www.kacs.ne.kr

2026 KACS SPECIAL REPORT

| 2026 KACS 스페셜리포트 |

사이버 복합 넥서스:

최신 동향 파악과 대응 전략 모색

한국사이버안보학회
KACS

| 2026 KACS 스페셜리포트 |

사이버 복합 넥서스:
최신 동향 파악과 대응 전략 모색

본 보고서는 한국사이버안보학회의 연구용역과제
(과제명 : '사이버 복합 넥서스: 최신 동향 파악과 대응 전략 모색', 수행기간 : 2025.04~2025.11)
결과물을 바탕으로 수정·보완한 것 입니다.

한국사이버안보학회
KACS

Contents

서 론
사이버 복합 넥서스의 필요성

1. 연구의 필요성 및 목적

서 론
사이버 복합 넥서스의 필요성

1. 연구의 필요성 및 목적

최근 사이버 안보는 AI·핵·공급망·규범 등 다양한 이슈와 연계되어 위협의 형태가 다변화하고 있다. 이는 단순한 IT 보안 문제가 아니라 AI, 데이터, 반도체, 국방, 외교, 경제 안보와 밀접하게 연결된 복합적 영역으로 확장되는 현상으로 나타난다. 사이버-AI-핵 안보 넥서스, AI 반도체-공급망-사이버 안보 넥서스 등 다양한 결합 형태의 위협이 등장하는 가운데 이에 대한 새로운 분석과 대응 전략이 필요하다.

한편 기술 패권 경쟁과 사이버 안보의 전략적 중요성도 높아지고 있다. 미·중 기술 패권 경쟁이 심화됨에 따라 국가 간 AI 및 사이버 안보 관련 외교 전략이 급변하고 있다. AI 기반 무기체계, 데이터 첩보(DATINT), 사이버 인지전 등의 기술적 진보는 기존 국가안보 전략을 재정립해야 하는 도전과제를 제기한다.

따라서 사이버 안보에 대한 접근은 다층적인 차원에서 이루어질 필요가

있다. 단순한 기술적 보안 조치뿐만 아니라, 거버넌스·정책·국제 규범·동맹 협력 차원에서 대응 전략을 마련해야 한다. 사이버-우주 안보, 디지털 플랫폼과 사이버 안보, AI 동맹외교 넥서스 등과 같은 새로운 영역에서 국가 간 협력이 필요함은 물론이다.

이러한 맥락에서 한국의 정책적 대응 방향을 새롭게 정립하는 노력이 추진되어야 할 것이다. 먼저 글로벌 사이버 안보 및 AI 규범 논의에서 한국의 역할을 강화하고, 국내 정책 수립에 국제적 시사점을 반영해야 한다. 또한 미국 및 동맹국과의 협력을 강화하면서, 한국의 산업 및 기술 경쟁력을 고려한 독자적인 사이버·AI 안보 전략 수립이 요구된다.

따라서 본 연구는 사이버 안보와 산업, 경제, 군사, 외교 영역과의 넥서스화를 검토함으로써 향후 연구 어젠다를 발굴하고 (총 15개 분야) 구체적인 분석을 시행하고자 한다.

제1장

사이버 복합 넥서스 : 개념과 사례의 탐색

김 상 배 | 서울대학교 정치외교학부 교수

제1장

사이버 복합 넥서스: 개념과 사례의 탐색

김상배 | 서울대학교 정치외교학부 교수

1. 머리말

최근 사이버 안보는 다양한 이슈와 연계되며 그 위협의 형태가 변화하고 있다. 좁은 의미에서 본 기술 시스템의 보안 문제를 넘어서, 인공지능(AI), 데이터, 공급망, 플랫폼, 핵, 우주, 전쟁 등 여러 이슈가 가세하면서 복잡해졌다. 이 과정에서 사이버 안보는 경제, 산업, 국방, 외교, 규범 등에 걸쳐서 명실상부하게 국가안보를 거론하는 문제로 증폭되었다. 특히 미국과 중국이 벌이는 글로벌 패권경쟁의 가속화는 사이버 안보의 지정학적 창발을 부추기는 주요 요소로 작동하였다. 또한 러시아-우크라이나 전쟁의 발발은 사이버 공격이 전통적인 물리전 결합하는 양상을 극명하게 보여주었으며, 드론과 같은 AI 활용 유무인 복합 무기체계나 우주 전략 자산, 인지전과 연계되는 모습도 보여줬다. 그 결과 사이버 안보는 기술 안보의 대책을 마련하는 차원을 넘어서, 이에 대응하는 정책과 제도, 거버넌스, 국제협력 등과 관련된 기존 국가안보 전략 전반을 재정비할 필요성을 제기하고 있다.

그야말로 이 글의 주제인 '사이버 복합 넥서스(Cyber Complex Nexus)'가 부상하고 있다. 이 글에서 제시하는 사이버 복합 넥서스는, 흔히 '사이버'로 줄여서 말하는 사이버 안보의 변수가 새로운 안보 위협의 구심점, 즉 넥서스가 되는 현상을 의미한다. 여기서 '사이버'는 이른바 해킹이 초래하는 좁은 의미의 사이버 안보 문제를 넘어서, 사이버 공간을 배경으로 제기되는 모든 안보 문제를 지칭한다고 보아야 할 것이다. 최근 디지털 기술, 특히 AI 기술의 발달은 사이버 안보의 넥서스 현상을 가속화하고 있다. 디지털 전환(DX), 특히 AI 전환(AX)은 사이버 안보의 전환에도 큰 영향을 미치고 있다. 이 과정에서 AI 안보는 사이버 안보, 데이터 안보, 인지 안보 등과 같은 '신흥안보(emerging security)' 위협을 창발(創發, emergence)시키는 새로운 넥서스로 작동하고 있다(김상배, 2018; 2023).

말뜻 그대로 넥서스는 단순한 '연결의 상태'라는 의미를 넘어서 여러 요소를 엮어주는 '결합의 고리'를 의미한다. 이 글에서 넥서스라는 용어를 원용하는 이유는, '사이버'와 'AI'로 대변되는 기술 변수가 핵심을 이루며 나타나는 사이버 안보 위협의 복합성을 보여주기 위함이다. 이러한 복합성은 단순히 '창발 현상'만으로는 파악하기 어렵고 이를 제어하는 '환원(reduction) 현상'과의 길항관계에서 이해해야 한다. 사이버 안보와 관련된 요소들은 각기 독립된 것이 아니라, 복잡하게 상호 연결되고 서로 영향을 미치며 집합적으로 하나의 시스템을 구성한다. 넥서스는 특정 시스템 안에 존재하는 포지티브 피드백으로서의 창발과 네거티브 피드백으로서의 환원의 상호의존성과 상호제약성을 담아내려는 개념이며, 시스템을 구성하는 각 요소의 최적화를 동시에 달성하기 어려운 '구조적 딜레마'를 상징하는 개념이기도 하다.

이처럼 넥서스는 단순한 연결 관계가 아니라 복잡계의 특성을 가진 시스

템 내에서 발견되는 상호의존적 관계들의 결합 고리이다. 이러한 넥서스의 개념은 사이버 안보 거버넌스의 관점에서 볼 때도 새로운 접근의 필요성을 제기한다. 넥서스의 개념에 입각한 사이버 복합 거버넌스는 신속한 정책적 대응뿐만 아니라 여러 변수를 고려한 복합적 대응의 중요성을 강조한다. 사이버 복합 거버넌스의 목표는 넥서스가 초래하는 복합 위기에 대처하고 궁극적으로 지속가능한 시스템을 관리하는 데 있다. 전통안보에 대한 대응 거버넌스를 넘어서 점차 복잡한 넥서스를 형성하며 진화하고 있는 사이버 안보 위협에 대응하는 효과적인 정책 마련의 필요성이 제기된다. 좀 더 구체적으로 말하자면, 사이버 복합 넥서스를 국가안보의 독자적 개념 범주로 설정하고 이에 대응하는 추진체계의 정비가 시급하게 요청된다.

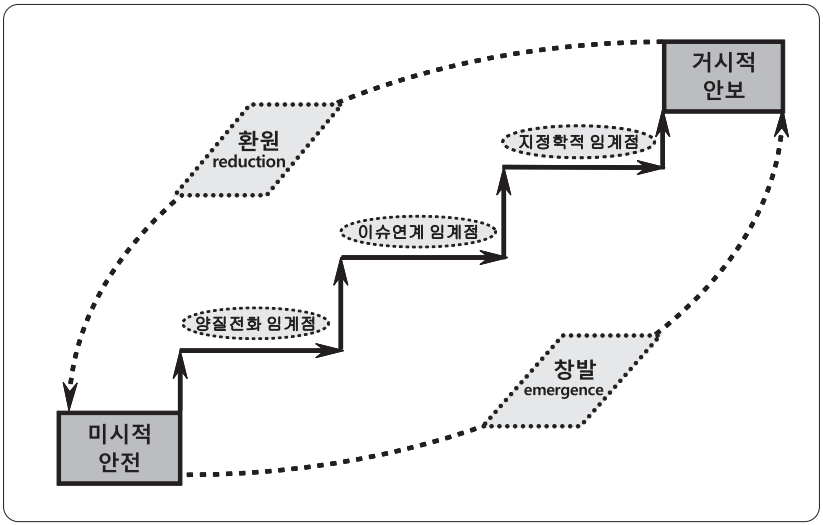
2. 사이버 복합 넥서스의 개념

1) 안보 위협의 창발과 환원

오늘날 사이버 안보는 새로운 안보이론, 즉 신흥안보의 시각으로 봐야 하는 논제다(김상배, 2016). 신흥안보는 복잡계 이론에서 말하는 창발의 개념에 기반을 둔다. '안보'와 합성어를 만들면서, '창발'보다는 좀 더 자연스러운 '신흥(新興)'으로 'emergence'를 번역했다. '창발/신흥'이란 미시적 안전의 문제가 양적으로 늘어나고 다양한 이슈가 연계되면서 임계점을 넘어서 거시적 안보의 문제가 되는 현상을 개념화하기 위한 시도다. 자연계에서 발견되는 거대한 개미탑의 건축이나 새 떼의 군무 등과 같은 현상을 사회

현상, 그중에서도 사이버 공간의 안보현상에 적용했다. 이렇게 이해한 신흥안보로서 사이버 안보는 '양질전화(量質轉化)'와 '이슈연계(issue linkage)', 그리고 '지정학(geopolitics)'의 3단계 임계점을 넘어서 창발한다(〈그림2-1〉 참조).

〈그림 2-1〉 '아래로부터의 창발'과 '위로부터의 환원'



출처: 김상배(2023), p.238.

첫째, 가장 포괄적인 의미에서 사이버 안보 위협은 이슈영역 내의 안전(safety)사고가 양적으로 증가하여 일정한 수준을 넘으면서 창발한다. 이는 양적증대가 질적변화를 불러오는 양질전화 현상의 전형적 사례이다. 평소에는 개별 단위 차원의 안전이 문제시될 정도의 미미한 사건들이었지만, 그 발생 숫자가 늘어나서 갑작스럽게 양질전화의 임계점을 넘게 되면 국가와 사회의 안보를 위협하는 심각한 문제가 된다. 이러한 와중에 미시적 안

전과 거시적 안보를 구분하던 종전의 경계는 무너지고, 사소한 일상생활 속의 안전 문제라도 거시적 안보의 관점에서 다루어야 하는 일이 벌어진다. 예를 들어 컴퓨터 한 대에서 발견된 악성코드는 그냥 무시될 수도 있겠지만 국가 기반시설을 통제하는 컴퓨터 시스템에 대한 해킹은 국가안보 차원에서 쉽게 지나칠 수 없는 중대한 위협이 된다.

둘째, 신흥안보로서 사이버 안보 이슈 간의 질적 연계성이 높아지게 되면, 어느 한 부문에서 발생한 안전의 문제가 임계점을 넘어서 거시적 안보의 문제가 될 가능성이 커진다. 이러한 이슈연계의 문제는 양적인 차원에서 단순히 링크 하나를 더하는 차원이 아니라 안보 위협의 구조가 질적으로 전환되는 문제이다. 다시 말해 끊어진 링크들이 연결됨으로써 전체 이슈 구조의 변동이 발생하게 되고 그 와중에 해당 이슈의 '연결 중심성'이 급속히 커지는 것을 의미한다. 이렇게 이슈연계 임계점을 넘어서 신흥안보 위협이 창발하는 사례는 사이버 안보의 여러 분야에서 발견된다. 예를 들어, 해킹 공격이 원자력 발전소의 컴퓨터 시스템에 대해서 감행될 경우는 그 위협은 더욱 커지며, 이러한 해킹이 정치적 목적과 결부된 테러의 수단이 되면 그 위험성은 더욱 증폭된다.

끝으로, 양질전화나 이슈연계를 통해서 창발하는 사이버 안보 이슈가 전통안보의 문턱을 넘으면 이는 명실상부한 국가안보의 문제가 된다. 사이버 안보 위협이 아무리 심하더라도 관련 행위자들의 협력을 통해서 무난히 해결할 수 있다면 굳이 '안보'라는 말을 거론할 필요도 없을 것이다. 그러나 그 위협이 '지정학적 임계점'을 넘어서 국가 간 분쟁의 대상이 되면 이는 명백한 안보 문제가 된다. 이 지경에 이르면 국가 행위자가 개입할 근거가 발생하게 되고 문제의 해결을 위한 국제협력의 메커니즘이 가동된다. 이러한 관점에서 보면 신흥안보는 '비전통 안보'의 개념과는 달리 전통안보 문

제도 포함하는 개념이다. 해커들의 장난거리였던 해킹이 테러리스트들의 공격 수단을 넘어서 최근 국가 간 사이버 전쟁으로 전화되는 현상은 신흥안보가 전통안보와 만나는 현상을 잘 보여주는 사례들이다.

여기서 한 가지 주목할 점은, 실제 현실에서는 사이버 안보 위협이 발생하는 과정이 양질전화-이슈연계-지정학의 단계를 따라서 순차적으로 발생하는 일방향적 '창발'의 현상만은 아니라는 사실이다. 실제로 사이버 안보 위협의 발생은 복합 네트워크 환경을 배경으로 '창발'과 '환원'이 상호작용하는 입체적 구도에서 보아야 하는 양방향적 현상이다. 사이버 안보 위협의 발생은 '아래로부터의 창발'과 '위로부터의 환원'의 상호작용한 결과라고 이해해야 한다. 다시 말해, 사이버 안보 위협은 아래로부터의 현상, 즉 창발의 포지티브 피드백(positive feedback)뿐만 아니라 위로부터의 현상, 즉 환원의 네거티브 피드백(negative feedback)이 복잡하게 오고 가는 과정에서 발생한다.

최근 사이버 안보 위협에 지정학적인 변수가 가미되면서 점점 더 환원의 피드백 메커니즘이 주목받고 있다. 다시 말해, 최근 사이버 안보 위협은 지정학 변수가 네거티브 피드백으로 작동하여 기존에 시스템 내에 잠재해 있던 구조적 취약성이 발현되는 과정에서 발생하는 경우가 늘어났다. 우크라이나와 중동 지역에서 발생한 전쟁이나 미국과 중국의 강대국 패권경쟁, 그리고 기타 세계 여러 지역의 국지적 분쟁의 발생과 전개는 사이버 안보 위협의 발생과 증폭을 부추기는 지정학적 변수들이다. 창발의 과정을 통해서 임계점을 넘는 위기의 양적 증가 이외에도, 환원의 과정을 통해서 위기 발생의 임계점 자체가 하락함으로써 전체 위기 구조가 질적으로 변화하고 있다(〈그림2-1〉 참조).

이러한 구도에서 보면, 사이버 안보 위협은 미시적 상호작용이 거시적으

로 창발한 결과물만은 아니고, 창발과 환원 두 변수의 길항관계 구도에서 이들의 상호작용과 상호제어의 결과물로서 이해해야 한다. 다시 말해, 신흥안보로서 사이버 안보 위협의 발생은 양질전화-이슈연계-지정학의 세 단계에 존재하는 각각의 요소들이 복잡하게 상호작용하며 상황에 맞춰 불거져 나오는 현상이라고 할 수 있다. 이 글은 이러한 사이버 안보의 복합적 창발-환원 피드백 과정을 좀 더 간결하고 개념적인 프레임워크에서 이해하기 위해서 '넥서스'의 개념을 원용하였다.

2) 넥서스의 개념적 이해

넥서스(nexus)는 '묶다,' '연결하다' 등의 뜻을 지닌 라틴어 동사 'nectere'에 어원을 두는데, 그 과거 분사형이 'nexus'이다. 영어 단어인 'connect'의 'nect'와도 어원이 같다. 넥서스는 단순한 연결(link)의 상태라기보다는 여러 요소를 서로 결합하는 '고리'를 의미한다. 달리 말하면, 네트워크상에서 서로 교차하는 요소들이 형성하는 관계의 '교차점' 또는 '구심점'을 뜻한다. 비슷한 용어인 '허브(hub)'가 링크가 교차하는 지점에서 중심이 되는 '노드(node)' 자체에 의미를 둔다면, 넥서스는 그 중심을 통해 여러 다른 것들과 이어지는 관계의 연계성까지도 포함하는 용어라고 할 수 있다. 이러한 점에서 넥서스는 허브와 링크를 함께 묶어서 이해하는 '부분 네트워크'의 다른 이름으로 이해할 수 있다.

넥서스라는 용어는 인문·사회과학, 환경·자원관리, 복잡계 이론 등 여러 분야에서 각기 다른 맥락에서 원용되고 있다. 국제정치학 분야에서 넥서스라는 말이 최근 널리 알려지게 된 계기는 '경제-안보 넥서스'라는 용어가 마련했다. 경제와 안보가 단순히 서로 관련이 있다는 뜻을 넘어서, 이른바

지정학 시대를 맞이하여 경제와 안보가 긴밀히 연계되어 서로 영향을 미치는 현상을 담는 용어이다. 특히 미중 글로벌 패권경쟁, 코로나19 팬데믹, 러시아-우크라이나 전쟁 등을 통해서 첨단기술, 공급망 안정, 산업·무역 정책 등의 경제적 요소에 국가안보의 프레임이 씌워지면서 좀 더 적극적으로 원용되고 있다.

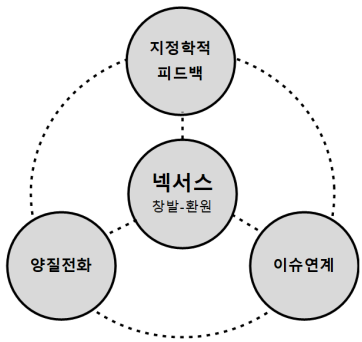
인문·사회과학 분야에서 넥서스라는 말을 유행시킨 학자는 유발 하라리(Yuval Harari)이다(하라리, 2024). 하라리는 넥서스를 인류 문명과 진화의 방향을 결정하는 데 중요한 역할을 담당한 '정보 네트워크'라는 관점에서 이해한다. 그러나 넥서스는 단순한 정보 네트워크라는 의미에만 국한되는 것은 아니다. 좀 더 넓은 의미에서 넥서스는 다양한 사회 구성요소를 연결하는 네트워크이고, 더 나아가 사회구조의 변화를 추동하는 동력이다. 이러한 과정에서 정보 네트워크가 권력 현상과 사회적 영향력을 형성하는 넥서스의 역할을 한다는 것이다. 하라리에 의하면, AI 시대에 접어들며 넥서스의 조직화 양상이 변화하고 있으며, 이는 인간 사회의 역사와 가치관, 그리고 윤리적·정치적 문제까지 변화시키는 사회적 영향력을 발휘한다고 한다.

자연과학 분야에서 넥서스에 대한 논의는 '물-에너지-식량 넥서스'의 개념에서 발견된다. 이러한 넥서스 개념은 물·에너지·식량 자원의 상호의존이 심화함에 따라 발생하는 '삼중고(trilemma)'에 착안한다. 따라서 이들 자원은 개별적으로 다루어서는 안 되고, 통합적으로 분석하고 지속 가능하게 관리돼야 한다는 것이다. 이러한 넥서스의 개념은 스톡홀름환경연구소(SEI)가 2011년 본(Bonn) 컨퍼런스에서 '물-에너지-식량 넥서스' 개념을 환경과 자원관리 측면에서 정립하고 이를 지속가능한 자원 확보와 정책 수립을 위한 기반으로 제시하면서 유명해졌다(Stockholm Environment Institute,

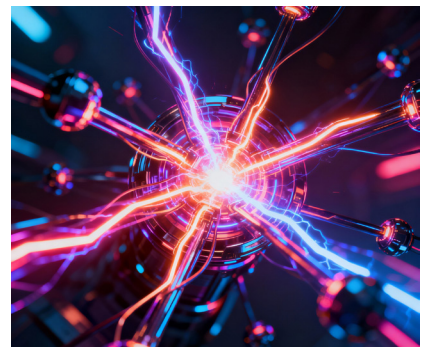
2011). 이러한 넥서스 개념은 이후 각국에서 물·에너지·식량의 상호 연계성을 연구하는 학술 및 정책 논의의 중요한 출발점을 제공하였다.

이상과 같이 거론되는 넥서스의 개념은 세 가지 전제를 바탕에 깔고 있다. 첫째, 넥서스의 개념은 복잡계 즉, 각 요소가 독립적인 것이 아니라, 서로 연결되고 복합적으로 얽혀서 하나의 시스템을 구성하는 현상을 전제로 한다. 둘째, 넥서스의 개념은 복잡계를 구성하는 여러 요소가 복잡한 상호작용을 통해 전체 시스템의 질서를 형성해 가는 '자기조직화(self-organization)'의 역동성을 전제로 한다. 끝으로, 넥서스의 개념은 각 요소 간에 발생하는 상호의존적 창발성과 이를 제약하는 환원의 네거티브 피드백 사이에서 발생하는 길항관계를 전제로 한다. 강조컨대, 이러한 과정에서 넥서스의 개념과 관련하여 중요한 것은 창발과 환원의 피드백 메커니즘이다.

〈그림2-2〉 넥서스의 개념적 구도와 이미지 구현



출처: 필자 작성



출처: 퍼플렉시티(Perplexity)에서 생성

결국 넥서스는 복잡계의 구성 요소들의 동적 상호작용과 이에 대한 환원의 피드백으로 인해 출현하는 현상을 파악하려는 개념이다. 넥서스는 어느

한 요소의 변화가 다른 요소들에 미치는 영향과 역으로 이를 제약하는 또 다른 영향 변수가 형성하는 복잡한 관계의 결절점에 주목하는 개념이다. 다시 말해, 창발의 포지티브 피드백과 환원의 네거티브 피드백이 만나는 지점에서 형성되는 교차점이다. 각 요소 간의 긴장 관계로 인해서 각기의 최적화를 동시에 달성하기 어려운 '구조적 딜레마'가 형성되는 지점이 넥서스이다. 예를 들어, AI-기술 경쟁력을 추구하려니 사이버-데이터 안보가 위험해지고, 이를 챙기려니 경제안보를 신경 써야 하는 지점에서 넥서스가 형성된다. 어느 한 부분에서 위기가 창발하지 않도록 환원을 부과하면 오히려 다른 부분의 위기를 창출하는 딜레마가 내재하고 있다는 것이다.

이러한 넥서스의 개념을 앞서 언급한 신흥안보의 구도에서 보면, 양질전화와 이슈연계, 그리고 지정학적 피드백의 상호접점으로 이해할 수 있다(〈그림2-2〉 참조). 단순한 창발을 넘어서는 통합과 복합의 과정과 구조를 담아내기 위해서 원용되는 개념이기도 하다. 하라리가 말하는 정보 네트워크는 이러한 상호접점 또는 이들이 형성하는 복합 네트워크의 구심점 역할을 하는 요소 즉, 넥서스의 대표적 사례이다. 이러한 관점을 연장해서 보면, 이 글에서 주목하는 '사이버(좀 더 넓은 의미에서 AI)' 변수가 그러한 복합적인 상호접점의 역할을 하는 넥서스라고 할 수 있다.

3. 사이버 복합 넥서스의 사례

이상의 문제의식을 바탕으로 이 글은 사이버 복합 넥서스를 다섯 개 범주에서 제기되는 15개 주제를 분석하고, 이를 바탕으로 향후 사이버 안보

연구의 학술적·정책적 어젠다를 제시하였다.

1) 사이버-AI-공급망 안보 넥서스

제2장 “AI 모델과 사이버 안보”(윤정현)는 거대언어모델(LLM) 기반의 생성형 AI가 편향과 환각 등 잘못된 정보의 산출 문제를 내재하고 있으며, 알고리즘 모델의 악용 이슈, 데이터 유출, 안정성 확인 미흡, 해커 공격 범위 확장 등 사이버 공격에 대한 다양한 취약점을 안고 있다고 지적한다. 특히 악의적 지시나 선동적 콘텐츠에 기반한 가짜뉴스 등 비합리적인 의사결정과 사회적 혼란으로 이어질 수 있는 위험이 존재한다는 것이다. 이와 같은 쟁점들이 향후 LLM 기반 생성형 AI 시대의 첨예한 사이버 안보 이슈를 낳을 것으로 전망한다. LLM 시대의 사이버 안보 양상과 복합적 파급력에 대해 면밀한 검토가 필요한 상황이라는 것이다. LLM에 기반한 AI 활용의 보편화는 단순한 경제산업적 파급력을 넘어 AI 활용 과정에서 제기되는 보안 문제와 첨예한 윤리적 쟁점을 유발한다. 나아가 미중 등 주요국과의 역학관계에 긴밀히 연결된 국가안보적 함의도 내재하고 있다. 특히, LLM의 학습데이터, 알고리즘, 운영 서버가 특정 국가나 기업의 통제하에 집중될 경우, 데이터 주권의 문제뿐만 아니라 AI 생태계 전반의 종속 문제로 이어질 수 있다.

제3장 “AI 반도체와 사이버-공급망 안보”(오승희)는 AI 반도체 산업이 글로벌 공급망과 사이버 안보에 미치는 영향을 분석하였다. AI 반도체는 GPU, FPGA, ASIC 등 고성능 연산을 최적화하도록 설계된 핵심 기술로, 자율주행, 클라우드, 국방 등 다양한 분야에서 경제 성장과 국가 경쟁력 확보에 핵심적인 역할을 담당한다. 그러나 제조·유통 과정이 일부 국가와 기업

에 집중되어 있어 공급망의 복잡성과 기술 특성이 사이버 공격 및 기술 유출의 주요 취약점으로 작용한다. 미중 기술패권 경쟁과 수출 규제는 글로벌 AI 반도체 공급망의 불확실성을 심화시키며, 이에 대응해 일본, 대만, 한국 등 중견국은 전략적 기술 균형을 통해 산업 경쟁력 유지와 사이버 방어 체계 강화를 추진하고 있다. 일본은 TSMC 구마모토 공장 유치, 정부 보조금 지원, 능동적 사이버 방어 체계 구축 등을 통해 산업 부활과 공급망 안정화, 보안 강화를 동시에 모색하고 있다. AI 반도체 산업에서 발생할 수 있는 사이버 위협과 지적재산권 유출 문제는 공급망 전반의 보안 관리와 사이버 회복탄력성 확보를 통해 완화될 수 있다. 기업과 정부가 협력하여 보안 정책을 통합·강화할 때, 글로벌 기술 경쟁에서 전략적 우위를 확보하고 산업 및 국가안보를 보호할 수 있다.

제4장 "커넥티드카와 사이버 안보"(엄도영)는 전기차와 자율주행차 기술과 시장이 전 세계적으로 급격하게 성장함에 따라 각국에서 개인정보 보호, 사이버 보안, 국가안보의 관점에서 다양한 우려가 나오고 있다고 지적한다. 미국은 이 사안을 국가안보 위협으로 보고, 바이든 행정부 하에서 커넥티드카 관련 정보통신 기술 및 서비스 공급망 안보 규칙을 마련했고, 해당 최종 규칙은 트럼프 2기 행정부 출범 이후 발효되었다. 미국 커넥티드카 규제의 주 내용은 중국 또는 러시아와 연계된 하드웨어 및 소프트웨어의 미국 유입을 규제하는 것이다. 미국은 차량 사이버 안보를 규정하는 국제기준이나 표준만으로 우려국이 초래하는 국가안보 위협을 차단할 수 없다는 논리를 근거로 미국 공급망에 대해 해당국 연계 기업들을 선제적으로 차단하기로 한 것이다. 이 지점에서 사이버 안보와 공급망 안보 사이의 넥서스가 드러난다. 미국은 중국을 배제한 공급망 재편 방안을 모색하고 있으며, 트럼프 2기 행정부 출범 이후에는 관세 조치를 규칙 이행과 병행하면

서 통상 측면의 압박을 강화함으로써 자국 산업의 경쟁력을 높이려는 의도를 드러내고 있다.

2) 사이버-AI-데이터 안보 넥서스

제5장 "사이버-AI-인지 안보 넥서스"(송태은)는 개인과 사회, 국가 지도층이나 군 지휘부의 인지 과정을 교란하는 인지전이 전시와 평시를 가리지 않고 전개될 수 있는 오늘날의 정보커뮤니케이션 환경에서 국가는 개인의 인지 영역도 국가안보를 위해 보호할 대상으로 인식하게 되었다고 주장한다. 즉 사이버 공간에서 인간과 인공지능 기술이 실시간으로 유통시키는 정보와 커뮤니케이션 활동이 국가안보에 영향을 끼치면서 안보의 영역이 사이버 공간을 넘어 인지 영역까지 확대된 것이다. 육상, 해상, 공중, 사이버 공간과 우주공간을 넘어 인간의 마음까지 전장화되고 있다. 군사적 차원에서 오늘날 적을 기만하거나 아군의 정보 및 인지 역량을 강화하는 데에 있어서 인공지능과 사이버 기술은 결정적인 영향력을 발휘하기 때문에 국가 기능을 수행하는 데에 관여하는 다양한 인공지능 시스템이나 이러한 인공지능 시스템과 연결된 사이버 공간은 국가의 인지 안보를 위협하기 위한 주요 공격 대상이 된다. 사이버-AI-인지 영역이 인지 안보 넥서스를 구성하는 주요 노드가 되는 것이다. 사이버-인공지능-인지 영역의 인지 안보 넥서스는 인지 공격과 인지 역량 강화의 두 차원을 모두 포함하게 되며 그러한 넥서스가 어떻게 현실적으로 나타날 수 있는지는 슈퍼 솔저를 이용한 인지 우세 전략과 합성데이터를 이용한 기만전술을 통해 설명할 수 있다.

제6장 "국방 AI·데이터와 사이버 안보"(이종진)는 지능화된 전장 환경에서 AI와 데이터가 국방력과 사이버 안보의 핵심 경쟁력으로 부상하고 있음

을 강조한다. AI 기반 무인체계, 데이터 파이프라인, 클라우드 인프라 구축, 그리고 국가 주도의 R&D와 민군 협력의 필요성이 특히 두드러진다. 또한 제6장은 미국의 합동전영역지휘통제(JADC2) 체계, 국방부의 책임 있는 AI(Responsible AI) 전략, 대규모 클라우드 사업, 팔란티어와 안두릴 등 미국 신흥 방산 AI 기업들의 사례를 통해, 데이터 개방과 접근성 제고, 클라우드 인증 제도, 정보 등급별 분류·공유, 그리고 AI 위협에 대한 공격·방어 전략이 어떻게 논의되고 있는지 분석하였다. 동시에 데이터 포이즈닝 등 적대적 AI 위협과 연합학습·동형암호 등 차세대 보안기술의 필요성, AI 모델의 신뢰성과 윤리적 AI 거버넌스 확립 방안도 함께 제시하였다. 이를 실현하기 위해서는 국방 AI 데이터와 AI 개발 생태계의 혁신, 국제 협력과 표준화, 민간 역량의 적극 활용, 체계적 조직·제도적 지원, 그리고 AI 인재 양성이 핵심임을 논의하였다. 이를 토대로 국방 AI와 데이터 활용의 패러다임 전환, 민간 기술의 도입, 좀 더 근거 있는 보안·책임성 강화, 그리고 윤리적이고 투명한 거버넌스 체계를 수립함으로써, 한국 국방이 미래 전장에서 지능 우위와 함께 안정적인 사이버 안보를 실현할 수 있음을 제시하였다.

제7장 "데이터 첩보(DATINT)와 사이버 안보"(정태진)는 데이터 첩보가 인공지능, 빅데이터, 클라우드 기술을 기반으로 방대한 데이터를 수집·분석하여 정책결정과 안보전략을 지원하는 새로운 첩보 형태로, 기존 인적·신호 첩보를 대체하는 정보 패러다임으로 부상하고 있다고 주장한다. 데이터 첩보는 정보 정확도와 효율성을 제고하지만, 개인정보 보호, 데이터 주권, 알고리즘 편향 등 윤리·법적 쟁점을 동반한다. 주요국들은 각기 다른 방식으로 데이터 안보를 강화하고 있으며, 미국은 국가 통제 중심, EU는 개인정보보호 중심, 중국·러시아는 주권 통제 중심, 일본은 신뢰 기반의 데이터 이동 규범을 주도하고 있다. 정보기관은 데이터 분석 조직 신설, 민관협력

강화, 사이버 안보 통합이 요구되며, 정부는 데이터 거버넌스 구축, 인프라 투자, 전문인력 양성, 법·윤리 제도 강화, 국제협력 확대가 필요하다. 데이터 첩보는 국가정보 체계의 핵심축으로, 디지털 주권과 안보 경쟁력의 새로운 기반으로 평가된다.

3) 사이버-가상자산-플랫폼 안보 넥서스

제8장 "가상자산과 사이버 안보"(이왕휘)는 가상자산·암호화폐 생태계에서 비트코인뿐만 아니라 스테이블 코인과 중앙은행디지털화폐(CBDC)도 빠르게 발전하고 있다고 주장한다. 가상자산·암호화폐 생태계가 발전하는 데 가장 중요한 요인 중의 하나는 사이버 안보이다. 탈중앙화와 익명성을 기반으로 구성된 가상자산·암호화폐는 사이버 공격에 취약하다. 이런 문제를 해결하기 위해 정부·기업·개인은 사이버 안보를 강화하고 있다. 그럼에도 거래소에 대한 해킹도 빈번하며 자금세탁과 자본도피의 수단으로 활용되고 있다. 사이버 안보가 보장되지 않을 경우, 투자자의 신뢰가 하락하고 가격변동이 불안정하게 변동하여 가상자산·암호화폐의 발행과 거래는 위축될 것이다. 가상자산·암호화폐의 사이버 안보는 단순히 기술적인 문제를 넘어, 금융 시스템의 안정성과 국가안보에까지 영향을 미칠 수 있다. 개인·기업·정부가 유기적인 협력 체제를 구축해야만 사이버 공격의 위협을 최소화할 수 있을 것이다.

제9장 "이커머스와 사이버 안보"(김주희)는 중국 이커머스 플랫폼을 둘러싼 사이버 안보 및 개인정보 보호 이슈를 심층적으로 분석하고, 이에 대한 국내 대응 방안을 제시하였다. 최근 쉬인, 테무 등 중국 이커머스 플랫폼이 빠르게 성장하면서, 이용자 동의 없는 개인정보 수집·국외 이전, 데이터 관

리의 불투명성, 보안 취약점을 악용한 피싱·사기 연계 등 다양한 사이버 안보 리스크가 부각되었다. 따라서 중국 이커머스 플랫폼의 데이터 수집 및 국외 이전 현황, 개인정보보호 정책과 보안 관리 체계를 심도 있게 살펴볼 필요성도 높아졌다. 제9장은 주요 이커머스 플랫폼의 사이버 안보 관련 쟁점들을 논의하고 한국을 비롯한 주요 국가의 규제 및 감독 정책을 분석하였다. 중국 플랫폼의 개인정보 처리 관행은 개인정보보호법(PIPA)을 비롯한 국내 법제와 동의 절차, 국외이전 고지, 정보주체 권리 보장 측면에서 구조적 괴리를 보인다. 또한 데이터 저장 위치의 불명확성, 제3자 서비스(광고·트래킹 SDK 등)에 대한 관리 부재, 알고리즘 투명성 결여 등이 국내외 공통된 보안 취약 요소로 지적되었다. 제9장은 데이터 국외이전 사전영향평가의 실효성 강화, 플랫폼 사업자 대상 사이버 보안 인증 및 사전심사 제도 도입, AI 기반 이상징후 탐지 및 경보체계 구축, 이용자 중심의 정보통지 및 피해구제 절차 개선, 국제공조와 정보공유를 통한 규제 협력 확대 등의 다층적 대응 전략을 제안하였다.

제10장 "디지털 플랫폼과 사이버-데이터 안보"(김명하)는 소셜 미디어, 메신저, 동영상 스트리밍 서비스를 제공하는 디지털 플랫폼은 방대한 이용자 데이터가 모이는 온라인 공간의 안보에 주목하였다. 개별 정보의 축적은 빅데이터의 형성으로 이어지며 특정 집단에 대한 정보심리전, 영향력 공작을 가능하게 하면서 오늘날 국가안보의 위협으로 부상하고 있다. 특히 디지털 경제의 핵심 기술이 인공지능의 부흥은 데이터가 가지는 전략적 가치가 확대되고 있으며, 이에 주요국은 자국에서 생성된 데이터에 대한 통제권을 주장하는 '데이터 주권'을 내세우고 있다. 데이터 확보를 둘러싼 경쟁이 첨예해지면서 플랫폼은 사이버 공격에도 점차 취약해지고 있다. 악성코드, APT 공격 등을 통한 대규모 데이터 유출은 단순히 보안 체계의 결함을

넘어 국가안보의 문제로 격상되고 있다. 이러한 상황은 사이버-데이터 안보 간 넥서스화를 가속한다. 그런데 이는 비단 경쟁 관계에 있는 국가들만의 문제가 아니다. 데이터가 국가 안팎으로 유통되면서 주요국 간 데이터의 소유, 관리 주체에 대한 명확한 경계를 요구하는 목소리가 커지고 있다. 이에 따라 디지털 플랫폼은 경제 활동의 장을 넘어 국가안보와 직결된 전략 자산으로 기능하게 되었다.

4) 사이버-AI-핵-우주 안보 넥서스

제11장 "AI 기반 무기체계와 사이버 안보"(윤대엽)는 AI 기반 무기체계의 운용 기반으로 구축되고 있는 AI 디지털 아키텍처가 사이버 안보의 전환을 수반하고 있음을 분석하였다. AI 기반 무기체계의 활용을 위한 국방 인공지능 전환이 사이버 안보에 부과하는 전환적 특징은 세 가지이다. 첫째, AI 기반 지휘통제 체계(AI-C2)의 통합이다. 미국은 육해공 및 우주·사이버·전자기 영역을 통합하는 합동전영역지휘통제(JADC2) 체계를 구축하고, 플랫폼 운용성, 분산에 의한 회복력과 함께 공세적 사이버 전략을 구축하고 있다. 팔란티어는 데이터 융합 운용체계, 멀티 인공지능 플랫폼(AIP) 및 사이버 안보의 혁신 사례를 제공한다. 둘째, 공세적 사이버 안보 전략이다. AI 디지털 아키텍처에 대한 사이버 공격이 막대한 피해를 수반하게 됨에 따라 선제적, 능동적 방어 전략과 능력을 구축하는 한편, 다영역TF사단과 같이 사이버 능력을 부대 차원에서 통합하는 부대구조 혁신이 추진되고 있다. 셋째, 카운터 AI 전략과 비대칭 사이버 리스크도 증가했다. AI는 AI 디지털 아키텍처의 취약점을 발견하고 데이터 흐름을 마비, 교란, 파괴하거나 차단하는 지능화된 적대적 공격수단이 될 수 있다. AI 기반 무기체계의 효과

적인 운용을 위해서는 AI 디지털 아키텍처에 대한 포괄적인 사이버 안보 전략과 함께 비대칭 리스크에 대응하는 민군 통합방위 체계의 혁신이 중요하다.

제12장 "사이버-AI-핵 안보 넥서스"(이중구)는 미국, 중국, 러시아의 핵억제 체계에 AI가 어떻게 결합되고 있는지를 분석하고, 이를 통해 AI-핵 넥서스의 국가별 유형을 제시하였다. 미국은 감시정찰·조기경보·지휘통제 등 C4ISR에 AI를 적극 활용해 '거부 위주' 넥서스를, 러시아는 자동화된 보복 체계와 핵 탑재 무인체계 개발을 추진하면서 '보복 위주' 넥서스를, 중국은 양자를 병행하는 '복합형' 넥서스를 형성하고 있다. 사이버-AI-핵 넥서스에서는 AI-핵 넥서스가 사이버 공간과 결합하면서 감시·방어체계까지 사이버 공격의 대상이 될 수 있게 되었다. AI-핵 넥서스 별로 사이버 공격이 야기할 위협을 살펴본다면, 거부형에서는 억제실패, 오폭으로 인한 확전가능성, 보복형에서는 자동보복체계의 오인발사 위험과 핵탑재 무기체계의 탈취 가능성이 존재한다. 복합형에서는 이러한 두 가지 문제가 중첩된다. 한반도의 경우, 북한이 한정된 국가자원과 핵억제력의 취약성을 고려해 보복형 AI-핵 넥서스를 구축할 가능성이 높다. 이 경우 보복형 AI-핵 넥서스가 갖는 문제인 오인발사와 통제실패의 위험이 제기될 것이다.

제13장 "사이버-우주 안보 넥서스"(이수연)은 사이버와 우주라는 두 개의 영역이 상호 의존하는 복합적인 안보 구조를 의미한다고 주장한다. 이 넥서스를 관통하는 것은 데이터 안보이며, 사이버-우주 안보 넥서스를 위협하는 것은 궁극적으로 데이터 안보에 대한 위협으로 귀결된다. 두 영역을 매개하는 데이터의 흐름은 최근 저궤도 군집위성이라는 인프라를 중심으로 이루어지며, 이러한 우주 기반 통신 인프라는 사이버 공격의 주된 표적이 된다. 사이버-우주 안보 넥서스에 대한 위협은 지상-우주, 우주-우주, 우

주-지상에서 데이터의 기밀성, 무결성, 가용성을 침해하는 양상으로 나타난다. 또한 스타링크 사례에서 확인할 수 있다시피, 뉴스페이스 시대가 도래함에 따라 민간 기업이 구축한 통신 인프라에 대한 의존도가 심화하면서 안보가 민간 기업의 의사결정에 종속되어 국가의 통제력을 벗어날 수 있는 위협이 발생하게 되었다. 이에 더하여, 사이버와 우주 영역에 대한 국제규범이나 제도가 별도로 형성되어 있어 두 영역을 복합적으로 고려한 규범이나 제도의 공백이 존재한다는 것도 위협요인이 될 수 있다. 사이버-우주 안보 넥서스의 상황 자체가 최근의 현상이기에 이것에 대한 깊이 있는 논의가 부재한 상황 속에서 인공지능이라는 기술 변수의 등장으로 사이버-우주 안보 넥서스는 사이버-우주-AI 안보 넥서스라는 도전과제에까지 직면하게 되었다.

5) 사이버-AI-외교-규범 안보 넥서스

제14장 "사이버-AI 넥서스와 미국의 동맹외교"(신승휴)는 사이버-AI 넥서스로 인해 여느 때보다 국제협력의 중요성이 커지는 상황에도 불구하고 사이버 안보와 AI 분야 미국의 전략은 거래적인 국제협력을 선호하는 방향으로 점차 나아가고 있다고 주장한다. 이에 주목하여 제14장은 사이버-AI 넥서스에 대한 미국의 대응 역시 가치 중심의 동맹에 기초한 포괄적·통합적 협력에서 점점 더 멀어지고 있음을 지적하였다. 이러한 시각을 뒷받침하기 위해 제14장은 트럼프 2기 행정부가 사이버 안보와 AI를 위한 국제협력에 어떻게 접근하고 있는가를 살펴보았다. 구체적으로 사이버 안보와 AI 전략에 담긴 국제협력의 기조, 이니셔티브, 플랫폼 그리고 추진체계의 내용을 검토하여 그 안에서 발견되는 특징을 분석하였다. 이를 바탕으로 미국의

동맹외교가 다양한 영역에서 발생하는 사이버-AI 넥서스 문제들에 어떻게 접근하고 있는지 그 추이를 포착하고자 했다.

제15장 "사이버-AI 넥서스와 중국의 연대외교"(박병광)는 중국의 디지털 실크로드 전략이 사이버 및 인공지능 영역에서 어떻게 전개되고 있는지를 주요 쟁점과 도전 요인을 중심으로 살펴보았다. 중국은 디지털 실크로드를 통해 사이버와 AI를 전략 핵심 축으로 삼고 있으며, 이들 분야의 국제규범 형성에도 적극 개입하고 있다. 중국은 사이버 공간을 단순한 기술 기반이나 경제 활동의 장이 아닌, 국가 안보·정치 체제·사회 안정과 직결된 전략 자산으로 인식하고, AI를 미래 성장 동력이자 국제질서에서 영향력 확대의 수단으로 활용하고 있다. 주요 쟁점은 '디지털 주권'과 '글로벌 규범'의 충돌, 그리고 AI의 군사적 활용 문제다. 또한 중국의 AI·사이버 외교는 기술 표준 경쟁과 산업 주도권 확보를 둘러싸고 논란을 낳고 있다. 그러나 중국은 기술 신뢰성 한계와 국제사회의 정치적 불신이라는 도전에 직면해 있다. 결국 중국의 사이버-AI 연대 외교는 기술·군사·규범을 아우르는 복합 전략이며, 국제사회는 이를 협력의 기회로 볼지, 디지털 권위주의 확산의 위험으로 볼지를 신중히 판단하고 있다.

제16장 "사이버-AI 넥서스와 국제규범 형성"(유준구)은 기술의 연계·융합적 성격으로 인해 사이버-AI 넥서스와 같은 신흥기술 간 연계된 안보 위협의 증대되고 있다고 주장한다. 신흥기술 간 연계·융합으로 인해 기존 사이버 안보 국제규범 형성 논의는 복잡해지고 있다. AI의 규범 논의는 이제 막 시작되고 있는 상황으로 사이버-AI 넥서스 국제규범 형성 과정은 여러 난제를 해결해야 과제가 안고 있다. 현 단계에서는 AI 기반 사이버 안보 위협에 대한 논의를 중심으로 국제규범 논의가 본격적으로 전개될 가능성이 높다. 이 경우 사이버-AI 넥서스로 인한 위험 및 위협에 대한 확인과 이에 대

한 대응 차원의 국제규범 형성 작업이 향후 유엔을 중심으로 전개될 것으로 전망된다. 본격적인 사이버-AI 넥서스 규범 형성 논의가 전개될 경우, AI 기술의 이중 용도와 관련한 상업적 이용과 군사적 이용 간 분리된 형태의 국제규범 논의가 점차 국제안보 맥락에서의 논의로 수렴될 가능성이 높다. 또한 현재 파편적인 국제규범 논의가 진행되고 있는 AI의 하위시스템인 데이터, 컴퓨팅, 알고리즘/모델에 대한 국제규범 논의 역시 사이버-AI 넥서스 규범 논의의 일부 포함되어 논의될 것으로 예상된다. 사이버-AI 넥서스로 인한 위협이 고도화되고 국제규범 형성 논의도 본격적으로 시작될 것이므로 이에 대한 국가전략 차원의 대응을 준비해야 할 것이다.

4. 사이버 메타 거버넌스의 모색

이상에서 살펴본 바와 같이 넥서스를 형성하며 점점 더 교묘해지는 사이버 안보 위협에 직면하여 이를 완전무결하게 막아내기는 어렵다. 모든 시스템이 취약점을 안고 있고 그것을 공격하는 악의적 시도를 완전히 근절하기는 어렵기 때문이다. 게다가 그러한 위협을 가하는 주체를 추적해서 확인하고 그 책임을 귀속하기도 쉽지 않다. 그야말로 사이버 공격은 마치 보이지 않는 위협으로서 '버추얼(virtual) 창'의 공격을 방불케 한다. 여기에 AI 기술의 가세로 인해서 사이버 복합 넥서스의 위협은 점점 더 '보이지 않는 방식'으로 감행되고 있다. AI로 강화된 버추얼 창을 막는 데 필요한 것은, 철벽방어를 목표로 '벽돌집'을 짓는 전통적인 안보 발상이 아니라, 나뭇가지 하나하나를 모아서 '그물망'을 짜는 것과 같은 신흥안보의 복합적인 발

상이다. 새로운 사이버 거버넌스의 발상으로서, 이른바 '그물망 방패'에 대한 논의가 제기되는 것은 바로 이 대목이다(김상배, 2018).

이러한 맥락에서 볼 때, 사이버 복합 넥서스 시대에는 사이버 위협은 제기되더라도 적절한 수준에서 관리되는 상태를 유지하는 새로운 개념의 거버넌스 개념이 필요하다. 일차적으로 넥서스를 이루는 사이버 위협이 증폭되지 않고 이에 대한 억제가 가능하도록 창발의 고리를 미리 끊는 것이 중요하다. 이렇듯 양질전화를 막고 이슈연계를 끊고 국가 간 지정학적 분쟁의 발생을 미연에 방지하는 것이 사이버 안보 거버넌스의 일차적 목표일 수밖에 없다. 그러나 여기서 더 나아가 창발과 환원의 연결고리. 즉 넥서스를 공략하여 원상태의 메커니즘을 회복하는 노력이 병행돼야 한다. 사이버 위협이 양질전화-이슈연계-지정학의 임계점을 넘어 창발하지 못하도록 환원적 제어가 꾸준히 부과되어, 시스템이 지속적으로 작동할 수 있게 유지하는 것이 넥서스 시대 사이버 안보 거버넌스의 요체이다.

사이버 안보 위협에 맞서는 거버넌스의 역할을 이해하기 위해서 복잡계 이론에서 거론하는 이른바 '속도조정자(pacemaker)' 또는 '유인자(attractor)'의 개념에 주목할 필요가 있다(김상배, 2023). 전통안보 분야에서는 전쟁을 막는 '평화조정자(peacemaker)'의 역할이 중요했다면, 신흥안보로서 사이버 안보 분야에서는 그 창발-환원의 연결고리를 공략하여 원래의 메커니즘을 회복하도록 나서는 속도조정자의 역할이 중요하다. 이 과정에서 속도조정자는 인격적 존재가 아니라, 네가티브 피드백과 포지티브 피드백이 교차하는 지점에 제도적으로 설계된 존재일 수 있다. 예를 들어, 페르 박(Per Bak)이 소개하는, 조직화된 무작위, 이웃간 상호작용, 분권적 제어, 메타 피드백(meta-feedback) 등의 개념에 주목할 필요가 있다(페르 박 2012).

이렇게 제도적으로 설계된 속도조정자로 거론되는 대표적 사례가 '네트

워크 국가(network state)'이다. 네트워크 국가의 개념은 영토적 경계의 안과 밖으로 다양한 비국가 행위자들과 네트워크를 형성하여 새롭게 제기되는 국내외적 도전에 대응하는 새로운 국가 모델에 대한 논의이다(하영선·김상배 편, 2006). 사이버 공간의 구조적 속성상 사이버 위협에 대한 대응은, 수평적 네트워크의 형태로 활동하는 비국가 행위자들과 밀접히 협력하는 동시에 다양한 수단들을 적재적소에 유연하게 동원하는 국가의 역할이 요구되는 분야이다. 실제로 사이버 복합 넥서스는 이러한 국가의 유연한 기능이 필요한 대표적인 분야이다. 이러한 거버넌스를 위해 동원하는 수단이라는 면에서도 기술과 인력, 국방의 역량을 강화하는 것뿐만 아니라 법제도 정비와 국제협력 등을 포괄하는 복합적인 대응이 필요하다. 이러한 과정에서 해당 당사자들이 담당할 수 없는 '구조적 공백'을 메워주는 네트워크 국가의 총괄·조정기능이 중요하다.

이러한 맥락에서 볼 때, '메타 거버넌스(meta governance)'는 속도조정자로서 네트워크 국가가 수행하는 역할을 잘 제시한 개념이다. 밥 제솝(Bob Jessop)이 주장하는 메타 거버넌스는 다양한 거버넌스 메커니즘들 사이에서 상대적 균형을 모색함으로써 그들 간의 우선순위를 조정하는 관리양식을 의미한다(Jessop, 2003). 메타 거버넌스는 시장의 무정부 질서(anarchy), 국가통제의 위계질서(hierarchy), '거버넌스'의 다층질서(heterarchy) 등이 내재적으로 안고 있는 실패를 바로잡기 위해서 동원되는 '거버넌스의 거버넌스'이다. 다시 말해, 메타 거버넌스는 국가가 사안에 따라 그 개입의 수준을 적절하게 조절하는 방식으로 여러 가지 거버넌스를 동시에 운용하는 관리양식으로 정의할 수 있다. 이러한 메타 거버넌스의 개념을 사이버 복합 넥서스에 대응하는 네트워크 국가의 역할에 대입해 볼 것을 제안한다.

이러한 역할과 관련하여 마지막으로 강조하고 싶은 것은, 사이버 안보의

특성상 사전적 예방과 방어만큼이나 사후적인 복원력(resilience)이 중요함을 놓치지 말아야 한다는 점이다. 복원력은 '위험으로 변화된 환경에 적응하여 지속가능한 상태로 스스로 재구성해 나가는 역량'을 의미한다. 복원력은 메타 거버넌스의 역량과 결합하여 위협 발생에 적합한 새로운 거버넌스를 창출하는 데 기여한다. 위협을 예측하는 것이 불가능한 사이버 안보 위협의 특성상 이 분야의 거버넌스에서는 사후적인 복원력을 갖추는 것이 중요하다. 즉 시스템 외부의 충격을 받아 원래의 균형으로 회복하지 못해도 시스템의 핵심 기능을 보완할 수단을 찾거나, 시스템의 정체성을 상실하지 않을 정도로 다른 기능적 대안들을 발굴하는 역량이 필요하다(Tierney and Bruneau, 2007).

제2장

AI 모델과 사이버 안보

윤정현 | 국가안보전략연구원 연구위원

제2장

AI 모델과 사이버 안보

윤정현 | 국가안보전략연구원 연구위원

1. 서론

오늘날 인공지능(AI)은 하나의 특정 기술 품목을 넘어서, 디지털 사회의 발전을 이끄는 핵심 인프라로 자리잡고 있다. 이는 AI가 경제, 산업, 사회 전반에 광범위하게 활용되며, 혁신을 불러일으키고 새로운 성장의 흐름을 창출하기 때문이다.[1] 실제로 AI는 '침투성(pervasiveness)', '향상성(improvement)', '혁신창출성(innovation spawning)'이라는 공통된 특성을 지니고 있으며, 최근 CES가 2년 연속 AI를 중심 주제로 삼은 미래 청사진에서 언급된 바와 같이 대부분의 신기술은 AI를 매개로 발전하고 있다. 이른바 'AX(인공지능 기반의 디지털 대전환)' 시대가 본격적으로 전개되고 있는 것이다.[2] AI와

1) 윤정현, "미중 강대국 AI 질서와 한국의 중견국 외교전략" 『21세기 정치학회보』, (2025년 9월), 제35집 3호. pp. 133-163.

