 이후 트럼프 대통령의 행보는 이러한 '사이버-AI-인지전 넥서스'의 부상 트렌드와 모순되는 다소 역행적 경향을 보이고 있는데, 이에 대해 주목할 필요가 있다. CISA의 조직 축소와 예산 및 인력 감축 등의 행보에서 보는 바와 같이, '표현의 자유 침해'를 거론하며 허위조작정보 대응을 경시하는 경향이 드러나고 있다. 인지전 인프라를 사이버 안보 영역에서 명시적으로 제외하고, 사이버 공격으로부터 기술 인프라를 보호하는 데 초점을 두는 경향이 드러나고 있다. 중국의 허위정보공작에 대응하는 기관과 예산은 폐지 또는 축소되었는데, 미 국무부의 해외정보조작 및 개입 대응 조직(The Counter Foreign Information Manipulation and Interference, R/FIMI)이 4월에 공식 폐지되기도 했다.

사이버 안보와 공급망 안보

둘째, 트럼프 2기에 주목할 이슈로는 '사이버-공급망 안보 넥서스'도 있다. 트럼프 1기에 제기된 대(對)중국 공급망 안보 갈등 이슈의 연장선에서 볼 때, 트럼프 2기에는 그야말로 '공급망 안보 이슈의 귀환'이 이루어질 가능성이 크다. 이미 바이든 행정부에서도 다양한 아이템과 관련된 공급망 안보 문제가 제기된 바 있는데, 바이든 말기에 커넥티드카 또는 스마트카와 관련된 사이버·데이터 안보 논란이 부각된 바 있다. 또한 공급망 관련 사이버·데이터 안보 이슈와 관련하여 드론에 대한 규제 법안 논의가 재등장하였으며, AI 반도체 관련 수출통제 강화도 쟁점으로 등장했다.

사이버 안보 분야와 관련하여, 미국 정부가 부과하는 통상 압력의 속내를 알아야 한다. 미국 정부는 자국 빅테크 기업들이 해당국 기업들보다 더 좋은 서비스를 제공할 수 있다고 주장하며 자유로운 시장 경쟁을 옹호하는데, 이러한 경향은 사이버 안보 분야에도 투영될 것으로 보인다. 한편, 트럼프 정부가 자국 사이버 보안제품 적용 확대 차원에서 관세 카드를 활용할 '사이버-관세 넥서스'의 가능성에도 주목할 필요가 있다. 예를 들어 관세 인하와 타 이슈에서 상대국의 양보를 교환하는 거래적 접근이 득세하여, 자동차-반도체 분야의 관세 유예의 대가로 사이버·데이터 안보 분야의 양보를 요구할 가능성이다.

사이버 안보와 플랫폼 안보

셋째, 트럼프 2기에 주목받을 이슈로 '사이버-플랫폼 안보 넥서스'도 살펴볼 필요가 있다. 최근 디지털 플랫폼 경제의 활성화에 영향을 받아 사이버 안보 이슈도 제품과 서비스에서 플랫폼으로 확장되고 있다. 바이든 행정부에서도 그랬지만 트럼프 2기에도 이러한 추세는 계속 이어질 것으로 전망된다. 플랫폼 안보에서의 쟁점은 서비스 제공 과정에서 발생하는 개인정보 유출과 데이터 안보의 문제인데 최근 중국 플랫폼의 해외 진출, 특히 미국과 유럽 진출이 활발히 진행되면서 '안보화(securitization)' 되고 있다.

가장 대표적인 사례는 동영상 플랫폼인 틱톡 금지이며, 이와 유사한 맥락에서 테무 등 '쉬인이나 커머스'의 개인정보유출 문제가 있다. 중국산 AI 모델인 딥시크를 둘러싸고도 비슷한 맥락에서 이 문제가 제기될 것이며, 중국 AI 플랫폼 전반으로 확산할 가능성이 매우 크다. 약간 결을 달리하지만, 이러한 플랫폼 안보는 트럼프 대통령이 강조하는 가상자산의 사이버 안보 문제로도 연계되어 쟁점화할 가능성이 있다. 다만 다른 이슈와는 달리 플랫폼 안보가 국민생활 전반과 연계된 특징으로 인해서 조심스럽게 전개될 가능성이 있다. 서슬이 퍼렇던 틱톡 금지법 시행 문제도 트럼프 취임 직후 75일의 유예 조치를 내린 바 있다.