2) 사실 AX라는 용어는 '가속화된 경험(Accelerated Experience)', '에이전트 경험(Agent Experience)', '인공 경험 디자인(Artificial Experience Design)' 등 다양한 맥락에서 사용되어 왔으

의 융합을 통해 진정한 디지털 혁신의 의미가 실현되는 AX 환경은 특히 AI 반도체, 합성생물학, 6G통신, 양자정보과학 등 핵심·신흥기술(critical and emerging technologies)들과 만나면서 새로운 기술적 돌파구를 열어나가고 있다.

일상에 스며든 AI의 활용 혁신은 어떠한가? 최근 생성형 인공지능(Generative AI)이 등장하면서 일상에서의 AI의 진입 장벽은 낮아지는 한편, 활용 범위는 대폭 증대되었다. 방대한 데이터를 사전학습(pre-train)하고, 이를 바탕으로 사용자가 원하는 창작물을 생성해내는 인공지능 모델인 생성형 AI는 텍스트, 이미지, 음악 등 다양한 형태의 이종적 콘텐츠 생산에 활발히 활용되고 있다.[3] 오픈 AI의 'Chat GPT'를 필두로, 구글의 'Gemini', 메타의 'Llama', 네이버의 'Clova x' 등 혁신적인 생성형 AI 모델이 연이어 나타났으며, AI가 사회 전반의 '일상기술(daily technology)'로 자리매김하는 중대한 동력으로 기능하였다.

생성형 AI 혁신을 언급할 때 빼놓을 수 없는 것은 바로 '(초)거대언어모델(Large Language Model, LLM)'이다. 생성형 AI가 보다 창의적이고 정교한 콘텐츠를 구현하는 한편, 기술적 진보를 이루기 위해서는 LLM을 기반으로 한 패턴 학습이 필수적이기 때문이다. 2022년 ChatGPT가 전 세계적인 주목을 받았던 것도 당시 오픈 AI가 개발한 GPT-3.5라는 LLM 학습에 있었

며, 각 맥락은 AI 기술발전이 초래하는 다면적인 경험의 측면들을 반영한다.
https://www.theax.ai/blog/ushering-in-the-new-age-of-accelerated-experience-%28ax%29-driven-by-ai;
https://biilmann.blog/articles/introducing-ax/; https://ax.dev/docs/why-ax/

3) https://www.samsungsds.com/kr/insights/generative-ai-trends.html

다. 기존의 단답형 AI 서비스와 달리 사용자와의 대화를 기억해 소통을 이어갈 수 있었던 ChatGPT는 인간과의 자연스러운 대화의 스킬을 익혔으며, 질문마다 능숙한 전문가처럼 대답하고 결과물을 산출할 수 있었다. 이처럼 향상된 기능에 따른 사용자들의 관심으로 ChatGPT는 2024년 8월 기준 전세계 주간 사용자 수 2억 명을 기록한 바 있다.[4] 2025년 1월 기준 국내의 ChatGPT 사용자는 약 682만명에 달했으며 이외에도 에이닷(245만명), 뤼튼(232만명), 퍼플렉시티(59만명), 코파일럿(31만명), 클로드(12만명) 등의 생성형 LLM 기반 AI를 사용한 것으로 나타난 바 있다.[5]

그러나 LLM 기반의 생성형 AI는 편향과 환각 등 잘못된 정보의 산출 문제를 내재하고 있으며, 알고리즘 모델의 악용 이슈, 데이터 유출, 안정성 확인 미흡, 해커 공격 범위 확장 등 사이버 공격에 대한 다양한 취약점이 존재한다. 특히, 악의적인 지시를 충분히 검토하지 못하고 반영한 결과물을 제공하기 때문에 선동적 콘텐츠에 기반한 가짜뉴스 등 비합리적인 의사결정과 사회적 혼란을 야기할 수 있는 위험을 안고 있다.

이러한 가운데, 지난 1월 20일 출시된 중국의 생성형 AI인 'DeepSeek R1'모델의 등장은 글로벌 LLM 기반 생성형 AI 시장 질서에 갖는 파급력뿐만 아니라 사이버 안보 측면에서도 주목해야 할 도전적 함의를 갖는다. ChatGPT 등 기존 LLM 기반 생성형 AI 모델이 갖는 사이버 보안의 취약성 뿐만 아니라, 민감 데이터의 무분별한 수집 가능성, 중국 정부로의 유출과 악용 가능성, 답변의 정치적 편향성 등 추가적인 위험성을 내포하고 있

4) https://www.yna.co.kr/view/AKR20240830075200009

5) https://www.newsis.com/view/NISX20250107_0003024188

기 때문이다. 또한 미중 AI경쟁 측면에서 볼 때, 개도국 등에 대한 글로벌 영향력 확대와 표준 선점 문제 또한 얽혀있다. 이 같은 쟁점들은 향후 LLM 기반 생성형 AI 시대의 사이버 보안 이슈를 넘어 양국 간, 진영 간의 안보 문제로 비화될 가능성이 높으며, 파급효과의 복합성에 대해 면밀한 검토가 필요한 상황이다.

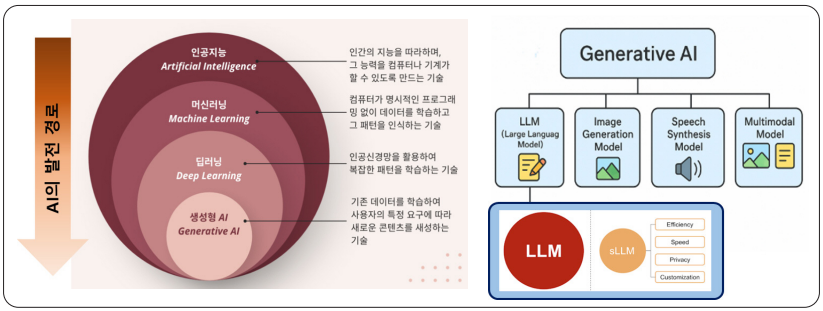
2. LLM 시대의 AI-사이버 안보 넥서스

데이터와 패턴을 학습해 프롬프트(자연어 처리)에 대응하여 새롭고 독창적인 콘텐츠를 만들어내는 생성형 AI는 앞서 딥러닝 기술과 그 이전 머신러닝의 비약적인 발전 속에 등장하였다. 이와 함께 대규모 텍스트 데이터를 학습할 수 있는 컴퓨팅 파워의 증가, 그리고 자연어 처리(NLP) 분야의 혁신이 핵심적으로 작용했다. 특히 2018년 구글이 발표한 BERT와 이후 OpenAI의 GPT 시리즈와 같은 대규모 언어 모델(LLM)의 등장은 AI가 문맥을 이해하고 자연스러운 문장을 생성할 수 있는 기반이 되었다. 다양한 생성형 AI 중 한 가지 하위분야인 LLM은 방대한 텍스트 데이터를 학습하여 언어를 이해하고 생성할 수 있는 AI 모델로 기능하고 있다.

대규모 텍스트 데이터를 학습하여 자연어를 이해하고 생성할 수 있는 LLM은 주로 딥러닝 기술을 사용하여 구축되며, 수십억 개의 파라미터를 포함한다. 특히, 이들은 문장 완성, 번역, 요약을 넘어 다양한 자연어 처리 작업에 활용될 수 있는 능력을 입증했다. 이를 토대로 생성형 AI는 단순한 자동화 도구를 넘어 창작과 의사소통의 영역까지 확장되었고, ChatGPT의

성공을 기점으로 본격적인 AI 대중화를 낳게 된 것이다. 최근에는 거대언어모델보다 작은 규모로 균형 잡힌 성능과 자원을 기반으로 효율을 내는 '소형 언어모델(Small Large Language Model, sLLM))도 주목받고 있다. sLLM은 매개변수 수가 수십억에서 수백억 개로 정도로 거대언어모델보다 작은 규모이나, 학습 비용과 시간을 절감할 수 있고 미세조정을 통해 특정 분야에서는 대형 모델과 비슷한 성능을 낼 수 있는 실용성 모델이다.[6] 특히 적절한 성능을 구현하기 위한 효율적인 자원 사용에 강점을 갖고 있어 많은 각광을 받고 있다. 최근에는 온디바이스 AI의 수요 증가로 각광받고 있다. LLM은 학습 데이터가 많을수록 더 세밀하고 인간의 사고 과정과 유사한 언어 처리가 가능하다. 생성형 AI는 이처럼 LLM을 기반으로 콘텐츠를 생성하며 두 기술은 다양한 산업 분야에서 혁신적인 솔루션을 만들어내며 상호보완적으로 발전해 왔다.

〈그림 3-1〉 AI의 발전경로와 생성형 AI 내 LLM



출처: Superb AI, (Aug 26, 2024)를 토대로 재구성

6) https://m.boannews.com/html/detail.html?idx=121029

GPT4.0/4.5, DeepSeek 등 최근 출시되고 있는 LLM 서비스들은 텍스트 데이터뿐만 아니라 이미지와 음성 등 다양한 형태의 데이터로 입출력이 가능한 '멀티모달(multimodal)'[7] 기능을 탑재하고 있어 다양한 형태의 창작을 보여주기도 한다. 즉, 하나의 모델이 처리할 수 있는 데이터의 종류에 제한이 점점 사라지면서 이미지와 텍스트 등 생성형 AI 간 구분의 경계는 점점 사라지고 있는 추세이다. 딥러닝까지는 주로 특정 작업에 특화된 모델들(ex. 이미지 분류기, 음성 인식기)이었으나 GPT, BERT, T5 같은 LLM이 등장하면서 마치 인간과 같이 다양한 작업을 동시에 수행하는 다차원적 작업 가능하게 된 것이다.

그러나 이러한 기술 확산은 긍정적 가능성만큼이나 심각한 역기능의 소지도 함께 내포하고 있다. 생성형 AI는 악의적인 목적에 따라 사회적으로 오용될 수 있음을 보여준 바 있다. 허위 정보(Disinformation)나 가짜 뉴스(Fake News)의 자동 생성 및 확산을 통해 여론 조작, 사회 혼란, 민주주의 질서 훼손의 위협은 문제는 이미 많은 자유민주주의 국가에서 제기되었으며, 생성형 AI를 기반으로 설계한 고도화된 사이버 해킹 수단 위협 시급한 도전으로 인식되고 있다. 특히, 생성형 AI 환경에서는 데이터 보안이 더욱 중요한 이슈가 되었다. 예를 들어, 태그 지정에 사용되는 구조화되지 않은 데이터에는 번호판, 얼굴, 민감한 의료 정보 등 개인 식별 정보가 포함되어 있어 적절하게 보호하지 않으면 심각한 데이터 유출로 이어질 수 있기 때문

7) 텍스트, 이미지, 오디오, 비디오 등 다종의 데이터를 함께 고려하여 서로의 관계성을 학습 및 처리하는 인공지능으로 이 중 상대적으로 크기가 큰 모델을 "거대 멀티모달 모델" 혹은 "대형 멀티모달 모델(Large Multimodal Model: LLM)"로 지칭한다.
https://kanerika.com/blogs/multimodal-models/

이다.

실제로 LLM 기반 생성형 AI는 상시적 Prompt Hacking의 위험성 및 편향성과 환각을 비롯한 한계점을 내재하고 있다. 이에 더하여, 소프트웨어 취약점을 노리는 기존 해킹과 달리 프롬프트 해킹은 프롬프트를 조작하여 LLM을 악용함으로써 의도하지 않은 동작을 유발한다. 악성 또는 의도하지 않은 콘텐츠를 추가하여 언어 모델의 출력을 탈취하는 'Prompt Injection'과 GPT와의 대화 과정에서 입력한 사용자의 민감정보를 즉각적으로 삭제하지 못함으로써, 향후 사용자도 모르는 다른 대화에서 다른 목적으로 활용될 가능성이 있는 'Prompt Leaking' 또한 존재한다. 전자가 악성 또는 의도하지 않은 콘텐츠를 추가하여 언어 모델의 출력을 탈취하는 것이라면, 후자는 GPT와의 대화 과정에서 사용자의 민감한 정보가 즉각적으로 삭제되지 않아, 향후 사용자도 모르는 다른 대화에서 다른 목적으로 활용될 가능성을 의미한다.

그리고 충분한 학습 데이터나 최신 데이터 업데이트 없이 치우친 잘못된 정보를 마치 사실인 것처럼 답변하는 '환각(Hallucination)' 문제는 생성형 AI 모델에서 더욱 빈번히 발생한다. 특히, 90%의 사실과 10%의 거짓을 조합하는 방식으로 콘텐츠를 생성하기 때문에 그럴싸한 정보로 포장하게 되며, 이에 대한 잘못된 믿음과 확신을 강화시킨다. 이처럼 어느 한 주입 단계에서 논리적 오류가 발생하면 다음 단계를 거치면서 더 큰 오류를 초래할 수 있기 때문에 환각은 다단계 추론이 필요한 영역에서 특히 문제를 초래한다.

생성형 AI가 악의적 시도에 따른 거짓·유해 정보 제공과 사이버 공격의 고도화 수단으로 활용되는 점도 주목할 만하다. 생성형 AI는 유해하고 악의적인 지시를 충실히 반영한 결과물을 제공할 수 있는데, 이는 선동과 여

론 형성을 통해 민감한 정치 국면에서 비합리적인 의사결정과 사회적 혼란을 야기할 수 있다. 더불어 텍스트, 이미지, 음성, 영상을 결합한 소셜 엔지니어링 기법을 사용하여 피싱 공격력을 극대화한다. 이것의 대표적인 사례로는 러우 전쟁 과정에서의 거짓 항복 선언 영상과 2022년 5월 '펜터곤 폭발 사건' 가짜 뉴스로 인해 S&P 지수가 30포인트 폭락한 사례 등이 있다.

또한 알고리즘의 입력과 작동이 항상 가시적인 것은 아니기 때문에 해당 모델 개발에 사용된 데이터의 신뢰성 평가 등에 대한 감독을 회피할 수 있는 가능성도 존재한다. 게다가 랜섬웨어 등 지능형 사이버 공격에 생성형 AI가 악용될 가능성도 있으며, 이로 인해 민감한 정보 및 훈련 데이터의 유출, 데이터의 불법 처리 등과 같은 신종 사이버 공격 도구로 사용될 수 있는 위험이 증가하고 있다. 특히, 다크웹 공간에서 챗GPT 기반의 새로운 악성코드를 생성할 수 있는 사이버 알고리즘의 출현이 우려되고 있다.

〈표 3-1〉 생성형 AI 보안이슈가 초래하는 사이버 보안 위협 요소

취약점	촉발경로	예상피해
AI 모델 악용	• 적대적 시스템 메시지	– 유해한 답변과 오인식 만연 – 가짜뉴스로 인한 비이성적 여론 형성과 사회적 혼란, 잘못된 의사결정 유도
유사AI 모델 서비스 빙자	• 유자 악성 서비스 접근 유도	– 신뢰할 수 있는 ai이름을 도용한 스쿼팅 URL, 가짜 앱을 통한 개인정보 대량 유출
데이터 유출	• 데이터 합성 과정의 문제 • 과도한 훈련 데이터 암기문제 • 대화 속 개인정보 등 민감정보 작성	– 민감한 훈련 데이터나 기밀 유출 – 데이터베이스 해킹시, 과거 이요자 중 주요 대상에 대한 표적 추론공격도 가능

취약점	촉발경로	예상피해
플로그인 취약점	• AI 모델의 적용 범위 확장 • 안정성 확인 미흡 • 해커 공격 법위 확정 • 취약점이 있는 서비스와 연결	- 에이전트화된 AI를 악용한 악성코드 전파 - 새로운 도메인에서의 모델 오작동 유도 - 취약점 서비스와의 연결을 통한 해커의 공격 범위 확장
확장 프로그램 취약점	• 확장 프로그램 내 악성서비스 설치 • 서비스 제공업체의 보안조치 미흡	- 사용자 권한을 남용한 사용자 시스템 공격 - 대량 좀비PC 생성 및 DDos 피해 발생 - 호스팅 서버 및 스토리지 시스템 위협
API 취약점	• 미흡한 API 관리 • 제어 불가한 악의적 프롬프트 주입	- 인증수단 약화로 데이터 및 시스템 보안 피해 - 위해 알고리즘, 불법적 무기제조 설계 등

출처: NIIS·NSR(2023), "챗GPT 등 생성형 AI 활용 보안 가이드라인" 기반으로 재구성

3. 딥시크의 충격과 사이버 안보의 도전 과제

이 같은 상황에서 등장한 중국의 스타트업 '딥시크(DeepSeek)'의 AI 모델은 글로벌 생성형 AI 시장 지배구도의 변화뿐만 아니라 사이버 안보의 새로운 도전 가능성을 제기하고 있다. 트럼프 대통령의 재임 첫날인 지난 1월 20일 발표된 '딥시크-R1(DeepSeek-R1)'은 애플 앱스토어 출시 일주일 만에 오픈 AI의 챗GPT를 밀어내고 무료 앱 다운로드 1위에 올라서는 돌풍을 일으킨 바 있다. 특히, 딥시크-R1 추론 모델은 일부 성능 테스트에서 오픈 AI가 2024년 9월 출시했던 논리적 추론이 가능한 최신 모델 'o1'보다도 앞선 것으로 나타나 시장을 충격에 빠뜨렸다. 미국의 첨단 반도체 수출통제에도 불구하고 저사양 연산장비의 효율적인 활용과 오픈소스 전략을 통해 고비

용 AI 모델에 필적하는 결과물을 보여주었기 때문이다.[8)]

딥시크의 주장에 따르면 이번에 출시한 '딥시크-R1'은 불과 560만 달러(오픈AI의 투자 비용 대비 약 5.6%)의 저비용으로 개발한 모델이지만, 각종 벤치마크에서 높은 등급을 받아 안정적 성능을 확보한 것으로 알려졌다. 주목할 부분은 하드웨어 측면이다. AI 모델 구현에 필요한 엔비디아의 고성능 GPU(H100)는 이미 수출통제 품목에 해당하기 때문에 딥시크는 저사양의 GPU(H800)를 활용했는데, 모델구조 최적화를 통해 메모리 대역폭과 처리능력의 제한점을 개선했고, 결과적으로 고가의 GPU 의존도를 줄일 수 있었다. 소프트웨어 측면에서도 딥시크는 기계가 데이터를 생성하고 스스로 학습하는 강화학습 단계의 효율화에 집중함으로써 모든 매개변수를 한꺼번에 활성화시키지 않고 필요한 부분만 작동시키는 '전문가 혼합(Mixture of Experts)' 방식을 적용하였다. 그 결과 에너지 소모량을 대폭 낮춤으로써 전통 모델의 학습·추론 비용을 절감한 것으로 알려졌다.

딥시크는 이렇게 구현한 R1 모델을 오픈소스로 공개했는데, 이는 다른 개발자들이 R-1 AI를 라이센스를 자유롭게 활용하면서 문제점 개선에도 일조할 수 있도록 허용한 것이다. 이는 소스코드나 모델 규모 등을 비공개하고 있는 오픈 AI나, 주력 모델이 아닌 의도적으로 낮춘 저사양 모델의 소스만을 공개하고 있는 구글, 메타의 행보와 대별된다. 이 같은 딥시크 AI의 자원 활용과 공개 방식은 기존의 AI 지배기업들이 구축해 왔던 고비용 투자 방식과 폐쇄적 운영 구조와 상반된 접근을 보여준 것으로 평가되었다.

물론, 서방은 첨단 반도체 기술의 수출 통제가 여전히 강고한 상황에서

8) 윤정현, "딥시크: AI 시대의 스푸트니크 쇼크인가?" 『ISSUE BRIEF』, 제665호 (2025. 3. 4.).

어떻게 중국이 국내 인재 양성만으로 이를 돌파했는지 의구심을 표하고 있다. 중국이 이른바 편법적인 '회색거래 네트워크'를 구축하고 싱가포르 등 우회국을 통해 고사양 반도체를 은밀히 사들이거나 다른 국적의 리브랜딩 사명으로 서버를 구축한 뒤 이를 활용하고 있다는 주장도 제기되었다. 하지만 중국이 낮은 수준의 범용에서부터 중간 미세공정까지 점진적으로 국산화하고 있다는 사실은 무시할 수 없는 부분으로, 광범위한 내수 시장을 바탕으로 끊임없이 활용·개선된 결과로서 나타난 딥시크는 'AI 시대의 스푸트니크 쇼크'로 비유되기까지 하였다. 보다 중요한 점은 중국 정부가 이번 사건을 계기로 향후 AI 개발 계획을 가진 글로벌 사우스 국가들에게 딥시크로 상징되는 중국식 저비용, 고효율 AI 표준을 전파하는 기회로 활용할 수도 있다는 점이다. 실제로 지난 2월 6일 러시아 최대 은행인 스베르은행이 국영은행에서 AI 기업으로 변신하고자 중국 연구자들과 공동 연구 프로젝트 계획을 발표한 것이 대표적이다.

딥시크가 미국 언론의 집중적인 조명을 받자 트럼프 대통령까지 나서서 "딥시크 출시가 미국 기업들에 대한 '경종(wake up call)'이 될 것이며, 중국과의 경쟁에 승리하기 위해 더욱 혁신에 집중할 필요가 있다"고 언급한 바 있다. 그러나 미국이 가장 먼저 시작한 조치는 데이터 보안을 위해 군과 정부 공공기관 네트워크에서 딥시크를 차단한 일이었다. 이어 EU 국가들과 일본 역시 민감한 보안 문제를 우려하며 공공 사이트에서 딥시크 사용을 제한하였고 한국 정부 행안부의 권고를 시작으로 제한 조치를 시행한 바 있다.

〈표 3-2〉 주요국별 딥시크 차단 및 자제 권고 조치 사항

국가	제한 내용
미국	- 국방부와 해군, NASA 등 일부 연방 기관에서 딥시크 사용 금지(1. 28) - 기존 전략물자 대중국 수출통제 범위 밖에 있던 품목(엔비디아의 저사양 AI 반도체 등)에 대해서도 추가 규제 방안 공론화 시작(1. 28) - 텍사스 주정부, 딥시크 사용금지(1. 31)
유럽연합(EU)	- 이탈리아 데이터 보호 당국, 딥시크 챗봇 서비스 및 애플리케이션 신규 다운로드 차단(1. 29) - 아일랜드 데이터보호위원회, 딥시크에 아일랜드 사용자와 관련 데이터 처리 정보 요청(1. 29) - 프랑스 개인정보보호위원회, 딥시크의 데이터 처리 방식과 개인정보 보호 문제를 파악하기 위해 자체 조사 착수(1. 30) - 아일랜드, 프랑스, 네덜란드 등에서 딥시크에 대한 조사 시작 - 네덜란드 당국, 딥시크의 개인정보 수집과 관련하여 조사를 시작하고, 자국 사용자들에게 딥시크 서비스 사용에 주의할 것을 경고(1. 30)
대만	- 대만 디지털부, 딥시크의 AI 서비스의 정보 보안을 위협 가능성 우려로 공공 부문에서의 사용을 금지(1. 31)
일본	- 일본 디지털상 내각사이버시큐리티센터(NISC), 데이터 유출 가능성을 우려로 각 부처에 딥시크 사용 주의를 환기(2. 2)
대한민국	- 행정안전부, 개인정보보호 우려로 딥시크 설치 자제 권고 (2. 4) - 산업통상자원부, 외교부, 국방부 등 주요 정부 부처 딥시크 차단(2. 5) - 한국 수력원자력, 한전, KPS 등 공기업에서 딥시크 사용금지(2. 5) - 한국거래소 및 증권사, 딥시크 접속 차단 조치를 시행(1. 30)

출처: 주요 언론기사를 종합하여 정리

현재 제기되는 딥시크 AI 모델 활용에 따른 우려는 크게 암호화 없는 전송체계와 보안에 취약한 알고리즘, 무분별한 민감 데이터 수집 위험, 중국 정부로의 유출과 악용 가능성과 정치적 편향성 및 제한된 답변 등을 들 수 있다.

먼저, 딥시크 앱은 민감한 사용자 및 기기 정보를 암호화 없이 인터넷으

로 전송하는데, 이는 데이터가 인터넷 트래픽상에서 패시브 및 액티브 공격에 노출될 위험을 높일 수 있다. 즉, 데이터가 중간자 공격(man-in-the-middle attack)이나 스니핑(sniffing) 같은 해킹 기법에 쉽게 노출될 수 있음을 의미하기 때문이다.[9] 실제로 iOS에서 딥시크 앱은 애플의 앱 전송 보안 기능을 비활성화한 상태로 운영되고 있었으며,[10] 이에 따라 암호화되지 않은 데이터가 온라인상에서 무분별하게 노출되어 있었다. 또한, 딥시크 앱이 채택한 암호화 알고리즘은 '3DES(Triple Data Encryption Standard)'로, 여러 취약점을 안고 있는 구식 체계이다.[11] 나아가 하드코딩된 암호화 키와 초기화 벡터를 재사용하고 있어 데이터 보안성 역시 크게 저하된 것으로 나타났다.[12] 보안 취약점과 관련하여 Security Scorecard는 딥시크의 안드로이드 애플리케이션이 약한 암호화 방식, SQL 인젝션 가능성, 하드코딩된 암호 키 등을 포함하고 있어 심각한 보안 위협을 야기한다고 지적했다. 딥시크의 데이터 수집 방침을 보면, 계정 생성 시 제공하는 개인정보 뿐만 아니라 사용 과정에서의 사용자 입력 패턴과 채팅기록, 심지어 휴대폰 모델

9) https://www.dailysecu.com

10) ATS는 iOS 플랫폼의 보안 기능으로, 민감한 데이터가 암호화되지 않은 채 전송되는 것을 방지하는 역할을 한다. https://www.dailysecu.com

11) 3DES는 1990년대부터 널리 쓰였던 오래된 대칭키 암호화 방식으로 현대의 컴퓨팅 파워로 쉽게 뚫릴 수 있으며, 최근 발견된 'Sweet32'라는 공격 방식에 3DES는 일정 조건에서 암호를 유출할 수 있다는 것이 밝혀진 바 있다. 따라서 최근의 LLM 보안 표준은 AES(Advanced Encryption Standard) 같은 더 안전한 알고리즘을 권장하고 있다. https://access.redhat.com/ko/articles/2621341?utm

12) 초기화 벡터는 암호화가 매번 다르게 작동하도록 도와주는 일회용 무작위 숫자로서 앱 안에 암호키와 초기화 백터가 직접 써있을 경우 앱 분석을 통해 이것이 그대로 노출되는 위험을 안게 된다. https://blog.humminglab.io/posts/tls-cryptography-3-block-cipher/; https://blog.pages.kr/3131

과 사용운영 체제, IP주소도 포함된다. 반면, 오픈AI의 챗GPT나 구글 제미나이, 네이버 클로바X 역시 사용자가 입력한 텍스트나 업로드 파일, 기기 식별 정보를 수집하지만, 정확히 누구로부터 수집한 정보인지 알 수 없도록 '토큰화(부분정보를 부호화하여 공개)'하는 과정을 거치기 때문에 비교적 안전하게 활용할 수 있다. 결국, 딥시크는 다른 LLM에 비해 해커가 암호화된 데이터를 쉽게 복호화하거나 앱 내부 통신 내용을 중간에서 탈취하거나 개인정보를 노출시키에 손쉬운 구조인 것이다.

〈표 3-3〉 딥시크와 이전 LLM 기반 생성형 AI와의 보안체계 비교

구분	DeepSeek	ChatGPT / Google Gemini / Clova X
사용 알고리즘	3DES (Triple DES)	AES-256, TLS 1.3 등 최신 표준
블록 크기	64비트	128비트 이상
보안 상태	국제적으로 사용 중단 권고	NIST 등에서 권장
위협 수준	Sweet32, 키 유출 가능성	고도화된 공격 대응 설계
암호 키 저장	앱 코드 내 하드코딩	KMS 또는 HSM 기반 안전한 키 저장
키 재사용	동일 키 및 IV 재사용	세션별 키 생성 및 주기적 키 회전
투명성/감사	확인불가	SOC 2, ISO 27001 등 보안 인증 기반 운영

출처: https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html;
https://developer.android.com/privacy-and-security/risks/hardcoded-cryptographic-secrets?hl=ko를 토대로 재정리

둘째, 딥시크는 사용자와의 상호작용을 분석하기 위해 광범위한 데이터를 수집하고 있으며, 여기에는 사용자의 채팅 기록 및 입력 텍스트, 업로드된 파일 및 첨부 데이터, 기기 정보(모델, 운영 체제, IP 주소 등), 키보드 입력 패

턴 및 리듬(Keystroke dynamics), 위치 정보 등이 포함된다. 특히 키보드 입력 패턴 및 리듬 데이터 수집은 상당히 논란이 되는 부분으로, 일반적으로 이러한 데이터는 사용자 인증 시스템에서 보안 강화를 위해 사용되지만 AI 서비스에서 이를 수집하는 것은 개인정보 침해 우려를 불러일으킬 수 있다. 오픈AI의 보관기간이 30일로 제한되어 있으며, 사용자가 자신이 입력한 정보를 생성형 AI가 학습에 활용하지 않도록 정보 수집을 거부하는 '옵트아웃' 선택이 가능한 반면, 딥시크는 이러한 토큰화 과정이나 옵트아웃, 보관기관 규정 없이 통째로 원하는 기간 동안 활용 정보를 수집할 수 있는 것으로 알려졌다. Wiz Research는 딥시크의 내부 데이터베이스가 잘못된 설정으로 인해 노출되어 있었고, 이를 통해 채팅 기록과 내부 정보 등이 외부에 유출될 가능성이 있었음을 밝혀냈다.[13)]

셋째, 중국은 국가안전법 및 데이터보안법에 따라 중국 내 모든 기업에게 고객 개인정보를 당국 요청 시 제공해야 한다. 따라서 중국에 서버를 둔 딥시크 내 개인정보가 중국 당국으로 유출될 가능성을 배제할 수 없다. 더욱이 딥시크는 사용자 데이터를 국영 통신사 차이나모바일의 IDC 서버로 전송하는 코드를 포함하고 있어 민감 데이터가 언제든지 중국 감시 체제에 노출될 수 있다. 지난 2월 15일 개인정보보호위원회는 이미 딥시크 사용자 정보가 중국 SNS 틱톡의 모회사인 '바이트댄스'에 넘어간 것으로 확인됐다고 밝히며 신규 앱 다운로드 중단을 권고한 바 있다.

넷째, 딥시크는 정치적 질문이나 민감한 사회 이슈에 대해 특정한 이념이나 입장에 치우친 응답을 내놓는 경향이 있는 것으로 지적되고 있다. 현

13) https://m.ytn.co.kr/news_view.php?s_mcd=0104&key=202502061955178919&pos=

재 중국의 모든 생성형 AI는 '사회주의 핵심가치관 준수' 하에 '국가정권 및 당과 안보 이익을 위해하는 모든 선동적, 위해 행위들을 금지한다'는 원칙을 강제받고 있다. 결과적으로 알고리즘의 설계와 훈련데이터 선택에도 당국의 검열을 피할 수 없는 것이다. 그 결과 중국공산당이나 시진핑, 중국의 영토분쟁 이슈, 민주화 운동에 대한 답변 자체가 거부되거나 검열된 답변을 제공하는 경향을 보이는 점도 딥시크 답변의 신뢰성을 훼손하고 있다. 이 뿐만이 아니다. 딥시크는 역사, 사회, 기술 문제 등 사실 기반의 질문에서도 존재하지 않는 인물이나 문서를 만들어내는 사례가 확인된 바 있으며, 이는 검증 가능한 출처 기반의 학습이 부족하거나 모델의 파인튜닝 과정에서 오류가 있었을 가능성을 시사한다. Enkrypt AI의 평가에 따르면 딥시크는 유해한 콘텐츠에 대한 노출 가능성이 기존 모델보다 최대 11배 높고, 정치적 편향성 또한 챗GPT 대비 3배 이상 심하다는 분석이 발표되기도 하였다.[14] 이 같은 문제는 단순한 응답 오류를 넘어, AI 모델이 사회적으로 미치는 영향력과 신뢰도, 그리고 정보의 중립성이라는 측면에서 중대한 문제로 간주되며, 이에 따라 딥시크의 기술적 개선과 외부 투명성 확보, 윤리적 통제가 필요하다는 지적이 제기되는 이유이다.

14) Enkrypt AI, "DeepSeek R1: Red Teaming Report" (Jan 2025), https://cdn.prod.website-files.com/6690a78074d86ca0ad978007/679918c4e37c71ea2179f6fb_Latest%20Red%20Teaming%20Deepseek_Jan2025.pdf?utm_medium=email&_hsenc=p2ANqtz-_MJiTMpN2y1bL5Le6n-UXyIz8ehY2Jxa_nruyOPZCNzpxWf_R7pLuHjsH3RbCvob9qb68ymrAvSbC0bcWxup8ccm5EId0OkblvU_a3v2w45RTQaQo&_hsmi=344571844&utm_content=344571844&utm_source=hs_email

4. 향후 전망 및 시사점

살펴본 바와 같이 LLM에 기반한 AI 활용의 보편화는 단순한 경제산업적 파급력을 넘어 AI 활용 과정에 제기되는 보안 문제와 첨예한 윤리적 쟁점을 낳고 있다. 나아가 미중 등 주요국과의 역학 관계에 긴밀히 연결된 국가 안보적 함의 또한 내재하고 있다. 특히, LLM의 학습데이터, 알고리즘, 운영서버가 특정 국가나 기업의 통제하에 집중될 경우, 데이터 주권의 문제 뿐만 아니라 AI 생태계 전반의 종속 문제로 이어질 수 있다.

그러나, 무엇보다도 LLM 기반 생성형 AI의 확산이 사이버 공간에서의 공격과 방어의 경계를 모호하게 만들고 있다는 점에 주목해야 한다. 프롬프트 인젝션, 데이터 중독(data poisoning), 알고리즘 조작 등, LLM AI의 취약성을 노린 공격들은 전통적인 네트워크 보안 체계로는 탐지·차단이 어려운 실정이다. 이에 각국은 'AI 보안 내재화' 뿐만 아니라 학습 단계에서부터 위·변조 탐지와 위험 예측역량을 갖추기 위해 노력하고 있다. 이처럼, 국가 안보 측면에서도 LLM의 도입은 새로운 과제를 안겨주고 있다. 더 나아가, 군사·외교·경제 데이터의 실시간 연계가 이루어지는 복합 네트워크 환경에서 LLM은 스스로 판단하는 '자율적 정보행위자(AI agent)'로 발전할 가능성도 배제할 수 없다. 이는 단순한 사이버 보안 문제가 아니라, 국가결정체계의 신뢰성과 통제권 문제로 연결된다.

LLM 기반 생성형 AI의 미래는 단순히 기술의 정교함만으로 설명되지 않으며, 그것이 어떤 정치경제적 배경과 결합하는가, 그리고 어떤 가치 기준으로 운영되는가에 따라 결정될 것이다. 이 같은 상황에서 우리는 글로벌 수준의 보안과 윤리를 담보한 고신뢰 AI 모델 개발에 선제적으로 투자

하고 국제협력의 선도적 역할을 수행할 필요가 있다. 특히, 개도국 대상으로 하는 AI 기술외교 및 규범 경쟁에서 주도권을 놓치지 않는 것이 중요하다. 이를 위해서는 국내 AI 생태계의 투명성과 경쟁력을 강화하고, 국가 차원의 AI 리스크 평가 체계 및 대응 전략을 수립해야 한다. 딥시크가 촉발한 더 매력적인 LLM 표준을 주도하기 위한 미중의 경쟁은 우리의 AI 전략에 도전과 제약 요소로 작용할 것이다. 그러나, 다른 한편으로 LLM 분야의 경쟁은 새로운 기회이며, 그 교차점에서 대한민국이 어떤 전략을 취하는가에 따라 미래 국가 AI 경쟁력의 향방이 달라질 것이다.

제3장

AI 반도체와 사이버-공급망 안보

오승희 | 국립외교원 외교안보연구소 조교수

제3장

AI 반도체와 사이버-공급망 안보

오승희 | 국립외교원 외교안보연구소 조교수

1. 서론

인공지능(AI)과 반도체는 21세기 기술 패권 경쟁의 핵심 축으로 자리 잡았다. 미·중 간 전략 경쟁은 단순한 경제 영역을 넘어 기술, 공급망, 사이버 안보 등으로 확장되고 있으며, AI 반도체 공급망은 이제 산업 구조를 넘어 국가 안보와 권력 투사의 수단으로 기능하고 있다(김상배 2022). 이에 이 글은 미·중 기술패권 경쟁이 AI 반도체 공급망 구조와 사이버 안보 체계에 미치는 영향을 분석하고, 일본과 대만의 대응 전략을 통해 중견국의 생존 전략을 모색하는 것을 목적으로 한다.

AI 반도체는 현대 산업 전반의 핵심 기반 기술로, 기술 패권의 중심 자산이라 할 수 있다. 반도체는 단순히 전자기기의 구동 요소를 넘어 자율주행, 인공지능, 데이터 분석 등 혁신 기술을 실현하는 핵심 부품이다. 특히 AI 반도체는 머신러닝과 대규모 데이터 분석의 연산을 담당하며, 경제 성장과 국가 경쟁력에 직접적인 영향을 미친다.

AI 기술의 급속한 확산은 GPU, NPU, ASIC 등 고성능 반도체 수요의 폭

발적 증가를 이끌었다. 자율주행차, 스마트폰, 클라우드, 국방 등 다양한 산업 분야에서 AI 반도체는 필수적 요소로 자리 잡았다. 그러나 이로 인해 특정 국가와 기업에 공급망이 집중되면서 공급 리스크가 심화되고 있다. 미국, 중국, 한국, 유럽연합(EU) 등 주요 국가들은 공급망 안정성과 사이버 보안을 새로운 전략 과제로 설정하고, 대규모 투자를 경쟁적으로 확대하고 있다.

글로벌 파운드리 시장을 선도하는 대만 TSMC는 엔비디아, AMD, 애플 등 주요 팹리스 기업들의 핵심 생산 파트너로서, 고성능 반도체 시장의 90% 이상을 점유하고 있다. AI 반도체 경쟁의 본질은 미세 공정 기술과 패키징 역량에 있으며, 두 영역 모두에서 TSMC가 압도적 우위를 확보하고 있다. TSMC의 매출은 2014년 240억 달러(약 34조 원)에서 2024년 880억 달러(약 126조 원)로 10년간 세 배 이상 증가했다. 2025년 3분기에는 AI 인프라 투자 확대와 수요 급증에 힘입어 순이익이 전년 대비 39.1% 증가한 4,523억 대만달러(약 21조 원), 매출은 9,899억 대만달러(약 46조 원)를 기록하며 사상 최대 실적을 경신했다.

이와 같은 AI 반도체 산업의 급성장은 새로운 사이버 안보 위협을 수반하기도 한다. 복잡한 글로벌 공급망 구조와 첨단 기술의 결합은 새로운 사이버 공격의 표적이 되면서, 기술 유출의 위험성이 증가하고 있다. 고성능 반도체를 기반으로 한 AI 모델은 공격의 자동화·정교화를 가능하게 하여, 피싱 이메일 생성, 보안 시스템 우회 알고리즘 학습 등 다양한 형태의 사이버 공격을 양산하고 있다.

AI 반도체의 설계·제조·유통 전 과정에서 발생할 수 있는 사이버 공격은 세계 경제와 국가 안보에 심대한 영향을 미칠 수 있다. 특히 반도체 설계 단계에서의 백도어 삽입이나 회로 도면 유출 등은 하드웨어 수준의 보안 위

협으로 이어질 수 있다. 이에 따라 하드웨어, 소프트웨어, 데이터 흐름 전반을 포괄하는 통합적 보안 체계의 구축이 요구된다.

글로벌 공급망 의존도가 높은 상황에서 이러한 위험은 더욱 증폭된다. AI 반도체는 군사 및 정보 분야에도 활용되는 전략 기술이기 때문에, 기술 유출은 국가 안보에 직접적인 타격을 초래할 수 있다. 따라서 AI 반도체의 자립화는 사이버 안보의 근간을 강화하는 핵심 전략으로 인식되고 있다. 이 글은 대만 TSMC의 일본 구마모토 공장 건설 사례를 중심으로 AI 반도체 공급망의 지정학적 중요성과 사이버 안보적 함의를 분석하고, 이를 통해 향후 AI 반도체 산업이 직면한 주요 과제와 대응 방향을 제시하고자 한다.

2. AI-반도체-공급망-사이버 안보 넥서스

1) AI와 반도체

2022년 OpenAI의 대화형 인공지능 서비스 ChatGPT의 출시는 전 세계적으로 AI와 AI 반도체 시장의 폭발적 성장을 촉발했다. AI 반도체는 대규모 데이터 처리와 복잡한 AI 알고리즘 계산을 고속·고효율로 수행하도록 설계된 특수 반도체로, 기존의 범용 프로세서 대비 연산 효율성과 전력 절감 효과가 탁월하다. 특히 심층학습(Deep Learning) 모델을 최적화하기 위한 구조를 지니며, 확장성과 맞춤 설계(Customization)가 가능한 아키텍처로 발전하고 있다.

AI 반도체의 주요 형태에는 GPU(Graphics Processing Unit), FPGA(Field Programmable Gate Array), ASIC(Application-Specific Integrated Circuit), 그리고 SoC(System on a Chip)등이 있다.

GPU는 대규모 병렬 연산에 특화되어 게임, 암호화폐 채굴, 생성형 AI 서비스 등에서 핵심적으로 활용되며, NVIDIA가 대표적인 제조업체로 자리 잡고 있다. FPGA는 현장에서 로직을 재구성할 수 있는 반도체로, 자동차·산업·IoT 등 다양한 응용 분야에서 유연한 반도체 솔루션을 제공한다. SoC는 복수의 기능을 단일 칩에 집적하여 스마트폰 등 다양한 전자기기에 필수적으로 사용되며, ASIC은 특정 기능 수행을 위해 설계된 맞춤형 칩으로, 특정 업무에 최적화된 효율성을 제공한다.

AI의 비약적 발전과 함께 대규모 언어 모델(LLM)의 등장으로 연산 수요가 폭증하였으며, 이에 따라 초병렬·고성능 반도체에 대한 수요가 급격히 증가하고 있다. 더불어 AI 기술 자체가 반도체 설계와 생산 효율을 향상시키는 방향으로 활용되면서, 반도체 개발의 가속화가 이루어지고 있다.

AI는 이제 단순한 첨단 기술을 넘어 사이버 안보, 국가 전략, 글로벌 기술 패권 경쟁의 핵심 요소로 부상하였다. 예컨대 미국 트럼프 2기 행정부는 AI 기반 글로벌 공급망 재편과 기술 표준 확립을 위해 약 5,000억 달러 규모의'스타게이트 프로젝트'를 개시한 바 있다. AI와 반도체의 융합은 제조업과 서비스 산업 간 경계를 허물며 상호 보완적 관계를 형성한다. 반도체는 AI 구현을 위한 핵심 인프라로서 연산 능력을 제공하고, 반도체 기술 발전은 AI 학습 속도와 정확도를 향상시킨다. 반면, AI는 반도체 설계 자동화, 품질 관리, 생산 최적화 등 다양한 공정에 활용되어 생산성을 높인다.

이러한 융합은 스마트 팩토리, 자동화 시스템, 클라우드 컴퓨팅, 데이터 분석등 산업 전반의 디지털 전환을 촉진하며, 혁신적인 생산 패러다임을

형성하고 있다. 그러나 AI의 확산으로 인해 개인정보 보호 및 데이터 관리가 중요한 윤리·법적 이슈로 부상하고 있으며, 이는 AI 반도체 기반 시스템의 신뢰성과 직결된다.

2) AI 반도체와 공급망 안보

AI 반도체를 포함한 반도체 공급망은 기획-설계-전공정-후공정의 단계별 전문 기업들이 전 세계적으로 분산되어 운영되는 복합적 네트워크이다. 이러한 구조는 효율성과 전문화를 촉진하지만, 동시에 지정학적 리스크에 취약하다.

미·중 전략 경쟁이 심화되면서 반도체 산업의 불확실성이 확대되고 있으며, 반도체가 군사·경제적 전략 자산으로 인식됨에 따라 각국은 공급망 안보를 국가 전략 차원에서 관리하고 있다. 특히 코로나19 팬데믹은 글로벌 공급망의 취약성을 여실히 드러내며, 각국이 공급망 재편과 리쇼어링(Reshoring) 정책을 추진하는 계기가 되었다.

중국은 '제14차 5개년 계획'과 '중국제조 2025(中國製造2025)' 전략을 통해 반도체 산업의 자급자족과 기술 자립을 목표로 하고 있다. 이를 위해 중국 정부는 공급 측면에서는 기술 개발과 생산 역량 강화를, 수요 측면에서는 자국 내 반도체 사용 확대를 추진하고 있다. 2023년 기준, 중국은 미국 반도체 판매의 약 31%를 소비하고 있으며, 전 세계 반도체 제조 능력의 약 20%, 특히 후공정(Back-end) 분야의 약 40%를 차지한다. 성숙 공정(〉28nm) 부문에서는 2027년까지 37%의 웨이퍼 제조 능력을 확보할 것으로 예상된다. 또한 2024년 5월, 중국은 자국 반도체 생태계 강화를 위해 475억 달러 규모의 제3기 국가집적회로산업투자기금(大基金 III)을 조성했다.

반면 미국은 'CHIPS and Science Act'를 통해 자국 내 반도체 생산 능력 강화와 동맹국 협력을 추진하고 있으며, 유럽연합(EU) 역시 'EU Chips Act'를 통해 공급망 안정성과 기술 자율성 확보를 도모하고 있다.

일본은 '경제안전보장추진법', 한국은 'K-반도체 전략', 대만은 '대만형 칩스법'과 TSMC 해외 투자 다변화 전략 등을 통해 글로벌 공급망 내 입지를 강화하고 있다. 이처럼 각국은 지정학적 이해관계와 경제적 인센티브를 종합적으로 고려하여 반도체 공급망 안정화를 위해 대응하고 있으며, 핵심 광물·소재·장비의 안정적 확보를 주요 과제로 삼고 있다.

3) AI 반도체와 사이버 안보

반도체는 디지털 산업 전반뿐 아니라 국방, 통신, 교통, 금융 등 주요 사회 인프라에 광범위하게 활용되는 전략 자산이다. 따라서 반도체 산업이 사이버 공격을 받을 경우, 공급망 중단·인프라 마비·산업 활동 정지 등 심각한 결과를 초래할 수 있으며, 이는 곧 국가 안보와 경제 안정성에 직접적인 영향을 미친다.

반도체 공급망의 사이버 위협은 크게 정보 탈취형 공격과 파괴형 공격으로 구분된다. 전자는 설계도면, 공정데이터, 운영정보, 직원 개인정보 등을 탈취해 산업 기밀 유출과 기술 경쟁력 약화를 초래하며, 후자는 설비 파괴, 생산 중단, 품질 저하 등을 유발하여 공급망 전체의 연속성을 위협한다.

국제반도체장비재료협회(SEMI)는 이러한 리스크 대응을 위해 다음 세 가지 원칙을 제시한다. 첫째, 물리적 보안 강화이다. 반도체 생산 시설은 고도의 정밀성과 청정 환경을 요구하므로, 외부 침입이나 설비 파괴는 생산 중단과 기술 유출로 직결될 수 있다. 둘째, 사이버 방어 체계 강화이다. 네

트워크 해킹, 악성코드, 피싱, DDoS 공격 등은 반도체 설계·제조 소프트웨어의 무결성을 훼손할 수 있으므로, 공정 데이터 보호 및 암호화 기술의 도입이 필수적이다. 셋째, 공급망 참여자 간 보안 신뢰성 확보이다. 공급망 내 어느 한 기업의 보안 취약점도 전체 체인을 위협할 수 있기 때문에, 모든 참여자가 일정 수준 이상의 보안 표준을 유지해야 한다.

결국, AI 반도체 산업에서의 사이버 안보는 단순히 기업의 정보 보호를 넘어 국가 경제 및 기술 주권을 지키는 핵심 요소로 자리 잡고 있다. 반도체 제조 전 과정에서 사이버 신뢰성이 확보되지 않으면, 해당 칩을 사용하는 AI 시스템과 일상적 디지털 기기의 보안성 또한 보장될 수 없다. 따라서 반도체 산업의 사이버 안보 강화는 글로벌 기술 경쟁력 확보와 국가 안보 유지의 필수 조건으로 인식되어야 한다.

3. 지정학적 리스크와 AI 반도체 공급망 재편

1) 미·중 기술패권 경쟁과 AI 반도체 수출 규제

2024년 10월 28일, 미국 정부는 2025년 1월 2일부터 반도체·양자기술·AI 분야에 대한 대중(對中) 투자 제한조치를 발표했다. 이 조치는 중국이 첨단 기술을 군사적 목적으로 전용할 가능성에 대한 우려에서 비롯된 것으로, 미국 자본과 기술이 중국의 첨단 산업 발전에 활용되는 것을 차단하기 위한 목적을 갖는다. 반도체·양자·AI 기술은 자율 무기, 암호 해독, 감시 체계, 사이버 공격 등 첨단 군사 기술의 기반이 되는 핵심 분야이기 때

문이다.

미국 정부는 자국 기업의 투자가 중국의 기술 혁신을 촉진하고 결과적으로 미국의 국가 안보를 위협할 수 있다고 판단했다. 이에 따라 중국 관련 투자에는 미국 재무부에 의무적 사전 통보가 요구되며, 일부 투자는 전면 금지된다. 이 조치는 단순한 투자 제한이 아니라, 경제·기술 안보를 강화하기 위한 전략적 조치로 해석된다.

이어 2025년 1월 13일, 바이든 행정부는 AI 반도체 수출에 대한 새로운 규제안(Interim Final Rule on AI Diffusion)을 확정했다. 이 규제는 고성능 AI 시스템이 대량살상무기 개발이나 사이버 공격에 활용될 위험을 지적하며, 국가별 리스크 수준에 따라 AI 반도체 수출을 3단계로 분류·통제하는 내용을 담고 있다.

일본을 포함한 18개 주요 동맹국은 수출 제한에서 제외되어 AI 반도체의 자유로운 구매가 가능하지만, 비동맹국 및 우려국은 강력한 수출 제한 대상이 된다. 특히 비상업적 연구기관·의료기관 등에는 제한적으로 첨단 GPU 도입이 허용되지만, 제3국을 통한 '우회 수출' 방지를 위한 통제 체계가 병행된다.

한편, 2025년 1월 20일 출범한 트럼프 행정부는 전임 정부의 AI 반도체 규제를 둘러싼 논란 속에 출범했다. 이에 대해 당시 NVIDIA는 "미국의 'AI Diffusion' 규제는 혁신과 경제 성장을 저해하는 과도한 조치"라며, "AI 기술 확산은 오히려 산업 경쟁력과 국가 안보를 강화할 수 있다"고 비판했다. NVIDIA는 해당 규제가 "중국 견제라는 명분 아래 미국의 글로벌 경쟁력을 약화시키는 결과를 초래할 것"이라고 지적했다.

TSMC 창업자 모리스 창(Morris Chang) 또한 "최첨단 반도체의 자유무역은 사실상 종언을 맞았다"며, "이러한 환경 속에서 지속 가능한 성장을 이

뤄내는 것이 최대의 과제"라고 언급했다. 그는 "TSMC가 군사적 전략 거점이 될 가능성을 5년 전부터 경고해왔으며, 현재 그 예고가 현실이 되었다"고 평가했다.

미국의 '중국 배제형 반도체 공급망 전략'에 대응해, 중국은 기술 자립을 위한 내재화 정책을 강화하고 있다. 자체 개발 AI 모델인 '딥시크(DeepSeek)'의 부상은 기술 자립 시도의 일부 성과로 평가되지만, 동시에 정보 보호 문제로 대만·일본·이탈리아 등 주요국이 공공기관에서의 사용을 금지했다. 한국 정부 역시 공공기관과 금융권에서 딥시크 접속을 차단하는 등 보안 우려가 확산되고 있다.

이처럼 미·중 간 기술패권 경쟁이 심화되면서, AI 반도체 산업의 지정학적 리스크와 사이버 안보 위협은 동시다발적으로 확대되고 있다. 각국은 기술 보호, 산업 경쟁력 유지, 공급망 안정성 확보를 위한 다층적 안보 전략을 수립할 필요성이 높아지고 있다.

2) 지정학적 불안정성에 대응한 공급망 다변화 전략

2019년 미국의 화웨이 제재를 기점으로 미·중 무역 갈등은 본격화되었고, 코로나19 팬데믹을 거치며 반도체를 포함한 글로벌 공급망 전반의 불안정성이 심화되었다. 이로 인해 각국은경제안보 강화와 공급망 재편을 국가 전략으로 추진하게 되었다.

2019년 여름, 일본의 반도체 장비업체 도쿄일렉트론 전 회장 히가시 테츠로(東哲郎)는 미국 IBM 부사장 존 켈리(John E. Kelly)로부터 일본 내 2나노 반도체 생산 협력 제안을 받았다. 이를 계기로 일본 경제산업성은 자국 내 첨단 반도체 생산 능력 복원을 추진하며, 대만의 TSMC 일본 공장 유치 계

획을 본격화했다(오승희 2024).

이후 2021년 4월, 스가 요시히데 일본 총리와 조 바이든 미국 대통령은 정상회담 공동성명에서 52년 만에 처음으로 "대만해협의 평화와 안정"을 명시했다. 이는 중국의 '하나의 중국' 원칙에 대한 도전으로 해석되며, 미·일 양국이 대만을 전략적 공급망 축으로 인정하기 시작한 결정적 전환점이었다. 2022년 8월 낸시 펠로시(Nancy Patricia Pelosi) 미 하원의장의 대만 방문은 양안(兩岸) 관계의 긴장을 최고조로 끌어올리며, 반도체 공급망의 지정학적 리스크를 더욱 부각시켰다.

대만의 TSMC는 이러한 환경 속에서 자국의 경제 성장뿐 아니라 '반도체 방패(Silicon Shield)'로서의 전략적 역할을 수행하고 있다. 미국 정부는 CHIPS and Science Act를 통해 TSMC의 미국 내 투자를 적극 지원하고 있으며, 애리조나에 건설 중인 TSMC 공장에는 보조금과 저리 대출이 제공되고 있다.

현재 TSMC는 세 가지 전략적 과제—① 지정학적 리스크 완화 ② 글로벌 공급망 다변화 ③ 대만의 기술적 전략 자산 보존—에 직면해 있다. 이를 위해 TSMC는 글로벌 생산 분산 전략을 추진 중이다. 미국 애리조나에는 총 1,650억 달러(약 236조 원)규모의 투자를 바탕으로 6개의 첨단 팹을 건설 중이며, 일본 구마모토에는 아시아 시장 공급 거점, 독일 드레스덴에는 유럽 시장 대응 팹, 싱가포르에는 동남아 허브를 각각 구축하고 있다. 2025년 한 해 동안만 대만 타이중·가오슝, 미국·일본·독일 등지에서 9개의 신규 팹이 착공 또는 가동될 예정이며, 2026년까지 TSMC의 글로벌 인력 규모는 10만 명 이상으로 확대될 전망이다.

그러나 이러한 다변화 전략에도 불구하고 정치·경제적 변수는 여전히 불확실하다. 트럼프 행정부가 검토 중인 대만산 제품 20% 관세는 현재 반

도체를 예외 품목으로 두고 있으나, 향후 정책 방향에 따라 변경될 가능성이 존재한다. 더불어 하워드 루트닉 미 상무장관이 "대만의 반도체 생산 능력 절반을 미국으로 이전해야 한다"고 언급하면서, TSMC에 대한 미국의 압박은 한층 강화되고 있다.

3) 인력 유출과 사이버 안보 위협

AI 반도체 공급망의 지정학적 리스크는 기술뿐 아니라 인력과 정보 보안 측면에서도 심화되고 있다. 2018년 TSMC 대만 공장이 바이러스 감염으로 3일간 가동 중단을 겪으며 약 190억 엔의 피해를 입은 사건은 공급망 보안의 취약성을 보여주는 대표적 사례다.

2019년부터 2023년까지 대만 당국이 적발한 산업기술 유출 사건은 총 110건으로, 이는 이전 5년(2014~2018년) 대비 31% 증가한 수치다. 이 가운데 2021년까지 보고된 51건 중 48건(94%)의 기술이 중국 본토로 유출된 것으로 확인되었다. 이는 미국의 수출 통제 강화 이후, 중국이 국가 주도의 기술 확보 전략을 추진하며 대만 내 산업 스파이 활동을 조직적으로 전개하고 있음을 시사한다. 2025년 들어 중국 정부의 지원을 받는 사이버 공격 그룹이 대만 반도체 기업을 대상으로 피싱, 악성코드, 내부망 침투 등을 집중적으로 수행하며 공격 빈도가 급증했다.

한편, 이직을 통한 기술 유출 문제도 심각하다. 2000년대 이후 다수의 TSMC 출신 고위 엔지니어들이 중국 기업으로 이직하였고, 중신궈지(SMIC) 창립 시에도 TSMC 출신 핵심 기술팀이 대거 영입된 바 있다. 대만 업계 관계자는 "내부 승진에 한계를 느낀 엔지니어들이 파격적인 조건을 제시하는 중국 기업의 스카우트 제안을 수용하고 있다"고 전했다.

2025년 8월, 대만 고등검찰청은 TSMC 전직 엔지니어 3명을 국가보안법 위반 및 영업비밀 유출 혐의로 기소했다. 이 중 한 명은 퇴사 후 일본의 반도체 장비업체 도쿄일렉트론(Tokyo Electron) 자회사로 이직한 인물로, 공급사 경쟁력 강화를 명분으로 TSMC 내부 정보에 접근을 시도한 것으로 드러났다. 이들의 목표는 TSMC의 2나노미터(2nm) 칩용 식각 장비 성능 개선 기술로, 향후 기술 경쟁력의 핵심 자산이었다. 검찰은 해당 전직 직원에게 징역 14년, 나머지 2명에게는 각각 9년과 7년의 중형을 구형했다. 이 사례는 기술 탈취와 인력 유출, 사이버 공격이 결합된 복합적 위협이 현실화되고 있음을 보여준다.

따라서 AI 반도체 공급망의 안정성을 확보하기 위해서는 물리적·기술적·인적 보안 체계의 통합적 관리가 필수적이며, 특히 국가 차원의 사이버 방위 체계와 법적 대응력 강화가 절실하다.

4. 일본의 반도체 부활 전략과 사이버 안보 강화

1) TSMC 공장 유치와 일본 반도체 산업의 부활

일본은 TSMC 공장 유치를 계기로 첨단 반도체 생산 역량을 확보하며, 글로벌 공급망 재편의 핵심 거점으로 부상하고 있다. 구마모토 지역은 반도체 부품·장비 기업이 밀집한 산업 클러스터로, TSMC의 진출은 지역 산업 생태계의 활성화를 촉진할 것으로 기대된다.

2021년 TSMC는 일본 구마모토 공장 건설 계획을 발표하며,소니·덴소·

토요타 등 일본 주요 기업과 합작해 JASM(Japan Advanced Semiconductor Manufacturing)을 설립했다. 2022년 착공 이후 2024년 말 제1공장이 가동을 시작했으며, 제2공장은 2027년 12월 완공 예정이다. 총 투자액은 2조 1천억 엔(약 19조8천억 원) 규모이며, 일본 정부는 두 공장에 총 1조 2천억 엔(약 11조 3천억 원)의 보조금을 지원할 방침이다. 이 같은 전폭적 지원은 일본 정부가 반도체를 국가 전략산업으로 명확히 규정했음을 의미한다.

일본의 반도체 부활은 단순한 산업정책을 넘어, 정치·관료·학계·산업계의 연합 구조를 통해 추진되고 있다. 2021년 5월, 자민당은 '반도체전략추진의원연맹(半導体戦略推進議員連盟)'을 출범시켰다. 아베 신조와 아소 다로(麻生太郎)가 특별 고문을, 아마리 아키라(甘利明)가 회장을 맡으며 자민당 내 핵심 인사들이 주도했다. 이 연맹에는 세키 요시히로(関芳弘), 고바야시 다카유키(小林鷹之), 야마기와 다이시로(山際大志郎) 의원 등 정치권은 물론, 경제산업성(経産省)의 노하라 사토시(野原諭), 수상관저의 아라이 마사요시(荒井勝喜) 총리비서관, 학계에서는 도쿄대학의 고노카미 마코토(五神真) 총장과 구로다 다다히로(黒田忠広) 교수, 라피더스(Rapidus) 참여 기업의 최고경영자들이 폭넓게 참여했다. 이 같은 산·관·학 협력 구조는 신속한 전략 수립과 법·제도 정비를 가능하게 했고, TSMC에 대한 대규모 보조금 지급의 법적 근거도 마련되었다. 정부는 민간 투자의 최대 50%를 지원하는 보조금 제도를 도입했으며, 제1공장에는 4,769억엔, 제2공장에는 최대 7,320억엔을 지원할 예정이다.

한편, 일본은 자국 주도의 첨단 반도체 기술 개발을 위해 라피더스(Rapidus) 프로젝트를 추진 중이다. 이 프로젝트는 2 나노미터(2nm) 공정 기술을 목표로 하며, 홋카이도(北海道) 치토세(千歳) 지역에 공장을 건설하고 있다. 라피더스는 도요타, 소니, NTT, 미쓰비시 등 일본의 주요 대기업이 참여하

는 국가 차원의 기술 자립 프로젝트로, 일본 반도체 산업의 "제2의 부흥기"를 목표로 한다.

2) 사이버 안보 체계 강화와 능동적 방어 전략

일본 정부가 사이버보안 산업 육성에 본격적으로 나선 것은, 디지털전환(DX)·녹색전환(GX) 등 신산업 확산 속에서 보안 취약성이 경제안보의 최대 위협으로 부상했기 때문이다. 일본은 소재·부품·장비 분야에서 높은 기술력을 보유하지만, 최근 기업 대상 해킹 공격이 급증하면서 산업 생태계 전반의 보안 역량 격차가 국가적 위기 요인으로 지목되고 있다.

2025년 3월 발표한 사이버보안산업진흥전략은 향후 10년간 자국산 보안 제품과 서비스를 우대하고, 스타트업 발굴·전문인력 양성·국제협력 강화를 통해현재 약 1조 엔 규모의 산업을 3조 엔 규모로 성장시키는 것을 목표로 한다. 이는 일본의 디지털 경제 성장 전략과 직결된 핵심 안보 프로젝트로 평가된다. 또한 일본 경제산업성은 반도체 장비 제어 시스템을 겨냥한 사이버 공격을 상정해, 보안 검토 조직의 역할 명확화, 비상 대응 및 사업 연속성 확보, 공급망 영향 평가, 다중 방어 및 네트워크 분리, 물리적 접근 통제 등 6대 대응 지침을 마련한다.

2025년 7월에는 기존 사이버 시큐리티 센터(NISC)를 개편해 사이버 보안 정책을 지휘하는 〈국가 사이버 통괄실(国家サイバー統括室)〉을 출범했다. '능동적 사이버 방어(Active Cyber Defense, ACD)' 체계를 구축하여 중대한 사이버 공격을 수동적으로 막는 데 그치지 않고, 평소 모니터링을 통해 공격 징후를 감시하고 필요할 경우 사이버 공격이 발생하기 전에 상대방 서버에 침입해 대응하는 공세적 대응 방식으로 대응한다(国家サイバー統括室 2025; 이정환 2024).

3) 공급망 리스크와 전략적 기술균형의 과제

반도체 공장은 규모가 크고, 범용 운영체제(OS) 기반 장비가 많아 해킹 위험이 높다. 2018년 TSMC 대만 공장은 웜 바이러스 감염으로 2일간 가동이 중단되어 약 3,000억 원(연매출의 3%) 손실을 입었다. 2022년에는 도요타 부품 협력사가 해킹 공격을 받아, 일본 내 14개 전 공장이 하루 동안 전면 중단되는 사태가 발생했다. 이러한 사건들은 공급망의 사이버 취약성이 국가 제조 경쟁력에 직결된다는 점을 보여준다.

해외 진출 역시 복합적인 리스크를 수반한다. TSMC 구마모토 공장은 일본 반도체 부활의 상징으로 평가되지만, 동시에 현지 설비·인건비 증가, 기술 이전 위험, 공급망 관리 복잡화 등 새로운 부담을 초래했다. 또한 지역 내에서는 지가 상승·물가 폭등·교통 혼잡 등 부작용이 나타나고 있으며, 막대한 보조금 지원의 정당성 논란도 제기되고 있다.

2024년 12월 가동을 시작한 구마모토 제1공장은 월 5만 5천장의 웨이퍼 생산 능력을 갖추고 있으나, 현재 가동률이 약 40% 수준에 머무르고 있다는 지적이 제기되었다. 자동차 및 산업용 반도체 중심의 제품 포트폴리오와 글로벌 수요 변동이 복합적으로 작용한 결과이다. 여기에 미국·일본·대만·독일 등 해외 팹 투자 확대로 감가상각비와 인건비 부담이 가중되면서 TSMC의 비용 구조가 비대해지고 있다는 지적이 제기됐다. 이 와중에 TSMC의 2나노 기술이 라피더스로 유출되었다는 의혹이 제기되면서 대만-일본 간 기술 협력에 균열이 생겼다. 도쿄일렉트론(TEL) 자회사로 이직한 TSMC 전 직원이 TSMC의 핵심 기술을 무단 반출해 라피더스 개발 과정에 참고 자료로 활용했다는 혐의다. 대만 정부는 이를 '국가 핵심 기술 무단 접근'으로 규정해, 2022년 개정된 국가보안법에 근거하여 간첩 행위로

처벌하기로 했다.

미국이 주도하는 기술 블록화 전략은 공급망 안정성을 강화하는 한편, 사이버 리스크의 외부화라는 새로운 문제를 낳고 있다. 이에 따라 일본·대만·한국 등 중견 기술국들은 미국과의 기술 협력을 유지하면서도, 중국의 경제적 영향력을 관리하고 자체적인 사이버 방어 체계를 강화해야 하는 복합적 과제에 직면해 있다.

결국 중견국에게 필요한 것은 전략적 기술균형이다. 이는 기술 주권을 지키면서도, 지정학적 리스크를 최소화하고 공급망·보안·외교를 통합적으로 관리하는 접근 방식이다. 일본의 반도체 부활과 사이버 안보 강화는 이러한 균형 전략의 가능성을 보여주는 중요한 사례로 중장기적 관찰을 필요로 한다.

5. 결론

AI 반도체 산업은 원재료 조달부터 설계·제조·유통·서비스에 이르는 복잡한 글로벌 네트워크를 기반으로 운영된다. 이러한 다층적 구조는 효율성과 혁신을 가능하게 하지만, 동시에 사이버 공격에 노출될 수 있는 취약 지점을 다수 내포하고 있다. 특히 AI 반도체의 제조 공정은 고도의 정밀성과 실시간 데이터 처리가 요구되기 때문에, 생산 설비나 제어 시스템에 대한 해킹은 생산 중단, 품질 저하, 대규모 경제적 손실로 직결될 수 있다.

공급망 역시 주요 취약 지점으로 지적된다. 외부 부품 공급 과정에서 악성코드가 삽입되거나, 서드파티 공급업체의 시스템 취약점을 통해 주요 기

업 네트워크로 침투할 가능성이 존재한다. 실제로 부품·장비·소프트웨어 등 어느 한 단계라도 보안이 약화되면, 전체 공급망의 신뢰성이 무너질 수 있다. 물류·유통 과정에서의 데이터 해킹은 제품의 이동 경로를 왜곡시키거나 배송을 차단할 수도 있으며, 이로 인해 기업의 생산 일정과 거래 신뢰도에 심각한 영향을 미친다.

특히 소프트웨어 업데이트나 설계 프로그램에 악성코드가 삽입되는 공급망 공격은 이미 여러 산업에서 현실화 된 위협이다. AI 반도체 산업에서도 이러한 공격이 발생할 경우, 설계 정보나 알고리즘, 공정 데이터가 유출되어 기술 경쟁력과 지적 재산이 심각하게 훼손될 수 있다. 2019년부터 2023년 사이 적발된 산업기술 유출 96건 중 38건이 반도체 분야에서 발생했다는 사실은, 기술보호의 중요성을 여실히 보여준다. 이에 따라 한국 정부는 핵심 인력 관리 제도 강화, 산업기술보호법 개정, 수사 권한 확대 등 제도적 대응을 추진하고 있다.

AI 반도체 산업의 사이버 위협을 최소화하기 위해서는, 공급망 전 과정에 걸친 통합 보안 거버넌스 구축이 필수적이다. 각 단계의 보안 기준을 통일하고, 협력업체와의 보안 수준을 공동으로 관리해야 하며, 정기적인 점검·취약점 분석을 수행해야 한다. 블록체인 기반의 공급망 추적 시스템, AI 기반 위협 탐지 체계 등 첨단 기술을 활용한 선제적 방어 전략이 효과적인 대안이 될 수 있다.

또한 AI 보안 기술 자체의 고도화도 중요하다. 암호화·프라이버시 강화 기술을 적용하여 데이터와 모델을 보호하고, AI 시스템이 백도어 삽입이나 적대적 공격에 노출되지 않도록 해야 한다. 더불어 AI가 사이버전·가짜뉴스·딥페이크 등에 악용되지 않도록 감시체계와 국제 규범을 마련해야 한다.

궁극적으로 AI 반도체의 사이버 안보는 개별 기업의 기술 관리 문제를 넘어, 국가 안보와 글로벌 기술 질서의 핵심 축으로 부상하고 있다. 따라서 정부와 기업은 공동의 리스크 관리 체계를 구축하고, 국제협력을 통해 데이터·지식재산·공급망의 안전성을 강화해야 한다. AI 반도체 시대의 지속 가능한 발전은 기술력뿐 아니라 사이버 회복탄력성 확보에 달려 있다.

제4장

커넥티드 카와 사이버 안보

엄도영 | 국립외교원 외교안보연구소 연구교수

제4장

커넥티드 카와 사이버 안보*

엄도영 | 국립외교원 외교안보연구소 연구교수

1. 서론

자동차에 첨단 기술이 접목되면서 자동차가 다양한 내·외부 환경과 통신할 수 있게 되고, 기기 간 연결성이 향상됨에 따라 취약성도 높아지고 있다. 전기차와 자율주행차 기술과 시장이 급격하게 성장하고 있으며, 이에 따라 각국에서 개인정보보호, 사이버보안, 국가안보의 관점에서 다양한 우려가 나오고 있다. 사이버안보가 국가안보의 핵심 이슈로 부각되면서 자동차를 둘러싼 안보 차원의 법제화가 진행되고 있다.

커넥티드 카는 온보드 네트워크 하드웨어를 자동차 소프트웨어 시스템과 통합하여 단거리 전용 통신, 셀룰러 통신 연결, 위성 통신, 또는 기타 무선 주파수 연결을 통해 다른 네트워크나 장치와 통신하는 차량을 의미한다

* 이 글은 저자가 2025년 3월 모빌리티연구 제5권 제1호에 게재한 "첨단 자동차와 안보: 주요국의 대응 및 한국에 주는 시사점", 2024년 12월 국립외교원 외교안보연구소가 발행한 저자의 보고서 주요국제문제분석 2024-35 "미국의 커넥티드 차량 규제: 주요 내용, 쟁점 및 시사점"의 내용을 발췌하여 재구성하고 수정한 것임을 밝힌다.

(U.S. Department of Commerce, 2024). 커넥티드 카는 이처럼 다양한 단거리, 장거리 통신 방식으로 다른 기기, 차량, 네트워크, 인프라 등과의 연결 및 실시간 데이터 교환을 가능하게 한다. 바이든 행정부 당시 커넥티드 차량과 관련하여 중국과 러시아 기술을 차단하는 규칙을 제안하며 "중국이나 러시아와 연관된 공급업체, 자동차 제조사 및 부품이 미국 자동차 산업에서 일방적이고 광범위하게 자리잡기 전에 새로운 국가안보 위협에 대응"(D'Innocenzio, 2024)하기 위한 것이라고 발표했다. 해당 규칙은 트럼프 2기 행정부 출범 이후 2025년 3월 17일에 최종 규칙으로서 발효됐다.

이 글은 미국에서 커넥티드 카 관련 정보통신 기술 및 서비스 공급망 안보 규칙이 마련되어 발효된 것을 계기로 사이버 안보와 공급망 안보 넥서스를 탐색하고자 한다. 2장에서는 커넥티드 카와 관련된 미국의 행정조치 추진 경과와 규제의 주요 내용을 살펴본다. 3장에서는 커넥티드 카를 둘러싼 사이버 안보 문제를 파악하기 위해 사이버 '보안' 이슈의 '안보화'를 살펴보고, 미국과 EU, 그리고 한국의 현황을 검토한다. 4장에서는 사이버-공급망 안보 넥서스를 커넥티드 카 규제의 맥락에서 정리하고, 5장에서는 결론을 제시한다.

2. 미국의 커넥티드 카 규제[15]

1) 미국의 행정조치 추진 경과

미 상무부는 커넥티드 차량을 국가안보 차원에서 규제하기 위해 '커넥티드 차량 관련 정보통신 기술 및 서비스 공급망 안보(Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles)' 사전규칙 제정안(Advance Notice of Proposed Rulemaking, ANPRM)과 규칙 제정안(Notice of Proposed Rulemaking, NPRM)을 각각 2024년 3월 1일과 9월 26일에 연방관보에 게재했다. 바이든 전 대통령의 임기 종료를 앞두고 2025년 1월 16일에 최종 규칙이 연방관보에 게재되었다.

바이든 전 대통령이 중국을 포함한 우려 대상 국가의 기술에 의존하는 커넥티드 차량이 미국의 국가안보에 주는 위험을 조사할 것을 상무부에 지시하면서 행정조치가 개시되었다. 동 규칙 제정안은 트럼프 1기 행정부 하에서 발행한 '정보통신 기술 및 서비스 공급망 안보(Securing the Information and Communications Technology and Services Supply Chain)' 행정명령(E.O. 13873)을 근거로 마련되었다. 이는 적성국[16]과의 '정보통신 기술 및 서비스

15) 우려국(countries of concern)과 적성국(foreign adversaries)을 명시할 때는 미국의 해당 명령, 규칙, 또는 법에서 표기된 표현을 그대로 사용한다.

16) E.O. 13873을 이행하기 위해 2021년 1월 19일에 발행한 잠정 최종 규칙(Interim Final Rule)에서 중국, 쿠바, 이란, 북한, 러시아, 베네수엘라 마두로 정권의 정부 또는 비정부 행위자를 적성국의 범주에 있는 것으로 정했다. 최종 규칙은 바이든 전 대통령의 임기 말인 2024년 12월 6일에 발표되었다.

(Information and Communications Technology and Services, ICTS)'[17] 거래를 국가안보 위협이 된다는 판단하에 규제하는 토대를 확립했다. 바이든 행정부는 규제 범위를 자동차 산업으로 확장하여 커넥티드 카와 관련된 ICTS 거래도 금지할 수 있는 조치를 도입한 것이다.

트럼프 대통령은 취임 즉시 '미국 우선주의 통상정책(America First Trade Policy)'의 일환으로 커넥티드 카에 대한 규제 검토를 지시한 바, 보다 광범위한 커넥티드 제품을 고려하도록 ICTS 거래에 대한 규제를 확대할 필요성이 있는지 검토할 것을 주문했다(The White House, 2025a). 2025년 4월 3일 트럼프 대통령에게 제출된 '미국 우선주의 통상정책'과 관련하여 향후 필요한 조치에 대한 권고사항 요약본이 공개됐다(The White House, 2025c). 2025년 10월 현재, 넓은 의미의 커넥티드 제품까지 ICTS 규제의 적용을 확대하는 공식적 발표는 확인된 바 없다. 커넥티드 카 ICTS 공급망 안보 최종 규칙의 시행은 2025년 3월 17일로 예정되어 있었으나 트럼프 대통령이 취임 직후 연방관보에 이미 발표된 모든 규정의 시행일을 60일 이상 연기하는 것을 검토하도록 하는 메모랜덤(memorandum)을 발표하여(The White House, 2025b) 최종 규칙의 시행이 지연될 예정이었으나 동 규칙은 예정대로 3월 17일 발효되었다.

2) 미국 커넥티드 카 규제의 주요 내용

미 상무부는 새로운 규칙을 통해 중국 또는 러시아에 의해 소유·통제되

17) ICTS는 전자적 방식으로 정보 또는 데이터 처리, 저장, 검색 또는 통신 기능을 주로 수행하거나 가능하게 하는 하드웨어, 소프트웨어, 또는 기타 제품이나 서비스를 의미한다.

거나, 해당국의 관할권 또는 지시 하에 있는("owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia") 개인·단체가 설계, 개발, 제조 또는 공급한 커넥티드 카 관련 하드웨어 및 소프트웨어를 위험하다고 보고, 이를 미국에서 수입하고 미국 내에서 판매하는 것을 금지하는 것을 제안했다(엄도영, 2024, 6). 즉, 중국 또는 러시아와 어떻게든 연계된 하드웨어 및 소프트웨어의 미국 유입을 규제하고자 했다.

중국과 러시아를 미국의 국가안보에 위험을 초래하는 국가로 특정한 이유는 두 국가의 정부가 커넥티드 카 공급망 내 기업에 대해 직·간접적으로 영향력을 행사할 수 있는 체제를 갖추고 있고, 자동차 시장에서 산업적 역량도 보유하고 있다고 판단했기 때문이라고 규칙에 명시하였다(엄도영, 2024, 7). 중국의 자동차 제조업체가 차량 위치정보 등의 실시간 데이터를 중국 정부에 전송할 의무가 있다는 보고와 기업들이 미국 내 커넥티드 카에 대한 원격 접속을 정부로부터 강요받을 가능성이 있다는 것을 근거로 특히 중국 정부의 영향력에 우려를 표명하고 있다. 동 조치에서 특정한 국가 중 실질적으로 규제 대상이 되는 커넥티드 카 기술과 역량을 보유한 국가가 중국뿐(이유진·한아름, 2024)이라는 점에서, 이는 중국을 겨냥한 것으로 볼 수 있다. 현재 미국의 대중국 완성차 수입은 다른 국가에 비해 낮지만, 완성차 수입액(170억 달러) 대비 부품 수입액(144억 달러)이 상당한 비중을 차지한다. 반면 러시아는 완성차나 부품 공급에 상대적으로 미미한 영향을 미치고 있어, 미국은 특히 중국이 초래하는 위협을 국가안보 차원에서 막는 데 방점을 두고 있다.

미국은 차량연결시스템(Vehicle Connectivity Systems, VCS) 하드웨어 및 소프트웨어와 자율주행 3단계 이상에 해당하는 자율주행시스템(Automated Driving Systems, ADS) 소프트웨어를 규제 대상으로 지정하여 하드웨어 수입

업자와 커넥티드 카 제조업자가 금지된 거래를 할 수 없도록 규정했다(엄도영, 2024, 8). NPRM 발행 이후, 규제가 다양한 기술에 광범위하게 적용된다는 우려가 표명되어 규제 대상이 되는 시스템이 6개[18]에서 2개로 축소되기도 했다. 금지된 거래를 하고자 할 때에는 일반 승인(general authorizations) 또는 특별 승인(specific authorizations)을 받아야 한다.

소프트웨어 금지 조치는 2027년 모델부터 적용되고, 하드웨어에는 2030년 모델부터 적용된다. 업계 대응 시간 부족으로 인해 현대자동차를 포함한 한국 기업, 해외 기업(포드, 폭스바겐, GM, 혼다, NXP 등), 협의체(자동차혁신연합(AAI), 미국소비자기술협회(CTA)) 등이 유예 기간을 1~2년 늘려줄 것을 미 상무부에 요청한 바 있다.

3. 커넥티드 카와 사이버 안보

1) 사이버 '안보'로 확장되는 사이버 '보안' 문제

지금까지 차량에 가해지는 사이버 공격에 관하여 사이버 '보안' 관점의 연구가 주로 수행되었다. 자율주행 차량에는 카메라 시야 차단과 GPS 스푸핑(spoofing) 위협이 있고, 협력주행이 가능한 커넥티드 카의 경우 허위

18) 차량 운영체제(OS), 텔레매틱스(telematics) 시스템, 첨단운전자보조시스템(ADAS), 자율주행시스템(ADS), 위성 또는 셀룰러 통신 시스템, 배터리관리시스템(BMS)이 이에 해당한다.

안전 메시지 전송과 지도 데이터베이스 오염으로 인한 보안 및 프라이버시 위협이 있다(Petit and Shladover, 2015). 차량의 센싱 계층은 도청, 스푸핑, 재밍(jamming)에 취약하고, 차량 내외부 통신으로 이루어진 통신 계층은 도청과 스푸핑 외에 위조 데이터를 주입하거나 데이터를 변조하는 중간자 공격(man-in-the-middle), 가짜 데이터를 전파하는 시빌(sybil) 공격에 노출될 수 있다(El-Rewini et al., 2020). 커넥티드 카와 관련하여 개발된 20가지 위협사건 시나리오 중 8가지가 데이터 수집, 오용, 탈취, 해외 유출, 보안 침해 등 데이터 보호와 보안에 관한 것이다(심우현·박정원, 2021).[19] 커넥티드 카 기술 수준이 발달하면 정보 유출, 제어권 탈취 등 네트워크를 통한 사이버 위협의 수준이 높아질 것으로 예상되어 개인정보, 위치정보, 통신망 보호 관련 규제의 신설 및 강화가 필요하다.

이제는 사이버보안 문제가 국가안보 차원의 문제로 격상되어 안보 관점의 입법이 가속화되고 있다. 민간 데이터의 안전과 보안 문제가 "지정학적 안보 문제로 창발"할 수 있는 바, 미국은 중국산 제품의 수입 규제를 넘어, 서비스 사용 금지와 개인정보 및 데이터의 이전 금지까지 포함하여 '안보화'의 범위를 확대하고 있는 것으로 평가된다(김상배, 2024). 이를 단적으로 보여주는 예가 커넥티드 카 규제이다. 특히 미국은 데이터, 기술적 문제로 인한 보안 위험성을 넘어 특정 국가와 연계된 국가안보 위협을 전제로 규제를 신설하고 확대하고 있다. 커넥티드 카 위협 시나리오(각주 19 참고) 중

19) ▲커넥티드 카 수집정보 탈취를 통한 범죄·테러 ▲수집정보의 오용에 따른 범죄에의 노출 ▲차량 제어권 탈취를 통한 범죄·테러 ▲타차 및 제3자에 대한 무분별한 정보 수집 ▲위치정보의 해외 유출 행위 ▲부품을 이용한 차량 보안 침해 ▲수집된 이용자 개인 정보의 무분별·광범위한 이용 ▲외국 정부의 국내 서버 열람을 통한 정보 유출이 8가지 시나리오 해당한다.

커넥티드 카 부품 공급업체가 카메라, 센서 등 부품에 백도어를 내장하여 해당 부품을 사용한 자동차 제조업체 차량의 이용자 정보를 유출하는 시나리오는 발생 가능성이 높고 위험 수준이 매우 높은 것으로, 미국이 우려하는 국가안보 위협 상황을 보여주는 예시이다.

2) 미국의 우려

미국은 커넥티드 차량과 관련해서 중국의 하드웨어 및 소프트웨어 통제를 데이터 유출 문제뿐만 아니라 국가 인프라의 안정성까지 위협하는 국가안보 문제로 보고 있다. 중국산 자동차 또는 중국산 부품이 탑재된 자동차에서 수집한 위치정보, 운전자의 행동 및 주행 데이터, 인프라 데이터를 제조업체가 중국 정부로 보내고, 이를 유출할 가능성을 우려하고 있다. 레이저를 이용해 주변 환경을 3D로 스캔하여 자율주행차가 도로 상황을 인식하게 해주는 라이다(LiDAR) 기술의 경우, 중국산 센서 장비가 미국에서 군사용으로 사용되면 장비를 통해 인프라의 정밀지도 데이터가 확보될 수 있고, 이는 미국 국가안보에 중대한 영향을 미칠 수 있다(Sutter and Sayler, 2024). 특히 라이다 개발 업체가 중국 국영기업과 협력하여 중국의 군사 프로그램을 지원한다는 점이 미국의 우려 사항이다.

현재 미국에는 커넥티드 카나 자율주행차의 보안, 안전, 프라이버시 보호와 관련된 포괄적인 연방 규제 체계가 없고, 주별로 이를 규제하고 있으며, 자율적으로 채택할 수 있는 연방 가이드라인이 존재하는 상황이다. 차량의 사이버보안 및 개인정보 보호(SPY Car Act, 2019), HAV(Highly Automated Vehicle)의 안전(AV START Act, 2017), 자율주행차 시험 및 운영(SELF DRIVE Act, 2017)에 관한 연방 기준을 수립하여 주별로 충돌하는 법률의 시행을 막

기 위한 시도가 있었으나 입법화되지 않았다. 일반적인 소비자에 초점을 맞춰 프라이버시를 보호하기 위해 주별로 시행하는 기존 법률이 커넥티드 카가 활용하는 다양한 데이터(위치정보, 카메라 영상 등)를 규율하지 못하는 한계에 따라 차량과 직접적으로 관련된 프라이버시 법안을 발의하기 위한 노력이 뉴저지, 테네시, 뉴욕, 캘리포니아 등의 주에서 2023년부터 지속되고 있다(Riley, 2024).[20] 첨단 자동차의 사이버보안, 안전, 프라이버시 보호 문제를 통합적으로 규제하는 연방 체계가 부재한 상황에서 국가안보를 근거로 중국산 자동차와 관련 기술에 대한 규제를 강화하고 있다.

3) EU의 우려

EU 내에서도 중국을 특정하여 전기차와 관련된 보안상 위험에 대응하는 EU 차원의 조치가 필요함을 역설하고 있다. 일부 유럽 의회 의원들은 중국 측이 이미 차량 데이터가 악용될 수 있다는 우려로 일부 도시의 특정 정치 행사장이나 군사 기지에서 테슬라 차량 운행을 금지한 이력이 있고, 중국 밖으로 자동차 제조사들이 데이터를 전송하는 행위를 금지한 것을 강조했다. 즉, 중국도 타국 기업의 자동차 운행과 데이터 국외 이전을 제한하는 상황에서 EU 또한 대중국 규제의 필요성을 주장하고 있다. 이를 토대로 EU 집행위원회도 '네트워크 및 정보시스템 보안 지침(NIS 2 Directive)'에 따라 중국산 전기차의 보안 위험평가를 시행하거나 차량 내 데이터 접근 관

20) 캘리포니아주는 자동차 제조업체가 차량 내 카메라가 존재한다는 사실을 공개하도록 의무화하여 차량 내부 감시 기능의 투명성을 보장하는 법을 2023년 10월에 제정했다.

련 법안을 마련할 것을 제기했다(European Parliament, 2023).

EU 사이버보안청(European Union Agency for Cybersecurity, ENISA)은 커넥티드 차량과 자율주행차가 직면하는 사이버보안 문제에 대한 심층적 분석을 수행한 바 있다(ENISA, 2021). 그러나 소비자 보호 문제, 표적 감시의 위험, 차량 마이크·카메라·센서를 통한 대규모 스파이 활동의 가능성을 포괄하는 폭넓은 논의가 부족하다는 지적이 있다(Oertel, 2024). 중국과 연계되어 제조된 차량에 대한 인식, 커넥티드 카 및 자율주행차를 둘러싼 사이버보안 위험성과 안보 위협에 관한 우려가 미국과 크게 차이 나지 않는다고 볼 수 있다.

미국과의 차이점은 EU는 유엔 유럽경제위원회(United Nations Economic Commission for Europe, UNECE) 산하 자동차 기준 국제조화 회의체(WP.29)가 채택한 사이버보안 국제기준을 입법화한 것이다. 사이버보안 관리체계(Cyber Security Management System, CSMS) 요구사항을 규정한 UN Regulation No. 155와 소프트웨어 업데이트 관리체계(Software Update Management System, SUMS) 요구사항을 규정한 UN Regulation No. 156을 채택한 것이 대표적이다. 2022년 7월부터 새로운 차량 형식에, 2024년 7월부터 모든 차량 형식에 동 기준을 적용하는 형식승인제도를 시행하고 있다. 차량이 EU 시장에 진입하기 위해서는 CSMS 인증서 취득, 차량 형식별 위험 평가 및 관리, 보안조치 등을 수행하여 형식승인을 받아야 한다. UN 기준은 자동차의 전 주기에 걸쳐 사이버보안 체계가 갖춰있을 것을 요구하기 때문에 공급망 관리 차원에서 OEM뿐만 아니라 Tier 1·2 공급업체가 제공하는 시스템이나 부품의 사이버보안 위험 관리까지 포괄한다. 이렇듯 EU의 입법은 사이버 '보안'에 초점이 맞춰져 있다.

EU는 미국처럼 국가안보 논리를 활용하여 중국산 자동차에 직접적인

제재를 가하는 데에 한계가 있다. 각 회원국 정부에 이러한 결정을 맡길 수 밖에 없고, 회원국마다 중국 시장에 대한 의존도나 중국으로부터 투자를 유치한 정도가 상이하기 때문이다.

4) 한국의 현황

한국은 2024년에 「자동차관리법」을 개정했다. 정부는 커넥티드 카 시대에 대비하여 국제기준을 바탕으로 자동차 제작사의 사이버보안 및 소프트웨어 업데이트 안전관리 조치를 위한 제도적 기반을 마련했다(국토교통부, 2024). 한국도 EU와 유사하게 UN 국제기준을 바탕으로 차량 사이버보안에 관한 요구사항을 법제화하였다. 개정된 법에 따라 국내에서 자동차를 판매하려면 사전에 국토교통부 심사를 통하여 별도의 CSMS 인증서를 획득해야 하고, 국토교통부 고시를 통해 구체화된 CSMS 세부 요건 및 기준을 준수해야 한다. 또한, 차량에 설치된 소프트웨어의 업데이트가 안전하게 수행될 수 있도록 SUMS 안전관리 조치도 의무화되었다.

한국은 EU와 마찬가지로 중국을 포함한 국가를 특정하여 사이버안보, 더 넓게는 국가안보를 이유로 커넥티드 카에 통합되는 하드웨어나 소프트웨어를 차단할 수 있는 법적 근거가 없다. 한국과 EU 모두 자동차 산업에서 중국이 주요 교역국이라는 측면에서 향후에도 미국과 같은 방식으로 차량 관련 규제를 도입하는 데에는 제약이 있다. 그러나 중국이 아니더라도 사이버 공격, 데이터 유출, 개인정보 침해 등에 대응하기 위해 차량 사이버보안을 데이터 및 개인정보 보호와 연계하여 유기적인 제도화 방안을 모색할 필요가 있다.

국내 법률상 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에

관한 법률」(정보통신망법), 「위치정보의 보호 및 이용 등에 관한 법률」(위치정보법), 「정보통신기반 보호법」 등이 데이터 수집 및 활용, 개인정보 보호에 적용된다. 이러한 국내 법률은 개인정보의 제공·처리·이용 제한, 위치정보 수집 금지 등을 규정하는 점에서 첨단 자동차와 관련해서도 적용 가능하다(민한빛, 2019; 심우현·박정원, 2021). 자동차 사이버보안 가이드라인과 후속 조치로서 개정된 「자동차관리법」은 네트워크, 보안과 관련된 기존 법률과 크게 상충하지 않고(국토교통부, 2020), 기존의 차량 인증제도에 사이버보안 관리체계인 CSMS 인증을 추가하여 국제기준과의 조화를 도모했다. 그러나 기존 법률은 차량과 직접적으로 관련된 데이터 보호, 네트워크 보안에 관한 것이 아니기에 차량에 관한 법률은 여전히 부재한 상황이다.

4. 사이버-공급망 안보 넥서스

미국의 커넥티드 카 규제는 명시적으로 사이버 위협으로부터 국가의 안보와 국민의 안전을 보장하는 목적을 내세우고 있지만, 중국을 견제하기 위해 자국 중심으로 자동차 산업을 재편하고 기술 및 산업 경쟁력을 강화하려는 의도가 내재해 있다고 볼 수 있다. 미국은 차량 접근 경로의 취약점을 통해 탑승자·차량·주행 데이터 탈취, 차량 원격 조작, 핵심 인프라 공격과 같은 악의적 행위가 발생할 위험이 커지는 사이버안보 위협을 부각한다. 이러한 위협을 억제하기 위해 중국이 관여한 기술의 사용을 사전에 차단하는 조치가 필요함을 정당화하며, 이를 통해 국가안보와 국민의 안전을 보장할 수 있다는 명분을 확보한다. 중국에 대한 경제적, 기술적 견제는 명

시적으로 드러나지 않지만, 동 조치가 특정 국가를 대상으로 하고 중국산 하드웨어나 소프트웨어가 제3국을 통해 미국에 우회적으로 유입되는 것까지 막는 점에서 지금까지의 對중국 경제안보 조치와 부합한다. 미국은 UN 기준이나 차량 사이버보안과 관련된 국제표준만으로 우려 대상 국가가 초래하는 국가안보 위협을 차단할 수 없다는 논리를 근거로 미국 공급망에 대해 해당국 연계 기업들을 선제적으로 차단하기로 한 것이다. 이는 사이버 안보와 공급망 안보 간 넥서스화가 나타나는 지점이다.

미국의 자동차 수입 중 중국산 완성차가 차지하는 비중은 2023년 기준 3.5%로 낮다. 그러나 중국산 부품 수입은 2023년 기준 10.7%로 비교적 높다. 즉, 미국의 자동차 부품 공급망에서 중국의 역할을 무시할 수 없다. 게다가 미국은 멕시코를 통한 중국의 우회 수출을 경계하고 있다. 미국은 자동차와 자동차 부품의 멕시코 의존도가 높은데(2023년 기준 각각 30.6%, 40.5%), 중국의 對멕시코 자동차 산업 수출이 2023년 86억 달러, 무역수지 흑자가 72억 달러에 달했다. 2022년 8월 시행된 인플레이션감축법(Inflation Reduction Act, IRA)으로 인해 중국 전기차와 부품의 對미국 수출 경로가 막히면서 이를 우회하는 방안으로 멕시코에서 조립하여 미국·멕시코·캐나다 협정(USMCA) 관세 혜택을 받아 미국으로 우회 수출하는 것으로 파악된다.

이렇게 다양한 경로로 중국산 자동차 및 부품이 미국으로 유입될 수 있는 것을 고려하여 미국은 중국과 연계된 기업과의 거래를 차단하는 방법으로 커넥티드 카 규제를 설계하고 적용하는 것이다. 이는 안보 위협을 차단하는 것뿐만 아니라 미국의 자동차 산업 경쟁력을 유지하는 것과도 직결된다. 중국과의 자동차 무역에서 자동차 부품은 2010년부터 현재까지 계속 무역수지 적자를 기록하고 있고, IRA를 통한 자국 산업 지원에도 불구하고 배터리 전기차(BEV)가 무역수지 적자를 기록하고 있어 미국으로서는 자국

산업의 경쟁력 저하가 우려되는 상황이다.

트럼프 대통령은 취임 직후 '미국 우선주의 통상정책'을 통해 제3국 우회를 통한 중국의 불공정 무역 관행을 검토하여 추가적인 관세 조정 필요성을 확인하도록 주문하였다(The White House, 2025a). 앞서 설명한 바와 같이 4월 3일에 이러한 주문에 대한 권고사항 요약본이 공개되었는데, USMCA와 관련하여 비(非)시장 경제권에서 유입되는 물품을 줄이기 위해 원산지 규정을 강화하는 등 다수의 개선이 필요하다는 행정부 입장이 제시되었다(The White House, 2025c). 이는 제3국을 경유해 중국산이 미국 시장으로 유입되는 경로를 차단해야 한다는 정당성을 확보하려는 것으로 보인다. USMCA는 또한 2026년 7월 공동 검토(Joint Review)를 앞두고 있는 바, 미국이 멕시코, 캐나다와 공정한 무역 촉진, 시장 접근 확대, 경제안보 공조 강화를 하기 위해 필요한 조치에 관하여 의견을 수렴하고 있다. 이를 통해 우회 수출을 차단하기 위한 제도적 강화가 추진될 것으로 예상된다. 이뿐만 아니라, 2025년 2월에 예고한 대로 수입 자동차 및 자동차 부품에 25% 관세가 4월과 5월에 걸쳐 부과되기 시작했다. 한국, 일본, EU 자동차를 대상으로는 15%로 인하된 관세율을 적용하기로 했으나 아직 높은 관세율이 유지되고 있다. 즉, 미국은 중국을 배제한 공급망 재편 방안을 모색하고 있으며, 트럼프 2기 행정부 출범 이후에는 조치를 규칙 이행과 병행하여 통상 압박을 강화함으로써 자국 산업의 경쟁력을 높이려는 의도를 분명히 하고 있다.

커넥티드 카 규칙이 발효됨에 따라 중국 브랜드에서 제조한 규제 대상 자동차는 당연히 미국 시장에 진입하지 못한다. 그 외에도 본사나 주요 사업장 소재국이 중국이거나, 미국 또는 제3국 기업의 중국 계열사에서 제조되거나, 중국 기업의 차량과 부품이 제3국에서 제조되거나, 제3국 기업이 중국 부품을 사용하여 차량을 제조한 경우, 대상 차량은 미국 시장에 진입

할 수 없고, 대상 하드웨어나 소프트웨어는 미국에 판매되는 차량에 통합될 수 없다. 즉, 규제 범위에 포함되는 주체(entity)가 광범위하게 정해져 있어 모호함으로 인하여 기업에 혼란을 준다는 비판도 제기된다. 예를 들어, 테슬라가 중국 생산 허브인 상해 공장에서 제조한 전기차를 현재는 중국에서만 판매하고 있지만, 미국에 수출하고자 하는 경우 동 규칙 적용 시 수출이 불가능하다. 미 GM이 중국에서 완성차로 제조하여 미국으로 수출하던 기존 모델(Buick Envision)은 미국에서 수입하지 못하게 된다. 스웨덴의 자동차 제조사 폴스타(Polestar)는 중국 지리(Geely)가 대주주로 있어 미국에서 완성차를 수입하지 못하게 된다. 그 밖에도 중국산 부품을 사용하여 자동차를 조립하고 제조하는 기업들이 미국에 수출하고자 하는 경우, 국가를 불문하고 공급망을 재편하는 과정에서 영향을 받게 된다.

이에 따라 미국의 조치가 공급망에 미치는 영향에 대한 논의가 활발해지고 있다. 바이든 행정부 하 발행된 동 규칙은 자동차 제조사들로 하여금 미국 중심의 공급망으로 재편하고 중국을 대체할 공급처를 찾도록 하는 조치로 평가되고, 미 상무부는 이 과정에서 수집한 방대한 공급망 데이터를[21] 바탕으로 중국산을 제한하는 조치를 더욱 정교화하는 전략을 추진할 것으로 전망된다(Goujon and Sebastian, 2024). 한편, 미국의 새로운 규제가 미국의 공급망 탄력성을 강화하거나 외국의 위협으로부터 미국에 더 안전한 환경을 제공하기 어려울 것이며, 그 과정에서 많은 비용과 노력이 들 것이라는 전망도 나온다(Elms, 2025). 차량이나 부품의 생산지, 기업의 소유권을 근거

21) VCS 하드웨어 또는 적용 대상 소프트웨어와 관련된 금지 거래에 관여하지 않는 수입업자 및 제조업체는 산업안보국(Bureau of Industry and Security, BIS)에 적합한 거래임을 증명하는 연례 적합성 선언(Declaration of Conformity)을 제출해야 하기 때문에 BIS는 공급망 데이터를 수집할 수 있다.

로 중국 정부와의 접점을 찾아 특정 제품의 "국적(nationality)"을 규명함으로써 중국산을 커넥티드 카 공급망에서 배제하는 것이 불가능에 가깝다고 보기 때문이다.

트럼프 대통령이 취임하며 광범위한 커넥티드 제품과 관련된 ICTS 거래를 규제할 필요성을 제기했으나 아직 ICTS 규제를 넓은 의미의 커넥티드 제품까지 확대하는 공식적 발표는 없는 상황이다. 다만, 커넥티드 카에 적용한 'ICTS 공급망 안보 규정'이 무인항공시스템(Unmanned Aircraft Systems, UAS)에도 적용될 가능성이 있다. 2025년 1월 3일 미 상무부는 UAS 관련 사전규칙 제정안(ANPRM) 'UAM 관련 정보통신 기술 및 서비스 공급망 안보(Securing the Information and Communications Technology and Services Supply Chain: Unmanned Aircraft Systems)'을 연방관보에 게재했다. E.O. 13873에 따라 외국 적대국과 연계된 ICTS 거래 중 드론의 설계, 제조, 유통 과정 전반과 관련된 규제를 검토하는 것을 내용으로 한다. 아직 ANPRM 다음 단계로의 진전은 없으나, 트럼프 대통령이 2025년 6월 '미국의 드론 지배력 강화(Unleashing American Drone Dominance)' 행정명령(E.O. 14307)에 서명하면서 드론 규제가 새로운 국면을 맞이했다. 동 행정명령은 드론 및 관련 부품의 연방기관 조달 계약에서 외국 적대국을 배제하고 미국산 드론이 우선 구매되도록 정하며, 중국산 드론에 대한 규제 강화와 제3국 공급 차단 가능성에 관한 내용을 담고 있다. 이 역시 아직 규칙으로 제정되지 않았으나 사이버-공급망 안보 넥서스를 드러내는 미국의 규제가 커넥티드 제품군뿐 아니라 드론과 같은 다른 분야로 충분히 확장될 수 있는 점을 암시한다. 그리고 이러한 일련의 조치가 미국산 기술의 국내 상용화를 촉진하고, 자국의 산업 기반을 강화하며, 자국 기술 및 시스템의 수출을 촉진하는 정책 목적을 지닌 것은 분명하다.

5. 결론

이 글은 사이버보안이 단순한 기술적 이슈를 넘어 국가안보 의제로 부상함에 따라 안보적 관점에서의 입법이 본격화되고 있음을 미국의 커넥티드카 규제 사례를 통해 보여주었다. 미국은 차량 네트워크의 취약점을 통해 발생할 수 있는 데이터 탈취, 원격 조작, 인프라 공격 등의 사이버 안보 위협을 우려하고 있다. 이러한 위험을 관리하기 위해 중국과 연계된 기업과 기술을 선제적으로 차단하는 조치를 정당화하고, 국가안보를 확보할 수 있다는 명분을 강화하여 규제를 확대하고 있다. 다만, EU와 한국의 경우에는 UN 기준과 국제표준에 근거하여 첨단 자동차를 둘러싼 사이버 '보안' 문제를 다루고 있으며, 자동차 산업에서 중국이 이들 국가에게 주요 교역국인 점을 고려할 때 미국처럼 국가안보를 이유로 중국산 자동차 및 자동차 부품에 직접적인 제재를 가하는 데 한계가 존재한다. 그러나 EU와 한국이 채택한 UN 기준 자체도 자동차의 전 주기에 걸쳐 사이버보안 체계 확립을 요구하여 공급망 전반에 걸쳐 자동차 제조업체와 부품 공급업체가 사이버보안 위험을 관리하도록 하는 점에서 공급망과 연계된 사이버보안의 중요성을 보여준다.

미국은 여기에서 한발 더 나아가 중국산 하드웨어나 소프트웨어가 제3국을 통해 미국에 우회적으로 유입되는 것 또한 막고자 하고, 교역국에서 수입되는 자동차 및 자동차 부품에 대한 관세율을 인상했다. 이는 기업의 소유권을 근거로 중국 정부와의 연계성을 규정하여 미국 공급망 유입을 차단하는 것에 더해, 관세 인상 등 다각적으로 무역을 제한하고 있음을 보여준다. 이렇듯 미국은 바이든 행정부부터 트럼프 2기 행정부에 이르기까지

중국을 배제한 공급망 재편 방안을 지속해서 모색하고 있다. 그 기저에는 미국이 자국 기술의 국내 상용화를 가속화하고, 산업 기반을 강화하며, 자국 기술의 해외 확산을 촉진하는 정책 목표가 있다. 이러한 조치는 향후 커넥티드 제품군뿐 아니라 국가안보에 영향이 있다고 판단되는 다른 분야에도 적용될 것으로 전망된다.

한국에서는 현재 외국의 기업이나 기관이 관여함으로써 위험을 발생시킬 수 있는 차량 제어권 탈취를 통한 범죄, 부품을 이용한 차량 보안 침해, 국내 서버 열람을 통한 정보 유출과 같은 사건에 대응하기에는 법률이 미비한 상황이다. 차량과 관련하여 국내에서 생산된 데이터의 국외 이전, 해외 기업 제품(부품 포함) 및 서비스의 국내 제공을 통한 데이터 취득 등 데이터의 이동성을 통상 관점에서 안전하게 관리하고, 필요시 제품 유입을 제한하고 데이터 유출을 막기 위한 정책 수단이 필요하다. 이를 위해서는 데이터의 국경 간 이동을 '보안'과 '안보'의 시각에서 통합적으로 보는 규제 체계의 필요성을 검토하여 차량 데이터의 활용과 이동에도 적용할 필요가 있다.

제5장

사이버-AI-인지 안보 넥서스

송태은 | 국립외교원 국제안보통일연구부 조교수

제5장

사이버-AI-인지 안보 넥서스

송태은 | 국립외교원 국제안보통일연구부 조교수

1. 서론

2022년 2월 러시아-우크라이나 전쟁과 2023년 10월 발발한 이스라엘-하마스 전쟁은 이미 2014년 이후 서구권에서는 오랫동안 대응 논의가 이루어져온 '인지전(cognitive warfare)'에 대한 각국의 논의를 본격화시키는 계기를 만들었다. 두 전쟁에서 인터넷과 소셜미디어에 확산된 전쟁과 관련된 기만적인 내러티브와 전장의 이미지 및 영상은 적의 항전의지를 좌절시키고 적 지휘부의 전장에 대한 정보분별을 교란하여 적이 잘못된 의사결정을 내리도록 유도하는 정보활동이었다. 두 전쟁의 인지전에서 정규군이나 테러 대원뿐 아니라 IT 프로그래머, 초국가 해커, 일반 시민까지 적국의 정상적인 인지과정(cognitive process)을 방해하고 교란하는 활동에 가담하면서 평시에도 기만적인 정보활동이 기획되고 실행될 수 있는 환경이 민간에도 조성되었다.

평시 인지전은 '戰(warfare)'으로서 표현되기보다 '영향공작(influence operations)'으로 일컬어지고 유럽연합(EU)은 '외국의 정보왜곡과 개입(Foreign

Information Manipulation and Interference)' 즉 'FIMI'라는 용어로 일컫는다. 하이브리드 위협(hybrid threats)의 한 형태인 이러한 기만적인 정보활동은 국가안보까지 위협할 수 있기 때문에 세계 각국은 방송통신 및 미디어와 관련된 정부 부처뿐 아니라 군, 정보기관, 외교부 등이 모두 범부처적으로 이러한 외부로부터의 공격적인 악의적 정보활동에 대응한다.

개인과 사회, 국가 지도층이나 군 지휘부의 인지과정을 교란하는 인지전이 전시와 평시를 가리지 않고 전개될 수 있는 오늘날의 정보커뮤니케이션 환경에서 국가는 개인의 '인지영역(cognitive domain)'도 국가안보를 위해 보호할 대상으로 인식하게 되었다. 이러한 인식은 동시에 적국의 인지영역이 자국의 정보작전과 군사작전의 대상이 된다는 것을 말해주기도 한다. 즉 사이버 공간에서 인간과 인공지능 기술이 실시간으로 유통시키는 정보와 커뮤니케이션 활동이 국가 안보에 영향을 끼치면서 안보의 영역이 사이버 공간을 넘어 인지영역까지 확대된 것이다. 육상, 해상, 공중, 사이버 공간과 우주공간을 넘어 인간의 마음까지 전장화되고 있는 것이다.

이러한 맥락에서 이 글은 현대의 사이버 공간, 인공지능 기술, 개인과 사회 전체의 인지영역이 서로 어떻게 연결되어 하나의 넥서스를 구성하며 국가안보의 중요한 축을 형성하는지 논의한다. 또한 이 글은 평시와 전시를 구분하지 않고 인지전이 전개되는 오늘날 사이버-인공지능-인지안보의 넥서스에 있어서 인공지능 기술 자체의 인지안보도 현대의 국가안보에 있어서 중대한 이슈가 될 수 있음을 논하는 것으로 이 글의 결론을 대신하며 마무리한다.