사이버 억지와 공세적 작전

넷째, '사이버 안보의 군사화'를 바탕으로 한 '사이버-국방 넥서스'의 부상이다. 러시아, 이란, 특히 중국에 대항하기 위한 공격적인 '사이버 억지(cyber deterrence)'에 대한 논의는 지속될 것이다. 사이버 공격에 대한 공격적 수단을 포함한 군사적·보복적 억지 중심으로 사이버 안보 전략의 무게중심이 이동할 가능성이 있다. 군사력을 중심으로 사이버 안보의 역량과 자원을 집중한다는 트럼프 2기의 기조는, 캐서린 서튼(Katherine E. Sutton) 국방부 사이버 정책 담당 차관보의 언급에서 드러났다. 서튼 차관보는 사이버 무기 사용 규정의 완화, 디지털 작전을 '전통적인 군사 활동'으로 규정한 국방 정책 법률의 완화 등을 지시했다. 또한 2025년 5월 상원 군사위원회에 출석해서는 신속한 사이버 대응태세, 특히 AI 기반 공격에 대한 대처를 강조했다.

한편, NSC 사이버 담당 선임국장 알렉세이 불라젤(Alexei Bulazel)도 공격적 사이버 전략을 제시했는데, 이른바 '공격의 갱신, 방어의 갱신(Updating offense, updating defense)'을 강조했다. 이렇게 국토방위와 군사적 대응이라는 측면에서 사이버 안보의 군사화 추세가 강화되는 트럼프 2기의 변화가 기존에 바이든 행정부에서 제기했던 '선제적 방어(defense forward)'와 얼마나 다를지가 관건이다.[5] 이외에 조직개편 차원에서 '사이버군'을 독립군으로 창설하는 문제나 국가안보국(NSA)과 사이버사령부의 구조 변경 문제도 제기되고 있다.

---

5) 선제적 방어개념은 "악의적 사이버 활동과 그 원천을 방해 또는 중지하기 위해 무력분쟁(armed conflict) 수준 이하의 행동까지 수행"하겠다는 전략을 의미하며, 바이든 행정부가 2018년 9월에 발표한 국방사이버전략(DOD Cyber Strategy)부터 등장하여 네트워크에 대한 방어에 집중해왔던 기존 사이버 전략으로부터의 전환을 상징한다. 오일석. 2022. "바이든 정부의 사이버안보 정책과 시사점: 사이버 억지를 중심으로." 『INSS 연구보고서』 2022-13호. p. 43.

사이버전(戰)과 미래전

다섯째, 트럼프 2기에 들어 주목받을 이슈 중의 하나는 '사이버-미래전 복합 넥서스'이다. 우크라이나 전쟁 발발 이후 오프라인 전쟁과 결합한 사이버전에 대한 관심이 국내외에서 증대하였는데, '미래전 복합 넥서스'로서 '사이버전 복합 넥서스'에 관심이다. 그중에서 트럼프 1기에서 이미 문제 제기된 이슈라는 점에서 주목해야 할 것이 '우주 사이버 안보' 이슈이다. 이는 어떠한 형태로건 트럼프 2기에 이슈로 제기될 것으로 보인다. 특히 이는 이미 창설된 미 '우주군'의 작전 영역과 관련하여 사이버전의 위상 설정 논의가 전개될 가능성이 있다.

또한 최근 국내외에서 큰 주목을 받는 것은 '사이버-AI-핵(nuclear) 넥서스'이다. 이는 트럼프 2기 미국의 사이버 안보 및 국방 전략과 관련하여 조만간 제기될 가능성이 있는 주제이다. 이른바 '확장억제' 전략에 기반을 두고 수립된 대북 군사전략도 사이버·AI 환경에 맞추어 전환이 불가피할 것으로 보인다. 전통적인 핵무기 이외에도 사이버·AI 기반 조기경보, 미사일 방어시스템 강화 등과 같이 사이버·AI 기술을 활용한 새로운 형태의 억지 수단 도입이 고려될 것이다. 사이버-AI-핵 넥서스의 부상에 대응하여 기존의 군사전략 개념을 새로이 설정하고 이를 지원하는 군사혁신을 추진할 필요성이 제기된다.