2. 인지안보의 개념

'인지안보'는 개인이나 국가가 온라인 공간과 오프라인 공간 모두에서 전개하는 악의적인 정보활동으로부터 개인과 사회 전체를 지키는 안보를 일컫는 개념인데 아직 학술적으로 정립된 개념이 아니고 널리 사용되는 용어도 아니다. 하지만 국가 간에 악의적으로 전개되는 디지털 프로파간다(digital propaganda), 허위조작정보 캠페인(disinformation campaign), 영향공작(influence operations)이나 인지전(cognitive warfare) 혹은 EU에서 사용하는 용어인 외국의 정보왜곡과 개입(Foreign Information Manipulation and Interference) 즉 'FIMI'가 국가안보에 대한 위협으로 인식되고 있기 때문에 향후 안보의 주요 개념으로 부상할 가능성이 크다. 즉 의도적으로 왜곡된 정보의 다양한 위험으로부터 개인과 사회, 국가를 보호해야 하는 개념을 '인지안보'로 일컬을 수 있다.

개인과 사회, 국가의 정책 결정자들은 모두 무엇이 개인의 안전이나 국가안보에 대한 '위험(risk)'이고 '위협(threats)'인지, 무엇이 충분히 회복력을 발휘하여 극복할 수 있는 수준의 '위기(crisis)'인지, 아니면 개인의 삶이나 국가안보 전체를 무너뜨릴 수 있는 수준의 영향을 끼칠 수 있는 중대한 위기인지 판단하는 데에 있어서 인지적 정보분별력을 사용한다. 사회에서 일어나는 크고 작은 사건과 사고, 국가 간의 갈등과 충돌 등에 대한 정확한 정보분별에 실패하여 위험이나 위협에 적절하게 대응하지 못하면 궁극적으로 개인의 안전이나 국가안보가 위기를 맞게 된다.

이러한 맥락에서 국가안보를 위협하는 외부 공격자 혹은 외부 공격자가 사용하는 프록시(proxy) 세력이 취할 수 있는 인지공격의 가장 쉬운 방법은

정보를 이용한 공격이다. 이는 공격 대상 국가의 개인과 대중, 국가 지도층과 군 지휘부의 사고, 즉 인지과정에 개입하여 조작된 정보를 통해 잘못된 정보분별과 판단, 그릇된 의사결정을 유발하고 호도하는 정보커뮤니케이션 활동이다. 최근 국가 배후 영향공작이나 허위조작정보의 유포 및 전시 인지전 전개에 있어서 대규모언어모델(Large Language Model, LLM) 혹은 생성형 인공지능(generative AI)이 빈번하게 동원되는 일도 기만적인 인지공격의 성공도를 높이기 위한 전술이다. 한편, 공격을 받는 국가의 입장에서는 이러한 정보활동에 기만당하지 않도록 자국 대중과 군의 인지역량을 강화할 필요가 생기고 미디어 리터러시(media literacy)와 사이버 공격에 대한 회복력(resilience) 증진에 노력을 기울이게 된다.

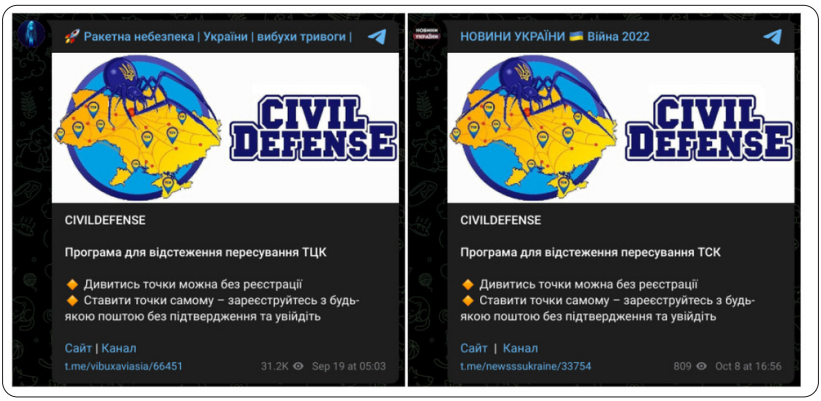
군사적 차원에서 오늘날 적을 기만하거나 아군의 정보역량·인지역량을 강화하는 데에 있어서 인공지능과 사이버 기술은 결정적인 영향력을 발휘하기 때문에 국가 기능을 수행하는 데에 관여하는 다양한 인공지능 시스템이나 이러한 인공지능 시스템과 연결된 사이버 공간은 국가의 인지안보를 위협하기 위한 주요 공격 대상이 된다. 선거철 인터넷과 소셜미디어 플랫폼에서 유통되는 허위조작정보와 가짜뉴스가 여론을 왜곡하고 시민들의 투표에 영향을 끼치는 일은 2010년 중반부터 전 세계 모든 국가에서 반복적으로 발생하고 있다.

미국에서는 2025년 6월경부터 인공지능 기술로 만든 국무장관 마크 루비오(Marco Rubio)의 합성음성과 가짜문자를 보안 메신저 앱인 시그널(Signal)을 통해 외국 외교부 장관, 미국 주지사 1명, 미국 하원의원 1명을 포함한 5명 이상의 고위 관료들에게 발신한 일이 있었다. 2024년 1월에도 美 뉴햄프셔주 민주당 예비선거를 앞두고 바이든 당시 대통령의 가짜 음성으로 유권자들에게 투표에 불참하라는 전화가 걸려 온 사례도 있었다. 최근 북

한 해커들은 해킹으로 탈취한 개인정보로 신분을 위장하고, 딥페이크(deep fake) 기술로 가상의 인물을 만들어 화상 인터뷰에 참여하는 방식으로 2017년부터 2023년 사이 미국의 테크 기업 등에서 약 130명이 취업에 성공했다.

또 다른 예로는, 적을 기만하기 위해 적에게 고의적으로 왜곡된 데이터 혹은 완전한 '허상'과 같은 데이터를 노출시킬 수 있다. 최근 러시아는 우크라이나 군 징집 대상 시민들의 개인 휴대폰이나 PC를 멀웨어(malware)로 감염시켜 허위조작정보를 지속적으로 제공하는 공격을 수행했다. 즉 러시아는 우크라이나 청년들이 러시아의 기만적인 앱이나 웹사이트를 사용하게 만들어 영향공작과 첩보활동을 한꺼번에 수행한 것이다. 우크라이나 정부가 징집 대상 연령을 25살로 낮추고 징병 대상이 되는 우크라이나 시민들의 개인정보를 업데이트하도록 했다. 이에 러시아 해커조직 'UNC5812'은 텔레그램에서 80,000명의 구독자를 보유한 'Civil Defense'라는 계정으로 우크라이나 청년들을 유인하여 사용자들에게 러시아의 미사일 발사 관련 정보, 징집 장소에 대한 정보 및 징집 관련 뉴스를 제공하는 멀웨어 바이러스가 숨겨진 소프트웨어를 사용자가 다운로드 받도록 유도했다. 'Civil Defense' 텔레그램 앱은 앱스토어 밖에서 다운로드 받을 수 있는데, 사용자의 익명성을 보장하고자 위장된 설명을 제공하고, 이 앱을 사용자가 실행하면 사용자는 멀웨어 앱을 탐지하는 'Google Play Protect'를 무력화시키도록 안내 받았다. 사용자는 이 앱을 통해 징집과 관련된 가짜뉴스, 예를 들어 징집센터에서 일어나는 구타 행위 등 징집에 대한 공포와 거부감이 생기게 하는, 징집과 관련된 부정적인 내용의 가짜영상을 지속적으로 제공받았던 것이다(Starks 2024).

〈그림 6-1〉 러시아 우크라이나의 군 징집 대상자를 유인하기 위해 운영한 가짜 앱 'Civil Defense' 텔레그램 계정



위와 같이 인공지능과 사이버 기술을 이용한 '인지공격' 만큼이나 '인지방어' 혹은 '인지역량 강화'도 인지안보에 있어서 중요한 이슈이다. 현재 인지전에 대한 연구와 논의는 보다 '공격'에 대한 내용에 초점이 맞춰져 있지만 최고의 공격력은 최고의 방어력이 부재할 경우 아무 의미가 없다. 인공지능의 도움에 의해서건 아니건 간에 적에 대한 아군의 상황인식 역량과 인지 우세가 압도적인 수준을 유지하면서 신속하고 정확한 의사결정 과정을 문제없이 수행할 경우, 적국의 아군에 대한 인지공격은 쉽게 무력화될 것이기 때문이다. 미국 국방부의 메이븐(Maven) 프로젝트는 인공지능이 전장의 이미지·영상을 인식하고 타겟에 대한 타격 결정을 지원하는 시스템으로서 이미 러우전쟁에 투입되어 운용되고 있다. 병사와 기계 간의 상호작용과 팀워크가 전장 상황을 더 빠르게 전개시키면서 효과적인 타격을 가능하게 하는 파괴력을 발휘하도록 가동시키고 있는 것이다.

이렇게, 사이버-인공지능-인지영역의 인지안보 넥서스는 인지공격과 인지역량 강화의 두 개 차원을 모두 포함하게 되며 그러한 넥서스가 어떻게

현실적으로 나타날 수 있는지는 슈퍼솔저를 이용한 인지 우세 전략과 합성 데이터를 이용한 기만전술을 통해 설명할 수 있다.

3. 인지역량 강화: 슈퍼솔저의 사례

아직까지 뇌과학과 인공지능 기술의 발전은 군사적 차원에서는 적군의 뇌에 대한 직접적인 공격보다 '슈퍼솔저(supersoldiers)'의 개발 등 아군의 인지능력 강화와 관련하여 가시적인 성과를 만들고 있다. 인공지능(AI), 센서, 네트워크, 생체·신경강화 기술 등이 결합되어 장병의 인지역량과 육체적 역량을 획기적으로 증강시켜 전장에 대한 더 뛰어난 상황인식(situational awareness)과 더 오래 버티고, 더 잘 싸울 수 있는 슈퍼솔저 양성이 실제로 가능해졌다. 인공지능 기술이 적용된, 인간이 몸에 착용하거나 입을 수 있는 기계 골격인 엑소스켈리톤(Eksoskeleton), 뇌-기계 인터페이스(Brain-Machine Interface, BMI), 야간비전(night vision), 생체모니터링기기(Biometric monitoring devices), GPS 및 커뮤니케이션 기능, 생체공학 기술이 적용된 웨어러블 기기는 모두 장병의 인지역량과 전투력 강화에 기여한다.

미국 국방부는 마이크로소프트(Microsoft)와 계약을 체결하고 'IVAS(Integrated Visual Augmentation System)'로 불리는 증강현실(Augmented Reality, AR) 기술이 적용된 스마트헬멧을 개발하고 있다. 이 기술은 현실을 보여주는 영상과 컴퓨터가 생성한 영상(Computer Graphics, CG)이 혼합되어 보이도록 만드는 것이 핵심이다. 세계 7위의 방산 업체인 영국의 'BAE Systems'이 개발한 전투기 조종사용 스마트헬멧인 'Striker II'는 조종사에게 실시간으

로 야간과 저조도에서도 표적에 대한 정보를 실시간으로 전송받아 신속한 의사결정을 돕는 데에 효과가 있는 것으로 평가되고 있다.

미국 기업인 퀘이크테크널러지(Qwake Technologies)는 화재 현장에서 소방관의 경로 탐색과 협업을 지원할 수 있는 'C-THRU'로 불리는 스마트헬멧을 개발했다. 이렇게 웨어러블 기기들은 벌써 국방과 소방 분야에서 빠르게 적용되고 있다. 국내에서도 한국전자통신연구원이 현장에 있는 소방대원의 안전 확보와 신속한 구조·구급 활동을 위한 스마트헬멧을 개발한 바 있다. 이 헬멧은 GPS와 생체신호 정보를 통합하여 대원의 위치를 실시간으로 파악하고 대원으로부터 비정상적 생체신호가 나타나면 신속하게 지원할 수 있도록 돕는 기술이다.

이탈리아에서는 2020년 초 코로나19 감염 가능성이 있는 사람들을 식별할 수 있도록 열 카메라를 장착한 중국이 개발한 'KC Wearable' 헬멧을 경찰이 착용하여 사용한 사례가 있다. 중국에서도 광범위하게 사용된 바 있는 이 헬멧은 한 번에 최대 13명, 1분 동안 200명의 체온을 96%의 정확도로 체크하는 것이 가능하다(박소영·이강복 2023). 이런 식으로 스마트헬멧은 사회감시나 치안에도 광범위하게 사용될 수 있다.

위와 같은 웨어러블 기기를 착용한 군 장병은 위험한 작전 지역에서 더 안전하고도 효과적이고 강력하게 자신의 임무를 수행할 수 있다. 슈퍼솔저는 시력과 청력을 향상시키는 장치를 착용하고, 뇌에 심어진 칩을 통해 전송받는 정보로 작전환경에 대한 더 높은 인지력을 갖게 될 것이고, 뇌파를 통해서 다른 군인과 통신하고 드론을 조종하며, 나노 입자 혈청이 팔과 다리에 이식되어 지구력, 근력 등이 향상되고 피곤하지 않도록 회복력을 향상시켜줄 것이다. 기분이 우울하거나 불안이나 두려움을 느끼는 것을 뇌파 분석을 통해 감지한 웨어러블 기기가 군인의 심리 상태를 정상적으로 만들

어주도록 뇌의 특정 부위에 자극을 주는 등 적절한 조치를 취해줄 수도 있다.

미 국방부는 초연결 전장에서 복잡한 무기 시스템을 조종해야 하고 많은 스트레스를 견뎌야 하는 군인들의 뇌를 보호하려는 목적의 'Neuro-FAST(Neuro Function, Activity, Structure, and Technology)'를 비롯하여 뇌가소성훈련(Targeted Neuroplasticity Training, TNT), 차세대비수술신경기술(Next-Generation Nonsurgical Neurotechnology, N3), 활성기억회복(Restoring Active Memory, RAM) 프로젝트 등을 추진해왔다. 미국은 중국과 달리 이러한 프로젝트들을 굳이 자극적인 용어인 '인지전' 타이틀 하에 두고 있지 않다.

중국 군의 인지전 교리에는 집중력을 높이거나 수면부족 상황에서도 신속한 의사결정 능력을 유지하는 등의 '인지능력강화기술(Cognitive Strengthening Technology)'과 아울러 아군에 유리한 내러티브를 발신할 수 있는 기술과 방법을 다루는 '잠재인지무기(Subliminal Cognition Arm)' 등을 다루고 있다. 한편 중국 군의 인지전 교리에는 '인지개입기술(Cognitive Interference Technology)'이 적시되어 있는데, 초단파(microwave)를 이용하여 적군 뇌의 기능에 물리적으로 개입하거나 해를 입힐 수 있는 기술에 대해서도 논하고 있다. 만약 멀리서도 그러한 기술을 사용하여 적의 고위 정부관료, 정보기관의 요원들이나 정치인들을 공격할 수 있는 기술이나 무기가 개발된다면 이는 분명히 전쟁에 있어서 막강한 게임체인저가 될 것이다(Mantua 2024).

4. 인지역량 약화 및 교란: 합성데이터를 이용한 기만전술 사례

인지전에 있어서 핵심은 적의 감정이나 논리적 사고를 교란하여 전장을 아군에 유리하게 이끄는 것이다. 현재 생성형 인공지능이 만들어내는 거짓 내러티브 와 딥페이크 영상 등이 원래의 사실에 변형과 왜곡을 시도하는 방식이라면, 아예 애초에 완전한 허상을 창조하여 적에게 노출시키는 것도 중요한 인지공격 전술이 될 수 있다. 귀신의 존재를 믿는 사람은 밤마다 자는 것이 두렵겠으나 그렇지 않은 경우 그러한 고통을 경험할 수조차 없다. 이렇게 적에게 기만적인 데이터를 통해 인지역량을 약화시키고 교란시킬 수 있는 수단으로 합성데이터를 이용한 기만전술이 사용될 수 있다.

'합성데이터(synthetic data)'란 AI의 기계학습을 통해 구현한, 실제 세계의 패턴을 흉내 낸 데이터다. 합성데이터는 개인의 실제 정보를 사용하지 않기 때문에 개인정보 보호 등 프라이버시 침해로부터 발생하는 데이터 규제로부터 자유롭고, 인권침해와 같은 문제로 인한 소송 비용 등 다양한 재정적 손실의 문제를 해결한다. 또한 합성데이터를 사용하면 개인정보를 보호하기 위한 복잡하고 많은 비용이 드는 익명화(anonymization) 작업이 불필요하다. 결과적으로 합성데이터는 알고리즘의 기계학습에 기여하고 알고리즘의 고도화를 위한 대안으로 인식되고 있다.

최근 인공지능 업체들이 합성데이터에 주목하는 것은 알고리즘 개발 과정에서 발생하는 데이터와 관련된 윤리적 문제로부터 자유로워지려는 것 외에도, 기계학습에 사용될 양질의 데이터를 확보하려는 유인 때문이다. 즉 합성데이터를 사용하면 고품질의 데이터를 얻기 위해 과학자, 의사, 엔지니어와 같은 전문가와 작가, 배우 및 금융업체, 제약회사, 유통사 등 대기

업이 보유한 데이터 구매에 드는 비용을 획기적으로 절감할 수 있다. 특히 군사데이터의 경우 전장에서 데이터를 직접 획득하거나 군사훈련을 통해 데이터를 수집해야 하는데, 이 또한 거대 예산을 필요로 하거나 실제 전투 자체가 부재할 경우 합성데이터를 사용하는 것이 유일한 대안이 될 수도 있다.

합성데이터를 이용하여 모의 군사훈련이나 전투기의 비행 시뮬레이션에 사용할 수도 있으나 적의 인공지능이 적용된 지휘통제 시스템을 해킹하여 아예 존재하지도 않는 가상의 작전환경을 실제 전장으로 오인하도록 하는 공격이 가능할 수 있다. 전황에 대한 정확한 정보는 군사작전에 있어서 가장 중요한 요소인데 만약 특정 지역에서의 아군과 적군의 점령 상황이나 군사배치와 관련하여 적군이 가짜지도를 보며 전투하도록 유인하는 전술은 얼마든지 등장할 수 있다.

예컨대 해킹을 통해 적의 전투기가 실제로 공중에서 이동하거나 군이 군사작전에 사용하는 네비게이션 시스템이 잘못된 지도를 사용하게 만들 수 있다. 허구의 지도를 통해 존재하지 않는 공격대상에 미사일을 떨어뜨리게 만들고 민간시설을 군사시설로 오인하여 대규모 공격을 감행하게 만들 수 있다. 전시 상황이 아닌 평시에도 테러 목적으로 허구의 네비게이션 시스템으로 인해 대규모 항공 사고를 빈번하게 일으키는 등 사보타주 위협을 하이브리드 위협의 일환으로 수행한다면 공격자는 무기를 전혀 사용하지 않고도, 전쟁을 일으키지 않고도 적국의 사회 전체를 혼란과 두려움에 빠뜨릴 수 있다.

2021년 보 자오(Bo Zhao) 교수는 'CycleGAN' 알고리즘 프로그램을 사용하여 시애틀(Seattle)과 베이징(Beijing)의 위성사진을 이용하여 시애틀이 베이징처럼 보이게 하는 딥페이크(deep fake) 지도를 제작해보였다. 이러한 딥

페이크 기술을 통해 도시가 정전이 일어난 것처럼 사진이나 영상을 편집할 수도 있고 도시 전체의 분위기를 완전히 바꿔 시현해보일 수 있다.

전시가 아니더라도 딥페이크 지도는 인신매매, 납치나 요인암살 등 다양한 범죄와 테러의 목적으로도 얼마든지 사용될 수 있다. 만약 통신이나 GPS 교란 문제가 아니라 해커가 특정인의 스마트폰이나 차량 혹은 여객기의 조종 시스템을 해킹하여 가짜 네비게이션 앱을 사용하도록 만들었다고 상상해보자. 조작된 지도는 운전자가 가려는 목적지를 입력했을 때 의도하지 않은 특정 지역으로 진입하게 만들고 혹은 반드시 사고가 생길 수밖에 없도록 길이 없는 낭떠러지로 인도하는 등 위험한 운전을 기획할 수도 있다. 자살이나 사고사로 위장하기 위해 은밀한 암살을 기획하여 인적이 드문 특정 장소로 유인할 수도 있다.

존재하지 않는 곳이나 잘못된 장소에 누군가가 원래 가고자 했던 곳에 있는 것처럼 착각하게 만드는 것을 '장소스푸핑(location spoofing)'이라고 일컫는다. 인신매매, 성폭행, 장기적출과 같은 범죄, 현금 갈취를 위한 협박이나 혹은 특정인의 명성을 훼손하기 위해 이러한 공격이 이루어질 수 있다(Crampton 2024). 당신이 지방 출장을 가거나 해외 출장 중 스마트폰의 네비게이션 앱을 따라 어떤 기업의 사무실을 방문하고자 했는데, 불법적인 도박장을 은밀하게 벌여놓은 건물에 들어가게 되고 마침 경찰의 검문이 이루어지는 상황이 전개된다고 상상해보라. 물론 반대의 상상도 가능하다. 적의 스파이를 추적하고 검거하기 위해 이들이 사용하는 스마트폰이나 차량을 해킹하여 가짜지도를 이용하게 할 수 있다.

인지전 수행을 위해 합성데이터가 향후 광범위하게 사용된다면 그러한 합성데이터를 통해 만들어진 정보를 신속하게 탐지할 수 있는 AI 기술이 인지방어 수단이 될 것이다. 예를 들면, 딥페이크 기술을 통해 제작된 지도

의 진위를 탐지하기 위해서는 시공패턴(temporal-spatial patterns) 분석이 활용되고 있다. 하지만 발전하는 인공지능 기술은 탐지를 막기 위한 패턴 조작 방법도 학습할 수 있기 때문에 인공지능 기술을 이용한 탐지와 탐지 방해 기술은 알고리즘 대 알고리즘의 대결이 되고 있다(Knight 2021).

딥페이크 탐지 알고리즘에 대해 해상도가 낮아지게 하는 공격 즉 '소음제거확산모델(denoising diffusion models, DDMs)' 공격을 수행할 경우 그러한 탐지 알고리즘의 정보분별 능력이 감소되는 등 딥페이크 탐지를 회피할 수 있는 공격 기술도 개발되고 있는 것이다(Ivanovska and Struc 2024).

5. 결론을 대신하여: 인공지능의 인지안보

사람뿐만 아니라 인공지능 모델도 인지적 취약성(Cognitive vulnerabilities in AI)의 문제를 가질 수 있다. 일부 모델은 '정체성 혼동(identity confusion)'이나 '출처 간섭(source interference)'에 취약하여 공격자가 시스템의 추론 과정을 조작할 수 있다.

예컨대, 복지 대상자나 교통관리 등 정부·공공기관의 인공지능 기술을 이용한 판단에 대한 신뢰가 사라지면 국가의 정책 집행이 마비될 수 있고, 인공지능 기반 데이터 분석에 의존하는 정책 결정이 대중의 신뢰를 상실하면 "AI가 결정한 정책"이라는 반발이 생길 수 있다. 또한 인공지능 판결 보조 시스템이 사법과 법 집행에 적용되고 있는 상황에서 범죄 예측 시스템이 불공정하다는 인식이 확산되면 국가의 정치적 정당성과 정의의 공정성 자체가 의심받을 수 있다.

또 다른 예를 들어, 2023년 Tesla의 잦은 사고와 과장된 홍보로 인해 자율주행 AI 시스템 전반에 대한 불신이 확산되어 자율주행차 구매율이 급격히 하락하고, 전체 자율주행 산업에 대한 투자가 감소했으며, 규제가 강화되는 사례도 있었다. 또 다른 예로, 2025년 1월 Apple이 인공지능 기반의 뉴스 요약 서비스 기능을 중단한 일이 있었다. 인공지능이 생성하는 뉴스 알림에서 사실이 아닌 알림이 사용자에게 전달되는 사례가 발생했었기 때문이다.

이러한 사례들은 끊임없이 나타나는 만큼 인공지능을 악용한 기만술도 고도화되고 있다. 최근 온라인 게임에 불법 인공지능 치팅(cheating AI) 프로그램이 사용되어 시각 데이터를 불법으로 읽으며 실시간으로 데이터를 해석하고, 마우스·커서 데이터를 조작해 자동 조준(auto-aim) 기능을 제공하여 특정 플레이어가 이기도록 조작한 일이 중국에서 적발되기도 했다.

이런 불법 기술을 사용한 플레이어들은 자신의 게임 실력이 향상된 것으로 착각하기도 하고 상대 플레이어는 전혀 이러한 자동 조작을 탐지할 수 없기 때문에 신뢰 기반의 게임에서의 경쟁이 불가능해진다. 공정성이 핵심인 경쟁 게임에서 "치트가 판친다"는 인식이 퍼지면 정상 이용자가 이탈하게 되어 게임 업체의 입장에서는 사용자 유지율(retention)이 급격히 하락하고 매출 감소로 이어진다. 또한 AI 치트를 탐지, 차단하는 보안 시스템 비용이 급증하게 되는 등 게임 산업 전체가 비용적으로 큰 피해를 입게 될 수 있다.

위와 같은 사례들은 인공지능의 인지안보 문제가 인간의 인지안보 문제로 직접 연결되고 있음을 극명하게 보여준다. 2025년 3월부터 8월까지 미국 연방거래위원회(FTC)에 접수된 200건 이상의 신고 중 일부는 Chat GPT와의 상호작용이 정신병증 증상을 악화시켰다는 내용을 포함하고 있

었다. Chat GPT를 일상적으로 상용하게 된 현재 사회에서 인공지능이 인간의 사고와 인지능력에 지대한 영향을 끼치게 된 것이다.

또한 한편, 반대로 이러한 인공지능 서비스에 다양한 정보분석 활동을 의지하고 있는 분야에서 만약 이러한 서비스를 사용할 수 없게 되는 상황이 발생할 경우 정책 결정자뿐 아니라 학생, 연구자, 직장인 모두 자료 수집 및 정리에 더 많은 시간을 사용해야 하므로 업무 효율이 떨어질 것이고, 프로그래밍·코딩 지원을 제공받지 못하게 되는 분야에서는 당장의 개발 생산성이 큰 타격을 입게 될 것이다.

결과적으로 이러한 문제가 빈번하게 발생하게 될 경우 인공지능 기술 자체에 대한 불신을 넘어서 사회, 경제, 안보 시스템 전체에 대한 개인과 대중의 신뢰가 흔들리는 문제로 이어진다. 이미 인공지능이 정보커뮤니케이션, 금융, 의료, 국방, 행정, 교육, 미디어, 군사 등 국가에서 이루어지는 거의 모든 핵심 의사결정 구조에 들어와 있기 때문이다. 즉 인공지능의 인지안보 문제도 인간의 인지안보 문제만큼 국가 안보를 심각하게 위험에 빠뜨릴 수 있기 때문에 사이버-인공지능-인지안보의 넥서스에 있어서 앞으로 인공지능의 인지안보도 핵심적인 인지안보 이슈로서 다뤄질 것이다.

제6장

국방 AI·데이터와 사이버 안보

이종진 | 서울대학교 통일평화연구원 선임연구원

제6장

국방 AI·데이터와 사이버 안보

이종진 | 서울대학교 통일평화연구원 선임연구원

1. 서론

인공지능(AI) 기술의 급속한 발전은 전 세계적으로 국방 분야의 패러다임을 근본적으로 변화시키고 있다. 현대전에서 사이버 공간이 지상, 해상, 공중, 그리고 우주에 이어 새로운 작전 영역(operational domain)으로 부상하면서, 국방 AI와 사이버 안보는 국가 안보의 핵심 요소로 자리 잡았다. 다가올 미래의 전장은 지능화된 전장(intelligent battlefield)으로 전환되고 있으며, 전장에서 '지능우세(intelligence superiority)'를 확보하는 것이 전쟁의 승패를 좌우하는 결정적 요인이 될 것으로 전망된다.

이러한 환경 변화 속에서 상대방보다 우위에 선 지능체계를 구현하기 위한 핵심 자산은 고성능의 AI 알고리즘과 고속 계산이 가능한 컴퓨팅 능력, 그리고 그 기반이 되는 고품질의 국방 데이터이다. AI가 전략적으로 활용될 수 있으려면 학습·검증·운용의 모든 과정에서 신뢰 가능한 데이터 생태계(data ecosystem)가 구축되어야 하며, 데이터의 수집·처리·보호 과정에서 사이버 안보가 체계적으로 통합되어야 한다.

국방 AI 데이터를 통한 7가지 핵심 응용 분야는 다음과 같다. 첫째, 자율 무기 및 차량 시스템 개발은 가장 중요한 AI 응용 분야 중 하나이다. AI가 탑재된 무인 항공기(UAV: Unmanned Aerial Vehicle)와 해상 시스템은 감시와 전투 작전에 사용된다. 완전 자율 시스템은 인간의 개입 없이도 표적 교전 등 중요한 임무를 수행할 수 있다. 미국, 중국, 유럽, 인도 등과 같은 군사 강국들이 자율 무기 개발에 투자하고 있으며, 이는 군사 작전의 운용 방식을 크게 변화시킬 수 있다.

둘째, AI 기반의 시각화 시스템은 센서, 보고서, 위성 이미지, 공개 출처 정보 등 다양한 출처에서 데이터를 추출하고 수집할 수 있으며, 머신러닝 알고리즘은 데이터 내 패턴을 분석하여 위협과 이상 현상을 감지하는 데 도움을 준다. 이에 기반하여 AI 시스템은 대량의 데이터를 빠르게 분석해 위기 상황에서 실시간 통찰과 정보를 제공한다. 예를 들어, AI는 여러 언어로 된 소셜 미디어 게시물, 뉴스 기사, 온라인 포럼을 분석해 불안 징후, 잠재적 공격, 허위 정보 캠페인을 조기에 탐지할 수 있다.

셋째, 오늘날 국방 인프라 시스템은 복잡하게 연결된 디지털 시스템과 사이버 보안 협업 도구를 통해 운영된다. 이는 다양한 군사 작전의 효율성을 높여주지만, 디지털 시스템은 사이버 보안 위협에 취약하며, 침해 사고가 발생하면 심각한 피해가 발생할 수 있다.

넷째, AI를 국방 군수 분야에 통합하면 자원 배분과 공급망 운영을 최적화할 수 있다. 교통 시스템, 기상 패턴, 지정학적 사건에 대한 실시간 데이터를 바탕으로 AI 시스템은 효율적인 경로를 파악하고 최적의 자원 분배를 계획한다. 또한 AI 도구는 공급망의 위험을 종합적으로 평가하고 회복력을 높여 필수 물자의 원활한 흐름과 작전의 연속성을 보장한다.

다섯째, 미국을 비롯한 주요 국가들에서는 군사 훈련 시뮬레이션 장비

및 소프트웨어를 활용해 자국 병사들이 실제 전투에 대비할 수 있도록 훈련시키고 있다. 병사들은 현실과 유사한 임무 수행을 통해 경험적 전투 이해도를 높인다. AI 기반 모델은 학습자의 현재 능력에 맞춘 개인화된 학습 가이드, 노트, 질문 등을 제작하여 군사 시뮬레이션의 효율성을 더욱 향상시킬 수 있다.

여섯째, 예기치 않은 장비 고장은 치명적이고 비용 부담이 크다. AI 기반 시스템은 차량과 장비의 상태를 사전 모니터링하여 유지보수가 필요할 시기를 예측하고 비용이 많이 드는 다운타임(downtime, 네트워크·서버 시스템이 오프라인이거나 사용할 수 없는 상태를 뜻함)을 최소화시킬 수 있다(한국과학기술정보연구원 2024). 예를 들어, 미 공군은 AI 도구를 활용해 운용 상황을 모니터링하고 고장 가능성을 조기에 발견한다. 자동화된 모니터링은 인력이 중대한 고장과 다운타임을 피하면서 함대 가용성을 높이는 데 도움을 줄 수 있다.

마지막으로, 복잡해지는 현대 전장 환경에서 신뢰성 있는 지휘 체계는 매우 중요하다. 군 지휘관들은 AI 도구를 사용해 실시간 위협을 파악하고 효과적인 대응 전략을 수립할 수 있다. AI 기반 지휘 통제 시스템은 강력한 팀 커뮤니케이션과 협업을 지원해 모든 병력이 동일한 정보를 공유하고 신속하면서도 공동 대응할 수 있도록 만들어 준다. 해당 시스템은 운영 상황에 대한 신속한 이해와 작전의 효율화, 필요시 통제실에서 공공 안전 커뮤니케이션 발신도 가능하게 한다.

이처럼 국방 AI 데이터는 작전 효율화·위협 탐지·의사결정 지원 등 모든 군사 활동의 중심 인프라로 기능하고 있다. 그러나 데이터 중심의 AI 체계가 확대될수록 데이터의 품질·보안·윤리적 사용 문제 등 새로운 도전 과제가 부상한다. 특히, 지능형 시스템이 사이버 공간을 통해 상호 연결되는 현

대 환경에서 데이터 왜곡, 적대적 학습(adversarial learning), 정보 변조 공격(data poisoning)은 국가 안보 차원의 심각한 위협이 될 수 있다.

이 글은 국방 AI 데이터와 사이버 안보의 상호 연계성을 심층적으로 분석한다. 2장에서는 각국의 국방 AI 데이터 현황과 주요 쟁점을, 3장에서는 국내외 국방 AI 데이터 산업의 전략 경쟁을 분석한다. 4장에서는 국방 AI 데이터 생태계와 사이버 위협을 고찰하며, 결론에서는 이러한 분석을 바탕으로 향후 국방 AI 데이터 관리 체계의 발전 방향과 사이버 안보 강화를 위한 대응 및 협력 방안을 제시한다. 본 연구는 사이버 안보 관점에서 향후 국방 AI 데이터의 구축 및 활용 가능성과 국방 AI 시스템의 신뢰성 확보를 위한 전략적 시사점을 도출하고자 한다.

2. 국방 AI 데이터의 현황과 주요 쟁점

1) 특수성과 내부 제약

국방 AI의 개발과 운용은 민간 영역과 본질적으로 다른 데이터 환경과 보안 제약 속에서 이루어진다. 특히 국방 AI의 근본적 특수성 중 하나는 평시에는 적성국 관련 데이터를 확보하기가 거의 불가능하다는 점이다. 전장 인식 및 위협 예측 모델은 적의 무기체계, 전투 행동양식, 감시·정찰 패턴 등과 같은 데이터를 기반으로 학습되어야 하지만, 이러한 정보는 비공개 군사정보로 분류되어 일반적인 연구환경에서는 접근이 불가능하다. 실제 작전 중 생성되는 전투데이터(Combat Data)는 전시에야 수집되며, 대부분

군사비밀로 취급되어 민간 AI 개발 기관 및 클라우드 사업자가 이를 직접 확보하거나 실증하는 것이 사실상 불가능하다. 이처럼 '데이터 부재(Data Scarcity)'는 단순한 기술적 차원의 문제를 넘어, 유효한 운용 데이터의 확보 자체가 어렵다는 근본적인 한계를 드러내며 국방 AI 시스템 발전의 구조적 제약 요인으로 작용한다.

또한 한국의 국방 AI 시스템 연구는 법령 체계에 근거한 고도의 폐쇄적 관리 구조 속에서 운영된다. 군사기밀보호법(법률 제19076호), 국방보안업무훈령, 보안업무규정, 국방데이터 관리 및 활용 활성화 훈령, 방위산업 보안업무훈령, 국방 공공데이터 제공 훈령 등 다층의 규제체계가 국방 데이터의 수집, 저장, 배포 과정을 세밀하게 제약한다. 예를 들어, 단순한 감시 영상이나 장비 로그파일조차도 전방 감시장비에 의해 촬영·기록된 경우 자동으로 군사 비밀 등급이 부여되어, 해당 데이터는 군사보안규정에 따라 관리된다. 이 때문에 군내 AI 연구자와 민간 협력기관 간 데이터 공유가 제한되고, 실험실 외부로 데이터가 반출되는 것은 원칙적으로 금지된다(팍스경제TV 2025/02/25).

이러한 구조는 기술 발전 속도를 떨어뜨리는 또 다른 요인으로 작용한다. 망 분리 정책(Network Separation Policy)에 의해 국방 시스템은 외부 인터넷망과 완전히 차단되어 있으며, 클라우드 기반의 AI 학습·분석 환경을 도입하기 어렵다. 데이터셋의 처리 과정 또한 폐쇄망 내에서만 가능하기 때문에 GPU 병렬 연산 및 대용량 파라미터 학습 등 최신 AI 기능 활용이 근본적으로 제약된다. 최근 국방부가 민간 클라우드 기업(예: 네이버클라우드, 메가존클라우드 등)을 제한적으로 도입하는 시범사업을 추진하고 있으나(전자신문 2024/08/21), 주요 군사정보 체계에는 여전히 물리적 망 분리와 접근 통제 원칙이 우선 적용되고 있다. 이와 같은 보안 우선 구조는 AI 기술의

신속한 검증과 모델 성능 개선을 어렵게 만드는 요인으로 작용한다.

이에 더해, 한국 국방기술 획득체계의 장기화된 절차성(Procedural Rigidity) 또한 AI 기술 도입을 지연시키는 주요 난관으로 확인된다. 국방기술품질원(DTaQ: Defense Agency for Technology and Quality) 및 방위사업청 자료에 따르면, 신기술의 실전 배치를 위해서는 평균 7~10년이 소요되며, 일부 첨단무기 체계는 15년을 초과하기도 한다. 그러나 AI 기술은 그 변화 주기가 수개월 단위로 진화하는 고유 특성을 지니고 있어, 이러한 장기화된 기술 획득 순환은 기술의 적시성(Timeliness)을 구조적으로 보장하기 어렵게 만든다. 개발 초기에 첨단이던 알고리즘이 실전 적용 시점에는 구형 기술로 전락하는 '기술갭(Technology Gap)' 현상은 국방 AI 도입의 대표적 병목으로 지적된다.

이와 같은 문제를 해소하기 위한 방안으로, 2023년 국방부는 '국방 AI 신속획득제도(Fast-Track Acquisition for AI Defense Systems)' 도입했다(문화일보 2023/05/09). 해당 제도는 인공지능·데이터 분석·소프트웨어 등 민간 첨단기술 분야에서 신속히 검증된 기술을 일정한 보안 검증 절차 후 시범 적용할 수 있도록 하는 일종의 '패스트트랙' 구조를 목표로 한다. 또한 '국방 AI 데이터 댐(Data Dam)' 사업을 통해 비군사정보 기반의 학습데이터를 확보하고, 이를 군사 상황에 맞게 전환하는 '데이터 시뮬레이션 합성(AI Synthetic Data)' 연구도 병행되고 있다. 그러나 이러한 노력에도 불구하고, 실제 적성국 데이터의 비공개성, 법률적 제약, 시스템 보안 요건, 인력부족 등은 여전히 국방 AI 연구의 본질적 병목을 형성하고 있다.

결국 한국 국방 AI 데이터의 특수성과 내부 제약은 법제·보안·기술·운용의 다층적 구조로 구성되어 있으며, 이는 민간 산업에서의 AI 발전방식과 근본적으로 상이한 패러다임에서 작동한다. 평시 데이터 비가시성, 폐

쇄적 보안체계, 인력 및 인프라 한계, 기술 획득의 비탄력성은 상호 복합적으로 작용하여 국방 AI의 실증·확산 속도를 저하시킨다. 따라서 향후 국방 AI 역량 강화를 위해서는 데이터 접근 체계의 보안 등급 세분화, 폐쇄망 내 고성능 컴퓨팅 허가체계 정비, 신속획득 절차의 제도적 보완 등을 통한 '사이버 안보와 도입 속도의 균형적 구조화(Balanced Governance)'가 필수적이다. 이는 국방 AI가 단순한 기술 실험 단계를 넘어, 실질적인 전력화 단계로 발전하기 위한 제도적 전제조건이라 할 수 있다.

2) 산업 및 제도적 제약

한국 방산 산업은 낮은 이윤율, 엄격한 원가 기반 계약 체계, 장기 개발 주기, 그리고 글로벌 경쟁 환경으로 인한 복합적 구조적 제약에 직면해 있다. 우선, 방산업체의 평균 이윤율은 약 3%로, 일반 제조업(5% 이상) 및 반도체 산업(30~50%)과 비교할 때 현저히 낮다. 이와 같은 낮은 수익성은 연구개발(R&D) 투자 여력을 제한하며, 이는 곧 최첨단 기술 확보와 우수 인력 유치에서의 경쟁력 저하로 이어진다. 또한, 설계·시험·인증 단계에서 요구되는 장기 자금이 기업의 재무구조를 압박함으로써 금융비용 부담을 가중시키고, 결과적으로 지속적인 기술 혁신과 설비 현대화를 저해한다.

둘째, 방위사업청은 '방산원가대상물자의 원가계산에 관한 규칙(국방부령)'을 통해 원가 산정 기준과 적정 이윤율을 엄격히 규정한다. 이는 계약 단계에서 기업에게 예상 가능한 수익을 보장하는 동시에, 실제 발생 비용과 산정 기준 간 차이가 발생할 경우 복잡한 추가 보상 절차와 반복적 심사·감사를 야기한다. 그 결과 기업은 시장 수요의 불확실성, 설계 변경, 생산 일정 지연 등 외부 변수로 인한 비용 상승 리스크를 효과적으로 관리하

기 어려워진다.

셋째, 무기체계의 개발·획득 주기는 수년에서 길게는 10년 이상 소요된다. 이러한 장기 프로젝트는 기술 진부화의 위험을 내포하며, 도입 시점에 국제 경쟁력을 상실할 가능성을 높인다. 더불어 예산 변동, 인플레이션, 환율 변동 등 외부 요인에 민감하여 사업비 증액 위험이 상존하며, 방위정책 변화나 해외 수출 환경의 불확실성은 매출 전망을 추가로 제약한다.

넷째, 국내 시장 규모의 제한으로 방산업체는 수출 확대를 통해 성장 동력을 모색해야 하나, 낮은 국내 이윤으로 충당된 R&D 투자만으로는 선진국 업체와의 기술 격차를 해소하기 어렵다. 해외 고객의 까다로운 인증·규격 요구에 대응하기 위해서는 추가적인 비용과 시간이 소요되며, 국제 정세 변화, 수출 규제, 외교적 요인으로 인한 계약 취소·지연 리스크 또한 수출 시장 진입 장벽으로 작용한다.

3. 국방 AI 데이터 산업의 전략 경쟁

1) 국내 AI 기업의 참여

2024년 이후 한국의 국방 AI 및 클라우드 분야에서 민간 주도의 디지털 전환이 본격적으로 추진되고 있다. 특히 네이버 클라우드와 KT는 국방 데이터 관리 및 AI 인프라 구축에 핵심적인 사업 주체로 부상하였다. 이들 기업의 국방 분야 진출은 기존의 폐쇄적 군 정보체계 운용 구조에서 벗어나, 민간 기술 역량을 활용한 새로운 협력 모델을 제시한 사례로 평가된다.

우선 네이버 클라우드는 2024년 8월 국방부가 시행한 '민간 클라우드 기반 신규 시스템 구축 사업'에서 메가존클라우드와의 컨소시엄을 통해 사업자로 선정되었다(전자신문 2024/08/21). 이 사업은 국방부 내 주요 행정 및 복지 시스템, 특히 '장병체감형 원스톱 서비스 플랫폼'을 포함한 다수의 정보체계를 민간 클라우드 환경으로 이전하는 최초의 시도라는 점에서 의의를 가진다. 네이버 클라우드는 클라우드 컴퓨팅 서비스 보안인증(CSAP: Cloud Security Assurance Program)을 획득함으로써 군 내부망과의 분리 및 다층 방어체계 구축이 필요한 국방부의 보안 요구조건을 충족시켰다.

이와 더불어 네이버 클라우드는 향후 자사 초거대 언어모델 하이퍼클로바X를 기반으로 한 국방행정 지원형 AI 기능 확장을 추진 중이다. 구체적으로는 문서 자동 요약, 행정 문서 검색, 자연어 질의응답 기반의 지식관리 기능 등이 시험적 도입 대상으로 검토되고 있으며, 국방 데이터의 민감도에 따른 등급별 관리체계 구축도 병행되고 있다. 이러한 접근은 민간 클라우드 인프라를 기반으로 군용 데이터의 안전한 처리와 AI 기능의 단계적 통합을 실현하기 위한 전략적 전환으로 볼 수 있다.

반면 KT는 직접적인 AI 모델 운용보다는 인공지능 및 데이터 운용을 위한 통신·인프라 구축 측면에서 영향력을 확대하고 있다. 2025년 현재 KT는 국방광대역통합망(M-BcN), 소프트웨어 정의 데이터센터(SDDC), 스마트 부대(Smart Base) 구축 사업 등을 통해 국방부와 각 군의 네트워크 현대화 및 디지털 전환을 주도하고 있다(뉴스 스페이스 2025/08/13). 5G 기반의 밀리터리 특화망과 에지 데이터센터(Edge-DC) 설립은 실시간 작전 데이터 전송 및 분석 체계 구축의 토대를 제공하고 있으며, 이러한 기술 기반 위에서 국방용 데이터레이크 및 제로트러스트(Zero-Trust) 네트워크 모델의 실증 연구도 수행되고 있다.

그동안 민간 기업의 국방 정보시스템 참여는 데이터 주권 규제, 보안등급 제한, 민감정보 보호 등의 제약으로 인해 극히 제한적이었다. 그러나 2023년 이후 국방부와 방위사업청이 공동으로 마련한 '민간 클라우드 도입 가이드라인'과 CSAP 등급 의무화 체계의 시행은 민간 클라우드 사업자의 참여를 제도적으로 가능케 하였다. 이로써 네이버 클라우드를 비롯한 국내 주요 기업들이 국방 AI 생태계에 본격적으로 진입할 수 있는 법적·제도적 기반이 마련되었다. 현재 삼성SDS와 NHN Cloud 등도 연구개발용 국방 데이터 관리 사업에 참여하면서, 국방 AI 생태계의 다원화 및 민·군 협력적 혁신 구조 형성이 가속화되고 있다.

그럼에도 불구하고 여전히 여러 구조적 제약이 상존한다. 한국경제(2023/05/14) 등의 분석에 따르면, 국방 데이터의 보안 구역 간 연동 제한, 실전형 학습데이터의 부족, AI 모델의 지속적 재학습 체계 부재, 국방 특화 인력과 GPU 인프라의 부족 등이 주요 한계로 지적된다. 특히 기술 조달 절차의 복잡성과 장기화된 검증 제도는 민간 기술의 신속한 적용을 저해하는 요인으로 작용하고 있다.

결국 네이버와 KT의 활동은 각각 모델·데이터 중심과 인프라 중심의 상호보완적 경로를 통해 국방 AI 데이터 생태계의 기반을 형성하고 있다. 네이버는 민간 클라우드의 보안성과 AI 모델의 응용 가능성을 중심으로 군 행정체계의 디지털화를 선도하는 반면, KT는 통신 인프라와 데이터 운영 체계의 현대화를 통해 AI 적용 환경의 토대를 강화하고 있다. 이러한 변화는 한국 국방의 디지털 전환 과정에서 민간기술의 전략적 가치가 점점 더 높은 비중을 차지하고 있음을 보여준다.

2) 해외 방산 AI 기업의 진입 노력

도널드 트럼프 대통령은 2025년 1월, 오픈AI(OpenAI), 오라클(Oracle), 소프트뱅크(SoftBank) 및 아랍에미리트 국부펀드(MGX) 등과 함께 '스타게이트(Stargate)' 프로젝트를 공식 발표하며, 5,000억 달러 규모에 달하는 민관 연합 인공지능(AI) 인프라 투자계획을 공개했다(Reuters 2025/01/22). 스타게이트는 미국 내 대규모 데이터센터 건설 및 AI 연구개발 환경 조성을 목표로 하며, 2025년 즉시 약 100억 달러가 초기 투입되어 텍사스 애빌린에 초대형 데이터센터 건설이 추진되고 있다. 트럼프 대통령은 해당 프로젝트가 '역사상 최대 인공지능 인프라 투자'임을 강조하며, 미국의 AI 기술 주도권 및 국방 기술 우위를 확보하려는 국가적 전략의 일환임을 밝혔다(AP News 2025/01/23).

국방 분야에서는 2019년부터 DARPA가 'AI Next 캠페인(Campaign)'에 20억 달러 이상을 투자하여 3세대 AI 기술, 즉 적응형 인공지능과 인간-기계 협업 알고리즘 연구를 본격화했다(FEDSCOOP 2018/09/07). AI Next는 실전 적용을 목표로, 보안성·설명가능성·융합성 있는 AI, 그리고 국방 데이터 활용 시 신속한 상태 인식 및 의사결정 지원이 핵심이다.

미국 팔란티어(Palantir)는 미 국방부 및 정보기관과 협력해 AI 플랫폼 Foundry 등 데이터 분석 인프라를 제공함으로써, 실시간 표적 식별, 정밀한 위협 분석, 합동 정보 융합 등에 핵심 기술을 지원하고 있다(DEFENSCOOP 2025/02/25). 특히 마이크로소프트, 팔란티어 등 굴지의 IT·AI 기업들과의 협력을 통해 분산 클라우드 환경과 AI 모델 배포, 상황 인식 자동화 등 군 작전 및 정보 분석의 서버-클라이언트 전환을 가속화했다.

2022년에는 미 국방부가 아마존웹서비스(AWS), 오라클, 구글, 마이크로

소프트 네 개 기업과 90억 달러 규모의 '합동 전투 클라우드 역량(JWCC: Joint Warfighting Cloud Capability)' 계약을 체결, 전 미군 도메인 및 분류 수준에서 엔터프라이즈 클라우드 환경을 구축 중이다(NextGov 2022/12/07). 이로써 클라우드 기반 인프라를 통해 데이터 접근성과 유연성을 극대화하고, 작전 현장부터 전략적 지휘소까지 즉각적인 데이터 활용을 보장하고 있다.

미국은 국방 데이터의 물리적·획일적 보호에서 탈피하여, 데이터의 중요도·민감도에 따라 단계별 분류와 통제를 시행한다. 특정 프로젝트나 민감 정보는 특별 액세스 프로그램(SAP: Special Access Program)이나 민감구획정보(SCI: Sensitive Compartmented Information)로 엄격히 구분되며, 방산업체 및 협력 기업과 안전하게 연계·공유하는 데이터 거버넌스 체제를 실현하고 있다(DoD News 2024/06/26). 2024년 12월 미 국방부는 생성형 AI 같은 차세대 AI의 도입에 속도를 내기 위해 AI 신속 역량반(AI Rapid Capabilities Cell)을 창설했다(National DEFENSE 2024/12/11). 미 국방부 디지털·AI사무국(CDAO: Chief Digital and Artificial Intelligence Office)이 관리하는 해당 조직은 프론티어 AI 모델을 비롯해 AI를 활용한 최첨단 도구를 국방부 전역에 적용하는 업무를 담당한다. 아울러, 2025년 9월 미 국방부는 OpenAI와 2억 달러 규모 계약을 체결, 프론티어 AI(Frontier AI) '프로토타입' 및 국방 맞춤형 LLM, 반(半)자율 에이전트 개발 등을 본격화했다(BreakingDefense 2025/06/17). 이는 방대한 데이터 분석 및 군사 현장 적용부터, 행정 업무 자동화, 실시간 정보요약, 작전 보조까지 AI 활용 폭이 확대되는 대표적 사례다.

정보기관 역시 아마존 웹서비스(AWS: Amazon Web Services) 등 민간 클라우드 서비스를 조기에 도입, 중앙정보국(CIA) 및 미 정보공동체는 2013년부터 AWS 기반 비밀 클라우드(C2S)를 장기적으로 운용하며, '최고기밀' 환

경에서도 대용량 데이터 처리 및 공유 효율화를 달성하고 있다(NextGov 2024/12/13).

이처럼 미국은 정권 차원의 대규모 AI 인프라 투자, 첨단 국방 AI 연구개발, 민간 빅테크와의 전략적 국방 데이터 협력, 단계적 데이터 보호와 선별적 공유체계, 클라우드·AI 융합을 통한 실시간 정보 활용에 이르기까지 전방위적 'AI 기반 국방 데이터 생태계'를 빠르게 확장 및 고도화하고 있다.

팔란티어가 2024년 4월 2일 대전에서 개최한 'AI·디지털 기술 국방 활용 제안발표회'에서 선보인 첫 번째 솔루션은 'MDO 수행을 위한 AI 기반 육군항공부대 지휘 관리 결심 지원체계 구축'이다(Target@Biz 2024/04/03). 팔란티어에 따르면 육군 항공사령부에 산재한 빅데이터를 통합해서 지휘관이 모든 휘하 부대 상황을 한 번에 파악할 수 있는 대시보드를 만든다. 이후 AI와 ML을 사용해서 항공기의 운용 사항을 점검해서 고장이나 문제가 생기기 전에 사전에 경고 및 정비 제안을 하는 것이다. 이미 팔란티어가 미 육군에 제공하고 있는 솔루션과 유사하다. 미 육군은 밴티지(Vantage)라는 프로그램으로 야전부대의 상황에 대한 대시보드를 제공하고 있다. 또한 PPMX라는 예측 정비 솔루션을 통해 AH-64E 아파치 헬기의 모든 부품 데이터를 파악해 고장이나 문제가 발생하기 전 90% 이상의 정확도로 사전에 경고하는 기능을 갖추고 있다.

두 번째 솔루션은 'AI 기반 공개출처정보(OSINT, Open Source Intelligence) 수집분석 플랫폼'이다. 해당 플랫폼은 공개된 정보로부터 의미 있는 군사정보를 추출하는 것이다. 과거에는 정보통신 기술이 부족해 필요한 정보가 매우 드물어 위험하게 적진에 정찰기를 투입하거나 인공위성, 혹은 스파이를 사용해 아주 적은 수의 정보로 적의 동향을 추적해야 했다. 하지만 현대는 모든 사람이 스마트폰을 가지고 미디어가 발달해 너무 많은 정보의 홍

수 속에서 적의 동향을 올바르게 파악하는 것이 오히려 어려운 실정이다.

팔란티어는 2024년 4월 HD현대중공업과 무인수상정(USV) 개발을 위한 업무협약을 체결했으며, 팔란티어의 미션 오토노미(Mission Autonomy) 기술과 HD현대의 자율항법 기술을 통합한 정찰용 USV를 2026년까지 개발하기로 합의했다. KT와의 전략적 파트너십도 중요한 이정표이다. 2025년 3월 팔란티어는 KT와 국내 최초로 전략적 파트너십을 체결하여 'Worldwide Partner Ecosystem'에 한국 기업으로는 처음으로 KT를 포함시켰다. 이 협력을 통해 KT 보안 강화 퍼블릭 클라우드(SPC, Secure Public Cloud) 환경에서 팔란티어 솔루션을 보안성이 강화된 환경에서 제공할 수 있게 되었다(The Korea Times 2025/03/13).

또 다른 미 방산 AI 기업 안두릴(Anduril Industries)은 한국 국방 AI 데이터 및 무인 전장 기술 분야에 적극적으로 접근하고 있다. 안두릴은 2025년 한국 지사를 공식 설립하며(NATE뉴스 2025/07/22), 대한항공, HD현대, LIG넥스원 등 주요 한국 방산업체와 합작을 통해 AI 기반의 무인기(UAV), 자율함정, 감시정찰 시스템 공동 개발에 착수했다(조선일보 2025/08/08). 특히 안두릴은 국내 방산기업과의 협약을 바탕으로 한국형 AI 무인기 모델을 지능형 데이터 기반으로 설계·생산하고, 한국 내 생산 거점 구축과 아시아 수출을 추진 중이다.

안두릴의 접근 방식은 '실제 국방 데이터 없이는 아무것도 할 수 없다'는 철학을 전제로, 현장 군 데이터에 대한 활용과 개방을 핵심적으로 강조한다. 즉, 한국군이 보유한 교육·운용·작전 데이터의 AI 및 자동화 시스템 적용을 위해 적극적인 데이터 유통과 플랫폼 표준화가 필수라는 목소리를 내고 있다. 이를 위해 안두릴은 데이터 파이프라인 구축, AI 임무 체계 현지화, 연합 데이터 학습 등 다양한 기술적 방법을 통해 한국 국방 AI의 실질

적인 효용 극대화를 도모하고 있다.

또한 안두릴은 미국 및 호주 국방부에 이미 공급하는 AI·자율 무기체계의 경험을 바탕으로, 한국의 방산 현대화와 군 인력 부족 대응, 전장 자동화 등에 필요한 솔루션을 제공함으로써 한국 국방부·방위사업청 등 공식 기관과의 협력 강화를 적극적으로 추진하고 있다(Yonhap News Agency 2025/08/06). 최근에는 AI 기반 자율 임무 수행·감시정찰·신뢰성 모니터링 등 데이터 중심 융합 기술이 전장 운영 최적화에 필요하다는 점을 강조하며, 한국 국방 AI의 글로벌 경쟁력 제고에 기여할 계획임을 밝혔다.

4. 국방 AI 생태계와 사이버 안보

한국의 국방 AI 시스템은 군사정보 자산을 기반으로 학습·추론·판단을 수행한다는 점에서, 그 데이터 관리와 보안 통제는 국가 안보의 핵심 기반과 직결된다. 국방 AI 데이터의 수집, 가공, 활용, 폐기 전 과정은 민간 IT 영역보다 훨씬 더 높은 민감성과 복잡성을 지니며, 이로 인해 다양한 형태의 복합 사이버 위협에 노출되어 있다. 이러한 보안 환경 하에서 국방 AI 데이터 보호는 단순한 기술적 문제를 넘어 작전 효율성과 전략 의사결정의 안정성에 직접적인 영향을 미치는 핵심 요소로 부상하였다(한국경제 2024/07/22).

우선 대표적 위협으로 지목되는 것은 데이터 탈취 및 오염(Data Poisoning) 공격이다. 군사용 AI는 작전계획, 감시·정찰 정보, 무기체계 운용 데이터 등 고급 군사정보를 기반으로 학습을 수행한다. 만약 공격자가 개발 또

는 운용 단계에서 데이터셋을 변조하거나 오염시킬 경우, AI의 출력 결과는 신뢰성을 상실하게 된다. 예를 들어 적대 세력이 의도적으로 라벨 정보를 바꾸거나 허위 데이터를 삽입할 경우, 자율운용 무기체계나 지휘결심 지원 AI가 오판을 내릴 가능성이 높아진다. 이는 곧 전장 판단력의 오류, 잘못된 위협 인식, 불필요한 전력 투입 등 치명적인 국방 운용상의 손실로 이어질 수 있다.

다음으로, 악성 코드 삽입 및 백도어 공격(Backdoor Attack)은 AI 모델 내부의 신뢰성을 훼손하는 또 다른 중대한 위협 요인으로 부상하고 있다(보안뉴스 2025/01/06). 최근 연구 결과에 따르면, 사전에 모델 파라미터에 백도어 명령을 숨기거나 특정 패턴을 학습시켜 두는 방식으로 AI의 작동을 조작하는 공격이 현실화되고 있다. 이러한 공격은 겉보기에는 정상적으로 작동하지만 특정 조건이 충족될 때만 악의적 출력을 발생시키는 특성을 가지고 있어 탐지가 매우 어렵다. 국방 시스템 내에서 이와 같은 백도어가 활성화될 경우, 적의 교란 신호나 위장 정보를 정당한 정보로 오인할 위험이 발생하며, 이는 지휘통제망·무기체계의 작전 통합 과정 전체를 위협할 수 있다. 이에 국방혁신기술보안협회는 AI 시스템 전 단계에 대한 코드·모델 검증, 정적·동적 분석을 포함하는 다층형 백도어 탐지체계 구축을 권고한 바 있다.(국방혁신기술보안협회 2024/03/27)

한편 모델 역공학(Reverse Engineering) 및 모델 추출(Model Extraction) 공격은 국방 AI의 내부 알고리즘 유출과 지식 침투를 겨냥한 지능형 위협으로 주목받고 있다. 외부 공격자가 API 또는 질의(Query) 요청을 반복적으로 수행하여 모델의 구조적 특징과 파라미터를 재구성하는 방식이다. 이러한 공격이 성공할 경우, 군사적 의사결정 로직이나 위협탐지 알고리즘이 복제되어 해외 세력의 정보전에 이용될 수 있다. 국방 AI의 특성상 완전한 네트워

크 격리를 유지하기 어렵다는 점에서, 이러한 공격 유형은 폐쇄망 외부 인터페이스(예: 연구 협력용 데이터 교환 API)를 통한 유입 위험이 상존한다. 이에 따라 국방 관련 연구기관들은 폐쇄형 연산망 내부에서 실행되는 모델 보호 프레임워크, 차등 개인정보보호(Differential Privacy) 기법, 그리고 질의 기반 이상행동 탐지(Abnormal Query Detection) 기술을 단계적으로 도입 중이다.

더불어 최근 AI 신뢰성과 데이터 편향성 문제는 AI 전장 환경의 학습 정확도와 판단 공정성에 직접적인 영향을 미친다. AI 시스템이 불완전하거나 왜곡된 훈련 데이터를 학습할 경우, 인식 오류와 의사결정 실패로 이어질 가능성이 존재한다. 예컨대 감시·식별용 AI가 특정 기상·지형 또는 적외선 조건에서 비정상적인 결과를 산출할 경우, 탐지정확도가 급격히 저하될 수 있다. 여기에 더해, 생성형 AI(Generative AI)와 대형언어모델(LLM)의 급속한 확산은 새로운 형태의 위협, 즉 딥페이크 영상·음성 기반의 심리전, 가짜정보 확산전 등으로 군 정보전 양상을 변화시키고 있다. 2024년 이후 실제로 국내외 방위연구기관들은 생성형 AI 기술이 적대 국가의 정보조작 및 여론 혼란 공작에 활용된 연구 사례를 다수 보고하였다.

이러한 복합적 위협에 대응하기 위해 국방 분야에서는 제로트러스트(Zero Trust) 기반 보안 프레임워크와 리스크 관리체계(RMF: Risk Management Framework) 도입을 단계적으로 확산하고 있다. 제로트러스트 모델은 사용자의 신원·접근 권한·데이터 흐름을 지속적으로 검증하는 보안 철학을 기반으로 하며, AI 데이터 및 모델에 대한 세분화된 접근통제(Role-based Access Control)와 실시간 이상 탐지를 핵심 요소로 포함한다.

아울러 AI 데이터 보호를 위한 세부 실무 대책으로는, 신뢰성 검증 및 학습 데이터 정제(Data Curation), 가드레일(Guardrail) 시스템 구축, 적대적 공격 대응 모의훈련(Red-Team Challenge) 등이 병행되고 있다. 이러한 체계는 모

델이 보안상 안전하게 작동하는지를 검증하고, 위조 데이터나 비인가 입력에 대해 방어적 반응을 유도하는 것을 목표로 한다. 나아가 실제 침해 사례 및 공격 시나리오를 기반으로 한 교육·매뉴얼화가 추진되어, 현장 담당자의 실시간 대응역량을 제고하고 있다.

결국 국방 AI 데이터의 안전한 생명주기 관리를 위해서는 기술적 안전장치뿐 아니라 정책적, 관리적, 인적 요소의 복합적 통합이 요구된다. 데이터 수집·가공·분석·폐기 각 단계에서의 위협 감시, 접근통제, 보안성 평가를 정례화하고, 악성 코드 삽입·데이터 오염·모델 유출 등 복합형 공격에 대응할 수 있는 실시간 모니터링 체계 구축이 필수적이다. 이러한 일련의 조치들은 향후 한국 국방 AI 생태계가 단순한 디지털 전환을 넘어, 자율·지능형 군사체계의 안정성과 신뢰성을 확보하기 위한 전략적 기반으로 작용할 것이다.

5. 결론

2025년 7월 이재명 대통령이 "군사 보안을 유지하면서 데이터 공유 범위를 확대할 방안 검토"를 지시함에 따라, 국방부는 상대적으로 보안 등급이 낮은 위성·무인기 정찰 데이터, 통신·항적 데이터를 우선 개방 대상으로 검토 중이며, 검증된 기업에 '비밀취급 인가증'을 부여하는 방안을 병행 추진하고 있다. 이러한 조치는 국방 데이터의 민간 활용도를 제고하면서도, NATO 합동사이버방위센터(NATO CCDCOE)나 미 국방부의 사이버보안 성숙도 모델인증(CMMC: Cybersecurity Maturity Model Certification)처럼 인증 기

반의 정보보호 프레임워크를 국내 실정에 맞게 구현하려는 시도로 평가된다(매일경제 2025/07/09).

방산업계는 한국도 미국과 유사하게 민간 클라우드 기업의 기술력을 활용하면 국방 AI의 성숙도를 크게 높일 수 있다고 본다. 국가정보원은 이미 클라우드 서비스 보안 수준을 상·중·하로 분류하여 국방 데이터 취급 가능 기업의 인증 제도를 도입했고, 삼성SDS와 KT 클라우드 등이 최고등급 '상' 인증을 획득하였다. 이와 같은 국가 차원의 클라우드 보안 체계 구축은 미 국방부의 CC-SRG(Cloud Computing Security Requirements Guide)와 유사한 로드맵으로, 향후 국방 데이터의 체계적 관리와 신뢰성 확보의 토대가 될 것이다.

다가오는 지능형 전장에서는 AI 기반 국방 역량이 국가 안보의 핵심 경쟁력으로 부상할 전망이다. 전통적 군사력의 물리적·인적 우위를 넘어, 전투 수행 과정에서 수집·분석되는 방대한 데이터의 실시간 처리와 AI 알고리즘 기반 의사결정이 전장 주도권을 좌우하게 된다. 특히 합동전영역지휘통제체계와 유사한 다영역 네트워크 중심 작전 체계가 확산됨에 따라, 데이터 상호운용성과 시스템 연계성 보장은 국방 디지털 전환의 핵심 과제가 되고 있다. 동시에, AI의 자율성 증대와 적대적 AI(Adversarial AI), 딥페이크 기반 기만 전술(Deepfake-based deception) 등 적대적 활용 가능성은 새로운 안보 위협을 야기하므로, 공격과 방어 양면에서의 AI 대응 전략을 병행해야 한다.

첫째, 데이터의 분류·관리·공유 체계를 재설계하여 보안성과 활용성 간 균형을 확보해야 한다. 한국의 망 분리 정책은 보안을 강화하는 한편 AI 학습 데이터 확충에 제약을 주고 있다. 이에 미국의 NIPRNET(Non-classified Internet Protocol Router Network)처럼 '비밀은 아니지만 보호가 필요한 정보

(CUI: Controlled Unclassified Information)'를 안전하게 유통하는 망 구조를 참고할 필요가 있다. 계층적 데이터 접근 권한 제도와 보안 등급별 관리 체계를 정립함으로써, 위성·정찰 이미지 등 낮은 보안 등급의 데이터를 점진적으로 개방하고 AI 연구 생태계의 기반을 확충할 수 있다.

둘째, 민군 협력과 국제 공조를 확대하여 기술·인력·자원의 시너지를 극대화해야 한다. 국내 민간 기업의 AI·클라우드 기술을 국방 프로젝트에 적극적으로 도입하고, 방산업체·연구기관과의 공동 R&D 플랫폼을 구축함으로써 운영 효율을 높일 수 있다. 또한 한·미·일 및 NATO와의 AI 기술협력·표준화 논의를 심화시켜 상호운용성과 글로벌 기술 경쟁력을 강화해야 한다. 미국 DARPA와 영국 국방과학기술연구소(DSTL: Defense Science and Technology Laboratory)이 추진 중인 AI 상호운용 표준 연구 협력 모델은 한국에도 시사점을 제공한다.

셋째, AI 모델의 지속적 신뢰 확보를 위해 제도적·조직적 지원체계를 구축해야 한다. 데이터 불균형과 전장 환경의 불확실성은 지속적인 재학습(Re-training) 체계를 요구한다. 이에 따라 국방부 내 AI 전담 조직의 상설화, 예산의 안정적 확보, 군·학·연 협업 훈련체계의 제도화가 필요하다. AI 모델 검증 윤리지침(Responsible AI Principle) 역시 NATO나 미 국방성의 AI 윤리 프레임워크(AI Ethics Framework)처럼 명문화되어야 한다.

넷째, 지능형 사이버 방어 역량을 강화하여 AI기반 위협에 대응해야 한다. AI를 활용한 사이버 공격(예: 데이터 중독, 자동화된 침투)은 탐지 속도와 정확도의 경쟁으로 전개된다. 이에 따라 위협 예측, 자가 복구(Self-healing), 자동 대응(Auto-response) 기능을 포함한 차세대 보안 플랫폼 개발이 시급하다. 양자암호통신, 동형암호(Homomorphic Encryption), 연합학습(Federated Learning) 등 첨단 기술의 조기 도입은 폐쇄망 환경에서도 데이터 보호와 학

습 효율을 동시에 달성할 수 있는 현실적 대안이다.

마지막으로, 국방 AI 전략의 투명성과 윤리성을 확보해야 한다. 국민적 신뢰를 전제로 하는 국방 AI 거버넌스 구축을 위해서는 감사·검증 체계를 강화하고, 알고리즘의 설명 가능성과 편향 관리 원칙을 제도화해야 한다. 이러한 '책임 있는 국방 AI 정책'은 미국 DOD의 '책임 있는 AI 전략 및 이행 로드맵(Responsible AI Implementation Strategy and Implementation Pathway 2022)과 같은 제도적 청사진을 참조할 수 있다. 이처럼 데이터 활용 체계 혁신, 민군 및 국제 협력 확대, AI 제도적 기반 강화, 지능형 사이버 방어 역량 향상, 그리고 투명한 윤리 기반 거버넌스의 확립을 통해, 한국은 국방 AI·데이터 생태계에서 지속 가능한 혁신 성과를 창출하며 미래 전장에서의 지능 우위를 확보하고 안정적인 사이버 안보 질서를 구축할 수 있을 것이다.

제7장

데이터 첩보(DATINT)와 사이버안보

정태진 | 평택대학교 국가안보대학원 교수

제7장

데이터 첩보(DATINT)와 사이버안보

정태진 | 평택대학교 국가안보대학원 교수

1. 서론

데이터첩보(Data Intelligence, DATINT)는 디지털 시대의 정보환경 변화를 반영하여 등장한 새로운 형태의 첩보 개념이다. 이 용어는 데이터(Data)와 인텔리전스(Intelligence)의 합성어로, 전통적인 첩보체계인 인적첩보(HUMINT), 공개정보첩보(OSINT), 기술첩보(TECHINT), 신호첩보(SIGINT), 영상첩보(IMINT) 등의 이론적 흐름에서 파생되었다. 아직 국내외 학계와 실무 영역에서 일반화된 용어로 정착되지는 않았으나, 사이버 공간에서 이루어지는 정보활동의 본질이 '데이터의 수집·분석·활용'에 있다는 점에서 데이터첩보는 사이버안보학의 새로운 연구 분야로 주목받고 있다(Omand, Bartlett & Miller, 2021).

데이터첩보는 기존 정보수집 방식과 구조적·기술적 측면에서 뚜렷한 차별성을 보인다. 전통적 정보활동은 인간의 직접 개입과 판단을 전제로 하며, 특정 임무 수행이나 목표 달성을 위한 제한적 정보 획득에 의존하였다. 인적첩보는 인간 관계망을 통해 정보를 확보하고, 공개정보첩보는 접근 가

능한 자료를 분석하며, 기술 및 신호첩보는 물리적 장비와 주파수 신호를 기반으로 정보를 수집하는 형태를 띠었다. 이에 비해 데이터첩보는 자동화된 시스템을 이용해 방대한 데이터를 수집하고, 인공지능(AI) 및 빅데이터 분석기법을 통해 의미 있는 정보를 도출한다는 점에서 가장 큰 차이를 보인다(Schneier, 2015).

데이터첩보의 범위는 메타데이터(metadata), 사물인터넷(IoT) 장치로부터 생성되는 센서 데이터, 공공 및 민간 부문 데이터베이스 등으로 확장된다. 이를 통해 데이터첩보는 과거의 제한적 정보수집 영역을 넘어 미세 단위의 정보까지 포착하는 정밀한 분석을 가능하게 한다. 과거에는 저장공간의 한계와 데이터 처리기술의 미비로 인해 대규모 데이터 축적과 장기 보관이 어려웠으나, 최근 클라우드 컴퓨팅과 분산저장기술의 발전으로 대량의 데이터를 안정적으로 관리·활용할 수 있는 여건이 마련되었다(Birch, Cochrane & Ward, 2021).

이러한 기술적 진전은 데이터첩보의 효율성을 높이는 동시에 새로운 윤리적·법적 과제를 수반한다. 전통적 정보활동이 정보공개와 프라이버시 침해의 문제에 집중하였다면, 데이터첩보는 데이터 소유권, 메타데이터 활용의 정당성, 인공지능 알고리즘의 투명성과 책임성 등 복합적인 논의로 확장되고 있다(Redman, 2018). 특히 메타데이터의 활용은 개인의 사회적 관계망이나 행동패턴을 간접적으로 복원할 수 있어 개인정보 보호의 새로운 쟁점으로 부상하고 있다(Schneier, 2015).

이러한 맥락에서 데이터첩보는 단순한 기술적 혁신이 아니라 정보활동의 철학과 윤리를 재정립하는 지점에 놓여 있다. 방대한 데이터의 자동화된 수집과 분석은 국가안보와 정책결정의 효율성을 제고하지만, 동시에 정보통제의 권한 집중은 감시사회로의 전이 위험을 수반한다(Zuboff, 2019). 이

로 인해 데이터첩보는 효율성과 통제, 기술과 윤리, 정보활동과 시민권 보호 간의 균형이라는 복합적 과제를 내포한다. 결국 데이터첩보는 정보사회에서 지식생산의 새로운 원형으로, 첨단기술의 활용을 통해 정보의 수집·분석·활용을 통합하는 전략적 체계로 발전하고 있다. 그러나 그 확장성과 영향력만큼 개방성과 책임성을 담보할 수 있는 제도적 장치의 확립이 중요하며, 향후 연구는 기술 발전과 민주적 통제의 조화를 중심 과제로 삼아야 한다.

2. 데이터첩보와 메타데이터

데이터첩보(Data Intelligence, DATINT)의 수집 및 분석체계는 첨단 정보기술(IT)과 자동화 시스템 활용에 기반한다는 점에서 기존 정보수집 방식과 뚜렷이 구별된다. 인공지능(AI)이 발전하면서 데이터 전 단계(수집, 정제, 분석, 시각화)의 효율성과 정밀성이 크게 향상되었고, 다양한 사이버 공간·IoT·민간/공공 데이터베이스로부터 웹 로그, 메타데이터, 센서 정보, 통신기록 등 각종 형태의 데이터를 자동화 시스템으로 확보한다. 따라서 정보기관은 과거 인간 경험과 제한된 정보 소스에 의존하던 방식에서 벗어나, 실시간의 대규모 데이터 기반 정보활동이 가능해졌다.

이러한 흐름은 저장/처리기술의 제한 해결(클라우드 컴퓨팅, 분산저장 기술 등)에 의해 가속화되었으며, 정보기관들은 실시간 데이터 모니터링·분석 체계를 구축하여 국가안보, 사이버위협 대응, 정책 수립 등 여러 분야에서 데이터 기반 의사결정을 내리고 있다(Schneier, 2015; Birch 외, 2021).

데이터첩보의 구조적 핵심은 메타데이터에 있다. 메타데이터는 데이터의 생성 시각, 작성자, 저장 위치, 형식, 크기, 수정이력 등 '데이터를 설명하고 조직화하는 정보'로서, 데이터 분산성과 비연속성 해소 및 맥락 부여, 정보 구조·관계 명확화, 신뢰성 확보 등 필수적인 역할을 한다(Redman, 2018). 정확하고 일관된 메타데이터 관리체계는 대규모 데이터 환경에서 필요하며, 조직은 이를 통해 방대한 데이터를 탐색하고 전략적 의사결정에 활용한다.

데이터첩보가 대중적 관심을 받은 계기는 2013년 스노든 사건으로, 미국 NSA의 대규모 통신 메타데이터 수집 실태가 폭로되었다(Gellman, 2013). 이에 대해 미국 정부는 "통화 내용이 아니라 메타데이터만 수집했다"는 입장을 밝혔지만, 시간·상대·위치 등 메타데이터만으로도 개인의 사회적 관계망, 이동경로, 행동패턴 복원이 충분히 가능하다는 점에서 논란이 커졌다. NSA 법률고문 및 국장 등은 "메타데이터만으로도 한 개인의 삶 전체를 파악할 수 있다"고 언급하며, 전략적 자산으로서 메타데이터의 현실적 위력을 강조했다. NSA의 "모두 수집하고, 모두 알아내며, 모두 활용하라" 모토처럼, 9·11 테러 이후 미국 정부는 대테러·사이버위협 방지 등을 명분으로 정보수집 권한을 강화하며, 민간 데이터·글로벌 IT 인프라까지 포괄하는 대규모 감시체계를 정착시키고 있다(Schneier, 2015).

결국 데이터첩보는 첨단 기술활동을 넘어, 사이버안보와 국가주권이 교차하는 전략적 체계다. 자동화된 데이터 수집·AI 분석은 국가안보 효율성을 최대화하지만, 동시에 개인정보 침해·윤리적 통제의 한계 등 복합적 과제를 수반한다. 데이터첩보의 제도적 발전은 기술혁신과 민주적 통제, 데이터 주권과 글로벌 정보질서 조화의 관점에서 추진되어야 한다.

3. 빅테크의 데이터 통제와 개인정보 탈취

글로벌 빅테크 기업들은 고객관리와 서비스 고도화를 명분으로 방대한 개인정보를 수집·저장·관리한다. 스마트폰 통화·문자, GPS 이동경로, 카드 결제, 차량공유, 온라인 쇼핑과 음식 주문 기록 등 일상생활 전반 데이터가 실시간 축적되고 있으며, IoT 확산으로 가정·사무공간의 전등, 냉난방, 주차장 출입 정보까지 디지털화되었다. 생체정보까지 더해지면서 개인 프라이버시 취약성은 더욱 커졌다. 공항·항만 등 국가기반시설, 웨어러블 기기에서 수집되는 생체 데이터는 고위험 정보로 사회적 민감성이 크다.

자동화된 데이터 수집은 민간·공공 영역에서 모두 확산 중이다. 민간에서는 하이패스 차량번호 인식을 통한 이동경로 실시간 감시가 이뤄지고, 인천공항 출입국시스템은 얼굴·지문·여권정보를 자동 저장해 개인 이동과 신원 추적 통제를 수행한다. 국가별 개인정보 보호법 차이가 있는데, 한국은 엄격한 개인정보보호법을 운영하는 반면 미국은 민간 기업 데이터 활용을 폭넓게 인정하며 차량번호판 데이터가 보험사, 법률사무소 등에 합법 판매된다. 미국 민간 위성통신·기상기업도 취득 데이터를 정부·연구기관에 상업 제공하며 자율적 데이터 생태계를 유지한다.

주요 빅테크 기업(Google, Meta, Apple, Microsoft, Amazon 등)은 이용자 온라인 활동을 실시간 수집·분석해 맞춤 서비스와 광고를 최적화한다. 그러나 동시에 이는 개인 정보주권 약화와 감시 권력 집중을 초래한다. 구글 전 CEO 에릭 슈미트가 “우리는 당신이 어디에 있고, 무엇을 하며, 무엇을 생각하는지 안다”고 한 것은 감시기술의 현실을 상징한다. 2018년 Cambridge Analytica 사건은 약 27만 명 사용자뿐 아니라 네트워크 9,700만 명

개인정보를 무단 수집해 정치 광고와 여론 조작에 활용한 분수령 사건이다. 미국 연방거래위원회와 영국 정보위원회가 조사했고 미국 정부는 러시아 정보기관 개입 일부를 인정했다. 데이터는 경제 자산을 넘어 정치적 영향력과 사회 권력 핵심 도구임을 보여준다. 빅테크 기업이 데이터 통제 통해 여론, 시장, 정책 결정 영향력을 행사하는것은 사실상 국가 정보주권에 준하는 권력 집중이고, 개인 프라이버시와 민주 질서에 대한 위협이다(Schneier, 2015; Siegelman, 2021).

2024~2025년 전 세계적으로 개인정보보호법 개정, AI·딥페이크 규제 강화, 빅테크 규제 의무화 움직임이 확산 중이다. 미국과 유럽연합은 프라이버시 권리 강화, 데이터 처리 투명성, AI 책임성 확보 법률·정책을 강화하고, 한국 개인정보보호위원회도 빅테크 자율규제 및 민관 협력체계 구축에 나서고 있다(개인정보위, 2025).

2000년대 중반 이후 데이터는 경제적 자산이자 전략 자원으로 인식되며 데이터 절도·불법 유출 피해가 폭증했다. 전 세계적으로 2020년 약 370억 건 개인정보가 해킹당한 것으로 추산된다(Afifi-Sabet, 2020). 개인정보 침해 사고 수는 감소했으나, 공격 대상이 대규모 데이터베이스 보유 글로벌 기업과 공공기관으로 이동하면서 피해 규모는 커졌다. 2022년 호주 대형 해킹 사건은 2,200만 명(호주 인구 76%) 개인정보 유출 피해를 입히며 단일 데이터 침해가 국가 차원의 정보보호 체계를 흔들 수 있음을 입증했다(Wadhwani, 2022).

2023년에도 미국 의료보험사 Change Healthcare 랜섬웨어 공격과 MGM 리조트 사이버 공격으로 각각 수백만, 약 1,500만 명 개인정보 유출 및 서비스 마비가 발생했다. 2024년 중국 상하이 공공데이터 플랫폼 해킹은 약 10억 건 시민정보가 탈취돼 중국 최대 규모 데이터 유출로 기록됐으

며, 중앙집중형 데이터 보관구조의 보안 취약성을 드러냈다(Schneier, 2015).

한국의 경우에도 2023년 대형 금융기관 데이터베이스 침투, 2024년 포털사이트 회원정보 대량 유출, 2025년 SK텔레콤 유심(USIM) 정보 해킹 등 민간 플랫폼 보안 취약점이 노출됐다. 특히 SK텔레콤 사건은 이동통신 핵심 인프라를 직접 공격해 국가 사이버보안 신뢰에도 심각한 영향을 미쳤다.

데이터 유출은 1차 정보침해에 그치지 않고 탈취 데이터가 다크웹 등에서 거래되며 명의도용, 보이스피싱, 전자상거래 사기, 불법 결제 등 2차 범죄가 반복된다. 특히 의료기록·생체정보 특성상 장기적 피해로 작용하며 사회 신뢰 붕괴와 디지털 사회 안정성 저하로 이어진다(Porcedda & Wall, 2021).

데이터 탈취 급증 원인으로는 복잡해진 디지털 생태계로 단일 보안침해가 연쇄 피해를 유발하고, 랜섬웨어 서비스화(RaaS)가 진입장벽을 낮추며 전세계 확산, 개인정보 디지털화와 클라우드 저장구조가 유출 확산 속도를 높인다. 기존 방화벽 중심 보호전략으로는 복잡한 공격 벡터 차단에 한계가 있으므로, 전 과정 법·제도적 보호체계 강화와 국가 간 정보공유체계, 국제 사이버범죄 대응협력 제도화가 병행되어야 한다(Kokas, 2018).

결과적으로 데이터 절도·불법 유출은 정보주권·경제안보·사회 신뢰에 복합적 영향을 미치는 현상이며, 데이터는 개인의 신원·경제활동·사회적 지위 등을 나타내는 중요 요소다. 따라서 현대 국가 데이터정책은 기술개발 중심을 넘어 법·제도·윤리·국제규범의 통합적 관점에서 데이터안보를 핵심 국가전략으로 인식해야 한다.

4. 데이터 첩보와 사이버 안보 간 융합

데이터안보는 21세기 디지털 패권 경쟁의 핵심 전략자산으로 각국이 국가안보의 필수 요소로 인식하고 있다. 미국과 중국은 데이터 주권을 둘러싼 치열한 경쟁 중이며, 중국은 정부와 공산당이 민간 데이터를 포함해 광범위한 데이터를 통합 관리하는 '전체주의적 데이터 거버넌스'를 구축하고 있다. 반면 미국은 데이터 이동 자유를 국제경제 원칙으로 유지하되 특정 국가와의 데이터 거래를 제한하는 이중 전략을 구사한다. 2023년 이후 생성형 AI 확산으로 민감 데이터의 비가시적 유출 문제와 대형 언어모델(LLM)이 국가기밀과 개인정보에 접근할 위험성이 대두되면서, 각국은 AI 학습 데이터 관리 및 사이버 윤리 규범 제정에 적극 나서고 있다. 2023년 일본 히로시마 G7 정상회의에서는 '신뢰할 수 있는 AI와 데이터 이동'을 공동 정책 목표로 선언하고, 일본은 '신뢰할 수 있는 데이터의 자유로운 이동(DFFT)' 원칙을 주도하며 국제협력 체계를 강화했다(Yuzue & Sekiyama, 2025).

국가별 정책을 보면, 미국은 2024년 행정명령 E.O. 14117로 위험국가와의 데이터 거래를 제한하고 '국가데이터보호위원회'를 설치해 민간 데이터 안보 영향 평가를 체계화했다. 2025년에는 AI와 데이터 보호를 결합한 정책(E.O. 14203)을 시행해 연방기관에 민간 AI 데이터 출처 검증을 의무화했다. EU는 GDPR과 함께 2023년 EU Data Act, 2024년 AI Act를 제정해 개인정보 보호와 AI 윤리를 통합 관리하고 빅테크 기업의 데이터 독점 견제와 디지털 자율성 강화에 주력한다. 중국과 러시아는 데이터 현지화 및 인터넷 독립 정책으로 국가 주권을 수호하며, 일본은 2019년 오사카 트랙과

2023년 DFFT 협의체 출범을 통해 자유롭고 신뢰할 수 있는 데이터 이동을 실현하고 있다(Tian & Feirong 2025).

데이터첩보(DATINT)와 사이버안보(Cyber Security)는 현대 정보전에서 불가분의 전략 체계다. 데이터첩보는 방대한 데이터를 수집·분석해 국가안보, 정책결정, 군사 전략에 활용하고, 사이버안보는 데이터 기밀성·무결성·가용성을 보장하며 정보자산의 유출·변조·파괴를 막는다. 2023년 이후 러시아-우크라이나 전쟁 등에서 AI 기반 자동화 공격이 확대되고 미국 사이버보안국(CISA)은 딥페이크, AI 탐지회피 및 생성형 AI 모델을 활용한 데이터 탈취 시도 급증을 보고했다. 이는 데이터첩보가 이용하는 대규모 AI 분석모델이 공격 대상이 될 수 있음을 보여준다(Lin, 2025).

사이버위협은 크게 사이버첩보(비인가 데이터 절취)와 사이버공격(시스템 교란·변조)으로 구분된다. 중국 APT, 북한 라자루스 그룹, 러시아 샌드웜 등이 금융기관과 방위산업체를 목표로 정교한 데이터 침투를 시도해 왔다. 데이터 폭증과 클라우드, IoT 보편화는 공격 표면을 확대해 데이터첩보와 사이버방어는 실시간·통합적으로 이뤄져야 한다. 미국과 중국은 AI 기반 데이터첩보 체계로 전략적 정보 우위를 추구하고, EU와 일본은 국제 협력과 투명성 확보에 집중한다. 한국은 국가데이터안보위원회를 중심으로 공공데이터 보호, 사이버 훈련, 민관 인력 양성을 추진하고 AI 기반 위협정보 공유체계를 시범 운영해 데이터첩보와 사이버안보 융합을 모색 중이다.

결론적으로 데이터첩보와 사이버안보는 상호 보완적인 전략 관계이며, 데이터·사이버 융합안보체계 구축은 미래 국가안보 대응의 핵심 축으로 발전할 전망이다. 양자컴퓨팅, 블록체인 등 차세대 기술과 결합해 미래 정보전 및 안보 체계의 중심이 될 것이다.

5. 주요 법률 및 정보기관의 역할

미국 국가안보국(NSA)의 데이터첩보 및 사이버정보활동은 대통령 행정명령 제12333호(1981), 미국애국자법(US Patriot Act) 제215조(2001), 해외정보감시법(FISA) 제702조(2008년 개정)를 법적 근거로 하고 있다. 이 법들은 NSA에 광범위한 해외·국내 정보수집 권한을 부여하였으며, 특히 FISA 702조는 외국인을 대상으로 하는 정보수집을 공식화하고 미국 내 거주자의 통신도 포함하는 포괄적인 법적 틀을 마련하였다(Miller, 2019).

2023년부터 2025년까지는 디지털 전환과 AI 확산, 개인정보 보호 및 사이버 위협 대응 강화를 반영한 법률 개정과 신설이 활발히 이루어졌다. 2024년 발의한 미국 개인정보 보호법(APRA)은 국가 차원의 통합된 개인정보 보호 기준을 마련하고 데이터 주체 권리를 강화했으며, 기업에는 투명성 규제를 강화했다. 2025년 발의된 No Adversarial AI Act(Braun, 2025)는 외국 적대국 소유 AI의 연방정부 도입 금지를 규정하며 AI 위험 관리에 중점을 두었다. 캘리포니아와 콜로라도 주에서는 AI 윤리 및 투명성 관련 주 차원의 법률도 강화되었다. 2025년 4월 미국 하원은 적대국 개입 사이버 위협에 대응하기 위한 사이버 복원력 강화 법안을 발의했고, EU도 사이버 보안법 개정을 통해 IOS와 ICT 인증 강화 및 국제 공조 확대에 나섰다.

미국 정보기관 조직은 2025년 빅데이터·AI·OSINT 분야 중심으로 대규모 인력 재배치 및 보강을 진행 중이다. CIA 중심으로 수천 명 규모의 조정이 이루어졌으며, 이는 핵심 데이터 및 AI 전문 인력 확보와 부처 간 협력 강화를 위한 조직 개편이다. 국가안보국, 국방부, 민간 보안기업과 협력해 '조기 AI 위협경보 체계'를 도입하고, 민관 통합정보분석센터와 실시간 대

응본부를 운영하고 있다. NASCIO 등 기관과 연계해 사이버보안, AI 및 자동화 기반 공공부문 협력 모델을 발전시키며, 동맹국과도 AI·사이버 위협 정보 공유 및 공동 대응을 강화 중이다(Russ-Eft, 2025).

영국 정부통신본부(GCHQ)는 2025년에 국립데이터분석센터를 설립해 AI 기반 데이터 분석과 사이버첩보를 융합했고, 사이버전자전사령부를 신설해 공세적 AI·데이터 주권 기반 사이버작전을 강화하고 있다. 일본과 호주는 민관 협력으로 첨단기술 개발, 위협분석, 디지털 인프라 보안 및 복원력 강화 조직 개편과 투자를 추진하고 있다. 조직 개편의 주요 방향은 빅데이터·AI·OSINT 중심 조직 확대 및 인력 재배치, 사이버·디지털 위협 통합·융합 조직 강화, 부처 간 실시간 협력 및 글로벌 민관 협력 확대, AI·클라우드·블록체인 인재 채용과 신속한 의사결정 체제 구축, 국가 AI 위협 조기경보 및 데이터 공유 시스템 구축 중이다(Dylan & Stivang (2025).

이는 2024~2025년 딥페이크, 생성형 AI 공격, 데이터 주권 분쟁 등 신흥 위협에 적극 대응하기 위한 전략적 필수 조건으로 자리 잡았다. 주요국 정보기관은 AI·빅데이터 시대의 융합 분석과 민관·국제 협력 네트워크를 확대해 다층적 사이버안보와 데이터첩보 전략을 혁신하고 있으며, 이는 글로벌 데이터 주권 경쟁과 미래 정보전 패러다임의 핵심 분기점이다.

6. 결론

데이터첩보와 사이버안보의 융합이 현대 국가안보의 핵심 전략 영역으로 떠오름에 따라, 이에 적합한 법·제도적 기반과 정책 방향 설정이 절실히

요구되고 있다. 최근 연구와 국제 동향을 토대로 다음과 같이 학술적 관점에서 종합적 제언을 제시하고자 한다.

첫째, 국가 차원의 사이버·데이터 안보 법체계 정비를 최우선 과제로 인식해야 한다. 미국은 전통적 정보수집 법률인 대통령 행정명령 12333호, 미국애국자법, 해외정보감시법(FISA)을 현대 디지털 환경과 AI 기술 확산에 맞게 개인정보보호법(APRA), No Adversarial AI Act 등으로 확장 개정하며, 디지털 권리 보호와 국가 안보 균형을 모색 중이다. 유럽연합 역시 GDPR, AI규제법, 데이터 거버넌스법을 통해 개인정보 보호와 AI 윤리의 법제화를 완성하여 글로벌 표준을 선도한다. 법률 체계는 데이터 이동성, 투명성 보장 및 외국산 적대 AI 통제 등 신흥 규범을 포괄해야 하며, 동시에 민주적 원칙과 인권보호를 강화하는 방향으로 설계되어야 한다.

둘째, 정보기관의 조직 구조 혁신과 민관 협력 강화가 필수적이다. 미국 NSA, CIA 등은 AI·빅데이터·OSINT 전문 인력의 조직 내 통합과 민간 보안기업 및 정부기관과 신속한 위협 공유·대응 체계를 구축하고, '조기 AI 위협경보 시스템'을 적극 도입해 실시간 통합 대응능력을 확보하고 있다. 영국 GCHQ는 국립데이터분석센터 설립과 사이버전자전사령부 운영으로 공세적·방어적 사이버 역량을 증강하고 있으며, 일본과 호주도 첨단기술 연구개발과 민관협력을 중심으로 디지털 인프라 보안 및 복원력 강화에 주력하고 있다.

셋째, 국가 간 데이터 주권 경쟁과 AI 기반 사이버 위협 증가에 대비해 국제 협력과 다자간 거버넌스 구축이 절대적으로 요구된다. 특정 국가 또는 다국적 기업에 의한 데이터 통제 강화를 넘어, 신뢰 기반의 데이터 공유 체계, 사이버 위협 공동 대응, AI 윤리·안전 표준 확립이 필수적이다. 이를 위해 정부 주도의 정보공유 체계 강화, 민간 부문의 역할 증대, 그리고 국제

사이버범죄 대응 협력 메커니즘 정비가 병행되어야 한다.

넷째, 신규 기술 도입과 동시에 실효적 민주적 통제와 윤리성 확보가 병행되어야 한다. AI, 양자컴퓨팅, 블록체인 등의 신기술은 데이터첩보와 사이버안보 혁신에 커다란 잠재력을 제공하지만, 이 과정에서 권력 집중과 감시 사회화 위험은 심화되기 때문이다. 따라서 기술 발전과 시민권 보호가 균형을 이루는 다층적 거버넌스 모델을 마련하는 것이 궁극적 목표여야 한다.

마지막으로, 각국 정부는 법률적 규제체계의 정비, 첨단 보안기술 개발, 전문 인력 양성 및 교육체계 확립, 국제규범 형성 참여, 그리고 민관 협업 모델의 강화 등을 포괄하는 종합적 국가 데이터 및 사이버안보 전략을 수립해야 한다. 이를 실질적으로 실행하기 위해서는 다자간 협력체계를 강화하여 사이버공격, 데이터 유출, 디지털 스파이 행위 등 초국경적 위협에 공동 대응할 수 있는 규범적 기반을 마련해야 한다. 이러한 노력을 통해 신뢰 기반의 사이버외교를 확대하고, 국제사회의 사이버안보 거버넌스에서 주도적 역할을 확보할 수 있을 것이다.

제8장

가상자산과 사이버 안보

이왕휘 | 아주대학교 정치외교학과 교수

제8장

가상자산과 사이버 안보

이왕휘 | 아주대학교 정치외교학과 교수

1. 머리말

가상자산·암호화폐 생태계에서 비트코인뿐만 아니라 스테이블 코인(stable coin)과 중앙은행디지털화폐(CBDC)도 빠르게 발전하고 있다. [22] 중국은 디지털 위안화(e-CNY, DCEP)를 2014년부터 개발하여 2020년부터 25개 대도시에서 사용이 확대되었다. 2024년 7월 기준 1억 8,000만 개 이상 개인 지갑을 개설되었으며 누적 거래액은 7조 3,000억 위안을 기록했다. 미국은 2025년 7월 지니어스법(Guiding and Establishing National Innovation for US Stablecoins Act: GENIUS Act)을 제정하였다. 이 법에 따라 미국은 지급결제용 스테이블 코인(payment stablecoin)을 발전시킬 수 있는 제도적 기반을 확보하

22) 엘살바도르는 2021년 세계 최초로 비트코인을 법정통화로 인정하였다. Fernando E. Alvarez, David Argente, and Diana Van Patten, Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador, NBER Working Paper No.29968 (2022)

였다.[23]

글로벌 금융거래에서 가상자산·암호화폐의 비중도 빠르게 늘고 있다. 지역적으로는 북미($633bn)와 아태지역($519bn)이 가장 활발하다. GDP와 대비해서는 라틴아메리카(7.7%)와 아프리카 및 중동(6.7%)이 가장 큰 비중을 차지한다. 북미에서는 스테이블 코인의 유출이 특징적이다.[24]

가상자산·암호화폐 생태계가 발전하는 데 가장 중요한 요인 중의 하나는 사이버 보안이다. 탈중앙화와 익명성을 기반으로 구성된 가상자산·암호화폐는 사이버 공격에 취약하다.[25] 이런 문제를 해결하기 위해 정부·기업·개인은 사이버보안을 강화하고 있다. 그럼에도 불구하고, 거래소에 대한 해킹도 빈번하며 자금세탁과 자본도피의 수단으로 활용되고 있다.[26] 사이버안보가 보장되지 않을 경우, 투자자의 신뢰가 하락하고 가격변동이 불안정하게 변동하여 가상자산·암호화폐의 발행과 거래는 위축될 것이다. 가상자산·암호화폐의 사이버안보는 단순히 기술적인 문제를 넘어, 금융

23) 김보영, 미국의 CBDC 입장 변화와 주요국의 CBDC 현황, 자본시장포커스 3호 (2025); 미국 GENIUS Act 입법 추진의 의의, 자본시장포커스 13호 (2025)

24) Eugenio M. Cerutti, Melih Firat, and Martina Hengge, Global Cross-Border Payments: A $1 Quadrillion Evolving Market?, IMF Working Paper No.25/120 (2025); Marco Reuter, Decrypting Crypto: How to Estimate International Stablecoin Flows, IMF Working Paper No.25/141 (2025)

25) Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch, Cyber Resilience of the Central Bank Digital Currency Ecosystem, IMF FinTech Note (2024); 오지윤, 이도경, 신하늘, 최원용, 글로벌 주요 사건을 통해 살펴본 암호자산시장의 취약성 평가 및 시사점, BOK 이슈노트 5호 (2023)

26) Clemens M. Graf von Luckner, Robin Koepke, and Silvia Sgherri, Crypto as a Marketplace for Capital Flight, IMF Working Papers No.23/133 (2024)

시스템의 안정성과 국가안보에까지 영향을 미칠 수 있다.[27] 개인·기업·정부가 유기적인 협력 체제를 구축해야만 사이버 공격의 위험을 최소화할 수 있다.

2. 가상자산의 사이버 안보 위협

1) 가상자산의 정의

암호화폐(cryptocurrency)와 가상자산(virtual Asset)은 동의어 사용되고 있다. 가상자산은 인터넷 공간에서 거래되고 가치가 형성되는 모든 디지털 자산을 포괄하는 개념이다. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」은 디지털 자산을 경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표로 정의한다. 가상자산에는 블록체인 기반의 암호화폐(코인, 토큰), 디지털 금융상품, 대체불가능토큰(NFT), 증권형 토큰(ST) 등이 포함된다. 암호화폐는 암호화 기술(블록체인)을 사용한 분산원장(DL)을 바탕으로 운영되는 비트코인, 이더리움과 같은 디지털 화폐를 의미한다. 국제경제기구와 규제 당국에서는 암호화폐가 법정 화폐로 오해될

27) Hamid Cheraghali, Peter Molnár, Mattis Storsveen, and Florent Veliqi, The Impact of Cryptocurrency-related Cyberattacks on Return, Volatility, and Trading Volume of Cryptocurrencies and Traditional Financial Assets, International Review of Financial Analysis, 95 (2024); Timothy G. Massad, Stablecoins and National Security: Learning the Lessons of Eurodollars, Brookings Institute (2024)

가능성을 우려하여 가상자산 또는 '암호자산(ㅊyptoasset)'이라는 용어를 선호한다.[28)]

〈표 9-1〉 가상자산과 암호화폐의 비교

구분	가상자산	암호화폐
범위	경제적 가치를 지닌 전자적 증표	가상자산의 한 유형
기술	모든 종류의 디지털 기술	블록체인
용도	투자, 결제, 권리 증명, 게임 아이템	투자·결제
사례	비트코인, NFT, 증권형 토큰 등	비트코인, 이더리움 등

2) 가상자산의 사이버 공격 피해 사례

블록체인 기술은 투명성과 변조 불가능성이라는 장점이 있다. 그렇다고 해서 이 기술에 기반을 둔 가상자산과 암호화폐가 사이버 안보 위협에 완전히 자유로운 것은 아니다. 가상자산과 암호화폐의 해킹 사고는 때때로 일어나고 있다. 비트코인의 가격이 급상승한 이후 그 피해 규모도 더 커지고 있다.[29)]

28) 박종세, 한명진, 최승조, 김성수, 류재민, 최지영, 암호자산 규제 관련 주요 이슈 및 입법 방향, 한국은행 지급결제조사자료 3호 (2022)

29) CSIS, Significant Cyber Incidents Since 2006 (2025)

〈표 9-2〉 해킹 사례

사건명	연도	피해 규모($)	주요 공격 방식	특징 및 영향
바이비트 해킹	2025	약 15억	콜드월렛 해킹	역대 최대 규모, 북한 라자루스 배후 의심
폴리 네트워크	2021	6억 1,100만	스마트컨트랙트 취약점	해커가 자금 반환, 보안 취약점 경고
FTX 해킹	2022	6억 이상	내부자/외부자 해킹	거래소 파산 직후 발생, 피해 심각
코인체크	2018	5억 3,400만	핫월렛 취약점, 피싱	고객 피해액 전액 보상
마운트곡스	2014	4억 7,000만	핫월렛 해킹	거래소 파산, 업계 신뢰도 하락
DMM 비트코인	2024	3억 5,000만	사회공학, 내부 시스템 침투	북한 라자루스 관련성 확인
웜홀 해킹	2022	3억 2,000만	크로스체인 브리지 취약점	Jump Crypto가 피해액 보전

출처: 언론보도 종합

3) 사이버 공격의 주체와 유형

가장 많이 알려진 위협은 조직 범죄단체이다. 해킹 기술로 무장한 이 단체는 금전적 이득을 얻기 위해 다양한 사이버 공격을 감행한다. 금전적 이득보다는 언론자유와 같은 정치사회적 대의를 주장하는 해크티비스트는 조직 범죄단체와 구분되어야 한다. 내부 정보를 폭로하는 고발자의 경우에는 금전적 이익과 정치사회적 대의를 모두 추구할 수도 있다.

국가기관이 정보를 선제적으로 확보하거나 차단하기 위해 직접 해킹에 가담하는 경우도 있다. 북한은 금융제재를 회피하는 통로로 가상자산·암호화폐를 사용하고 있다. 다른 사례에서는 해커 그룹이 주요한 행위자인데

반해, 북한 사례는 국가의 후원을 받고 있다. 탈집중화된 익명성이 보장되는 네트워크에서는 북한 정부의 개입을 공식적으로 파악하는데 한계가 있다.[30] 러시아도 가상자산·암호화폐를 미국과 EU의 금융제재에 대응하는 수단으로서 활용하고 있다.[31]

〈표 9-3〉 위협 행위자 범주

범주	내용	동기	주요 영향	자원
국가 및 관련 그룹	사이버 스파이 기능을 갖춘 정부 기관, 정보 기관, 국방 정보	정치적 우위 확보	중요한 서비스의 중단, 재정적 및 사회적 불안정, 시민들의 신뢰 상실	고도로 숙련되고, 자원이 풍부하며, 끈기가 있을 가능성이 높다. 또한 내부자에게 영향을 미쳐 위협을 더욱 증폭시킬 수도 있다
조직 범죄 단체	기술적 노하우를 가진 사이버 갱단과 개인 범죄자들	몸값과 괴롭힘 전술을 통한 금전적 이득	사기, 자금 손실, 데이터 누설 및 유출, 그리고 평판 손상	일반적으로 기술과 노하우 면에서 자원이 풍부하지만 사이버 범죄를 추적하는데 항상 IT 장비에 의존하는 것은 아니다

30) 이승열, 북한 사이버 공격 전략의 진화: 대북제재 회피를 위한 외화벌이 수단으로서 사이버 전략, 통일정책연구, 32/1 (2023)

31) William Alan Reinsch and Andrea Leonard Palazzi, Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia, CSIS (2022)

범주	내용	동기	주요 영향	자원
내부자	시스템에 대한 특권과 비즈니스 프로세스에 대한 깊은 지식을 가진 기관 또는 주요 공급업체의 직원	금전적 이득이나 평판 손상에 대한 보복. 종종 이 그룹은 다른 범주의 행위자에 의해 조작된다	서비스 중단, 데이터 유출, 사기, 평판 손상, 자금 손실	자원이 부족하지만 종종 권한이 있는 접근 권한을 가진다. 일부는 악의가 아닌 부주의한 행동으로 인해 취약성을 유발할 수 있다
해크티비스트	기술 및 사이버 전문가 그룹은 지리적으로 분산되어 하나의 대의를 위해 일하고 있다	정치적 또는 사회적 대의(예: 언론의 자유)를 진전	기관에 대한 불신과 평판 손상	자원이 부족하지만 추구하는 원인에 따라 지속적이다

출처: Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch, Cyber Resilience of the Central Bank Digital Currency Ecosystem. IMF FinTech Note (2024), pp.5-6.

사이버 공격이 집중되는 취약점은 블록체인 자체보다는 가상자산과 암호화폐의 거래와 보관이 이뤄지는 거래소, 지갑, 스마트 컨트랙트 등에 있다. 빈도도 높고 피해 규모가 큰 사례는 거래소 해킹이다. 거래소는 수많은 익명의 사용자들이 참여하고 있어 해커들이 암약하기에 매우 유리한 환경이다. 시스템 취약점 악용, 내부자 공모, 피싱 공격을 통한 직원 계정 탈취, DDoS 공격으로 인한 시스템 마비 후 공격 시도 등을 통해 마운트곡스, FTX, 바이낸스, DMM 비트코인 등 세계적 거래소가 해킹의 피해를 보았다. 우리나라의 업비트에서는 북한 해킹 조직의 이더리움 탈취 시도가 발생하였다. 거래소 해킹은 가격 조작, 강제 폐쇄 등뿐만 아니라 사용자의 비밀번호, 개인 정보, 가상자산 손실 등으로 이어질 수 있다.

개인 사용자의 가상자산 지갑을 직접 공격하여 자산을 탈취하는 사례도

있다. 인터넷에 연결되지 않은 콜드월렛보다 인터넷에 연결된 핫월렛이 해킹에 더 취약하다. 익명으로 거래되기 때문에 개인 사용자가 피해를 신고하거나 보상받기가 쉽지 않다.

사용자를 속여 개인 키(private key)나 로그인 정보 등 민감한 정보를 탈취하는 피싱 및 소셜 엔지니어링 수법도 있다. 위조된 에어드롭과 유명 거래소를 모방한 웹사이트 등의 사기 사건이 발생하고 있다.

계약 조건을 디지털화하여 자동으로 이행되도록 하는 블록체인 기반 기술인 스마트 컨트랙트(smart contract)의 버그도 공격 대상이다. 탈중앙화 금융(DeFi) 서비스에서 버그를 노린 해킹이 가끔 일어난다. [32)]

〈표 9-4〉 사이버공격 유형

공격 유형	영향
서비스 거부(DoS)/분산 서비스 거부(DDoS)	서비스 거부는 네트워크 대역폭을 인위적으로 압도하여 합법적인 사용자에 대한 액세스를 거부한다. 그 변형으로는 다양하고 널리 분산된 소스에서 실행되는 DDoS가 있는데, 그 규모가 더 크고 영향이 더 심각하다
시스템 침입 및 데이터 침투	데이터, 프로그램, 프로토콜 및 구성에 무단 접근으로 인해 데이터가 누설되고 민감한 정보, 코드 및 논리가 유출된다.

32) Douglas Arner, Raphael Auer and Jon Frost, Stablecoins: Risks, Potential and Regulation, BIS Working Papers No.905 (2020); Giulia Fanti, Kari Kostiainen, William Howlett, Josh Lipsky, Ole Moehr, John Paul Schnapper-Casteras, and Josephine Wolff, Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency, Atlantic Council (2022); BIS Innovation Hub, A Security and Resilience Framework for CBDC Systems. BIS (2023);

공격 유형	영향
멀웨어, 랜섬웨어 및 와이퍼웨어	악성 코드를 주입하여 운영을 중단하고 몸값이 지불될 때까지 민감한 데이터를 암호화한다
피싱 및 소셜 엔지니어링 공격	행동 조작과 자격 증명 도용을 위해 소셜 엔지니어링 기법이 사용되는 사람들과 관련된 위험이다
타사 및 공급망 공격	주요 공급업체 시스템에 대한 중단 또는 무단 접근으로 인해 연쇄적인 영향으로 귀결된다
암호화 키 훼손	"비밀" 암호화 키에 무단으로 접근하면 데이터 유출 및 사기로 연결된다

출처: Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch, Cyber Resilience of the Central Bank Digital Currency Ecosystem. IMF FinTech Note (2024), p.3.