사이버 안보와 동맹·연대

여섯째, 바이든 시기의 '신뢰 기반 동맹관'을 넘어서 이른바 '거래적 동맹관'을 제시할 것으로 보이는 트럼프 2기 쟁점 중의 하나는 '사이버-동맹 넥서스'의 전환(transformation)이다. 다자외교보다는 양자외교를 강조하는 트럼프 외교에서 소다자 외교 프레임은 유지될 가능성이 있다. 대중국 대응에 집중한다는 측면에서 인태 지역 국가들과 미국 중심의 양자 및 소다자 사이버 안보협력은 트럼프가 보기에 '효율적인 프레임워크'이다. 그러나 이러한 소다자 협력에 참여하고 있는 다수 국가가 미국 우선주의와 동맹 경시로 직·간접적인 피해를 보고 있어서 향후 그 응집력이 유지될 것인지가 관건이다.

이러한 소다자 협력체 중에서 대표적 사례는 파이브아이즈(Five Eyes)이다. 최근 파이브 아이즈의 확장 논의(프랑스, 일본, 한국 등 참여)가 제기되었다. 그러나 최근 미국-캐나다 관계의 악화로 파이브아이즈의 틀 자체를 활용하기에는 난관이 있을 것으로 보인다. 그 대신 파이브 아이즈 내의 오커스(AUKUS) 3국, 즉 미국, 영국, 호주 정보협력이 파이브 아이즈의 핵심으로 작동할 가능성이 있다. 한편, 트럼프 취임 직후의 양상을 보면 트럼프 2기에도 중국을 견제하는 '쿼드(Quad) 안보협력체'는 유지될 것으로 보인다. 트럼프 취임식 다음 날 쿼드 외교장관 회의를 열었으며, 쿼드 정상회의 개최도 유력하게 전망되었다. 이런 맥락에서 '쿼드 플러스'에 한국이 참여하는 문제가 쟁점으로 제기될 가능성이 있는데, 좀 더 유력하게 거론되는

것은 한국이 오커스(AUKUS) 필라-II에 참여하는 문제가 쟁점이다. 오커스 필러-II는 6개 기술 분야(사이버, 인공지능, 양자 컴퓨터, 해저 기술, 극초음속 미사일, 전자전)와 2개 기능 분야(혁신, 정보공유)로 구성된다.

사이버 안보와 한미일 관계, 한미동맹

일곱째, 사이버 안보 분야의 동맹과 연대라는 시각에서 볼 때, 미일 관계, 한미일 관계, 한미 관계의 맥락에서 제기되는 사이버 안보 협력의 미래에 대한 전망도 큰 쟁점이다. 트럼프 취임 이전에도 '미일 사이버 동맹'의 지속되는 조짐이 드러나고 있는 가운데, 미국과 일본은 AI를 악용한 사이버 공격에 공동 대응하기 위한 연구 협력에 착수한다는 보도가 나왔다.[6] 트럼프 2기 행정부 출범 후인 2025년 2월 10일에 개최된 미일 정상회담에서도 양 정상은 "쿼드, 한·미·일, 미·일·호주, 미·일·필리핀 등의 다층적 협력을 강화할 예정"임을 강조했다. 이런 맥락에서 보면, 트럼프 2기에도 미국은 미일동맹과 한미일 안보 협력체제의 중국 견제 기능을 인정할 가능성이 있다.

'한미 사이버 안보 동맹'의 미래도 관건이다. 한미 간 사이버 안보 영역에서는 2023년 4월 26일 체결된 「한-미 전략적 사이버 안보 협력 프레임워크」를 발전시키는 것이 매우 중요하다. 이에 근거한 협력체계로서 사이버 안보 고위급 회의체(Senior Steering Group)가 2023년부터 매년 협의를 진행하고 있다. 바이든 시기 '한미 사이버 동맹'이 다소 '선언적 성격'을 띠었다면, 트럼프 2기 거래적 동맹관에 기반을 둔 '사이버 동맹'은 좀 더 구체적인 문제와 연계될 가능성이 있다. 예를 들어, 미국이 한국에 대한 방위비 분담 추가 요구와 사이버 안보 동맹 이슈가 연계될 가능성이 우려된다.