결제수단에 따라 사이버 공격의 피해가 다르게 나타날 수 있다. 중앙은행이 직접 발행하는 소액결제용(retail) CBCD는 법정통화이기 때문에 사이버 보안이 침해될 경우 위험이 매우 높다. 반면 민간이 발행하는 암호화폐와 전자화폐는 피해가 특정 기업과 사용자로 한정될 수 있다.

〈표 9-5〉 디지털 결제 수단 간 사이버 위험 노출 비교

		전자 화폐	암호화폐/ 스테이블코인	소액결제용 CBDC
악의적 및 비악의적이지 않은 사건 모두의 가능성	사용 사례의 다양성. 복잡성과 따라서 목표의 수가 증가함에 따라 위험이 증가	중간 (일반적으로 하나 또는 몇 가지 목표—금융 포용)	중간 (사용 사례는 탈중앙 금융 투자부터 효율적이거나 포괄적인 국경 간 결제 시도까지 다양)	높음 (종종, 때로는 경쟁하는 목표들의 긴 목록)

		전자 화폐	암호화폐/ 스테이블코인	소액결제용 CBDC
악의적 및 비악의적이지 않은 사건 모두의 가능성	최종 사용자 접근 메커니즘. 접근 방법의 다양성에 따라 위험이 증가	높음 (물리적 카드, 휴대폰 지갑, 브라우저, ATM 등 다양한 접근 방법)	낮음 (일반적으로 브라우저, 그리고 덜하지만 휴대폰 지갑과 ATM)	중간 (다양한 접근 방법, 주로 휴대폰 지갑; 카드와 같은 물리적 장치)
	감독 및 프레임워크의 커버리지. 커버리지가 낮으면 위험이 증가	낮음 (성숙한 감독 프레임워크 및 집행)	높음 (공식 감독 없음)	중간의 (일부 기존 프레임워크는 적용될 수 있지만 금융 부문 감독 외부의 많은 구성 요소)
	보안 제어 프레임워크의 성숙도. 해당 프레임워크의 성숙도에 따라 위험이 감소	낮음	높음	중간
	사고를 관리하는 데 필요한 기술과 역량의 적절성은 위험을 축소	낮음	높음	높음
공격자의 매력	처리되거나 저장된 데이터의 양. 데이터 수집에 따라 인력이 증가하고 따라서 위험이 증가	높음	낮음	디자인에 따라 추후 변경
	채택 수준 (위와 같이)	높음	낮음	높음 (특히 민족국가로부터)

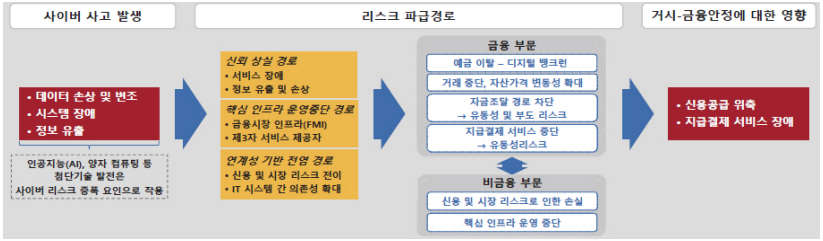
		전자 화폐	암호화폐/ 스테이블코인	소액결제용 CBDC
사이버 공격 표면	생태계의 복잡성과 범위. 그에 따라 위험이 증가	중간	높음	높음
	지리적 분산. 그에 따라 위험이 증가	낮음-중간 (PayPal 또는 Revolut과 같은 일부 주요 PSP는 해외에 진출)	높음	중간 (가치 사슬의 일부 참가자는 원격)

출처: Arvinder Bharath, Anca Paduraru, and Tamas Gaidosch, Cyber Resilience of the Central Bank Digital Currency Ecosystem. IMF FinTech Note (2024), p.42.

4) 사이버 리스크의 파급 경로

사이버 리스크는 금융안정에 세 가지 경로를 통해 심각한 피해를 줄 수 있다. 첫째는 대규모 예금 이탈(디지털 뱅크런)이다. 개인정보 데이터가 대규모로 유출된 직후 예금자들이 일시에 예금을 인출하면 금융기관은 지급불능 상황에 직면하게 된다. 둘째, 대체 불가능한 핵심 금융인프라의 장애이다. 금융인프라의 작동 중단 또는 오작동은 금융시장을 일시적으로 마비시켜 연쇄적 혼란을 야기할 수 있다. 셋째, 네트워크 효과이다. 사이버 공격을 받은 금융기관과 네트워크로 연계된 금융기관들이 폐해를 입을 수 있다. 사이버 리스크가 금융시장 전반으로 파급되면, 신용공급 위축과 지급결제 기능 장애로 인해 금융 불안정성을 단시간에 증폭될 수 있다.

〈그림 9-1〉 사이버 리스크의 파급 경로



출처: IMF, Global Financial Stability Report (April 2024), Ch.3. Cyber Risk: a Growing Concern for Macrofinancial Stability, p.6. 한국은행, 금융안정보고서 (2025), p.91에서 재인용.

3. 해결책

1) 기술

거래소/서비스 업체에 대해서는 다섯 가지 조치가 필요하다. 첫째는 로그인 및 자산 인출 시 여러 단계의 인증을 거치도록 하는 다단계 인증(MFA)의 의무화이다. 둘째는 대규모 자산은 인터넷과 분리된 콜드월렛에 보관하는 것이다. 셋째는 코드의 취약점을 사전에 검증할 수 있는 스마트 컨트랙트 보안 감사이다, 넷째, 비정상적인 거래나 접근 시도를 실시간으로 감지하고 대응할 수 있는 AI/머신러닝 기반 실시간 모니터링 및 이상 거래 탐지 시스템이다. 마지막으로 해킹 발생 시 신속하게 대응하고 피해를 최소화할 수 있는 침해사고 대응 체계의 구축이다.

개인 사용자도 자체적인 노력이 필요하다. 첫째, 비밀번호를 주기적으로

변경하고 다른 서비스와 중복되지 않도록 관리한다. 둘째, 모든 가상자산 관련 계정에 OTP/MFA 등의 2단계 인증을 설정한다. 셋째, 운영체제, 백신 프로그램 등 사용 기기의 모든 소프트웨어를 항상 최신 버전으로 업그레이드한다.

2) 법·제도

가장 중요한 과제는 관련 범죄를 예방하고 처벌하기 위한 명확한 규제 프레임워크의 구축이다. 대표적 사례는 2024년 금융위원회가 제정한 「가상자산 이용자 보호 등에 관한 법률」(약칭: 가상자산이용자보호법)이다. 이 법은 △이용자의 예치금 및 가상자산 보호, △시세 조종 등 불공정거래행위 규제, △금융당국의 가상자산사업자 등에 대한 감독·검사·제재 권한 및 불공정거래행위자에 대한 조사·조치 권한을 규정하였다.[33)]

국경을 넘나드는 가상자산 범죄에 대처하기 위해서는 고객 확인 의무(KYC), 의심스러운 거래 보고 (STR), 고액 현금 거래 보고 (CTR) 등 자금세탁방지(Anti-Money Laundering) 및 테러자금조달방지(Countering the Financing of Terrorism)를 위한 국제 협력도 필수적이다. 국제자금세탁방지기구(Financial Action Task Force)의 권고가 많은 국가에서 채택되었다.[34)]

글로벌 차원에서 법·제도의 조화는 상당히 어려운 과제로 남아있다. 미

33) 금융위원회, 가상자산 이용자 보호 등에 관한 법률 (2024)

34) 최준혁, 임지훈, 박혜성, 권헌영, 국내외 디지털자산의 사이버보안 규제 현황과 시사점. 정보법학, 27/1 (2023); 김범준, 이채율, 금융투자자 보호를 위한 가상자산(Virtual Assets)의 법제화 방안, 법학연구, 21/1 (2021)

국과 중국이 통화 패권을 둘러싼 경쟁으로 협력의 여지가 매우 적다. 중국이 중심적 역할을 하는 브릭스를 중심으로 탈달러화를 위한 노력이 가속화되고 있으며, 유로화라는 기축통화를 보유한 EU도 미국과 차별화된 전략을 추구하고 있기 때문이다.[35)]

3) CBDC/스테이블 코인 사례

사이버 보안은 중앙은행이 발행한 CBDC와 민간기업이 발행한 스테이블 코인에 대한 규제 정책에서 가장 핵심적 문제 중 하나이다. 미국은 스테이블 코인, 중국은 CBDC를 각각 추진하고 있다. 양국이 근본적으로 다른 정책을 채택하게 된 동인은 사이버 보안에 대한 상이한 평가에서 기인한다.

지니어스법을 제정한 미국은 정부 주도의 CBDC를 포기하고 민간 주도의 스테이블 코인의 발행을 준비하고 있다. 디지털 결제 혁신을 중시하는 이 법안은 스테이블코인을 발행하는 민간기관이 금융시장 안정성, 소비자 보호, 자금세탁방지(AML)를 위협하는 사이버 보안을 자체적으로 관리할 수 있다는 평가에 기반을 두고 있다.

반면 CBDC를 이미 도입해 사용하고 있는 중국은 민간기관의 스테이블 코인 발행을 금지하고 있다. 스테이블 코인이 금융안정, 자금세탁방지, 통화주권 등에 심대한 위협을 줄 수 있다고 판단한 중국인민은행과 국가인터

35) Anoosh Kumar, China's Blockchain Playbook: Infrastructure, Influence, and the New Digital Order, CSIS (2025); 이왕휘, 미중 디지털 통화 경쟁: 디지털 위안 대 디지털 달러, EAI Special Report (2020)

넷정보판공실은 알리바바와 징둥닷컴이 홍콩에서 스테이블 코인을 발행하려는 계획의 승인을 보류했다.[36] 스테이블 코인이 활성화되면 디지털 위안화가 위축되는 문제도 있다.

〈표 9-6〉 가상자산 암호화폐 정책 비교: 미국과 중국

구분	미국	중국
규제	점진적 법제화, 복수 감독 기관 분산 관리	강력 단속 및 금지, 중앙집중적 통제
주체	은행 포함 다양한 기관 가능, 규제 준수 필수	민간 발행 사실상 금지, 중앙은행 CBDC 집중
금융안정	준비금 100% 보유, 상환 의무 강화	금융안정 위협 경고, 민간 확산 차단
정책	시장 혁신과 안정 조화, 소비자 보호 및 자금세탁방지 강조	통화주권 보호, 국제 금융시장 안정 및 자금세탁방지 중점
디지털화폐	민간 주도 암호자산과 연계된 혁신 허용	디지털 위안화(CBDC) 중심 생태계 구축

아직 CBDC를 공식적으로 발행하지 않은 국가는 미국과 유사하다. EU는 시장 내 암호자산법(Markets in Crypto-Assets; MiCA)에 입각하여 포괄적인 스테이블 코인 규제 체계를 도입하였다. 스테이블 코인 발행자는 완전한 준비금 유지와 투자자 보호, 자금세탁방지 규정을 통과해야 한다. 영국도 법정화폐 연동 스테이블 코인을 결제 관련 디지털 자산으로 공식적으로 인정했다. 일본도 엄격한 자격을 갖춘 은행·신탁회사·자금이체업체가 발행

36) Cheng Leng, Zijing Wu and Arjun Neil Alim, and Ryan McMorrow, Chinese Tech Giants Pause Stablecoin Plans After Beijing Steps in, Financial Times (October 19, 2025)

한 스테이블 코인을 '디지털 결제 수단'으로 승인했다.[37)]

한국은 CBDC를 개발하였으나 법적으로 공식화하지 않았으며 스테이블 코인도 조심스럽게 접근하고 있다. 한국은행은 스테이블 코인의 위험성을 경고했다. 첫째, 코인런의 위험이다. 다수 이용자가 동시 상환 청구 시 발행사의 준비금 부족으로 인한 결제 실패와 이에 따른 금융시장 불안이 초래될 수 있다. 둘째, 금융사고 가능성이다. 운영 중단, 해킹, 사기 등 기술적·운영적 사고가 스테이블 코인의 신뢰성을 훼손하고 시장 혼란을 유발할 위험이 상존한다. 셋째, 자본도피이다. 비기축통화국에서 외화 기반 스테이블 코인이 국내 금융자산에서 자금을 해외로 빠르게 이동시키는 수단으로 악용될 경우 자본통제가 사실상 무력화된다. 마지막으로 통화정책 유효성의 제약이다. 스테이블 코인이 급격히 확산될 경우 한국은행의 통화정책 집행 및 금융안정 목표 달성이 어려워진다.[38)]

4. 결론

가상자산·암호화폐는 혁신적 금융 도구이자 동시에 사이버 안보의 새로운 핵심 이슈로 부상하였다. 이 문제를 해결하기 위해서는 기술적·제도적·

37) Jack Spira and David Wessel, What are Stablecoins, and How are They Regulated?, Brookings Institution (2025); 이정두, 스테이블코인 제도화에 따른 규제 이슈, 금융브리프 34권 특별호 17호 (2025)

38) 한국은행, 금융안정보고서 (2025), pp.37-41.

국제적 협력과 함께, 전방위적 보안 강화 노력이 필수적이다.

사이버안보에 가장 큰 위협은 양자컴퓨터의 발전에 있다. 암호화 기술이 약화된다면, 가상자산·암호화폐는 존립의 위기에 처하게 된다.[39] 아직 충분한 수의 큐비트(qubit)를 갖추지 못했다는 기술적으로 제한이 있지만, 양자 컴퓨터는 슈어 알고리즘(Shor's algorithm)을 이용해 가상자산에서 사용하는 타원곡선암호(ECDSA)와 RSA 암호의 개인키를 추출할 수 있는 잠재력을 가지고 있다. 이 위협에 대비해 미국 국립표준기술연구소(NIST)는 2022년부터 포스트 양자암호(Post-Quantum Cryptography, PQC) 알고리즘 표준화를 추진 중이다.[40]

미국과 중국의 통화 패권 경쟁도 가상자산·암호화폐의 사이버안보를 강화하는 데 방해가 된다. 글로벌 시장에서 가장 큰 시장과 첨단기술을 가진 양국이 대립하면서 국제협력의 가능성이 점점 희미지고 있다. 만약 두 강대국이 서로를 배제하는 봉쇄 전략을 추구할 경우 사이버 안보도 양분화될 수 있다.

39) Callum Reid, Can AI Bots Steal Your Crypto? The Rise of Digital Thieves, Cointelegraph (2025);

40) McKinsey & Company, Quantum Technology Monitor (2025), p.66.; Leeor Shimron, Quantum Threat: Bitcoin's Fight To Secure Our Digital Future, Forbes (June 30, 2025); Itan Barmes, Bram Bosch and Olaf Haalstra, Quantum Computers and the Bitcoin Blockchain, Deloitte (2025)

제9장

이커머스와 사이버 안보: 중국 플랫폼 사례를 중심으로

김주희 | 동덕여대 문화지식융합대학 교수

제9장

이커머스와 사이버 안보: 중국 플랫폼 사례를 중심으로

김주희 | 동덕여대 문화지식융합대학 교수

1. 들어가며

중국발 글로벌 이커머스 플랫폼들이 한국 소비자 시장에서 빠르게 영향력을 확대하고 있다. 대표적으로 초저가 쇼핑앱 '쉬인(Shein)'과 '테무(Temu)'는 저렴한 가격과 방대한 상품을 앞세워 한국을 비롯한 전 세계에서 사용자를 늘리고 있다. 2024년 기준 테무는 한국에서 월간 활성 사용자 수 800만 명을 돌파했으며, 쉬인 역시 20-30대 소비자를 중심으로 급속한 성장세를 보이고 있다[41]. 이러한 중국계 플랫폼의 부상은 소비자 편익의 증대를 배경으로 하지만 사이버보안과 개인정보보호 측면에서 다양한 우

41) 조선일보사. (2024, April 4). 中 테무, 韓 이용자 8개월만에 16배 늘었다… 알리 바짝 추격. 조선비즈. https://www.chosun.com/economy/market_trend/2024/04/04/XO2IAQJ2CNCIZLJM3W3V5UHJOM/

려를 낳고 있기도 하다. 이들 앱이 대량의 이용자 데이터를 수집·분석하여 사업에 활용하면서, 한국 개인정보보호법(PIPA, Personal Information Protection Act) 등 국내 법제와 사이버보안 체계에 부합하지 않는 관행(예: 동의·고지 절차의 비준수, 해외이전 및 제3자 제공 절차 미준수)들이 지적되고 있다. 특히 이들 플랫폼이 중국 기반 기업인 만큼, 데이터 주권(국가가 자국민 데이터에 대해 행사하는 통제권) 침해, 국외 데이터 이전, 알고리즘의 불투명성, 악성코드 위험 등이 두드러진 위험 요인으로 거론되고 있다. 이에 따라 2024년 하반기 한국 개인정보보호위원회가 테무에 대한 조사를 시작하고,[42] 해외의 경우에도 EU가 디지털서비스법(DSA)을 통해 중국계 플랫폼 규제를 강화하는 등 국제적 우려가 구체적 행동으로 이어지고 있다.[43]

이러한 논의를 바탕으로 본고에서는 2020년 이후 한국 시장에 진출한 중국계 이커머스 플랫폼을 중심으로 사이버보안에 대한 쟁점을 종합적으로 분석한다. 먼저 쉬인과 테무의 데이터 수집 및 알고리즘 구조를 상세히 살펴본다. 이어서 알리바바, PDD홀딩스의 핀둬둬 등 중국계 이커머스의 사례들을 폭넓게 분석하여 기술·보안 구조를 살펴보고 사이버보안 관련 시사점을 도출한다. 또한 한국의 사이버보안 및 개인정보 보호체계와 충돌하는 지점을 법적·기술적 관점에서 검토하고, 미국 연방거래위원회(FTC), EU 집행위원회, 한국 개인정보보호위원회 등 국내외 규제기관의 실제 제재·조사 사례를 살펴본다. 마지막으로 이러한 이커머스 플랫폼들로 인해

42) 중앙일보. (2024, March 22). "알리·테무, 韓 개인정보법 위반 결과 상반기 나온다". 중앙일보. https://www.joongang.co.kr/article/25244317

43) 연합뉴스. (2024, October 31). EU, 中플랫폼 '테무' 디지털서비스법 위반 조사(종합). 연합뉴스. https://www.yna.co.kr/view/AKR20241031080351009

제기되는 사이버보안 위험의 유형을 체계적으로 분류하고, 한국 정부 및 기업 차원의 대응 방안과 정책적 시사점을 도출하고자 한다.

2. 중국 이커머스 플랫폼과 사이버 안보: 주요 쟁점

인은 2008년 설립된 이커머스로 철저한 데이터 기반 비즈니스 모델로 성장한 기업이다. 창업자 쉬양톈(Chris Xu)이 검색엔진 최적화(SEO) 분야 출신인 만큼, 쉬인은 초창기부터 사용자 데이터와 인공지능(AI) 알고리즘에 의존해 소비 트렌드를 파악하고 신상품 기획에 반영해왔다. 구체적으로 쉬인은 사용자의 검색 이력, 클릭 및 구매 기록 등을 빅데이터로 수집·분석하며, 이를 통해 급변하는 패션 선호도를 실시간으로 포착한다(Kaufman, 2023).[44] AI 알고리즘은 소셜미디어 등 다른 앱의 활동 데이터까지 연계하여 새로운 유행 아이템을 예측하고 디자인에 반영하는 것으로 알려져 있다(USCC, 2023; Lee, 2024). 이용자는 할인코드 등의 혜택을 받기 위해 타 앱 데이터 공유에 동의하도록 유도되는데, 사실상 앱 사용자의 광범위한 정보 접근 권한을 요구하는 셈이다(이은서, 2024). 이러한 알고리즘 중심 운영 덕분에 쉬인은 초단기 공급망을 통해 Zara, H&M 등 기존 패션 기업을 제치고 글로벌 패스트패션 시장 1위를 차지할 정도로 성장했다(Kaufman, 2023).

44) Kaufman, N. (2023). Shein, Temu, and Chinese E-commerce: Data Risks, Sourcing Violations, and Trade Loopholes. US-China Economic and Security Review Commission.

테무의 경우, 2022년 9월 미국에 진출한 신생 플랫폼으로, 그 모기업은 중국 내 거대 이커머스 기업 판둬둬(Pinduoduo)이다. 테무 역시 방대한 상품을 중개하며 AI 기반 추천 알고리즘과 소셜미디어 마케팅을 활용해 단시간에 사용자를 끌어모았다. 테무 앱은 특유의 게이미피케이션 요소와 틱톡식 피드 알고리즘을 도입하여 이용자가 오래 머무르며 쇼핑하게 만든다(Rinaldo, 2023[45]). 문제는 이 과정에서 테무 앱이 과도한 기기 권한과 이용자 정보를 요구하고 있다는 점이다. 미 아칸소주 소장[46]에서 드러난 바에 따르면, 테무는 위치정보, 연락처, 문자메시지, 저장파일 등 휴대폰 내 개인정보에 사실상 무제한 접근하도록 설계되어 있으며, 심지어 사용자 휴대폰의 보안 설정마저 우회할 수 있는 것으로 지적되었다(Kundavaram et al., 2024[47]). 다시 말해 테무는 겉보기에는 쇼핑 앱이지만 실제로는 이용자 정보를 수집하는 스파이웨어에 가깝다는 비판까지 제기되고 있다(Rinaldo, 2023).[48] 테무의 이러한 데이터 수집 행태는 대용량 사용자 데이터 확보를 통해 구매 패턴

45) Rinaldo, R. (2023). SISTEM INFORMASI AKUNTANSI, MOBILE APPLICATION, E-COMMERCE DAN P2P LENDING SEBAGAI FAKTOR YANG MEMPENGARUHI MINAT MAHASISWA AKUNTANSI UNTUK BERWIRAUSAHA (Doctoral dissertation, UNIVERSITAS BINA DARMA).

46) 에포크타임스 Korea. (2024, June). 美 아칸소주, 中 테무 '개인정보 침해' 혐의로 소송 제기. 에포크타임스. Retrieved from https://www.epochtimes.kr/2024/06/686137.htm

47) Kundavaram, R. R., Roberts, C., Onteddu, A. R., & Devarapu, K. (2024). Sculpting Dynamic Intelligence in E-Commerce Vendor-Customer Relations with Advanced Big Data Analytics Integration. American Journal of Trade and Policy, 11(2), 49-66.

48) 아칸소주 법무장관의 공식 발표와 관련 소장에서는, 테무가 단순 쇼핑앱을 넘어 "데이터 절도형 스파이웨어"에 가깝다고 명시하고 있다. 앱 자체가 기기의 보안설정을 우회하고, 무제한적 데이터 접근을 통해 사용자를 모니터링하며, 수집 데이터를 3자에 판매함으로써 본질적으로 악성 소프트웨어(Malware) 및 스파이웨어적 속성을 가진다는 분석이다.

을 파악하고 공급망에 신속히 반영하려는 전략으로 풀이된다. 더불어 테무와 판둬둬는 개발한 공동 기술 인프라를 공유할 가능성이 높다. 실제로 핀둬둬는 자사 앱에 안드로이드 운영체제의 취약점을 악용한 악성코드를 심어 사용자 기기에 루트 권한을 획득하려 한 정황이 2023년 밝혀졌는데, 해당 해킹팀 인력 상당수가 테무 앱 개발에 투입된 것으로 보도되었다(Gan et al., 2023;[49] Rinaldo, 2023). 이처럼 쉬인과 테무 모두 공격적인 데이터 수집과 불투명한 알고리즘 운영을 기반으로 성장하고 있어, 이용자 개인정보 및 기기 보안 측면에서 상당한 위험성을 내포하고 있다.

또한 데이터 국외이전 구조도 주목할 필요가 있다. 쉬인은 본사는 싱가포르에 두고 있지만 주요 개발·운영은 중국에서 이루어지며, 테무 역시 북미·유럽에서 수집한 이용자 데이터를 중국 본토나 제3국 서버로 전송·저장하는 것으로 파악된다(개인정보보호위원회, 2025). 구체적으로 테무의 경우 한국 이용자 데이터를 중국과 싱가포르의 서버로 전송하여 보관하였으며, 이러한 사실을 국내 이용자에게 명시적으로 알리지 않은 채 서비스를 운영해왔다. 이는 중국 이커머스를 이용하는 고객의 정보가 중국으로 이전된 이후 관리에 있어 보안상 위험에 노출될 수 있는 우려가 있다는 점에서 문제이다. 쉬인도 마찬가지로 글로벌 이용자 정보가 중국에 연계될 수 있다는 우려가 꾸준히 제기되어 왔으며, 실제 2018년 쉬인의 모기업 'Zoetop'이 해킹당해 3,900만 명의 고객 계정 정보(이름, 이메일, 비밀번호, 일부 신용카드 정보 등)가 유출됐으며, 미국 뉴욕주 검찰 등은 피해 사실을 늦게 통보한

49) Gan, Y., Ma, J., & Xu, K. (2023). Enhanced E-Commerce Sales Forecasting Using EEMD-Integrated LSTM Deep Learning Model. Journal of Computational Methods in Engineering Applications, 1-11.

점, 정보의 일부만 알린 점 등을 비판하며 'Zoetop'에 벌금 190만 달러를 부과하기도 했다[50]. 결론적으로 쉬인과 테무는 국가 간 경계를 넘어 방대한 데이터 수집망과 AI 알고리즘을 결합하여 사업 모델을 구축하고 있으나, 이러한 데이터의 흐름과 처리 방식이 상당 부분 블랙박스로 남아있고, 중국이라는 특수한 법·제도 환경의 영향 아래에 있다는 특징으로 인해 데이터 관리의 보안상 위험, 개인정보보호의 침해 등 문제가 발생할 수 있다.

한편 쉬인과 테무 외에도 중국 이커머스에는 알리바바(Alibaba), 징둥(JD 닷컴), 샤오홍슈(RED) 등 다양한 플랫폼들이 존재한다. 알리바바 그룹은 중국 최대 전자상거래 기업으로, 대표 플랫폼인 알리익스프레스(AliExpress)와 타오바오, 티몰(Tmall) 등을 통해 글로벌 시장을 공략해왔다. 알리바바 계열 플랫폼들은 일찍이 방대한 클라우드 인프라(AliCloud)와 정교한 추천 알고리즘을 구축하여, 사용자 행동 데이터를 마케팅과 판매 전략에 활용하고 있다. 예를 들어 알리익스프레스는 한국을 포함한 전 세계 소비자의 검색·구매 데이터를 수집하여 개인맞춤형 추천과 실시간 할인 등을 제공하며, 이는 쉬인이나 테무의 데이터 활용 방식과 유사하다. 다만 알리바바는 기업 규모가 크고 비교적 오랜 운영 경험이 있는 만큼, 글로벌 규제환경에 대응하기 위해 나름의 보안 관리 체계를 마련해온 것으로 평가된다. 실제 알리바바 산하의 알리익스프레스는 유럽 GDPR에 대응하여 일부 데이터 접근권 요청에 응하지 않는다는 지적을 받았으나(Noyb, 2023), 기본적으로 HTTPS 통신 암호화, 이용자 계정 보호 등 표준적 보안 대책은 준수하고

50) BBC. (2022, October 14). Shein owner Zoetop fined $1.9 m over data breach response. https://www.bbc.com/news/technology-63255661

있다. 또한 알리바바 그룹은 전 세계 각지에 데이터센터를 운영하며 지역별 법규에 맞게 데이터를 저장하려는 시도를 하고 있는데, 한국 시장에서도 서울에 콘텐츠 전송 네트워크(CDN)를 두어 서비스 품질과 함께 보안을 높이려 노력한 바 있다.[51)]

그러나 알리익스프레스도 개인정보 처리 관행 면에서는 쉬인과 테무의 경우와 크게 다르지 않은 한계를 드러냈다. 알리는 '판매자-소비자 직거래 모델' 특성상, 한국 소비자의 이름·연락처·주소·결제정보 등을 중국에 있는 수십만 개의 판매자에게 곧바로 제공해왔는데, 이 과정에서 이용자 동의 및 고지 의무를 소홀히 한 사실이 적발되었다[52)]. 즉, 알리 측은 해외 판매자가 상품 배송에 필요하다는 이유로 한국 고객 정보를 광범위하게 넘겼지만, 정작 이를 어떤 국가의 누구에게 어떤 정보가 공유되는지 투명하게 밝히지 않았다. 또한 계정 삭제 절차를 의도적으로 복잡하게 설계하여 이용자가 자신의 데이터를 삭제하기 어렵게 만드는 등 이용자 통제권을 제약한 정황도 확인되었다(신민경, 2024). 이러한 문제들은 쉬인이나 테무 역시 동일하다. 실제 쉬인도 회원 가입 시 마케팅 목적 제3자 정보제공에 대한 필수 동의를 요구하여, 관련 국내법 기준으로 보면 선택동의로 분류해야 할 항목을 무조건 받는 방식으로 운영하고 있었다(이은서, 2024). 테무도 마찬가지로 해외 사업자라는 점을 내세워 한국 개인정보보호법상의 세부 규

51) Alibaba Cloud. (2025, June 23). Alibaba Cloud to launch second data center in South Korea. Alibaba. https://www.alibabacloud.com/blog/alibaba-cloud-to-launch-second-data-center-in-south-korea_602310

52) The Korea Times. (2024, July 25). China's AliExpress handed US$13 mil fine for privacy violations. The Korea Times. https://www.koreatimes.co.kr/southkorea/law-crime/20240725/chinas-aliexpress-handed-13-mil-fine-for-privacy-violations

정을 준수하지 않는 약관을 적용해 온 것으로 나타났다.

기술적 보안 사건 측면에서 보면, 알리바바 계열은 아직 쉬인이나 핀둬둬만큼 심각한 악성코드 적발 사례는 알려지지 않았다. 하지만 중국계 플랫폼이 공통적으로 데이터 주권을 침해할 수 있다는 점에서 우려되고 있다. 중국 정부는 2017년 사이버보안법과 국가정보법 등을 통해 자국 내 기업의 데이터에 대한 국가 접근 권한을 폭넓게 확보해 놓고 있다.[53] 이에 따르면 중국에 기반을 둔 기업은 필요 시 정부 기관에 데이터를 제출하거나 네트워크 보안 협조를 해야 할 의무가 있다. 알리바바처럼 규모가 큰 기업이라 해도 중국 당국의 영향력에서 자유롭기 어렵다. 종합하면, 알리바바/알리익스프레스, 쉬인, 테무 등 중국계 이커머스 플랫폼들은 AI·빅데이터 활용과 공격적인 시장전략이라는 공통점을 지니며, 개인정보 처리에 있어서 이용자 권리보호 미흡과 중국 정부의 개입 가능성이라는 측면에서 본질적으로 사이버 안보상의 이슈를 지니고 있다. 다만 알리바바의 사례를 통해 알 수 있듯이 기업별로 글로벌 규제 대응 수준에는 차이가 존재하기도 한다.

53) Harrell, P. (2025, January 30). Managing the risks of China's access to U.S. data and control of software and connected technology. Carnegie Endowment for International Peace. https://www.carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en

3. 한국 사이버 보안상 충돌 지점

1) 한국 사이버보안 및 개인정보보호 체계와의 충돌 지점

한국은 개인정보보호법(PIPA)을 중심으로 비교적 엄격한 개인정보 보호 체계를 갖추고 있으며, 정보통신망법 등 관련 법률과 KISA(한국인터넷진흥원) 등의 기관을 통해 사이버보안을 관리·감독하고 있다. 이러한 한국의 법·제도와 중국계 플랫폼들의 관행 사이에는 여러 충돌 지점이 발생하고 있다. 첫째, 개인정보의 국외 이전 요건에 대한 충돌이다. 한국 개인정보보호법상 사업자가 이용자 개인정보를 해외로 이전하거나 해외 사업자에게 위탁 처리하려는 경우, 정보 이전 국가, 제공받는 자, 이전되는 항목, 이용 목적 등을 명확히 고지하고 사전 동의를 받아야 한다(개인정보보호법 제17조, 제39조 등). 그러나 쉬인, 테무와 알리익스프레스 모두 한국 이용자 정보를 중국 등 해외로 전송·저장하면서 이러한 고지·동의 절차를 제대로 이행하지 않았다. 앞서 살펴보았듯이 테무는 한국 고객 데이터를 중국·싱가포르 서버에 저장하면서도 처리방침에 국외 이전 사실을 공개하지 않았고, 개별 통지나 동의를 받지도 않았다[54]. 알리익스프레스 역시 180,000여 중국 판매자에게 한국인 정보를 제공하면서 이용자에게 어떤 정보가 어느 나라로

54) Freedman, L. (2025, July 28). Privacy Tip #452 – Temu & TikTok—Assess risk before downloading. Robinson + Cole Data Privacy + Security Insider. https://www.jdsupra.com/legalnews/privacy-tip-452-temu-tiktok-assess-risk-4454337/

넘어가는지 알리지 않았다.[55] 이러한 행태는 한국 법규를 정면으로 위반한 것이다. 즉, 데이터 국외 이전 문제는 한국의 개인정보 자기결정권 보호 원칙과 중국계 플랫폼의 무분별한 데이터 이동 관행의 충돌을 잘 보여준다.

둘째, 민감정보 및 고유식별정보 처리 제한의 충돌이다. 한국법은 주민등록번호와 같은 고유식별정보나 민감정보를 처리할 때 높은 수준의 요건을 요구한다. 그런데 테무는 2025년 초 한국인 판매자를 유치하는 과정에서 주민등록번호와 얼굴 영상까지 수집한 사실이 드러났다(신용현·유채영, 2025). 이는 법적 근거 없는 주민번호 처리로서 명백한 위법 행위이며, 개인정보보호위원회 조사에서 문제가 되어 해당 정보 파기와 시정명령이 내려졌다(신용현·유채영, 2025).

셋째, 마케팅 활용 동의 절차의 충돌이다. 한국 개인정보보호법 제22조는 영리 목적의 개인정보 이용 동의는 다른 동의 사항과 구분하여 명확히 받도록 규정하고 있다. 이에 따라 국내 쇼핑몰들은 이메일 광고나 제3자 제공 동의를 선택사항으로 처리해, 동의하지 않아도 회원가입이 가능하게 하고 있다(이은서, 2024). 그러나 쉬인과 테무는 마케팅 목적 개인정보 제공을 '필수 동의' 항목에 포함시켰다. 소비자가 쉬인에 가입하려면 계열사 등 제3자에게 개인정보를 공유하는 것에 반드시 동의해야 하며, 이를 거부하면 가입 자체가 불가능하다(이은서, 2024). 이는 국내법 기준으로 볼 때 위법은 아니지만 국내 사업자에게는 허용되지 않는 관행이다. 결국 같은 한국 이

55) Digital Policy Alert. (2024, July 24). Republic of Korea: Issued PIPC ruling in investigation into AliExpress imposing a KRW 1.978 billion fine for non-compliance with Personal Information Protection Act. https://digitalpolicyalert.org/event/21718-issued-pipc-ruling-in-investigation-into-aliexpress-imposing-a-krw-1978-billion-fine-for-non-compliance-with-personal-information-protection-act

용자를 상대로 하면서 국내외 사업자 간 규제 격차가 생겨 소비자 보호 수준에 차이가 발생한다.

넷째, 데이터 주권과 사이버 안보상에서도 주요 쟁점이 있다. 한국 개인정보보호 체계는 기본적으로 개인의 권리 보호에 중점을 두지만, 최근 사이버 안보 측면에서 국가 차원의 데이터 주권 개념도 중요해지고 있다. 중국의 국가정보법(2017)은 모든 조직과 시민은 국가 정보활동을 지원·협조해야 한다고 규정하고 있어 중국 기업이 수집한 해외 사용자 데이터도 중국 정부가 요청하면 제공될 가능성이 있다. 이는 한국 국민의 정보가 한국 사법권의 미치지 않는 외국 정부의 통제 하에 놓일 수 있음을 의미한다. 예컨대 한국 소비자가 쉬인이나 테무에 제공한 구매 이력, 위치정보 등이 중국 정보기관에 넘어가 감시나 첩보 목적으로 활용되는 최악의 시나리오도 배제할 수 없다(Rinaldo, 2023). 한국 사이버 안보 전략에서는 국내 중요한 정보가 외부로 유출되지 않도록 관리하는 것이 강조되는데, 중국 플랫폼의 활동은 이러한 원칙과 상충될 소지가 있다. 최근 미국, 인도 등 여러 국가들이 중국 앱을 국가안보 위협으로 간주하여 제재하거나 금지하는 조치를 취하고 있는데, 그 배경에는 이러한 데이터 주권 충돌 문제가 자리한다. 한국도 비록 공개적으로 중국 앱을 금지하고 있지는 않지만, 국내 주요 인프라 내 중국산 기술 제품 통제 등 유사한 데이터 주권 보호 조치가 필요하다는 논의가 이루어지고 있다.

2) 국내외 규제기관의 제재·조사 사례

중국 이커머스 플랫폼의 개인정보 침해 우려가 현실화되자, 한국을 비롯한 여러 나라의 규제기관이 제재와 조사를 본격화하고 있다. 한국에서는

2024년부터 개인정보보호위원회를 중심으로 중국발 플랫폼 특별조사가 이루어졌다. 2024년 7월, 개인정보보호위원회(PIPC)는 알리익스프레스에 대해 개인정보보호법 위반을 인정하고 과징금 19억7800만원과 과태료 780만원을 부과하였다. 이는 한국에서 외국 온라인 사업자가 개인정보 국외유출로 제재를 받은 첫 사례이기도 하다[56]. 개인정보보호위원회는 알리에 대해 국내 기업과 동등한 수준의 개인정보 보호조치를 취하도록 시정명령을 내리는 한편, 향후 재발 방지를 위한 개선을 권고하였다(개인정보보호위원회, 2024). 이어서 2025년 5월, 테무에 대해서도 조사를 마무리하고 과징금 13억6900만원과 과태료 1760만원을 부과하는 결정을 내렸다. 테무의 위반 사항은 개인정보 국외 이전 미고지·미동의, 주민번호 불법 수집 및 국내 대리인 미지정 등이었다. 특히 테무가 매출액 자료 제출을 지연하고 조사 협조에 불충분했던 점을 고려해 가중처벌이 이뤄졌다는 언급도 있어, 규제 불응 시 더 강한 제재가 따를 수 있음을 보여주었다.

한국 외 해외에서도 다양한 움직임이 있었다. 미국에서는 연방 차원의 직접 제재는 아직 없지만, 입법·사법 영역에서 경고음이 커지고 있다. 2023년 미 연방 하원 산하 '미중전략경쟁특별위원회(Select Committee on the CCP)'는 쉬인과 테무의 사업행태를 조사하여, 이들이 미국의 법망을 교묘히 회피하며 성장했다고 지적하는 보고서를 발표했다(Rinaldo, 2023). 이 보고서는 쉬인과 테무가 디지털 플랫폼을 통한 미국 소비자 데이터 수집이 광범위하며, 그 배후에 중국 공산당의 전략적 이해관계가 있을 수 있다고

56) Pulse by Maeil Business News Korea. (2024, July 26). AliExpress fined for unauthorized customer data sharing. https://pulse.mk.co.kr/news/english/11077673

우려하였다(Select Committee on CCP, 2023). 유럽연합(EU)에서도 GDPR(일반 개인정보보호규정)에 비추어 중국 플랫폼들을 견제하려는 움직임이 있다. 오스트리아의 개인정보단체(Noyb)는 2023년 초 틱톡, 알리바바 등에 대한 GDPR 위반 신고를 제기하며, 이들 기업이 유럽 이용자의 데이터 접근 요구 등에 제대로 응하지 않고 있다고 비판했다(Noyb, 2023[57]). 특히 알리익스프레스의 경우 GDPR상 정보주체 권리를 무시한 채 운영되고 있어 최대 글로벌 매출의 4%에 달하는 과징금도 부과될 수 있다는 경고가 있었다(Noyb, 2023). 이처럼 각국 규제기관과 정부는 데이터 유출 위험과 국가안보 위험을 근거로 중국 플랫폼들을 제재하고 있으며, 한국 정부도 이러한 국제 흐름 속에서 대응 방안 마련을 위한 논의가 적극적으로 이루어지고 있다.

3) 주요 사이버보안 위험 유형 분석

지금까지 살펴본 내용을 토대로, 중국 이커머스 플랫폼이 야기하는 사이버보안 위험을 다음의 유형들로 제시할 수 있다.

❶ 데이터 주권 침해 및 해외유출 위험: 한국 이용자의 개인정보가 자국법의 보호 울타리를 벗어나 외국(중국 등)으로 이전됨으로써 발생하는 위험이다. 데이터가 해외로 나가면 한국 당국의 감독과 통제권이 약화되고, 외국 정부나 제3자에 의해 오·남용될 소지가 커진다. 특히 중국처럼 국가가

57) noyb – European Center for Digital Rights. (2024, July). Annual Report 2023. https://noyb.eu/sites/default/files/2024-07/Annual_Report_2023_EN.pdf

기업 데이터에 접근할 수 있는 환경에서는, 한국 국민의 민감한 정보가 한국의 동의 없이 타국에 저장·분석되고 심지어 정치적 목적에 활용될 수 있다는 점이 우려된다. 이는 개인의 프라이버시권 침해일 뿐 아니라 국가안보 차원의 위협으로도 이어질 수 있다. 예를 들어 대량의 한국인 소비 데이터가 축적될 경우, 중국은 이를 통해 한국 사회의 소비 트렌드, 경제활동 패턴 등을 분석하여 경제적 영향력을 행사하거나 여론을 조성하는 데 활용할 수 있다. 또한 유출된 개인정보가 사이버 공격이나 표적 스피어피싱에 악용되어 국가기관이나 기업을 겨냥한 보안 위협으로 이어질 가능성도 있다. 따라서 데이터 주권 침해는 단순한 개인 정보 유출을 넘어 국가 차원의 정보주권 약화라는 심각한 위험으로 분류된다.

❷ 개인정보 보호 권리 행사의 제한: 앞서 본 바와 같이, 중국 플랫폼들은 한국인의 개인정보를 국외(중국 등)로 자유롭게 이동시키는데, 이는 한국 이용자가 가지는 개인정보 자기결정권 및 권리 구제 측면에서 문제를 일으킨다. 이용자는 자신의 정보가 어디에 저장되고 누가 처리하는지 알 권리와 통제권이 있지만, 정보가 해외로 넘어가면 권리 행사가 사실상 불가능해진다. 예컨대 테무나 쉬인에 가입한 한국인이 본인 정보의 열람·삭제를 요구하더라도, 그 데이터가 중국에 있으면 한국 법률의 강제력이 미치지 않아 실질적 구제가 어렵다. 또한 분쟁 발생 시에도 해당 기업이 한국에 법적 실체가 없으면 행정처분의 집행력 확보나 피해보상이 난관에 부딪힌다. 따라서 개인정보의 국외이전은 개인정보보호 법체계의 사각지대를 발생시켜 이용자 보호 공백을 야기한다. 이는 사이버 안보 측면에서도 위험한데, 데이터가 어느 나라 어떤 서버에 있는지 모르면 보안 사고 시 신속한 대응이 어렵고, 침해사고 통지 등 의무 이행도 기대하기 어렵다. 이러한 국경 간 데이터 이동의 투명성 부족은 글로벌 디지털 경제에서 핵심 이슈로,

현재 국제 규범 논의에서도 중요한 위험 요인으로 다뤄지고 있다.

❸ 알고리즘 불투명성과 조작 가능성: 중국 이커머스 플랫폼들은 추천 알고리즘과 AI 시스템의 내부 작동이 외부에 거의 공개되지 않고 있다. 이로 인해 첫째, 개인맞춤형 콘텐츠 제공의 이면에 어떠한 데이터 수집·활용이 일어나는지 이용자나 규제자가 알기 어렵다. 알고리즘이 이용자의 어떤 정보를 학습하고 어디에 전송하는지 불투명하면, 민감한 개인정보까지 모르게 축적될 수 있고 편향된 의사결정이 일어날 수 있다. 둘째, 알고리즘 조작의 위험이 있다. 플랫폼이 임의로 특정 상품이나 정보를 노출하거나 숨기는 행위를 통해 소비자 행동을 통제할 수 있는데, 만약 외부 개입으로 이러한 조작이 이루어진다면 소비자 후생과 시장 공정성이 훼손된다. 예를 들어 중국 당국이 정치적으로 민감한 상품을 추천 알고리즘에서 제외시키도록 압력을 넣거나, 반대로 자국에 유리한 콘텐츠를 노출하도록 요구할 경우, 플랫폼은 이를 거부하기 어려울 수 있다. 알고리즘은 블랙박스 상태이기 때문에, 그 속에 검열 코드가 삽입되어도 이용자는 알 길이 없다. 셋째, 보안 취약점 은폐 가능성이다. 알고리즘과 소프트웨어 구조가 폐쇄적이면, 악성코드나 백도어가 내장되어도 외부 보안 전문가가 발견·검증하기 힘들다. 핀둬둬 사례에서 보듯 앱이 기기 설정을 변경하고 삭제를 어렵게 만드는 기능을 숨겨둘 경우, 일반 사용자는 물론 보안솔루션도 즉각 탐지하지 못할 수 있다(Gan et al., 2023).

❹ 악성코드 및 해킹 리스크: 중국발 앱에 실제 악성코드가 내장되거나 사이버 공격 통로로 악용된 사례가 발생하면서, 이에 대한 경계심이 높아지고 있다. 대표적으로 2023년 3월 구글은 핀둬둬의 안드로이드 앱에서 심각한 보안 취약점 악용 코드를 발견하고 플레이스토어에서 퇴출시켰다. 조사 결과 핀둬둬 앱은 이용자 동의 없이 문자메시지와 알림을 읽고, 다른 앱

의 데이터를 훔치며, 기기에 영구 설치되어 삭제를 방해하는 등 전례 없는 수준의 악성 행위를 수행한 것으로 드러났다(Rinaldo, 2023). 이러한 사실은 자매 앱인 테무에 대한 의혹으로도 이어졌다. 테무 자체는 현재 구글·애플 공식마켓에서 배포되지만, 핀둬둬에서 문제가 된 악성코드의 상당 부분이 테무에 공유되었을 가능성이 제기되었다(Rinaldo, 2023). 이 경우 테무 앱 역시 사용자 몰래 정보를 빼내거나 원격에서 디도스(DDoS) 공격 등에 악용될 수 있는 좀비 단말로 만들 잠재력이 있다(Rinaldo, 2023). 앱이 필요 이상으로 광범위한 권한을 요구한다는 점에서 지속적 위험이 존재한다. 정리하면, 악성코드 심기 및 해킹 리스크는 단순한 개인정보 침해를 넘어 이용자 기기를 통제하고 전체 네트워크에 위해를 줄 수 있는 중대한 사이버보안 위험으로 대두되고 있다. 이는 국가 차원에서도 공격 표면 확대와 대규모 사이버 위협을 의미하므로, 매우 심각한 유형으로 분류될 수 있다.

4. 정부 및 기업 차원의 대응 필요성과 방향 모색

지금까지 논의한 상황들을 고려할 때, 한국 정부와 산업계는 중국발 이커머스 플랫폼에 대응하여 종합적인 사이버보안 전략을 마련할 필요가 있다. 먼저, 법·제도적 대응 강화의 필요성이 있다. 우선 해외 온라인 플랫폼에 대한 국내법 적용을 현실화하는 노력이 요구된다. 다행히 개인정보보호위원회가 알리익스프레스, 테무에 과징금을 부과한 것은 "국내에서 한국인을 대상으로 영업하면 국적 불문 법을 지킨다"는 원칙을 천명한 것으로 평가할 수 있다. 향후에도 개인정보보호위원회와 KISA는 상시 모니터링 체

계를 통해 해외 사업자의 개인정보 처리 실태를 점검하고, 위반 시 국내 사업자와 동일하거나 그 이상의 제재를 가해야 할 것이다. 또한 국내 대리인 제도의 실효성을 높여, 해외 플랫폼이 법적 책임을 회피하지 못하도록 해야 한다. 테무 사례에서처럼 매출 자료 제출을 거부하거나 조사 비협조 시 가중처벌 규정을 적용하는 등, 집행력 담보 수단을 강화할 필요가 있다.

둘째, 데이터 국외 이전 관리 및 협약 체결이다. 개인정보 국외 이전 문제를 해결하기 위해 국제 공조와 양자 협약을 병행할 수 있다. EU의 GDPR은 역외로 나가는 데이터에 대해 적정성 평가나 표준계약조항(SCC)을 요구하고 있는데, 한국도 중국을 포함한 국가들과 데이터 이전에 관한 협정을 모색할 수 있다. 예컨대 한-중 개인정보보호 협력 MOU를 체결하여, 중국 기업이 한국인 데이터 처리 시 지켜야 할 원칙을 상호 확인하고 이행을 감시하는 체계를 구축할 수 있다. 실제 개인정보위는 2024년 중국 인터넷협회(ISC)와 간담회를 열어 한국 개인정보법을 준수해달라고 요청했고, 중국 측도 협력 의사를 보인 바 있다(진길유, 2025).[58] 이러한 대화를 더욱 공식화하여 국제규범 수준의 개인정보 보호장치를 중국 기업들도 준수토록 유도해야 한다. 아울러 한국 정부 내에서 데이터 주권 태스크포스를 운영, 국민 개인정보의 해외유통 현황과 위험요인을 상시 분석하고 필요한 경우 국외 이전 제한조치(예: 클라우드 사용 제한 등)도 검토하는 종합 정책이 필요하다.

셋째, 기술적 검증 및 보안성 제고이다. 정부와 보안업계는 중국발 앱들의 보안성에 대한 기술 검증을 강화할 필요가 있다. 현재 구글 플레이스토어 등 플랫폼 사업자가 1차적으로 앱 심사를 하지만, 그 한계를 핀둬둬 사

58) 진길유. (2025). 중국 국경간 데이터 이동의 법률규제에 관한 재고 (再考). 동아법학, (107), 127-162.

건이 보여주었다. 한국에서도 KISA가 주축이 되어 인기 앱의 코드 분석 및 트래픽 모니터링을 수행하고, 악성행위가 발견되면 즉각 경고를 내리거나 해당 기업에 소명 요구를 할 수 있어야 한다. 예컨대, 테무 앱이 과도한 권한을 요청하면 이에 대한 위험성을 분석하여 대중에 알리고, 필요시 구글·애플과 협력해 한국 지역에서 다운로드를 일시 중단하는 등의 선제적 조치를 취할 수 있을 것이다. 또한 공개 취약점 신고제도(bug bounty) 등을 통해 민간 보안 전문가들이 이러한 해외 플랫폼의 취약점을 찾아내도록 장려하고, 발견 시 투명하게 공표하여 이용자들이 인지하게 하는 것도 방법이다. 암호화 통신 사용 의무, 데이터 최소 수집 원칙 등 기술 규정을 국제 표준에 맞게 제정하여, 해외 사업자도 한국 이용자 데이터를 처리할 때 지켜야 할 보안 기준을 명문화하는 작업도 고려할 시사점이다.

넷째, 이용자 교육과 인식 제고이다. 사이버보안 대응에서 간과할 수 없는 부분이 개별 이용자의 보안의식 향상이다. 정부와 시민단체, 기업은 협력하여 중국발 플랫폼 이용 시 개인정보보호 요령을 지속적으로 안내해야 한다. 예를 들어 KISA는 "해외직구 앱 안전하게 이용하기"와 같은 가이드라인을 만들어 필요 권한만 허용하기, 가상결제 수단 사용하기, 의심스러운 링크 클릭 주의 등의 수칙을 홍보할 수 있다(최형욱, 2023[59]). 실제 보안 전문가들은 테무나 쉬인을 꼭 이용해야 한다면 앱 권한을 최소화하고, 가능하면 모바일 앱 대신 웹을 활용하며, 결제는 신용카드보다는 PayPal 등 제3자 지급수단을 쓰는 것을 권장한다. 이러한 사용자 차원의 예방조치는 설

59) 최형욱. (2023). "피싱"범죄의 현황과 대응 방안 모색: Current Status of Phishing Crimes and Search for Countermeasures.

령 플랫폼 측에 일부 보안 미흡이 있어도 피해를 줄이는 데 도움을 준다. 특히 10~20대 젊은 이용자층이 소셜미디어 마케팅에 이끌려 무분별하게 개인정보를 넘기지 않도록 디지털 리터러시 교육도 병행해야 한다. 정부 차원에서는 대국민 캠페인 등을 통해 "싼 가격 이면의 위험"을 알리고, 신중한 이용 문화를 정착시키는 것이 중요하다.

다섯째, 국제 공조 및 글로벌 가이드 구축을 위한 노력이다. 한국 정부는 미국, EU 등과 공조하여 글로벌 차원의 규범 형성에 적극 참여해야 한다. 중국 플랫폼의 문제는 비단 한국만의 이슈가 아니므로, 여러 국가들이 정보 공유와 공동 대응에 나서고 있다. 예를 들어 미국의 클린네트워크 이니셔티브나 일본의 경제안보법 등은 중국 IT에 대한 견제 정책을 포함하고 있다. 한국도 필요시 정보공유 협정 등을 통해 중국발 사이버 위협에 대한 인텔리전스를 교환하고, 국제회의에서 디지털 무역 규범 논의 시 개인정보 보호와 보안 기준을 높이는 방향을 지지해야 한다. 또한 APEC 프라이버시 프레임워크나 OECD 디지털 가이드라인 등 기존 논의에 참여하여, 국경 간 데이터 이동의 투명성, 알고리즘 책임성, 공급망 강제노역 금지 등 조항이 세계적으로 자리잡도록 노력해야 한다. 이를 통해 한국 내 정책 대응에도 정당성과 동력을 부여할 수 있다. 나아가 국제표준기구(ISO) 등에서 소프트웨어 보안성 검증 표준을 마련하고 중국도 따르도록 유도한다면, 장기적으로는 중국 기업들의 보안 수준 개선을 견인할 수도 있을 것이다.

5. 결론 및 시사점

중국 이커머스 플랫폼의 성장은 한국 사회에 편익과 위험을 동시에 가져오고 있다. 저렴한 제품과 편리한 쇼핑 환경이라는 장점 뒤에는, 대규모 개인정보 수집과 국외 이전, 불투명한 알고리즘 운영, 악성코드 및 해킹 위험이라는 심각한 사이버보안 도전이 도사리고 있다. 본 보고서의 분석을 통해, 이러한 플랫폼들의 데이터 수집·활용 구조가 한국의 개인정보보호 원칙과 상당 부분 상충하며, 실제로 국내외 규제기관의 제재 사례가 속출하고 있음을 확인하였다. 데이터 주권 확보와 국민 사이버 안전을 위해 한국 사회는 중국 플랫폼에 대한 감시와 관리를 더 이상 소홀히 할 수 없는 단계에 이르렀다.