사이버 안보와 국제질서의 미래

끝으로, '사이버-국제질서 넥서스'이다. 바이든 정부 시기 '민주주의 대 권위주의' 구도로 중국과 러시아를 권위주의 축으로, 동맹 등 동지국가들과의 협력을 핵심 축으로 구분 짓던 가치와 규범 기반의 사이버 안보 외교는 약화될 것으로 전망된다. 바이든이 공들였던 '민주주의 정상회의', '인터넷의 미래 선언' 등은 중단될 가능성이 크다. 「랜섬웨어 대응 이니셔티브」(CRI: Counter Ransomware Initiative)'와 같은 다자적 틀에서 진행되던 사이버 국제협력도 경시할 가능성이 있다. 미국이 나토에서 탈퇴할 가능성도 언급되고 있는 상황에서 바이든 말기 나토-인태 협력 차원에서 진행된 사이버 안보 국제협력도 약화 될 가능성이 있다. 예를 들어 'IP-4(Indo-Pacific 4)'에서의 사이버 협력 및 방산 협력 등이 지속될지에 대해서는 의문이 제기된다.

6) 박상현. 2025. "미일, AI 악용한 사이버 고엮 공동 연구." 『연합뉴스』. 1월 2일.

서방 진영 내 입장 차이가 명확하게 드러난 계기는 2025년 2월 10일 프랑스에서 열린 ‘AI 행동 정상회의(AI Action Summit)’였다. 미국은 정상회의에서 채택할 공동성명에 서명을 거부하였고, 영국도 미국과는 다른 이유에서 서명을 거부했다. 이러한 갈등 양상은 2월 14일에 열린 뮌헨안보회의에서의 J.D. 밴스(J.D. Vance) 미 부통령의 연설에도 이어졌다. 결국 트럼프 2기 서방 진영의 내부 결속 원리가 달라지는 ’ 질서 재편‘의 가능성마저도 엿보인다. 이는 사이버 안보 관련 국제규범이나 국제기구 활동의 약화 가능성을 전망케 한다. 이러한 행보가 낳을 국제질서의 변화는 어떤 모습을 보일지에 대한 면밀한 분석이 필요하다.

결론

요컨대, 트럼프 2기 미국의 사이버 안보 전략은 연속성과 변화의 양상을 동시에 드러내며 전개될 것으로 전망된다. 기존 정부의 사이버 안보 관련 행정명령은 그대로 유지하며 이 분야에서의 초당적 대응 기조를 강조하는 가운데, 공급망 안보의 지속적 강조, 사이버 안보 추진체계의 재편, 민간 기업에 대한 규제 완화와 민관협력의 강조, 경제·군사안보 차원에서의 대중국 견제 기조 유지 등에 주목할 필요가 있다. 이러한 과정에서 이 글이 강조한 ‘사이버 복합 넥서스’ 분야에서 나타나는 변화의 양상에 주목해야 한다. 특히 기존의 사이버 안보 영역을 넘어서 다양한 이슈들이 연계되는 상황에서 이를 전략적으로 활용하려는 트럼프의 정책 불확실성이 새로운 변화를 초래할 변수가 될 것이다. 사이버 안보 분야의 새로운 변화에 대응하는 중견국 한국의 고민이 깊어질 수밖에 없는 대목이다.

저자소개: 김상배

서울대학교 외교학과를 졸업하고 동 대학교 외교학 석사를 취득하고 미국 인디애나대학교에서 정치학 박사를 취득하였다. 서울대학교 국제문제연구소장을 역임하고 현재 서울대학교 미래전연구센터장을 맡고 있다. 학회 활동으로는 한국국제정치학회장, 한국사이버안보학회장을 역임했으며, 현재 정보세계정치학회장을 맡고 있다. '디지털 기술의 국제정치와 국가전략'에 대한 연구와 강의를 하고 있으며, 저서로는 『미중 디지털 패권경쟁: 기술-안보-권력의 복합지정학』 (한울, 2022), 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 (한울, 2018), 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 (한울, 2014), 『정보혁명과 권력변환: 네트워크 정치학의 시각』 (한울, 2010), 『정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터산업』 (한울, 2007) 외에 다수의 편저서 및 공저서가 있다.

2025년 7월