앞으로 한국 정부는 법적 제도적 장치를 정비하여 해외 사업자라도 국내 이용자 데이터에 대해 동일한 책임을 지도록 해야 한다. 기업들은 보안과 신뢰를 경쟁력으로 삼아 스스로를 보호함과 동시에 소비자 정보를 지켜야 한다. 이용자들 또한 자신의 데이터 가치와 위험을 인식하고 현명한 소비 행태를 가져야 할 것이다. 국제적으로는 한국이 글로벌 데이터 거버넌스 논의에 적극 참여하여, 디지털 시대 개인정보보호와 사이버보안의 새로운 규범을 형성하는 데 기여해야 한다. 결국 사이버보안은 국경이 없다. 중국발 이커머스 플랫폼의 영향에 대응하는 과정은, 한국의 사이버보안 체계를 한 단계 성숙시키는 계기가 될 수 있다. 개인정보 보호와 디지털 경제 진흥이라는 두 목표 사이에서 균형을 잡으며, 한국이 안전하고 신뢰할 수 있는 디지털 환경을 구축한다면, 이는 국내 이용자뿐만 아니라 글로벌 시장에서도 경쟁력을 갖추는 바탕이 될 것이다. 쉬인과 테무의 사례는 우리에게 편

리함의 이면에 숨어있는 보안 위험을 환기시키며, 선제적이고 다층적인 대응의 중요성을 일깨워주고 있다. 향후 지속적인 연구와 정책 노력을 통해 한국이 데이터 주권을 지키고 사이버 안보를 확보하면서도, 개방된 디지털 경제의 혜택을 누릴 수 있기를 기대한다.

제10장

디지털 플랫폼과 사이버·데이터 안보

김명하 | 서울대학교 외교학 전공 박사과정

제10장

디지털 플랫폼과 사이버·데이터 안보

김명하 | 서울대학교 외교학 전공 박사과정

1. 서론

미국과 중국 간의 기술 패권 경쟁은 현재 기술 개발과 군사력의 싸움이 아닌, 사이버 공간(플랫폼)을 중심으로 세력을 형성하는 양상으로 전개되고 있다. 특히 군사용 플랫폼뿐만 아니라 이커머스, 소셜 미디어, OTT 서비스 등 일반 상업 플랫폼에서 발생하는 개인 데이터 유출 문제가 국가안보 위협으로 인식되면서 플랫폼은 더 이상 단순한 민간 기술이 아닌 국가 전략 자산으로 간주되고 있다. 플랫폼 이용자들의 위치 정보, 결제 패턴, 관심 콘텐츠 기반 알고리즘과 같은 개인정보의 국외 유출은 단순히 프라이버시 침해 이상의 문제를 야기한다. 이 데이터가 축적될 경우 자국민 집단의 성향을 파악할 수 있는 빅데이터로 축적되어 심리전·정보전의 표적이 될 수 있기 때문이다. 이처럼 디지털 플랫폼은 적성국이 악의적으로 활용할 수 있는 사이버 안보 위협 요소로 인식되고 있으며, 데이터 안보와 다른 안보 영역 간의 이슈연계성은 미국과 중국뿐만 아니라 주요국 간 갈등을 빚는 요소로 작용하고 있다.

본고는 디지털 플랫폼 산업에서 민감 데이터 국외 유출 문제가 가지는 국제정치학적 함의를 검토한다. 미·중 기술 경쟁을 배경으로 삼되, 양국 간 마찰뿐만 아니라 디지털 플랫폼이 가진 사이버 안보적 취약성이 주요국에서 어떤 갈등을 빚는지 보여주고자 한다. 이를테면 미국 정부는 과거 화웨이와 ZTE 같은 중국 통신장비업체들이 네트워크 침입, 해킹, 백도어 설치 등 사이버 안보를 위협한다는 명분으로 자국 시장에서 퇴출 조치를 취한 바 있다. 또한 디지털 플랫폼 산업에서는 소셜 미디어 서비스 틱톡(TikTok)에 대한 민감 데이터의 국외 유출 문제 삼아 강제 매각을 요청한 바 있다. 미·중 양국뿐만 아니라 데이터 안보는 플랫폼 기업을 보유한 국가 간 갈등을 심화시키기도 한다. 라인-야후 사태가 대표적인데, 이는 데이터 주권에 대한 한국과 일본 간 외교적 마찰로 이어졌다.

데이터 수집을 기초로 플랫폼이란 환경은 사이버전의 수단과 동시에 전장 환경으로 기능한다. 특히 최근 사이버전이 전력망과 정부 통신망을 교란하는 전자전의 범주를 넘어, 영향력 공작을 통한 개인의 인식 구조와 여론을 왜곡하는 형태로 발전하면서, 사이버-데이터 안보의 넥서스 현상이 더욱 두드러지고 있다. 나아가 인공지능(AI) 기술의 발전으로 데이터 확보를 둘러싼 국가 간 경쟁이 치열해지고 있으며, AI를 통해 개인행동 예측과 정교한 감정 분석이 가능해지면서, 동 기술과 결합한 플랫폼 산업의 안보적 중요성은 더욱 부각되고 있다.

2. 미·중 플랫폼 경쟁과 데이터 안보

1) 중국 소셜 미디어 플랫폼의 부상과 정보 검열 이슈

디지털 플랫폼 산업에서의 경쟁력은 양질의 데이터를 얼마나 확보할 수 있는가에 달려있다. 중국은 거대한 인구 규모와 사회 내부에서 작동하는 감시 시스템 덕분에 데이터 수집에 유리한 환경을 갖추고 있다. 다수의 중국 플랫폼 기업들은 이러한 환경을 바탕으로 괄목할 만한 성장세를 보여왔다. 현재 5억 명 이상의 이용자 수를 보유한 중국 플랫폼 기업만 7개에 이르는데, 여기에는 틱톡(더우인), 타오바오, 알리페이, 바이두 등을 포함한다. 특히 틱톡은 출시 4년 만에 10억 명 이상의 사용자를 확보하는 독보적인 성장을 보여왔는데, 이는 미국의 주요 소셜 미디어 플랫폼(인스타그램, 유튜브, 왓츠앱 등)이 10억 명 사용자를 달성하는 데 걸린 시간의 절반에 불과하다. 2024년 기준 미국 10대 청소년의 틱톡 사용률은 63%로, 90% 점유율을 차지하고 있는 유튜브에 이어 두 번째로 높은 수치를 기록했다 (Pew Research Center 2024). 또한 2020년부터 2023년까지 전 세계 모바일 앱스토어 다운로드 횟수 1위를 꾸준히 차지하였다. 2024년에는 중국 이커머스 플랫폼인 테무가 1위, 틱톡이 2위를 차지하면서 중국의 플랫폼의 미국 시장 내 경쟁력을 다시 한 번 입증했다 (Backlinko 2025).

틱톡의 부상은 미국 소셜 미디어 플랫폼 기업에 위협으로 인식되었다. 틱톡은 숏폼(1분 미만 영상) 서비스를 처음 선보이면서 전 세계 10~20대 중심으로 인기를 얻게 되었는데, 이에 유튜브는 틱톡에 대한 전략적 대응으로 기존의 롱폼(1분 이상 영상) 콘텐츠 중심에서 벗어나 '쇼츠(Shorts)'로 불리는

숏폼 중심의 마케팅을 펼치기 시작했다. 메타 또한 인스타그램에 '릴스'를 출시하면서 숏폼 시장에 뛰어들었다. 중국 기업의 비즈니스 모델을 미국 기업이 벤치마킹하는 현상은 소셜 미디어 플랫폼 시장에서 중국의 경쟁력을 단적으로 보여준다. 그러나 미국 내 틱톡의 급부상은 단순히 시장 점유율 경쟁의 문제를 넘어 안보적 우려로 이어진다. 틱톡을 통해 뉴스를 접하는 인구도 상당수에 이르기 때문이다. 2024년 진행된 여론조사에 의하면 미국 내 틱톡을 사용하는 성인의 52%가 정기적으로 틱톡을 통해 뉴스를 접한다고 답했다 (Pew Research Center 2025). 틱톡을 통한 뉴스 소비는 중국에 우호적이지만 미국에 비판적인 콘텐츠에 노출될 수 가능성을 높이며, 동시에 틱톡이 수집한 개인정보를 기반으로 중국 정부가 미국인을 대상으로 정보심리전을 펼칠 수 있다는 점에서 국가안보에 잠재적 위협이 될 수 있다. 소셜 미디어 플랫폼은 이렇듯 데이터 안보, 정보심리전(영향력 공작)의 다층적인 안보 이슈를 내포하고 있다.

중국 플랫폼 기업의 부상과 당국의 엄격한 정보 검열 제도는 그동안 국경 간 자유로운 데이터의 유통을 추구해왔던 미국이 데이터 보호의 필요성을 인식하게 되는 계기가 되었다. FBI, CIA 등 미국의 주요 정보기관은 2010년대 이후 중국이 대규모 해커를 동원하여 지적 재산, 기업의 영업 기밀을 지속적으로 탈취하고 있음을 경고해 왔다. 실제로 중국 해커 중 일부는 미국 및 해외의 수십 개 기업, 대학, 정부 기관의 시스템에 침입해 신기술 사업 정보, 핵심 산업에서의 연구 데이터를 중국으로 유출한 혐의로 기소되기도 하였다 (US Department of Justice 2021). 사이버 공격을 통한 민감 데이터의 유출은 미국 정부가 데이터 안보를 국가 안보의 핵심 영역으로 간주하고 자국 내 외국 플랫폼 기업 규제를 강화하게 된 배경 중 하나로 작용했다.

미국의 국토안보부(DHS)는 중국 정부가 데이터를 탈취·조작하며, 이를 정치적 목적에 활용한다는 문제를 지적한 바 있다. 중국 공산당은 2010년대 후반부터 본격적으로 자국 내 정보 검열, 감시 시스템, 데이터 통제를 강화하였으며, 해외 지식재산권이나 기업의 영업 기밀을 탈취하여 '중국제조 2025,' 디지털 실크로드, 군민융합의 정책적 목표를 달성하는 데 이용하는 것으로 추정되고 있다. DHS의 주장에 의하면 도용당한 해외 데이터는 인민해방군의 현대화, 중국 반체제 인사 활동 추적, 공산당의 소수민족 탄압에 대한 국제 정서를 모니터링하는 데 활용되고 있다 (US Department of Homeland Security 2020). 중국 공산당은 자국 기관과 시민을 감시하고 이들의 정보를 정부가 요구하면 제출하도록 강제하는 여러 법제를 형성해왔다. 2017년 제정된 국가정보법은 중국 기업이 정부의 요청이 있을 시, 정보 수집에 협조하도록 규정한다. '네트워크안전법'은 네트워크 운영의 안전과 핵심 데이터 인프라 시설의 보호, 불법 정보를 단속할 것을 명시하고 있다. 2021년 6월 제정된 '데이터안전법'은 중국 내에서 데이터를 수집·처리·저장·유통 등의 활동을 규제하는 법률로, 데이터의 관리가 중국의 국가 안보와 공익을 보호하는 것으로 목표로 한다. 같은 해 11월에 등장한 '개인정보보호법'은 개인정보 처리 원칙과 역외전송 제한의 내용을 담는다. '네트워크안전법,' '데이터안전법,' '개인정보보호법'은 현재 '데이터3법'으로 지칭되며 중국의 정보 검열 체계의 중추를 이루고 있다.

이와 같은 데이터 안보와 관련된 법률은 사이버 공간이 부상하면서 생성되는 다양한 데이터를 국가 차원에서 관리해야 할 필요성에서 제정되었다. 중국의 데이터3법은 안보를 명분으로 기관이나 개인이 수집한 정보를 공산당이 요구할 때 언제든 제공해야 할 의무를 부과한다. 이에 따라 미국은 중국 기업 또는 정부 관련 기관 및 단체와 데이터를 공유하는 자국 기업이

데이터 유출 문제에 노출되었다고 지적하였다. 공산당의 정보 통제 시스템은 기본적으로 해외에 기반을 둔 중국 기업이나 중국 내 위치한 기업으로 유통되는 데이터에 강제적으로 접근할 수 있도록 한다. 공산당은 중국산 부품을 사용하는 해외 데이터 센터에도 영향을 미칠 수 있는데, 백도어를 통해 중국 정보기관의 접근 경로를 확보해두는 방식이다. 또한 중국 기업이 소유하거나 운영하는 모바일 앱에 접근할 수 있으며, 외국 기업과의 합작 회사를 만들 때도 중국 법률에 근거하여 합작사의 데이터를 요구할 수 있다. DHS는 이러한 안보 위험을 지적하며 중국에서 운영되는 회사의 통신 기기나 소프트웨어 사용을 자제할 것을 요청했다 (US Department of Homeland Security 2020).

이러한 배경에서 미국은 중국으로 향하는 미국 데이터와 미국 내 중국산 하드웨어와 소프트웨어 기술 사용에 대한 규제를 강화하기 시작했다. 데이터 안보를 명분으로 틱톡을 규제한 것이 대표적이다. 미국에서는 민영 플랫폼 기업 사이에서 축적한 데이터를 서로 사고파는 관행이 존재해 왔지만, 미국 정부가 특별히 우려하는 부분은 바로 중국 민영 기업들의 공산당과의 유착 관계이다. 전술한 바와 같이 중국 법률에 따라 틱톡 사용자들의 데이터에 중국 정부가 접근 권한을 가지면서 미국은 자국민들의 인적 사항, 물리적 위치, 성향, 온라인 활동내역 등을 모두 조회할 수 있다는 문제를 제기하였다. 이와 같은 우려는 틱톡뿐만 아니라 텐센트 소유의 플랫폼인 위챗, 바이트댄스의 동영상 편집 앱인 캡컷, 그리고 전자상거래 서비스를 제공하는 테무와 같이 미국 사용자 기반이 확대되고 있는 다른 중국 앱에도 발생하고 있다 (Minges 2025).

2) 미국의 틱톡 제재

틱톡에 대한 미국의 우려는 트럼프 1기 행정부 때부터 나타났다. 당시 미·중 무역 전쟁이 시작되면서 사이버 안보와 미국의 데이터 유출 문제가 제기되었다. 2019년 미국은 화웨이의 간첩 위험을 이유로 자국 기술을 사용하지 못하도록 블랙리스트에 올렸으며, 이후 2022년에는 ZTE와 함께 화웨이의 통신장비 판매를 금지하는 시장 퇴출 조치를 내렸다. 화웨이의 사이버 안보 위협 문제가 처음 제기되었던 2019년 미국의 싱크탱크 PIIE(-Peterson Institute for International Economics)는 통신장비뿐만 아니라 소셜 미디어 플랫폼도 국가안보 차원에서 정밀한 조사를 받을 필요가 있다는 내용의 글을 게재했다 (Biancotti 2019). 이를 기점으로 디지털 플랫폼 사업에서 발생하는 데이터 안보 이슈가 정치권에서 다뤄지기 시작했고, 양당은 틱톡에 대한 국가안보 차원의 검사를 시행해야 한다고 주장했다. 중국 회사로의 자국민 데이터 유출에 불안감이 계속 해소되지 못하는 상황 속에 2020년 8월 14일 트럼프 대통령은 틱톡 퇴출 행정명령에 서명하기에 이른다.

바이든 행정부에서도 틱톡에 대한 우려는 수그러들지 않았다. 트럼프와 달리 바이든은 해외 플랫폼 기업의 무조건적 시장 퇴출을 철회하고 본격적인 조사와 체계적인 데이터 관리 제도를 마련하고자 하였다. 이를테면 2021년 데이터 안보와 관련된 행정명령은 적성국이 자국민의 개인정보와 정부 데이터에 대한 접근하는 것을 제한하고 데이터 브로커, 클라우드 서비스, 고용 계약 등을 통해 자국 데이터를 외국이 획득하는 것을 규정하겠다고 명시하였다 (The White House 2024). 이것의 연장선에서 미국 정부는 데이터 안보를 위해 '프로젝트 텍사스'라는 데이터 보안 이니셔티브를 추진하였다. 해당 프로젝트는 미국 사용자의 데이터를 100% 자국 기업인 오

라클의 클라우드에 저장함으로써 미국 정부의 틱톡에 대한 데이터 안보 우려를 해소하는 것을 목적으로 한다. 틱톡 측은 미국에 자사의 데이터 센터를 두기 때문에 미국민의 데이터가 철저히 관리되고 있음을 주장하였으나, 여전히 틱톡의 개인정보처리 방침에 의하면 중국과의 데이터 공유가 가능한 것으로 확인되고 있다.

이러한 배경 속에 2023년에는 미국 상·하원에서 데이터 안보와 관련된 일련의 법안이 발의되었다. 당시 하원은 DATA(Deterring America's Technological Adversaries) 법을 통해 미국인의 민감 데이터의 외국인과의 거래를 금지하였으며, 상원은 RESTRICT(Restricting the Emergence of Security Threats that Risk Information and Communications Technology) 법을 발의하여 연방정부가 소프트웨어 기술에서 발생하는 위협을 식별하고 적성국과의 거래를 제한·금지하는 규제 시스템 구축을 촉구했다. 해당 법안은 중국의 '만리 방화벽'과 마찬가지로 미국 내 운영되는 통신 기술 서비스 중 국가안보를 위협할 수 있는 부분에 대한 식별, 중단, 조사에 대한 광범위한 권한을 상무부에 부여하는 내용을 포함한다 (외교부 경제안보센터 2023). 또한 2024년에는 PAFACA(Protecting Americans from Foreign Adversary Controlled Applications Act), 일명 '틱톡 금지법'을 제정하여 틱톡을 운영하는 바이트댄스가 270일 이내에 틱톡을 미국 사업체에 매각할 것을 요구하기도 하였다.

한편, 현재 트럼프 대통령은 이전에 틱톡에 대한 강경한 규제를 주장해 왔던 것과는 달리 틱톡의 시장 퇴출을 반대하는 입장으로 선회하였다. 이러한 번복은 공교롭게도 2024년 3월 공화당의 적극 후원자이자 틱톡 자회사인 바이트댄스의 핵심 투자자(주주)인 Jeff Yass와의 미팅 시기와 맞아떨어졌다는 점에서 트럼프 자신의 정치적 이해관계에 따른 전략적 행보로 여겨진다. 트럼프가 틱톡을 자신의 선거 캠페인에 유리한 정치적 플랫폼으로

인식하고 있다는 점도 중요하다. 실제로 그는 틱톡에서 약 1,500만 명의 팔로워를 보유하고 있으며, 바이든의 틱톡 규제를 표현의 자유에 대한 탄압이라고 비판하며 이를 자신의 정치적 기회로 활용하고자 했다 (Marcus 2025). 틱톡은 바이든의 강제매각 조치(틱톡 금지법)에 따라 2025년 1월 19일까지 미국 기업에 사업권을 매각해야 했으나, 취임 직전 트럼프는 연방대법원에 법 시행 유예를 요청했다. 그 결과 틱톡은 미국 시장에 잔존할 수 있게 되었고, 현재 트럼프 대통령의 계속되는 일방적인 시한 연장 방침에 따라 임기 내 틱톡이 퇴출당할 가능성은 낮아지고 있다.

3) 미·중 정보심리전과 담론 경쟁

소셜 미디어는 단순한 물리적 폭력을 유발하는 집단을 형성하는 것에 그치지 않고 정치적 양극화를 심화시키거나 잘못된 정보로 인한 여론 조작을 통해 영향력 공작을 수행하는 방식으로도 개인의 안보에 위협이 된다. 이러한 특성은 소셜 미디어가 정보심리전의 도구로 이용될 수 있다는 점에서 특정 국가의 사이버 안보에도 중대한 위협이 될 수 있다. 앞서 언급하였듯이 틱톡을 통해 뉴스를 접하는 미국 사용자 수가 증가할수록 중국에서 생산되는 편향된 콘텐츠를 무비판적으로 소비하는 인구도 증가할 수 있다. 특히 정치적 성향이 확실치 않은 집단이 타깃이 된다면 극단적인 여론이 형성되고 선거 결과에도 영향을 미칠 공산이 작지 않다. 미국에서 이전부터 데이터 브로커를 통해 민간 행위자들 사이에 개인정보를 사고파는 관행이 있음에도 불구하고 데이터 이전의 문제를 심각하게 보는 이유는 바로 이러한 중국 정부의 선전 활동의 가능성 때문이다.

미국 예일대학교의 스티븐 로치(Stephen Roach) 교수는 미·중 갈등을 "바

이럴(viral) 서사의 산물"이라고 표현하며, 양국이 마찰을 일으키게 된 주요 원인이 서로를 향해 생산하는 거짓 서사 때문이라고 주장한다(스티븐 로치 2022, 120). 이는 미·중 갈등이 실제 사건(사실)에 기반하여 초래되기보다는 양국이 서로를 위협적으로 묘사하는 서사와 담론의 상호 생산을 통해 형성되고 고조된다는 의미다. 이를테면 중국은 미국의 내부 문제를 과장하여 쇠퇴하는 국가로 묘사하면서 중국 체제의 우월성을 주장하려고 한다. 반면에 미국은 (특히 트럼프 대통령은) 무역적자와 제조업 붕괴의 원인을 모두 중국의 책임으로 돌린다. 서로가 생산하는 내러티브의 진위 여부와 무관하게 이와 같은 담론, 달리 말해 '구성된 위협'은 지속적으로 생산·강화되고 있다. 즉, 미국과 중국 간 갈등이 증폭되는 핵심 이유가 이들 사이에 벌어지는 서사 경쟁이라 할 수 있다.

상대를 향한 편향된 메시지, 허위 정보는 소셜 미디어 플랫폼을 통해 빠르게 확산된다. 그리고 왜곡된 정보(거짓)는 정보심리전 수행을 위한 핵심 자원이다. 이는 대중들이 진실보다 거짓에 대한 수용성이 훨씬 높기 때문이다. MIT 미디어랩에서 트위터에 올라온 트윗과 리트윗을 대상으로 진행한 연구에 의하면 거짓 소문을 보는 사용자의 숫자, 리트윗 횟수, 확산의 속도가 진실보다 월등히 높다는 결과가 나타났다 (스티븐 로치 2022, 123; Soroush et al. 2018). 해당 연구에서 특히 주목할 것은 일반적인 거짓보다 정치적 거짓 소문이 훨씬 빠르게 확산된다는 점이다. 이는 만약 틱톡에서 미국민을 상대로 가짜 정치 뉴스를 확산시킨다면, 사용자들은 이를 사실로 받아들이고, 그들의 정치적 성향이 결정될 수 있음을 시사한다. 틱톡은 이미 천안문 사태, 티벳 독립, 양안 문제, 신장 위구르 지역의 강제 노동과 관련된 영상을 검열하는 알고리즘 조작을 펼쳤다는 정황이 포착된 바 있다 (Radio Free Asia 2024). 실제로 인스타그램이나 유튜브와 같은 경쟁 플랫폼과 비

견하여 틱톡은 친중국 편향이 두드러지는 것으로 평가된다. 실제로 다수의 영상에서 중국을 비판하는 댓글이 검열되는 현상이 포착되고 있으며, 이는 소셜 미디어 플랫폼이 정치 프로파간다의 수단으로 활용되고 있음을 시사한다. 물론 대부분의 젊은 이용자들은 중국 정부의 콘텐츠·알고리즘 조작을 인지하면서도 오락을 목적으로 틱톡을 계속 사용하고 있다. 이렇다 보니 틱톡을 일상에서 계속 사용하는 미국인들은 중국 정부가 틱톡을 정치적으로 활용하는 이상 정보심리전의 타깃이 될 공산이 크다.

틱톡 사태는 단순히 정보전을 넘어 사이버 안보 문제이다. 일반적으로 사이버 안보는 화웨이·ZTE 사태와 같이 백도어, 랜섬웨어, 해킹 등 하드웨어/네트워크 장비에 대한 공격과 같은 보안 기술적 문제로 인식된다. 이는 협의의 사이버 안보 영역으로 볼 수 있다. 어떠한 의도된 방향으로 개인이 사고하도록 정보를 생성하는 정보심리전은 온라인 공간에서 정치적 영향력을 투사한다는 점에서 사이버 안보의 개념을 확장시킨다. 다시 말해 사이버 공간의 창출은 정치 프로파간다, 정보전을 용이하게 하는 동시에 이러한 정보심리전의 효과를 확대할 수 있다. 정보심리전은 전통적인 사이버 공격을 감행하지 않더라도 상대 국가의 정보 생산 체계, 인지 영역을 지배함으로써 정치적 목적을 달성하려는 시도이기 때문이다. 가령, 틱톡 내 중국 공산당에 대한 우호적인 영상, 미국의 정치적 불안정성을 과장하는 콘텐츠가 자연스럽게 추천 피드에 등장하도록 하는 콘텐츠 우선순위 조작, 허위 정보/가짜 뉴스 유포를 통한 여론 조작을 유도할 수 있다. 이슈 프레이밍(framing)과 프라이밍(priming)은 특정 사건에 대한 대중의 관심이 경도될 수 있도록 유도하고, 편향된 방향으로 사건을 해석하게 만든다. 이는 대외 위협인식을 기반으로 확산되는 미국과 중국 간의 담론 경쟁이 디지털 미디어 플랫폼을 통해 더욱 강화될 수 있음을 의미한다.

3. 라인-야후 사태와 데이터 주권 논란

2023년 10월 네이버가 운영하며 일본의 대표 메신저로 알려진 라인(LINE)의 악성코드 감염으로 인한 해킹으로 몇십만 명의 개인정보가 유출되는 사건이 발생했다. 일본에서 라인은 월 사용자가 9600만명에 달할 정도로 우리나라의 카카오톡과 같은 일본의 국민 메신저로 기능하고 있다. 라인은 데이터 및 네트워크 관리를 네이버클라우드에 의존하였는데, 네이버클라우드 협력사 PC에 심어진 악성코드가 라인-야후 시스템에 접근하여 앱 이용자 및 거래처의 개인정보 약 52만 건이 유출되었다. 해커가 네트워크 관리자 권한을 탈취하였기에 가능한 일이었다. 유출된 정보는 앱 사용자의 성별, 나이뿐만 아니라 구매 내역, 이메일 주소 등을 포함했다.

라인은 본래 네이버의 일본 자회사인 NHN재팬을 통해 서비스가 제공되었으나 이후 야후 재팬과 경영이 통합되었다. 이에 따라 새로 발족한 라인-야후(LY Corporation)는 네이버와 소프트뱅크가 각각 50%의 지분을 보유하는 공동 경영 체제를 갖추게 되었다. 2024년 3월 일본 총무성은 '통신 보안에 대한 사이버 보안 확보'라는 행정지도를 발표하며 데이터 유출의 재발 방지를 촉구했다. 이후 4월 총무성은 2차 행정지도를 내어 네이버의 지분을 소프트뱅크에 매각할 것을 요구하였다. 두 차례의 행정지도 라인-야후의 온라인 시스템 보안을 한국 기업인 네이버가 맡으면서 해킹 문제에 발 빠른 대응을 하지 못했다는 판단 때문이었다. 특히 자민당 의원들은 이번 데이터 유출 사건을 일본의 국가안보적 위협으로 인식했다. 이에 대해 한국 정부가 일본 총무성의 행정지도를 일방적인 지분 매각 강요로 받아들이면서 해당 사건은 한·일 외교전으로 이어졌다.

이러한 네이버와 일본 정부와의 갈등은 데이터 주권에 대한 우려에 기인한다. 메신저 플랫폼에 축적되는 방대한 양의 개인정보는 플랫폼의 실질적인 운영자인 네이버(한국기업)이 보유하지 않고, 데이터가 발생한 현지 정부와 기업이 관리해야 한다는 것이다. 자국민의 데이터를 외국 기업이 소유하는 방식은 국가안보적 위협이 될 수 있기 때문이다. 따라서 일본 정부는 현지법인이 데이터 보호에 대한 책임을 져야 한다는 공식 입장을 발표하였다. 이는 앞서 미국 정부가 틱톡에 대한 제재를 가한 연유와 동일하다. 행정지도에 대한 대응으로 라인-야후는 네이버의 기술에 대한 의존도를 축소하고 '보안 거버넌스 위원회'를 설치하여 보안 부문을 보강하겠다는 뜻을 밝혔다 (김민국 2024).

이렇듯 라인-야후 사태는 사이버 공격으로 촉발된 데이터 주권 논의라는 점에서 사이버-데이터 안보의 이슈 연계성을 보여준다. 데이터 주권 문제는 이제 기업이 관리해야 할 핵심 리스크로 부상할 뿐만 아니라 국가전략 차원에서도 주목해야 할 이슈로 부상하고 있다. 기술 종속성에 대한 우려와 향후 AI 및 플랫폼 산업 진흥을 위한 데이터 확보라는 측면에서 단순한 보안 이슈를 넘어 국가 전략적 이해관계와 직결되기 때문이다. 이는 앞서 틱톡이 플랫폼 서비스를 통해 축적하는 미국민 데이터에 대한 통제권을 요구하는 미국의 논리와도 상통한다. 미국 정부의 틱톡 규제가 전략적 경쟁 관계에 있는 중국과의 지정학적 안보 문제에 기인한 것과 달리, 라인-야후 사태는 사이버 공간에서 나타나는 보안기술의 취약성에서 비롯된 연쇄적 피해이다. 이는 사이버-데이터 안보 이슈는 국제정치적 이해관계와 무관히 안보 환경의 불안정성을 확대시키는 요인으로 부상하고 있음을 시사한다.

4. 결론

디지털 전환으로 형성된 초연결 사회는 인류에 전례 없는 정보공유, 소통의 장을 제공하였다. 현재 소셜 미디어 플랫폼에서 전 세계 사람들이 실시간으로 정보와 의견을 주고받으면서 개인, 집단에 대한 다양한 정보가 비약적으로 생성·축적·활용되고 있다. 개방성과 초연결성을 특징으로 하는 플랫폼 공간은 가짜 뉴스와 왜곡된 정보의 급속한 확산과 이로 인한 여론 조작이 일어난다는 점에서 국가안보의 주요 현안으로 자리매김했다. 특히 미국과 중국 간의 전략경쟁의 맥락에서 틱톡을 통해 미국민의 개인정보가 유출되고 정보심리전이 이루어질 수 있다는 가능성은 안보적으로 민감할 수밖에 없다. 중국의 데이터법에서 모든 기업이 국가의 정보활동을 지원해야 하며 언제든 정부의 정보요청에 응해야 할 의무가 적시되어 있는 만큼, 미국은 데이터 안보에 대한 경각심이 큰 상황이다. 여기에 더해 라인-야후 사태는 특정 기업에 보안 기능을 위탁하는 과정에서 발생한 해킹 사건으로, 민간 기업 간 데이터 유출 문제가 한국과 일본 간 외교 문제로 격상된 사례이다. 명백한 물리 공격을 수반하지 않더라도 국가 안보의 위협이 될 수 있다는 점, 무엇보다 민간 기업이 제공하는 서비스와 이러한 민영 플랫폼에서 발생되는 개인의 데이터가 안보적 목적으로 활용될 수 있다는 점은 오늘날 신흥안보가 창발하는 양상을 단편적으로 보여준다.

최근에는 넷플릭스, 디즈니플러스와 같은 OTT 플랫폼 서비스에서 개인정보가 다량 유출되는 사건이 발생하며 데이터-사이버 안보의 넥서스 현상으로 빚어지는 안보 문제가 다시 거론되고 있다. 약 700만 건의 계정 정보가 유출된 이 사건은 특정 집단을 겨냥하여 실시된 사이버 공격이 아닌,

사용자의 휴대기기가 악성코드에 감염되며 발생하였다. 이러한 양상은 사이버 공격의 주체가 분산되면서 나타나는 책임 귀속의 모호함이라는 문제를 노정하며 새로운 제도적 장치 마련을 요구하고 있다. 이처럼 많은 사람이 일상적으로 사용하고 있는 디지털 플랫폼이 부지불식간에 사이버 공격에 노출될 수 있는 환경이 되면서 데이터 거버넌스의 불안정성을 증폭시키고 있다.

특히 AI 기술의 진화는 사이버 공격을 더욱 정교하고 다양한 형태로 이루어질 수 있음을 시사한다. 최근 생성형 AI 시장이 성장하며 주목받고 있는 중국의 딥시크(DeepSeek) 또한 바이트댄스의 데이터 센터를 사용한다는 점에서 안보적 우려를 낳고 있다. AI 시대에 데이터 안보에 대한 우려는 사이버 안보와 더불어 다양한 신흥안보 이슈와의 연계성으로 인해 더욱 확대되고 있다. AI 경쟁이 치열해질수록 데이터의 수집과 유관 인프라에 대한 통제가 중요해지고 있으며, 생성형 AI가 학습한 데이터와 알고리즘 설계에 따라 출력되는 편향적 응답은 은연중에 특정 이념의 정치 담론을 확산시킬 수 있다는 점에서 새로운 안보 위협으로 떠오르고 있다. 이처럼 기술의 발전에 따라 사이버 공간에서의 영향력 투사가 강화되는 현상은 국가 차원의 데이터 관리 체계를 다시 정립할 필요성을 시사한다.

제11장

AI 기반 무기체계와 사이버 안보

윤대엽 | 대전대학교 군사학과 교수

제11장

AI 기반 무기체계와 사이버 안보

윤대엽 | 대전대학교 군사학과 교수

1. 문제제기

러우전쟁과 이-하마스 전쟁은 AI-사이버가 통합된 인공지능전쟁(AI War)의 시험장이 되었다. 제한적 AI 기술이 통합된 반자율 드론은 조종지원, 경로점 탐색, 장애물 회피는 물론 표적선택과 타격능력을 고도화하면서 드론전쟁(drone warfare)의 미래를 현재화했다. 우크라이나와 러시아는 드론에 AI 기능을 탑재하여 날씨, 지형, 은폐를 극복하여 표적을 식별하고 전장정보를 수집하는 데 활용했다. 공격 기능까지 통합된 저가의 배회형 자폭 드론(loitering munition)은 고가의 미사일이 전술적 한계를 뛰어넘어 표적을 식별하고 추적하여 타격했다. 우크라이나가 러시아 내륙의 공군기지를 타격한 '스파이더 웹' 작전 역시 인간-AI 혁신의 결과물이다. Tu-95MS, Tu-22M3, A-50 등 표적 항공기의 데이터를 온보드 컴퓨터에 탑재한 공격 드론은 표적을 정밀 타격했다(Bondar 2025). AI 기반 지휘통제체제(AI-C2)도 고도화되었다. AI는 다양한 정보자산에서 수집된 레이더, 적외선, 신호정보, 드론영상, 공개출처정보(OSINT)를 융합하여 표적정보를 식별하고 의사결

정을 지원했다. AI 기반 디지털 타겟팅의 혁신 주역은 팔란티어(Palantir)다. 팔란티어 고담 시스템은 드론영상, 휴민트와 테킨트로 수집된 정보를 실시간으로 분석하여 전장을 컴퓨터 비전(computer vision)으로 시각화하는 '디지털 트윈'을 제공했다.

AI 기반 무기체계가 '전쟁의 안개(fog of war)'를 제거하고 디지털 킬 체인(Digital F2T3EA)을 고도화하면서 공격자 우위의 수단이 되었지만 동시에 AI 지원무기의 활용, 대응에 대응하는(counter-countermeasure) 군사혁신의 과제도 분명해졌다. 조종사의 숙련도에 의존해야하는 제한적 드론의 운용인력이 증가시키면서 포병화력과 항공우세를 대체하는 양적우위의 수단이 되지 못했다(윤대엽 2025). 2025년까지 우크라이나가 운용한 원격조정 드론 중 실제 작전목표를 달성한 것은 20-40%에 불과하다(Goncharuk 2025). 드론 장비와 핵심부품의 60% 이상을 중국 DJI에 의존하는 우크라이나는 값싸고 많은 스마트한 드론을 소모적인 무기로 사용하지 못했다(Pusztaszeri 2024). 전장 사물인터넷(IoBT), 클라우드, 우주정보자산 등 AI 지원무기를 감시정찰-정보분석-의사결정-작전운용에 통합하여 운용할 수 있는 'AI의 디지털 기반'의 취약성으로 인해 AI 지원무기의 활용은 전술차원으로 제한되었다.

대드론작전(counter-UAV), 카운터 AI(Counter AI) 등 AI의 방어적 혁신 역시 AI의 군사적 활용을 제한했다. 사이버·전자기 무기는 AI 기반 무기체계의 통신, 조정, 운용이나 기능을 방해, 파괴, 교란했다. 우크라이나와 러시아는 재밍이나 GPS 스푸핑 수단을 활용하여 드론을 방어했다. 우크라이나의 전자기 방어시스템인 포크로바(Pokrova)는 러시아의 공격드론을 최소 22%, 최대 50%까지 방어하고 공격드론의 경로를 변경했다(Vakulina 2024). 또, AI 기반 무기체계의 영상인식을 기만하는 데이터 기만(data deception), 레이저

와 전자기(EMP) 공격을 통해 센서와 디지털 기기를 무력화하는 공격수단도 사용되었다. AI 기반 지휘통제체계를 대상으로 하는 카운터 AI전략의 리스크도 증가했다. AI-C2에 연결, 통합되어 운용되는 AI 기반 무기체계를 무력화히기 위해 사이버·전자기 수단으로 UAV 감시정찰 네트워크를 파괴하거나, 과잉신호, 전파, 위장영상을 통해 전장데이터를 위장, 교란했다(Cunningham 2024). 은폐, 엄폐, 위장 등 물리적 기만, AI 기반 정보수단의 디지털 기만, 그리고 사이버공격을 통해 데이터를 위조하거나 AI-C2체계를 직접 마비시키는 공세적 수단은 AI 기반 무기체계의 활용을 제한할 수 있다.

사이버-AI 넥서스는 군사전략과 사이버안보 전략에 어떤 변화를 수반하는가? 본 연구는 AI 기반 무기체계의 체계(AI weapon system of system)를 플랫폼으로 통합해야하는 국방 인공지능 전환(Defense AX)이 억지-방어-공세의 전략적, 시간적 사이클을 축소하면서 공세적 사이버 전략의 전환을 수반하고 있음을 분석한다. 제2장에서는 사이버전의 신화(myth of Cyber War) 논의를 비판적으로 검토하고 디지털 전환(DX), 인공지능 전환(AX), 플랫폼 전환(PX) 등 데이터의 흐름을 만드는 AI 디지털 아키텍쳐가 사이버안보의 전환(CX)을 수반하고 있음을 분석한다. 제3장에서는 미국의 합동전영역지휘통제(JADC2)와 팔란티어 플랫폼의 사례를 통해 AI-C2 통합과 사이버안보의 전환을 분석한다. 제4장에서는 공세적 사이버전략을 부대에 통합하는 사례로서 다영역TF사단을 분석한다. 제5장에서는 카운터 AI 전략과 디지털 리스크의 맥락에서 사이버안보의 전략적 쟁점을 분석하고 통합적 AI-사이버안보 전략과제를 제시한다.

2. AI 디지털 아키텍쳐와 사이버 안보의 전환

사이버 공간이 군사적 전장영역(domain of warfare)으로 인식되기 시작한 것은 1991년 걸프전이다. 컴퓨터, 인터넷과 네트워크 기술이 정찰-타격 체계(reconaissance-strike system)를 혁신하면서 사이버 리스크가 증가했기 때문이다. 1993년 랜드연구소는 '사이버전이 온다(Cyberwar is Coming)'는 제목의 보고서를 통해 네트워크를 전장화하는 넷 전쟁(Netwar) 개념을 확대하여 공간으로서 사이버, 그리고 광범위한 정보를 활용하는 사이버전을 쟁점화했다(Arguilla and Ronfeldt 1993). 사이버전은 국가 또는 비국가 세력이 소프트웨어 등의 수단을 활용하여 국가의 컴퓨터 네트워크나 정보 네트워크에 중대한 위해를 가하는 공격을 의미한다(송태은 2024, 218). 디지털 정보통신 기반이 확대되고 사이버 공간에 대한 의존에 비례하여 사이버 공격수단이 고도화되면서 사이버안보는 양질전화, 이슈연계를 넘어 복합지정학의 문제가 결부되어 있는 거시적 안보문제로 창발되어 왔다(김상배 2024). 사이버공격 수단은 해킹을 통한 데이터 유출, 시스템 마비에서 데이터 조작(Data Manipulation), AI 체계에 대한 데이터 오염(Data Corruption), 영향공작과 인지전으로 고도화되었다 (윤정현 2024, 184-194). 사이버위협이 고도화되면서 세계 각국은 국가차원의 사이버 안보 전략은 국방 사이버전략을 재편하고 사이버 전력체계를 구축하고 있다. 2012년 레온 파네타 국방장관이 말한 디지털 기반에 대한 파괴적인 공격이 '사이버 진주만 공격(Cyber Pearl Harbor)'이 될 수 있다는 비유는 사이버 위협을 넘어 사이버전에 대한 전략적 인식을 대변한다.

그러나, 사이버전이 정치적, 군사적 목적을 달성하는 독립적 전장이 되

었는지는 여전히 쟁점이다(Gartzke 2012). 기술이 무기체계, 부대구조, 군사전략과 전쟁 양상을 변화시켜 온 것처럼 사이버 공간은 군대가 준비해야하는 새로운 전장이다. 국가, 비국가 행위자가 저가의 비용으로 대규모 피해를 초래할 수 있는 사이버 무기는 비대칭 위협(asymmetric threat)이다. 광범위한 사용자 기반 디지털 기기가 네트워크로 연결되어 데이터 경제가 확산되고 플랫폼으로 통합되면서 방어할 수 없는 사이버 취약성(cyber vulnerability)도 증가한다. 공격자를 식별할 수 없는 책임귀속의 딜레마로 인해 억지, 방어는 물론 보복의 딜레마도 존재한다.

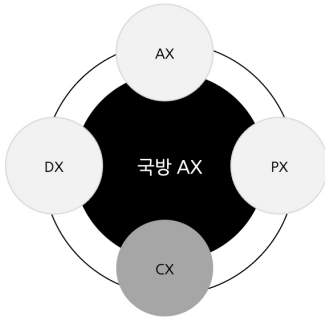
그러나, 다양한 사이버 무기를 동원한 대규모 사이버 작전이 수행된 러우전쟁에서 조차 사이버전은 전쟁의 승패를 결정하는 독립적 전장이 되지 못했다(Pytlak 2024). 물리적 공격보다 앞서 러시아는 사이버전을 수행했다. 폭스 블레이드(Foxplade)를 동원해 우크라이나 정부와 주요 기반 시설의 데이터를 삭제했고, 군 통신망을 교란하기 위해 비아셋 위성시스템을 공격했다(신범식·양정윤 2024). 전쟁 초기 러시아의 사이버 공격은 민간 부문 59.6%, 국가공공기관 31.9%에 집중되었고 정부군에 대한 공격은 8.5%에 불과했다(신범식·양정윤 2024, 133). 러시아의 클라우드 공격에 대응하여 MS 클라우드와 스타링크는 우크라이나가 AI 기반 무기체계를 운용하는 디지털 플랫폼이 되었다(송태은 2024, 229-230; Kirichenko 2025).

사이버 공간은 강압이나 정복 목적의 군사작전을 수행하는데 중요한 전장이 되었지만 여전히 물리적 공격보다 열등한 대체품이다(Gartzke 2013, 42). 적대국의 군사력을 마비시키고, 사이버 정보활동을 통해 정보를 수집하며, 정부 및 민간기관을 대상으로 하는 네트워크 공격은 사이버 공간의 확대에 비례하여 중요한 군사적 표적이 되었다. 그러나, 군사력은 전쟁의 수단일 뿐만 아니라, 사용하지 않고도 적대국의 강압, 무력을 억지하는 보

이는 힘(visible power)다. 무력을 사용하지 않고도 상대국에게 영향력을 행사할 수 있다면 비용을 최소화하면서 정치적 목적을 달성할 수 있다. 반대로 군사적 수단이 적대국에 위협, 공포라는 신뢰를 전달하지 못하면 억지, 강제의 효과는 상실된다. 군사력의 전략적 가치는 사용하지 않고도 상대에게 영향력을 행사할 수 있는 상징성과 함께, 실제 사용해야 하는 경우 군사적 목적을 달성하는 수단이 되어야 한다. 또, 군사력이 전략적 목표를 달성하는 수단이 되기 위해서는 감당할 수 없는 피해를 줄 수 있다는 '강압의 신뢰성'도 중요하다.

사이버전의 회의론이 제기하는 본질적인 쟁점은 사이버 공격이 다른 물리적 수단에 의해 보완되어야만 군사적 효과성을 발휘할 수 있다는 점에 있다. 사이버 공간에서 이루어지는 사이버 전쟁의 효과는 일시적, 단기적이다. 사이버 공격으로 얻을 수 있는 전략적 우위는 사이버 공격의 우위를 지속적인 효과로 활용할 수 있는 군사적 역량에 달려있다. 사이버 공격은 소프트킬로 '피해'를 입힐 수는 있지만 상호확증파괴 수준의 손실을 가시화하는 데는 제한적이다. 사이버보안과 회복탄력성이 혁신되면서 사이버 공격은 마비, 탈취, 파괴를 통해 일시적 우위를 달성할 수 있다. 이는 화력이 적대국의 작전능력의 구조적, 지속적 비용을 강제하고 우세를 달성하는 것과 상이하다. 이 때문에 보이지 않는 사이버 무기는 핵 보유와 혁신, 발신과 설득, 타협과 안정이라는 핵억지력의 논리와 심리적 억지 효과도 제한적이다.

〈그림 12-1〉 AI 디지털 아키텍쳐와 사이버안보의 전환



구분	리스크의 전환과 안보화
AX	데이터는 AI 학습, 추론의 기반
CX	사이버안보 리스크의 거대한 전환
DX	데이터를 활용을 위한 디지털 기반
PX	데이터를 축적, 분석, 활용하는 기반
리스크 전환 (RX)	네트워크 효과와 플랫폼 권력·독점 데이터 주권, 데이터 편향, 알고리즘 편향 디지털 기반의 비대칭적 취약성 디지털 공급망, 공급망 공격과 취약성 AI 보안, 데이터 공격, 자율무기 해킹

그러나 국방 인공지능 전환(defense AX)이 데이터-디지털-플랫폼의 통합을 촉진하면서 사이버안보 전략, 능력과 수단을 변화시키고 있다. 인공지능 전환은 알고리즘, 빅데이터, 클라우드를 핵심 기반으로 데이터를 생성, 축적, 전달, 활용하기 위한 광범위한 디지털 기반을 구축하는 과정이다. 미중은 디지털 기술의 표준, 산업 생태계를 혁신하고 안보, 경제, 군사적 이해가 결부된 AI 패권의 우위를 위해 경쟁하고 있다(김상배 2025, 103). 인공지능 전환(AX)은 알고리즘, 클라우드 컴퓨팅, 빅데이터 등 인공지능의 디지털 기반의 통합적, 동시적 혁신을 수반해야 한다. 동시에 인공지능 전환은 디지털 기술, 공급망, 인프라의 상호의존을 심화시키는 디지털 전환(DX)과 연계되어 있다. AX-DX의 본질적인 목표는 데이터의 활용을 위한 디지털 기반을 구축하는 데 있다. 이 때문에 데이터 수집, 저장, 분석은 물론 이를 경제적, 안보적 목적에서 활용하기 위한 플랫폼 전환(PX)을 촉진하고 있다.

디지털-데이터-플랫폼이 상호연계, 통합된 인공지능 전환은 사이버 안보의 전환(Cybersecurity Transformation, CX)을 수반한다. 데이터-디지털-플

랫폼은 사이버 네트워크로 연결되어 AI 디지털 아키텍쳐를 구성한다. AI 디지털 아키텍쳐란 데이터의 생성, 전달, 축적 및 이를 인공지능으로 활용하기 위해 데이터-디지털-플랫폼-사이버안보의 기술, 운용을 위한 체계를 의미한다. AI 디지털 아키텍쳐는 안보-경제의 문제가 상호 통합되어 있다. 정보화 기술의 혁신이 표준경쟁이었다면 데이터 기반 디지털 인프라를 구축하는 AI 패권경쟁은 AI 디지털 기반을 안보화하는 '규제경쟁'이다(Mügge 2023). 규제경쟁은 디지털, 데이터, 플랫폼, 사이버, 궁극적으로는 인공지능 전환이 경제적, 안보적, 기술적 이해가 중첩되어 있기 때문이다. 비고갈적 재화인 데이터의 비경합적, 탈정치적 활용이 가능하다면 산업혁명, 정보혁명보다 비약적인 사회경제적 혁신의 도구가 될 수 있다. 그러나, 데이터는 탈정치화된 비경합적 재화가 아니다. 신뢰할 수 있는 데이터의 질과 양은 경쟁우위를 위한 자원일 뿐만 아니라 경제적, 사회적, 안보적 이해가 동시화된(synchronized) 재화라는 점에서 겸용기술(dual-use technology)과는 그 성격이 본질적으로 상이하다. 데이터는 목적에 따라 상업적, 군사적, 사회적 용도로 겸용되는 재화가 아니라, 경제적, 기술적, 안보적 이해가 이미 통합된 전략 자산(strategic assent)이기 때문이다.

데이터를 국가가 아닌 외부와 민간 부문의 혁신에 의존해야 하는 국가-기업 관계의 변화는 디지털 리스크를 관리해야 하는 안보적 이해를 강화시킨다(Mügge 2023, 1432). 디지털 전환은 디지털 기술, 경제, 산업기반의 육성과 함께 공급망의 안보화와 통합되어 있다(유인태 2024). 데이터의 경제적 활용은 데이터 주권, 데이터 안보의 문제와 일체화되어 있다(윤대엽 2024). 빅테크 플랫폼의 독과점은 정치적, 경제적, 안보적 리스크가 되었다. 빅데이터를 수집, 저장, 분석하고 이를 활용하는 AI 플랫폼(AIP)은 가치중립적인 중개자가 아니라, 가치 편향적인 지식과 인식을 생산할 수 있다. 알고리

즘으로 데이터를 활용하는 AI 플랫폼은 정치적, 경제적 이해뿐만 아니라 안보적 이해가 중첩되어 있다. 디지털 기술, 공급망은 물론 클라우드, 빅데이터와 디지털 기반의 복합적인 연계와 통합이 소버린 AI, 디지털 주권, 클라우드 주권, 컴퓨팅 주권, 플랫폼 주권와 동기화되어 있는 것도 이 문이다.

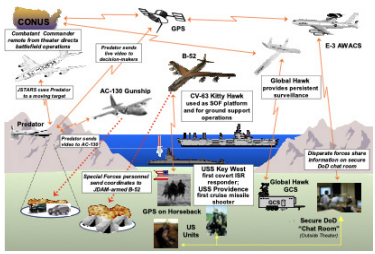
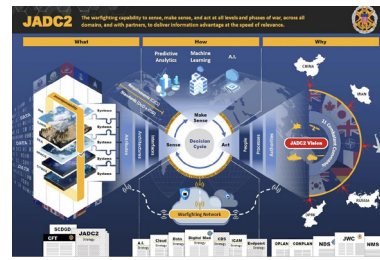
경제-안보적 이해가 통합된 AI 디지털 아키텍쳐를 구축해야하는 국방 인공지능 전환은 사이버 안보와 국방 사이버 안보 전략에 본질적인 전환을 수반한다. 국방 인공지능 전환은 군사적 목적의 데이터의 생성, 축적하고 데이터를 전달, 활용할 수 있는 AI 디지털 아키텍쳐를 구축하는 것이다. 반대로 군사적 데이터의 생성, 축적, 전달, 활용하는 AI 디지털 아키텍쳐를 교란, 마비, 파괴할 수 있는 사이버 위협은 파괴적인 손실을 초래할 수 있기 때문이다.

3. AI-C2 플랫폼과 사이버 안보

미국이 추진하는 합동전영역지휘통제체계(JADC2)는 AX·CX·DX를 AI 기반 지휘통제플랫폼에 통합하는 선도적인 사례다. JADC2의 목적은 데이터 기반 지능형 통합지휘통제 체계를 구축하여 정보우위, 의사결정 우위를 기반으로 6차원 스펙트럼에서 합동성을 증진하는 것이다(DoD 2022,2). AI기반 지휘통제 플랫폼인 JADC2는 전통적인 킬 체인을 감지(sense), 이해(make sense), 행동(act) 3단계로 축소했다. 첫째, 정보수집을 위한 광범위한 전장사물인터넷(IoBT)과 정보관리 기술이다. 6차원 스펙트럼의 원격센서,

정보자산 및 오픈소스 등 데이터 및 정보센서 체계에 기반한다. 정보우위를 위해서는 우호적, 적대적, 중립적 데이터를 수집, 처리, 활용할 수 있는 지능형 데이터 생태계가 형성되어야 하며 이를 전장에서 활용하는 체계를 구축한다. 둘째, 정보이해(make sense)역량의 혁신이다. 군사적 목적의 정보분석의 본질적인 목적은 적대국의 행동, 의도, 능력에 대한 분석은 물론 전략적, 작전적 행동을 이해하고 예측하는 것이다 (DoD 2022, 5). 이를 위해 다출처 데이터를 통합하고 분석, 예측할 수 있는 지능형 플랫폼을 구축한다. 셋째, AI-C2를 AI 기반 무기체계와 통합하는 것이다. AI-C2를 전장에서 활용하기 위해서는 AI 디지털 아키텍처의 사이버 리스크에 대응하여 중첩적, 탄력적, 분산된 의사결정 애플리케이션과 전달수단이 구축되어야 한다.

〈그림 12-2〉 군사체계의 시스템 통합과 플랫폼 통합

시스템의 시스템 (SoS)		플랫폼의 플랫폼(PoP)
		
정보화 전쟁	시기	지능화 전쟁
네트워크중심전(NCW)	전장	인공지능전(AIW)
소프트웨어	수단	데이터
미소 컴퓨터 군비경쟁	기술	인공지능의 디지털 기반

AI-데이터-디지털-플래폼이 연계와 통합이 가속화되면서 사이버 작전도 변화되었다. 첫째, 사이버안보는 플랫폼 운용성과 일체화된 과제가 되었다.

좁은 의미의 디지털 상호운용성(digital interoperability)은 '두 개 이상의 시스템 또는 구성요소가 정보를 교환하고 활용할 수 있는 능력'으로 정의할 수 있다. 그러나, AX·CX·DX가 통합된 AI기반 지휘통제 플랫폼 전환은 시스템 호환성을 넘어 사이버 보안성, 데이터 신뢰성, 디지털 호환성이 통합되어 있다. 둘째, 제로트러스트(zero-trust) 보안을 넘어 분산에 의한 회복력 체계(resilience by distribution)를 구축하는 것이다(Burdette et al, 2025). 선제적 억지가 제한적인 디지털 리스크에 대한 회복력을 강화하기 위해서는 센서 네트워크의 다원화, 데이터 패브릭, 지휘통제 노드 등의 분산 및 중첩된 AI 디지털 아키텍쳐를 구축해야한다. 셋째, 동시에 공세적, 선제적 사이버 작전의 중요성이다. 광범위한 디지털 기반이 네트워크로 연계되어 데이터 기반의 플랫폼으로 통합되면서 공격표면의 취약성도 확대되었다. 네트워크 기반 데이터의 흐름이 전장의 신경망이되면서 사이버 공격, 데이터 변조, 디지털 마비로 인한 사이버 리스크는 곧 광범위한 작전능력의 무력화로 이어질 수 있다. 따라서 사이버 작전은 제로 트러스트 아키텍쳐, AI 기반 위협식별, 회복력의 구축과 함께 선제적, 공세적 사이버 전략이 형성되었다.

AI 기반 지휘통제체계의 통합을 주도하는 팔란티어는 디지털-사이버-데이터 안보가 결부된 AI 플랫폼 구축에 흥미로운 혁신 사례를 제공한다. 팔란티어는 2004년 CIA 벤쳐부문(In-Q-Tel)이 지원하는 국방벤처로 출발했다. '천리경'을 뜻하는 사명이 대변하듯 팔란티어는 정보기관, 군사데이터를 분석하는 소프트웨어 기업으로 성장했다. 2014년 민간부문이 주도하는 AI혁신의 군사적 활용을 목표로 2014년 국방혁신단(DIU)가 신설되고 2017년 알고리즘전 교차기능팀(메이븐 프로젝트)를 수준하면서 전장분석 및 AI 기반 디지털 타켓팅(digital targeting)을 주도하는 국방 빅테크로 성장했다.

러우전쟁과 이-하마스 전쟁은 팔란티어가 주도하는 AI기반 지휘통제 플

랫폼의 파괴적인 능력의 실험장이 되었다. 팔란티어는 이스라엘군이 '킬웨어(Killware)'를 통해 통신 메타데이터, 감시영상, 위치정보, SNS를 통합하여 하마스 요원의 표적화를 지원했다. 2022년 6월 카프(Alexander Karp)는 우크라이나를 직접 방문하고 무료로 팔란티어 시스템을 제공했다. 카프는 2023년 2월까지 우크라이나군이 수행한 작전에서 표적화를 지원했다고 공개적으로 언급하기도 했다. 두 개의 전장에서 혁신의 속도를 가속화한 팔란티어는 2024년 4억 8천만 달러 규모의 미 육군 메이븐 스마트 시스템(Maven Smart System) 프로젝트를 수주했다 (DoD 2024). 육군이 추진하는 메이븐 프로젝트는 다출처 정보를 융합하여 전장정보, 표정정보를 제공하는 AI 플랫폼으로 CJACDC2 통합을 목표로 2029년까지 추진하는 사업이다. 그러나, 팔란티어의 비즈니스 모델은 국방영역에 국한되지 않는다. 2024년 기준 팔란티어 고객은 711개로 29억달러의 매출액의 55%는 정부기관, 45%는 상업 부문에서 발생했다. 또, 매출액의 34%는 해외고객에서 발생했고, 고객은 금융, 석유, 자동차, 제약, 경찰까지 다양하다 (US SEC 2025, 6). 2025년 2월에는 국토안보부와 이미자 추적 플랫폼 구축으로 3,000만 달러의 계약을 체결했다.

팔란티어 AI 플랫폼은 고담(Gothan), 파운드리(Fountry), 아폴로(Apollo), AIP로 구성된다 (SEC 2024, 5; Palantir). 수직적으로 통합된 네 개의 플랫폼은 고객의 데이터를 통합, 운용하고 모든 환경에서 실행할 수 있는 인프라를 제공한다. 네 개의 플랫폼은 사용자의 필요에 따라 하나의 플랫폼으로 통합하여 활용할 수 있다. 고담은 정보분석, 임무기획, 군사표적과 같은 임무를 지원하기 위해 데이터 소스를 통합하는 AI 지원 플랫폼이다. 파운드리는 데이터를 조직운용에 활용하는 플랫폼으로 사용자가 데이터 활용 요구에 따라 워크플로와 도구를 만드는 기능을 지원한다. 고담과 파운드리가

데이터를 운용, 분석하는 뇌라면 AIP(인공지능플랫폼)은 외부세계와 연결하는 신경망이다. AIP는 멀티AI 플랫폼으로 상업적으로 이용가능한 LLM을 활용하는 인터페이스를 제공한다. 마지막으로 아폴로(Apollo)는 데이터의 지속적인 전달시스템이다. 모든 환경에서 데이터 활용 및 소프트웨어 수집을 위해 상업적 클라우드(AWS, Azure, GCP 등), 사적 클라우드, 온프레미스 데이터 센터는 물론 네트워크 연결의 단절 환경에서 에어갭 분류 및 엣디 디바이스를 제공한다.

팔란티어 플랫폼은 데이터-사이버-디지털 안보가 통합되어 있는 인공지능 플랫폼은 안정성, 보안성, 신뢰성에 기반하여 데이터 안보와 디지털 주권을 침해하지 않는 팔란티어 모델이 'AI의 스위스 모델'로 비유되는 것은 네 가지 이유 때문이다(Kitishian 2025). 첫째, 팔란티어는 LLM 모델을 개발하는 빅테크가 데이터의 운영체계(data OS)를 제공하는 소프트웨어 기업이다. 팔란티어는 다출처 데이터를 통합하여 AI에 활용할 수 있는 임무지향적 디지털 트윈을 구축한다. 둘째, 팔란티어는 데이터를 수집, 소유, 저장, 판매하는 데이터 브로커가 아니다. 사용자의 데이터를 AI 모델에 활용(data-to model)해야하는 AI 빅테크와 달리 보안성, 주권성을 충족하는 폐쇄루프에서 AIP를 제공한다. 셋째, 플랫폼은 락인효과(lock-in effect)에 기반하는 플랫폼이 아니라 개방성, 유연성을 가진 플랫폼의 플랫폼이다. AIP는 멀티AI이 개방성 상호운용성을 지원하며, 아폴로는 멀티 클라우드 기반을 제공함으로서 거대 플렛폼에 종속의 위험을 배제한다. 마지막으로 연결성과 보안성을 강화한 아폴로 플랫폼은 불확실한 전장환경에서 데이터 기반 네트워크를 가능하게 하는 연결성 플랫폼이다.

4. 공세적 사이버 안보 전략과 부대구조

AI-데이터-디지털-플랫폼의 연계와 통합은 사이버공격을 선제적, 공세적으로 방어해야 할 필요성을 증가시킨다. 사이버 공격의 취약성이 증가하는 것은 물론 사이버 공격에 의한 피해가 플랫폼의 플랫폼에 광범위한 피해를 수반할 수 있기 때문이다. 능동적 사이버 방어 개념은 '공격자의 공격 능력을 무력화하고 공격의 이익보다 더 큰 비용을 공격자에게 부과'하는 것이다. 미 국방부는 2011년 사이버공간작전전략에서 '능동적 사이버 방어(Active Cyber Defense)'을 처음 채택했고 트럼프 1기 행정부 시기인 2018년 완성된 사이전략으로 체계화했다. 이후 영국, 중국, 일본 등도 능동적 사이버 방어전략을 사이버전략으로 채택했다(이정환 2024, 162-163).

능동적 사이버 방어의 목표는 '명령이 내려질 경우 사이버 작전을 통해 적의 지휘통제망이나 주요 인프라에 혼란을 유도하고, 이를 국방전략과 계획에 통합'하는 것이다. 능동적 사이버 방어는 '지속적 개입' 능력에 달려있다 (김소정 2025, 12). 지속적 개입은 이미 적대국의 사이버 공간에서 활동하면서 적대 행위를 실시간으로 감시하고 방해함으로써 공격이 발생하기 이전에 억지하는 것이다. 선제적, 능동적 방어를 위해서는 사이버 방어의 경계를 사이버 경계 밖으로 확장하여 동맹국, 적대국으로 확장해야한다. 능동적 사이버 방어작전을 위해 미 사이버 사령부는 133개 이상의 팀으로 구성된 사이버 국가임무부대(Cyber National Mission Force)를 구성하고 헌트포워드(Hunt Forward), 선제적 방어(defense forward) 등 공세적 사이버작전을 수행한다. 미국은 러우전쟁에서 22회 이상의 헌트포워드작전을 시행했다 (김소정 2025, 14).

전후 평화헌법의 구속에 따라 수동적, 반응적 전수방위 전략을 추진해왔던 일본이 2022년 능동적 사이버 방어(ACD) 전략을 법제화한 것은 국방 인공지능 전환에 따른 사이버 안보 전략의 전환적 성격을 대변한다. 일본의 전후 사이버안보 전략은 역사적, 전략적 특성을 가지고 있다(윤대엽 2024a). 일본은 미국에 이어 2002년 사이버안보 전담기구를 설치하고 2004년 아시아국가 최초로 '정보시큐리티 기본계획'을 발표하고 사이버 안보 전략을 공식 추진했다. 아베 내각 직후인 2013년 정보보호에서 사이버 공간의 포괄적 위협에 대응하기 위해 '사이버시큐리티 전략'으로 변경하고 안보개혁의 맥락에서 사이버 안보 전략을 재편했다. 2014년 자위대 사이버방위대를 신설한 일본은 2014년 사이버시큐리티기본법을 제정하고 총리 주도의 사이버안보 거버넌스를 구축했다. 그리고 2022년 능동적 사이버 방어의 법제화와 함께 반격 능력으로 개념화된 적기지 선제공격 능력, 방위비의 GDP 2% 증액과 군사력 건설을 목표로 하는 중기방위계획이 명시되었다. 선제공격을 배제하지 않는 능동적 사이버 전략은 전수방위 원칙으로 제한된 전후 방위전략의 본질적인 변화다. 일본의 사이버 안보 전략은 지상, 육상, 해상, 우주·사이버·전자기를 통합하여 전장화하는 미국의 다영역작전(MDO)를 수용하고 반영한 결과다(심혜인·김지영 2025; 이정환 2024). 그러나, 선제공격을 배제하지 않는 공세적 방위전략은 이미 2000년대 검토되어 왔다 (윤대엽 2023, 54-55). 북한과 중국의 핵·미사일 위협이 고도화되면서 방어적 전략이 막대한 피해를 감수해야하고, 적기지 공격능력 없이는 지속적인 강압과 피해를 감수해야하기 때문이다. 능동적 사이버전략은 위협을 억지하고 피해를 최소화하기 위해서는 선제적으로 공격, 격퇴해야하는 기술패러다임의 변화에 따른 군사전략의 변화를 대변한다(윤대엽 2023, 54).

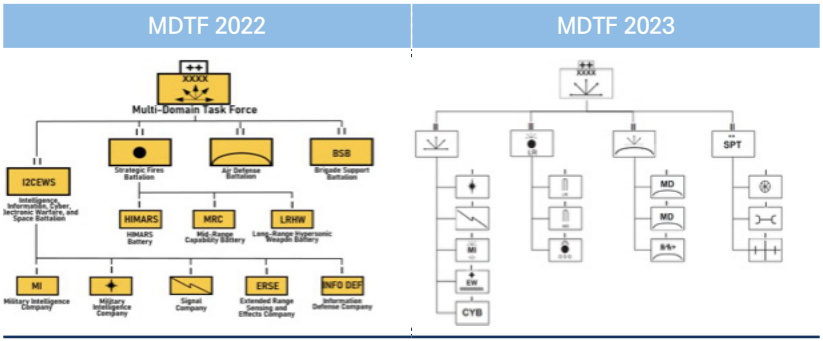
선제적, 공세적 사이버 작전 교리와 함께 주목할 것은 공세적 사이버 능

력이 부대차원에서 통합하고 재편하는 것이다. AI기반 무기체계의 군사적 활용 능력은 데이터를 군사적 목적에서 활용할 수 있는 AI 디지털 아키텍쳐에 달려있다. 공격자가 AI 기반 무기체계를 전구, 전단 수준은 물론 전술부대 차원에서 활용하기 위해서는 부대 차원의 AI 디지털 아키텍쳐가 구축되어야 한다. 방어자에게 부대 차원의 AI 디지털 아키텍쳐는 사이버·전자기 공격에 의해 선제적으로 공격해야하는 취약점이다. 중앙집중화된 사이버사는 전략적 수준에서 사이버 작전을 담당했지만 실시간 전장 데이터를 생성, 전달하여 AI 기반 무기체계를 전장 차원의 활용을 제한했다. 또. 전술차원의 작전부대는 AI 디지털 아키텍쳐는 사이버·전자기 공격에 가장 먼저 노출된다. 따라서, 사이버·전자전 능력을 부대 차원에서 통합, 분산하는 것은 AI-C2 플랫폼에서 데이터 기반 지휘결심을 보장하고 AI 기반 무기체계의 회복력을 확보하는 필수조건이다. 특히, 방어자의 전자기 스펙트럼 거부, 사이버 공격, 데이터 교란과 마기 등 AI 디지털 아키텍쳐의 데이터 흐름과 연결성을 차단하는 전략이 발전하는 가운데, 사이버 효과(cyber effect)는 화력에 기반한 물리적 타격 수단과 대등한 전투효과를 발휘할 수 있다. AI 전장에서 데이터-전자기-사이버 융합 체계는 물리적 타격 수단과 상호보완적으로 AI 기반 디지털 킬체인. 또는 AI 기반 킬웹(AI-enabled Kill Web)을 구성하는 다영역 전투의 핵심 영역이다. 결국 사이버 능력의 부대통합은 AI 기반 분산형 지휘, 지능화된 전투는 물론 분산된 회복력과 생존성을 보장하는 국방 인공지능 전환의 구조적 기반이다.

미국의 다영역TF사단은 사이버 능력을 부대차 원에서 통합하는 선도적인 사례다. 미국이 중국의 비대칭 위협에 대응하여 2018년 처음 창설하여 독일, 하와이, 미국 본토에서 운용하고 있는 다영역TF사단(MDTF)는 선제적, 공세적 사이버 작전을 부대구조에 통합했다. 광범위한 디지털 기기와

네트워크가 데이터 기반의 플랫폼을 구축하는 JADC2 플랫폼은 사이버 공격, 전자전, 데이터공격에 따른 디지털 리스크에 대한 취약성이 증가한다. 전장 차원에서 AI, 데이터(정보, 첩보), 사이버·전자기 능력은 전장에서 교전하는 부대의 작전적 효과성과 직결되어 있다. 아울러 적대국의 디지털 기반체계를 교란, 마비, 파괴하는 것은 생존성을 위한 핵심 과제다.

〈그림 12-3〉 다영역TF사단(MDTF)과 다영역효과대대



자료: 장재규 (2023) 참조

MDTF 사단은 장거리타격능력을 보유한 전략화력대대, 방공대대, 지원대대와 함께 정보, 첩보, 사이버전자기, 우주가 통합한 다영역효과대대(I2CWES)로 편제되어 있다. 다영역효과대대의 경우 정보수집에만 그치지 않고 분석업무를 수행한다. 정보분석은 지상과 공중, 우주, 사이버, 전자기 스펙트럼에서 수집되는 다출처 정보를 인공지능을 활용하여 분석한다. 확장감지효과중대는 감지 및 재밍 기능을 보유한다. 또, 전자기스펙트럼 작전을 기획하고 가시화하며 전자전 공격과 제한적 사이버 공격능력을 제공하는 공중 다기능전자전 플랫폼을 운용한다(장재규 2023, 74-76). 부대 차원에서 사이버, 전자기전 능력을 정보분석, 첩보능력과 통합하는 것은 부대

차원의 사이버 리스크가 네트워크, 플랫폼 전반의 리스크로 확산될 수 있기 때문이다. 또, 사이버, 전자기 능력의 최전선에서 적대국의 취약점을 파악하고 공격할 수 있는 전장의 디지털 안개(digital forg of war)를 해소할 수 있는 수단이기 때문이다.

5. 카운터 AI 전략과 사이버안보

AI 디지털 아키텍쳐를 AI 기반 무기체계의 기반으로 활용해야하는 국방 인공지능 전환은 공격자의 일방적 우위를 보장하는 것이 아니다. 상호통합 관계에 있는 인공지능과 사이버안보를 활용하여 비대칭 공격수단으로 활용할 수 있다. AI는 AI 디지털 아키텍쳐의 취약점을 발견하고 데이터 생성, 전달, 축적, 활용 등 데이터 흐름을 마비, 교란, 파괴하거나 차단하는 지능화된 공격을 통해 적대적 공격의 위험을 증대시킨다. AI 디지털 아키텍쳐에 통합된 고가의 지능화된 군사체계를 저가의 비대칭 수단으로 무력화할 수 있는 비대칭 리스크도 증가한다. AI 디지털 아키텍쳐의 데이터 흐름의 모든 단계는 카운터 AI 공격의 리스크에 노출되어 있다.

첫째, 데이터의 생성 단계의 사이버·전자기 공격이다. 은폐, 엄폐, 위장을 통해 디지털 ISR 자산의 정보수집 및 표적화를 거부하는 물리적 기만은 이미 러우전쟁에서 AI 활용을 제약한다(Biddle 2023). 기만적인 기동, 표적위장 등의 기만전술은 더 많은 전장사물인터넷, 고도화된 디지털 킬체인이 전장의 불확실성을 완전히 해소할 수 없다는 AI 전장의 교훈을 제공한다. 영상, 음성, 전자신호를 합성하여 디지털 ISR 정보를 왜곡하거나, 레이더, EO/IR,

신호정보(SIGINT)에 가짜신호를 주입하는 센서 스푸핑(Sensor Spoofing)은 표적위치를 왜곡하고 거부하는 수단이다. 센서 하드웨어를 물리적, 전자기 수다으로 파괴하거나 사이버공격을 통해 데이터를 왜곡할 수 있다. 요컨대, 생성단계의물리적 기만과 사이버공격은 데이터의 생성을 교란, 거부, 왜곡함으로써 데이터의 생성에 기반하는 AI 기반 디지털 킬체인, 또는 데이터 전쟁을 무력화할 수 있다.

둘째, 데이터 전달 단계는 사이버·전자기 공격에 더 많은 취약점이 노출되어 있다. AI 디지털 아키텍쳐에서 모든 센서, 디지컬 기기, 네트워크에 대한 공격은 데이터의 전송을 지연, 왜곡하거나 실패시킬 수 있다. 전파교란, 재밍, 통신차단은 전장 데이터에 기반하는 AI-C2 체계를 무력화한다. 데이터의 재전송, 변조, 왜곡함으로써 전장 데이터의 타이밍을 지연시켜 의사결정을 방해한다. 셋째, 데이터 분석과 활용 단계의 적대적 사이버 리스크도 증가하고 있다. 알고리즘 학습과정의 무결성 검증이 취약한 경우 공격자는 알고리즘의 취약성을 AI 기반 무기체계의 오작동, 또는 회피의 수단으로 악용할 수 있다. 적대적 기계학습(AML)은 AI가 알고리즘을 통해 물리적, 디지털 인식 및 해석하는 알고리즘을 직접 교란하는 것이다. 학습 데이터의 조작은 인밀한 편향과 오류를 유발할 뿐만 아니라 해킹 없이도 오인식을 유도함으로서 AI 기반 구사체계의 실패를 초래할 수 있다. 사이버공격을 통해 데이터를 오염data poisning)시키거나 데이터셋의 공금망에 침투하여 데이터의 신뢰성을 약화시킬 수도 있다. 오픈소스 데이터를 오염시키거나 가짜정보를 유포하여 정보분석의 혼란을 유도하는 경우 AI 기반 의사결정에 오류를 유도할 수 있다. 만일, AI-C2 체계의 모델 내부에 침투를 허용하여 알고리즘 모델이 노출되는 경우 AI 기반 무기체계의 우위는 상실되고 적대적 반격의 기회를 허용할 수도 있다.

카운터 AI 전략은 AI 기반 무기체계를 무력화하는 직접적 공격을 넘어 AI 디지털 아키텍쳐를 대상으로 데이터의 흐름을 왜곡, 지연, 교란, 마비시키는 포괄적인 전략이라는 점에서 디지털 비대칭 리스크도 심화되고 있다. 러시아의 사이버·전자기 공격대상 중 군대는 8.5%를 점유했을 뿐 민간시설 59%, 공공기관 31.9%를 점유했다(신범식·양정윤 2024). 그 이유는 AI 디지털 아키텍쳐가 광범위한 민간의 상업적 시설에 의존하게 되면서 데이터의 흐름을 대상으로 하는 카운터 AI 전략은 필연적으로 민간에 대한 비대칭 공격을 수반하게 되었기 때문이다. AI 디지털 기반의 민간의존, 민군 디지털 인프라의 높은 상호의존성으로 인해 민간의 디지털 기반을 표적으로 한 사이버, 전자적 교란은 사회적 혼란은 물론 군사작전의 리스크를 수반한다.

〈표 12-1〉 AI 전장의 디지털 비대칭 리스크

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">목표</td></tr>
<tr><td>대군사(Counterforce)</td><td>대가치(Countervalue)</td></tr>
<tr><td rowspan="2">수단</td><td rowspan="2">살상 및
비살상 수단</td><td></td><td rowspan="2">디지털 비대칭 전략</td></tr>
<tr><td>대칭적 군사전략</td></tr>
</table>

AI 디지털 아키텍쳐와 카운터 AI 전략의 디지털 리스크가 증대되면서 민군통합방위체계의 혁신도 중요한 과제가 되었다. 국방 인공지능 전환에 따라 군사적 디지털 취약성이 증가하는 동시에 민간 디지털 인프라의 비대칭 리스크가 증가한다. 데이터, 클라우드, 플랫폼 등 국방 AI 디지털 기반은 민간 디지털 기반과 통합되어 있다. 민간 디지털 기반에 대한 적대적 공격은 사회경제적 혼란을 수반할 뿐만 아니라 국방 디지털 기반의 오류, 마비 등

과 연계되어 있다. 민간 디지털 기반은 후방, 지원영역이 아니라 통합된 전장영역이다. 비대칭적 디지털 리스크에 대응하기 위해서는 기술적, 제도적, 그리고 전략적 민군 사이버 안보 거버넌스의 구축이 강조되어 왔다. 민군 통합 사이버 안보의 핵심과제는 실시간 위협정보의 공유와 신속한 협력을 통해 분산된 네트워크 간 가시성과 신속대응능력을 확보하는 것이다(The White House, 2023). 디지털 공급망, 데이터, 소프트웨어 등의 안전을 위해서는 민간 운영자가 국가안보 수준의 보안 및 복원성의 요건을 충족하도록 책임을 제도화해야한다. 디지털 기반의 신뢰성 협력은 민군에 그치지 않는다. 디지털 기반과 데이터를 공유하는 동맹, 우방과의 역량강화, 신뢰구축, 위협대응 체계를 통해 상호적, 다자적 사이버 안보 역량을 강화하는 것이다. AI 디지털 아키텍쳐의 구축, 보안, 거버넌스에 있어서 민군통합방위체계가 구축되어야 한다.

6. 결론 및 전략과제

군비경쟁은 결승선이 없는 연쇄적인 혁신경쟁이다. 군사혁신에 대한 대응과 대응에 대해 대응하는 군비경쟁 가운데 국방 인공지능 전환(Defense AX)은 전환적 과제가 되었다. AI 기반 무기체계가 전장활용이 확대되고 지능형 지휘통제체계로 통합되면서 표적을 식별하고 타격하는 킬 체인의 속도는 빛의 속도로 단축되었다. 광범위한 디지털 기반의 군사체계가 육해공 및 사이버·우주·전자기 영역을 통합하면서 전장의 공간적 제약도 축소되었다. 지능화된 정보자산, 정보분석, 공격무기는 신속하고 정확하게 상황을

인식하고 지휘통제할 수 있는 군사적 효과성을 비약적으로 발전시키고 있다.

그러나, 데이터-디지털-사이버를 플랫폼으로 통합해야하는 군사체계의 지능화는 광범위한 디지털 리스크의 전환을 수반한다. 다양성, 신속성, 신뢰성, 정확성을 갖춘 군사 목적의 데이터를 수집, 분석하여 활용해야하는 군사체계의 지능화는 광범위한 리스크에 노출되어 있다. 플랫폼과 플랫폼이 연결성, 개방성, 통합성을 원칙으로 운용하기 위해서는 보안성을 최우선으로 플랫폼 운용성(platform operability)이 진전되어야 한다. 전구차원의 연합작전을 위해서는 부대는 물론 동맹국 차원의 정보-무기-지휘-부대가 지능형 지휘통제체계에 통합되어야한다. 플랫폼 운용성은 AI 지원무기체계를 통합적으로 운용하는 작전적 효과성을 증대시키지만 동맹국의 데이터, 디지털, 사이버 등 디지털 플랫폼의 모든 개체, 정보, 네트워크 등 디지털 취약성은 무기, 부대는 물론 지능형 지휘통제체계 전체의 취약점이 될 수 있다. 미국은 동맹국과 공통의 사이버 표준, 위협정보 공유, 클라우드, 데이터 보안협력을 강화하고 있으며, 이는 보안성, 신뢰성을 가진 디지털 지정학적 쟁점과 광범위하게 연계되어 있다.

AI 기반 무기체계의 발전 및 지능형 지휘통제체계의 통합은 사이버 안보 전략에 전환적 과제를 부과한다. 첫째, AX, DX, PX가 상호 연계 및 통합되면서 사이버 안보는 사이버 전쟁 회의론과 달리, 전장우위와 전략적 우위를 결정하는 필수불가결한 요소가 되었다. 둘째, 사이버 안보의 전환은 AX, DX, PX와 통합된 과제가 되었다. 복합적인 디지털 리스에 선제적으로 대응하는 것은 부수적인 문제가 아니라 ACDP·X에 통합된 과제다. 셋째, 따라서 사이버 안보 전략은 플랫폼 운용성이라는 통합적 시각에서 재편되어야 한다. 팔란티어 플랫폼은 데이터 운용체계의 혁신을 통해 사이버 안보,

데이터 주권문제를 해결하면서 멀티 AI, 멀티 클라우드의 개방적 연결성을 제공하는 사례를 제공한다. 부대, 각군은 물론 동맹차원에서 데이터 기반 플랫폼 운용성의 기반 구축에 참고할 수 있다. 다영역효과대대를 부대에 통합한 다영역TF사단은 사이버·전자기, 정보, 첩보, 우주기능을 부대에 통합하여 선제적, 공세적 능력으로 활용해야하는 미래전장의 사이버 전략의 중요한 사례가 될 수 있다.

제12장

사이버-AI-핵 안보 넥서스:
AI-핵 넥서스와 사이버안보의 결합

이중구 | 한국국방연구원 연구위원

제12장

사이버-AI-핵 안보 넥서스: AI-핵 넥서스와 사이버안보의 결합

이중구 | 한국국방연구원 연구위원

1. 들어가며

인공지능(이하 AI)와 사이버 기술의 군사적 응용이 확대된 결과, 핵무기 분야에도 AI가 통합되어가고 있다.[60] AI는 '환각(Hallucination)' 현상 때문에 믿기 어렵다는 지적도 있지만, 핵무기 분야에서 조기경보, 감시정찰(ISR), 표적화, 유도 및 항해, 미사일 방어, 사이버 보안, 대잠수함 작전 등에 AI가 쓰이면 관련 기능이 더욱 완벽해질 수 있을 것으로 기대된다(Chernavskikh, 2024: 4-5). 기존에 사이버 기술이 핵지휘통제 및 군사 인프라에 통합되면서, 사이버-핵 넥서스라는 용어가 보편화되었다면,[61] 이제는 AI와 여러 관련 기술들의 군사적 응용이 확대되면서 핵억제전략과 위기관리 전략에도 영

60) 이 글에서 AI는 소프트웨어와 같은 '정적인 AI(AI at rest)'와 무인체계에 필요한 '동적인 AI(AI in motion)'를 모두 의미한다(이중구, 2025).

61) 전통적인 지휘통제 및 감시정찰 체계를 뜻하는 C4ISR이 사이버 안보를 포함하여 C5ISR로 불리고 있다.

향을 미치고 있다.

하지만, 핵무기 분야의 자율성이란 통제할 수 없는 핵전쟁의 위험성을 보여주는 상징이기도 했다. 과거에 핵무기 분야에서 자율성이 언급되었던 사례는 냉전기 소련의 소위 '데드 핸드(Dead Hand)'였기 때문이다. 데드 핸드는 만약 외국의 군사적 공격으로 소련 지도부가 모두 사망한 경우에 자동적으로 핵보복을 실시하게 하는 로봇형 지휘통제체계를 개발한다는 구상이었다(호프먼, 2015: 217-218). 오늘날의 러시아 역시 핵무인잠수정인 포세이돈을 개발하고 있다. 이에 대해 미국과 영국 등 서방 국가들은 AI 등 첨단기술이 군사적으로 활용되기 위해서는 신뢰성과 안전성이 담보되어야 한다며, 핵무기 분야에서 자율성 기술이 활용되는 데 대해 우려를 표하고 있다.

이러한 불안감에도 불구하고 핵무기 분야에서 AI의 이용이 확대된다는 것은 어떠한 의미인지 생각해보아야 한다. 더욱이 러·우전쟁에서 보듯이 미국, 러시아, 중국 간의 강대국 경쟁이 본격적으로 진행 중인 가운데, 핵강대국들 간의 핵무기 현대화 경쟁도 가속화되고 있어 강대국들의 군사적 AI 활용을 막기 어려울 수 있다. 미국, 중국, 러시아 등 주요 핵보유국들은 자신들의 환경과 전략에 따라 AI-핵 넥서스에 대한 접근법을 만들어갈 것이다. 이러한 접근법은 하나로 수렴할 수도 있지만, 서로 다른 유형으로 분화될 수도 있다.

이에 이 글에서는, 주요 강대국들의 AI-핵 넥서스가 어떻게 형성될지를 생각해보고, 오늘날 우리가 직면한 사이버-AI-핵 넥서스의 문제를 이해해보고자 한다. 새로운 안보 및 군사질서는 한국의 안보역량과 동맹역량에 함의를 지닐 수 있다.

2. AI-핵 넥서스의 부상

통상 사이버-핵 넥서스가 핵무기체계와 인프라에 대한 사이버 위협의 가능성과 그로 인한 위험에 대한 논의였다면, AI-핵 넥서스는 기존의 핵억제체계를 강화시키기 위해 AI를 어떻게 활용하느냐라고 하는 기회에 대한 논의라고 할 수 있다. 물론, 기존 연구들에서 AI와 핵안정성의 관계가 다루어진 바 있다. Chernavskikh와 Palayer(2025)는 비핵무기 분야의 AI 활용이 의사결정자를 더욱 서두르게 하고, AI 기반의 의사결정지원체계도 편향된 결정을 유도할 수 있다고 지적했다. 그러나, 이는 지휘통제에 대한 AI의 적용에 한정된 논의이다. AI가 전반적인 핵억제체계를 어떻게 변화시키는지의 문제를 검토해보아야, AI-핵 넥서스 발전의 성격을 볼 수 있다.

이 글에서 핵억제체계는 감시정찰, 조기경보, 미사일 방어, 지휘통제, 핵타격(1격, 2격)의 그리드로 구성된 전략적 네트워크를 의미한다. 현대전에서 전투체계는 감시정찰, 지휘통제, 타격, 그리고 지속 및 군수 그리드로 이루어지는데, 이 가운데 전투체계의 핵심은 감시정찰, 타격, 지휘통제 그리드이다. 여기에, 핵무기 분야에서 특히 중요한 조기경보, 미사일 방어 분야를 포함하여 핵억제체계를 위와 같이 제시한 것이다. 이러한 5개의 그리드에서 미국, 중국, 러시아가 어떻게 AI 기술을 응용하고 있는지 살펴보면, 각국의 AI-핵 넥서스의 특징을 꼽을 수 있을 것이다. 물론, 핵무기 분야에서 실제로 각 핵보유국들이 어떻게 AI를 활용하고 있는지는 확인하기 어렵기 때문에, 외부 전문가의 견해나 분석을 주로 활용하였다.

1) 미국

미국은 첨단기술을 군사적으로 활용하는 분야에서 선두주자 역할을 지켜왔다. 전투네트워크의 각 부분에 자율체계와 자율성 기술을 도입한다는 제3차 상쇄전략이 발표된지 이미 10년이 지났다. 미국이 AI 기술을 군사적으로 활용한 사례로는, 육·해·공·해병대·우주의 센서를 하나의 네트워크로 연결하고 지휘관이 최적의 판단을 내릴 수 있도록 지원하는 JADC2(Joint All-Domain Command and Control), 넓은 지역에 대한 정찰활동을 인공지능 기술로 효율화한 프로젝트 메이븐(Project Maven), 수천대의 소모성 자율체계를 도입하여 군집작전을 꾀하는 리플리케이터(Replicator) 등이 꼽힌다(Stokes at al, 2025).

미국이 핵억제체계에 AI를 활용하는 양상을 보면, 거부억제에 방점을 두는 양상이 보여진다. 미국은 AI의 활용이 조기경보 능력, 감시정찰 능력, 미사일 방어 능력에 도움이 된다고 보고 있는 것이다. 이러한 능력은 킬체인이나 미사일 방어 등 거부능력과 직결되어 있다.

우선, 감시정찰 분야에서 미국은 AI를 적극적으로 활용하고 있다. 예를 들어, 상대국의 군사력을 실시간으로 시각화할 수 있는 프로젝트 메이븐의 노하우는 핵억제 분야의 감시정찰에 활용될 수도 있다. 러시아나 북한 등의 이동식 핵무기들이 어디에 위치해 있는지를 탐지하는 데 기여할 수 있기 때문이다. 아울러, 전영역과 전군종의 센서와 타격체계를 연결하여 운용하는 JADC2도 NC3와 연결되어갈 수 있다. 전통적으로 핵과 재래식 분야는 별개로 나눠져 각각의 정찰체계를 필요로 하는 것으로 이해되어 왔으나, AI 기술 등을 기반으로 재래식 상황인식 능력이 강화되면서, 이 동태적 상황인식 생태계가 잠수함 등 전략자산의 탐지 및 추적, 타격까지 기여할

수 있게 된 것이다.[62] 그에 따라 핵과 재래식 분야 간의 방화벽이 약화된 것으로 평가되고 있다. 러시아는 미래에 미국이 AI-우주 기반 광학-전자기 감시정찰 체계를 구축할 것이라고 우려하고 있다.

한편, 조기경보 분야에서, 기존의 핵지휘통제통신(NC3)에도 규칙 기반 AI는 활용되어 왔다. 하지만, 1980년대 초반 소련이 구름반사를 핵공격 신호로 오인할 뻔했던 사건도 있었기 때문에, 당시 소련의 페트로프(Stanislav Petrov) 중령이 신중하게 상황을 확인하여 오판을 막았던 것처럼, 조기경보 분야에는 전략상황에 대한 이해를 갖춘 인간 담당자의 이중/복수확인(dual/multiple phenomenology)이 필요하다는 인식이 유지되고 있다(Stokes, 2025: 7).

또한, 미국은 지휘통제 분야에는 AI의 정책 추천 기능을 활용할 수는 있더라도, 결정은 인간의 영역임을 강조한다. 2022년 핵태세 검토보고서는 '휴먼 인 더 루프(Human in the loop)'가 지켜져야 한다고 강조했고, 2024년 11월 앤서니 코튼(Anthony J. Cotton) 미 전략사령관은 AI는 정책결정 능력을 강화시켜주지만, 사람 대신 결정할 수는 없다고 언급한 바 있다.

그럼에도 불구하고, 핵무기 분야의 타격체계에도 AI가 적용되어 군사적 효율성을 높일 수 있다. 트럼프 2기 행정부가 추진 중인 골든돔(Golden Dome) 사업에서도 인공지능은 실시간 데이터 처리, 궤도 분석, 정책결정 지원 등의 역할을 수행할 수 있을 것으로 기대된다.[63]

62) 이러한 상황인식 체계는 고대역폭 네트워크, 양자컴퓨팅, 데이터 융합, AI 도구를 활용해 상대국의 전력 배치와 활동을 더욱 빠르게 알게 해준다(Hersman and Younis, 2021).

63) Vincent Carchidi and Carter Palmer, "Is AI Ready for Golden Dome's Three-Minute War?" Defense and Security Monitor, October 3, 2025.

또한, 상대의 핵억제체계에 대한 비핵타격에도 AI 기술이 접목될 수 있다. 미국 국방부의 리플리케이터 구상은 소모성 자율체계를 필요시 대량으로 운용할 준비를 하는 사업으로, 이 역시 사이버-AI-핵 넥서스와 연결될 수 있다(Stokes at al, 2025). 나아가, 소모성 자율체계보다 더 정교한 재사용 자율체계로 눈을 돌리면, 이들 체계가 핵·재래식 대상 이중임무를 수행할 잠재력은 뚜렷해진다. 전문가들은 이러한 체계가 첨단 스텔스 및 센서 기술을 통해 상대적으로 작은 나라의 이동식 미사일은 추적할 수 있을 것이라고 본다(Lieber and Press, 2017). 러시아는 미래에 미국이 고정밀 스워밍 기술로 러시아 전략군과 관련 시설을 공격할 수 있을 것으로 우려하고 있다. 중국 역시 미국의 군집드론이 다층방어를 뚫고, 핵운반수단, 핵지휘통제통신 인프라 및 조기경보 등 핵억제체계를 위협할 수 있다는 점에 주목한다(Richter, 2025).

다만, 미국은 핵타격수단에 대한 AI의 응용에는 거리를 두고 있다. 미국은 미사일과 같은 회수 불가능한 무기에는 핵무기를 실을 수 있지만, 무인기와 같이 회수가능한 무인체계에는 핵무기가 실려서는 안된다는 입장이다. 2016년 지구권타격사령부 사령관 로빈 랜드(Robin Rand)는 반드시 유인체계로 핵무기를 운용해야 한다고 언급했다(Depp and Sharre, 2024). 그에 따라, 미국은 2차 타격 능력을 개선하는 데 AI가 도움이 된다고 보지만, 타격수단에 무인체계를 도입하는 데에는 거리를 두고 있다.

2) 러시아

러시아는 전통적인 핵강국이지만, 경제적 자원의 제약상 AI 기술을 핵억제체계 전반에 도입하기보다는, 핵안정성을 강조하면서 보복능력을 확실

히 하는 데 AI 기술을 사용하고 있는 것으로 보인다. AI의 군사적 활용 역시 개발 무기체계의 개발에 활용되는 비통합적인 면모를 보여준다.

물론, 러시아도 조기경보 체계에 AI를 도입해 정보처리 속도를 단축시킬 수는 있다. 하지만, 러시아가 조기경보 체계에 AI를 적극적으로 도입하는 데 대한 국내적 우려도 존재한다. 러시아는 이미 '경보 시 발사' 태세를 실현하기 위한 조기경보체계를 가동하고 있는데, 이 체계에 AI를 활용한다면, 조기경보체계가 사이버 공격에 더욱 취약해질 수 있기 때문이다. 이처럼 AI의 도입에 우려하는 전문가들은 사이버공격으로 핵미사일 경보가 잘못 발령되는 가능성을 의식한다. 물론, 이는 AI의 도입에 따른 새로운 우려라기보다는 사이버-핵 넥서스의 측면에 대한 논의일 수도 있다. 과거에도 사이버-핵 넥서스에 주목하는 연구들은 조기경보체제가 사이버 공격을 받아 잘못된 핵미사일 탐지 신호를 보낼 수 있다고 지적해왔다(Stoutland and Pitts-Kiefer 2018).

러시아는 냉전기에도 지휘통제에 자동화 기술을 도입하려고 노력해왔다. 러시아 내에서도 정책결정자가 AI의 조언과 판단에 과도한 의존하는 것은 위험요인으로 꼽힌다. 그러나 오히려 핵보복을 위해서는 지휘통제를 자동화할 수 있다는 시각도 존재해왔다. 그 이유는 냉전기에도 구소련은 미국의 제1격 능력을 우려해왔고, 상대의 선제공격으로 지도부가 모두 사망하는 경우를 걱정해왔기 때문이다. 그 경우에는 핵보복이 사라질 수 있었다. 이에 구소련은 핵보복 능력을 유지하기 위해 자동 핵보복 체계를 구축하고자 했다. 핵보복체계의 완전 자동화와 반자동화 옵션 중에서 구소련은 로봇식 자동화(데드 핸드)는 달성하기 어렵다고 보고, 반자동화된 체계인 '패러미터(Parameter)'를 구축했다. 이 체계는 핵공격으로 최고지도자들이 모두 제거되는 경우, 핵공격 신호에도 일정 시간 동안 지휘부로부터 지시

가 없으면, 권한을 위임받은 하위지휘관이 핵무기를 사용할 수 있게 한다. 특정한 조건이 충족되면 핵발사권한이 활성화된다는 면에서 반자동화 체계이지만, 권한을 위임받은 지휘관이 임무를 실행한다는 점에서 '휴먼 인 더 루프'의 원칙은 지켜지는 체계라도 할 수 있다. 그럼에도 불구하고, 러시아의 접근법은 앞으로 AI를 이용해 더욱 자동화 발사체계를 만들어갈 수도 있음을 보여준다.

이외에도, 러시아는 타격 분야에서 요격과 타격수단에도 AI 기술을 접목하고 있다. 먼저, 요격수단에서, 러시아는 고성능 요격 체계인 S-500를 위한 AI를 개발 중인 것으로 알려져 있다.[64] 위험평가와 손실예측과 같이 AI의 오류가 중대한 영향을 주지 않는 분야에서 AI의 적용이 모색되고 있다.

핵타격수단 분야에서는, AI 기술 도입의 사례로 러시아가 개발해 온 핵무인잠수정 '포세이돈'을 들 수 있다. 이는 푸틴 대통령도 핵무기를 탑재하는 무기라고 공인한 것인데, 포세이돈은 원자로에 의해 추진되는 전장 24m의 거대 무인잠수정이다. 대양을 횡단해 핵폭발로 상대국의 주요 항만에 피해를 줄 수 있다. 이 개념은 스탈린 시대부터 내려온 것인데, 푸틴 시대의 러시아가 그를 마침내 실현한 것이다. 2023년 1월 첫 포세이돈이 생산되었고, 최신 핵잠수함 벨고로드급 잠수함에 장착되었다.[65]

64) Starchak, M., "Russian defense plans kicks off separate AI development push," Defense News, August 16, 2024, https://www.defensenews.com/global/europe/2024/08/16/russian-defense-plan-kicks-off-separate-ai-development-push/ (검색일: 2025년 10월 29일).

65) Guy Faulconbridge, "Russia produces first set of Poseidon super torpedoes - TASS," Reuter, January 17, 2023, https://www.reuters.com/world/europe/russia-produces-first-nuclear-warheads-poseidon-super-torpedo-tass-2023-01-16/ (검색일: 2025년

3) 중국

중국은 2030년대까지 핵무기를 1,000기까지 늘리고, 전쟁승리를 위해 군사력의 정보화, 지능화를 가속한다는 입장이다. 중국은 미국의 첨단기술 활용으로 대군사공격 능력이 강화되고 있다는 데 우려를 표하면서, 궤도폭격 체계 등 미국이 방어하기 어려운 핵능력을 건설하고 있다.[66]

그에 따라, 핵무기 증강 및 현대화 과정에서 중국은 미국처럼 감시정찰과 조기경보 분야에도 AI 기술을 접목하고 있다. 또한, 전통적으로 보복능력을 중시하는 시각에 맞춰, 2격 능력 분야에도 AI를 응용할 가능성이 크다. 결국 중국은 거부억제와 보복억제 양 부문에서 모두 AI 기술을 도입할 가능성이 있다.

먼저, 감시정찰 분야에서, 중국은 미국의 핵무기 탑재 군사력의 이동 동향을 파악하기 위해 우주센서, 해저센서를 개발 중이다. 이러한 능력은 미국 잠수함이나 전폭기의 위치를 파악해 유사시 공격할 수 있게 할 것이다. 특히, 미국이 탄도미사일잠수함(SSBN)의 핵억제력에 크게 의존하고 있는 상황에서, 수중목표물을 탐지, 추적, 공격할 수 있는 무인잠수정은 상대측 잠수함 전력의 생존성과 작전반경을 제약한다.

조기경보 분야에서도 중국은 AI를 도입하고 있다. 중국이 전통적인 최소억제의 핵태세에서 벗어나 '경보시 발사(launching on warning)' 태세를[67] 개

10월 29일).

66) 정영교, "中 극초음속 미사일 두차례 쐈다… FT '7, 8월 각각 한번씩,'" 중앙일보, 2021년 10월 21일자, https://www.joongang.co.kr/article/25017002.

67) 상대의 공격으로 자국의 핵무기고가 파괴되기 전에 핵미사일을 발사하는 태세를 의미한다. 중국의

발하고 있기 때문에, 상대국의 핵무기 발사를 신속히 확인하기 위한 조기경보 능력이 필요하다.[68] 그리고 중국은 조기경보 데이터를 빠르게 처리하는 데 AI를 활용할 수 있다. AI가 방대한 조기경보 데이터를 신속하게 처리해주면, 정책결정자는 조기경보신호에 대처할 시간을 벌 수 있다(Rechter, 2025).

다만, 중국은 지휘통제 분야에서는 인간의 통제 원칙을 강조하고 있다. 중국은 미국의 AI의 군사적 활용 규범을 구축해야 한다는 요구에도 일부 부응하고, 군사영역에서 AI의 책임있는 활용을 위한 REAIM(Responsible Artificial Intelligence in the Military domain Summit) 회의에도 참가하고 있다. 2023년 10월에는 중국 자체의 지구 AI 거버넌스 규범을 발표하기도 했고, 2024년 3월 유엔에서는 '안전하고 확실하고 믿을 수 있는(safe, secure, and trustworthy)' 결의안에도 찬성했다.[69] 2024년 11월 시진핑 주석은 바이든 대통령과 회담에서 핵무기에 대한 인간의 통제를 유지해야 할 필요를 천명했다(White House 2024). 이에 더해, 중국은 러시아와 달리 '데드핸드'를 구축하려 한다는 동향을 보이고 있지도 않다.

그럼에도 불구하고, 중국은 미중경쟁을 의식하여 미국 중심의 군사 AI 규범 정립 노력에는 찬성이나 참여를 유보한다. 나아가, 중국은 러시아와

이전 핵태세는 상대의 핵무기가 자국의 영토에서 폭발한 직후에 핵보복공격을 가한다는 것이었다.

68) 중국의 이러한 NC3 구축 노력은 러시아도 지원하고 있다(Stocks at el, 2025: 10).

69) Edith Lederer, "The UN Adopts a Resolution Backing Efforts to Ensure Artificial Intelligence Is Safe," The Associated Press, March 21, 2024, https://apnews.com/article/united-nations-artificial-intelligence-safety-resolution-vote-8079fe83111cced0f0717fdecefffb4d (검색일: 2025년 10월 29일).

트랙 I 회담을 통해 군사 AI 동향을 함께 평가하고 있다.[70] 이처럼, 중국은 미국과 같이 핵무기에 대한 인간의 통제를 강조하면서도, 군사 AI 규범을 형성하기 위한 미중협력을 본격적으로 추구하고 있지는 않다.

동시에, 중국은 핵타격 분야에도 AI 기술을 응용하고 있다. 중국이 2025년 9월 제2차 세계대전 종전 80주년 기념 열병식에서 선보인 AJX-002 무인잠수정은 길이가 20m에 이르는 초대형 무인잠수정으로서 핵탄두 탑재가 가능하고, 감시 및 정찰도 수행 가능할 것으로 평가된다.[71]

3. AI-핵 넥서스의 유형

이상과 같이 AI와 핵억제체계의 연계를 AI-핵 넥서스의 문제를 살펴보았다. 먼저, 핵억제는 거부억제와 보복억제의 분야로 이루어진다(Bennett 2012, 131-132). 거부억제란 상대방이 공격으로 이익을 보지 못하도록 하기 위한 노력으로서, 대군사공격(킬체인), 적극적 방어(미사일방어), 수동적 방어(핵방호), 피해관리(구호, 제염 등)를 아우른다. 반면 보복억제란 상대방이 공

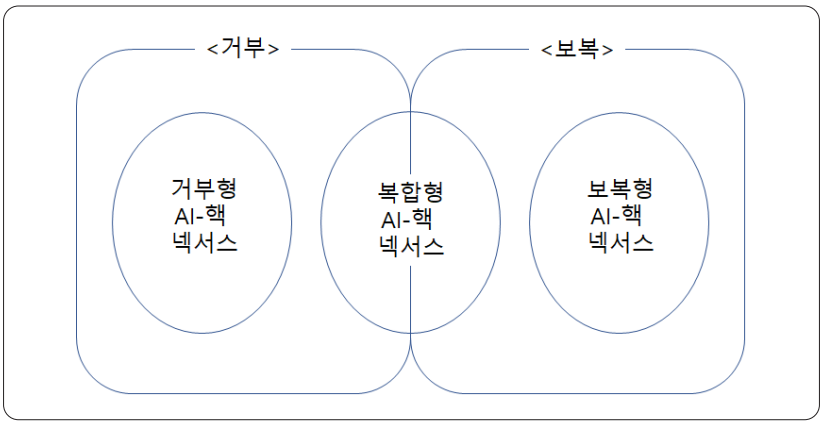
70) Laura Zhou, "Russia and China Compare Notes on 'Military Use of Artificial Intelligence,'" South China Morning Post, February 4, 2024, https://www.scmp.com/news/china/diplomacy/article/3250893/russia-and-china-compare-notes-military-use-artificial-intelligence.

71) Tessa Wong, "What new weapons on show at huge parade say about China's military strength," BBC, September 3, 2025, https://www.bbc.com/news/articles/cjr1reyr059o (검색일: 2025년 10월 28일).

격에 따라 더 큰 손해를 받도록 하기 위해, 보복공격을 가하는 분야이다.

그렇게 볼 때, AI-핵 넥서스는 거부억제에 AI 활용의 방점을 두는 유형, 보복억제에 AI 활용의 방점을 두는 유형, 거부억제와 보복억제 모두에 대한 AI의 활용을 추구하는 유형으로 구분해볼 수 있을 것이다.[72] 이를 각각 거부 위주의 넥서스, 보복 위주의 넥서스, 거부와 보복 균형 넥서스라고 부를 수 있을 것이다(〈그림 13-1〉 참조)

〈그림 13-1〉 사이버-AI-핵 넥서스



이 세 가지 유형에 따르면, 미국은 거부 위주의 넥서스, 러시아는 보복 위주의 넥서스, 중국은 거부와 보복 위주의 넥서스를 각각 예시해준다고 할 수 있다(〈표-1〉). 미국은 첨단 AI 기술을 통해 감시정찰, 조기경보, 표적화로 이어지는 상황인식 체계를 구축하고 있는데, 이것이 전략임무에도 활용될

72) 이러한 유형화에 대해서는 추가적인 연구작업이 필요할 수 있다.

수 있기 때문에 핵억제체계의 앞단인 거부억제 능력을 강화시키고 있는 것이다. AI는 신속한 정보처리와 행동을 가능하게 해 발사준비 중인 핵무기를 파괴하는 킬체인 능력과 발사된 미사일을 요격하는 미사일방어 능력을 더욱 강화시킬 것으로 예측된다. 러시아는 보복 위주의 넥서스를 추구할 가능성을 예시해주는데, 핵공격을 받더라도 핵보복 능력을 유지하기 위해 지휘통제를 반자동화한 역사가 있고, 핵무기체계 자체에도 무인로봇 기술을 도입하고 있기 때문이다. 한편, 중국은 거부와 보복 양 분야에 AI 기술을 도입할 수 있다. 미국의 전략자산을 탐지할 수 있는 해저센서, 우주센서의 도입을 강조하고 있고, 러시아와 유사하게 무인잠수정을 개발해 정찰만이 아니라 핵무기도 탑재하려 한다.

〈표 13-1〉 주요 핵보유국의 핵억제체계와 AI 활용 징후와 AI-핵 넥서스 유형

구분	감시·정찰	핵지휘통제통신		타격			비고 (AI-핵 넥서스 유형)
		조기경보	지휘통제	요격	비핵타격	핵타격	
미국	AI-우주-전자기	AI 유용 (이중확인)	휴먼 인 더 루프	AI 유용	자율무기 군집작전		거부형
러시아	-	-	휴먼 인 더 루프/파라미터 (보복)	AI 접목	-	AI 접목	보복형
중국	무인센서	AI 지원	휴먼 인 더 루프	-	-	체계개발	복합형

이 국가들이 AI-핵 넥서스에서 이러한 발산(divergence)를 보이는 이유는 기술 및 경제력과 핵전략에서 찾을 수 있을 것이다. 미국은 AI의 군사적 이용을 선도하고 있고, AI를 전투체계 전반에 적용하고 있다. 동시에 핵잠수

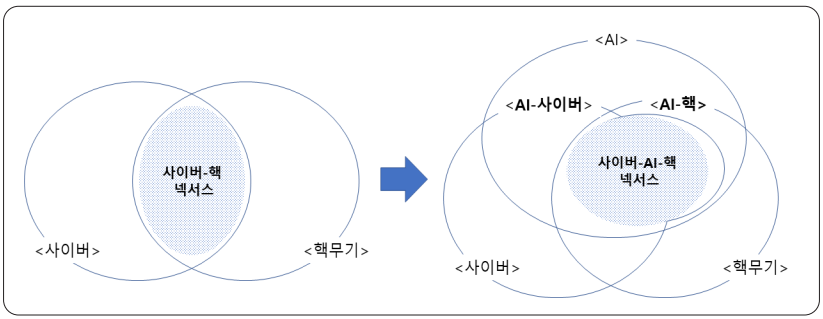
함을 통한 보복억제력이 안전한 상태에 있기 때문에, AI의 효과는 신속한 탐지와 결정, 행동이 필요한 거부억제 분야에 집중적으로 나타나는 것으로 보인다. 한편, 러시아는 미국과 같은 수준으로 방대한 핵무기고를 가지고 있지만, 미사일능력에 대부분 의존하고 있기 때문에 미국의 감시정찰 및 타격 능력이 발전하면 자신의 핵보복 능력이 위협받는다고 본다. 이에 핵보복능력을 첨단기술을 통해 더욱 보강하는 방향으로 나가는 것이다. 미국과 똑같이 전투체계 전반에 AI 기술을 도입하기에는 기술력과 경제력도 충분하지 않다. 끝으로, 중국은 보복타격 위주의 핵전략을 오랫동안 추구해 온 국가로서, 아직 핵무기 수량이 부족하기 때문에 그에 대한 외부의 공격을 거부하는 데 노력하고 있다. 또한 보복능력의 생존성을 높이기 위해 향후 자율무기체계 기술을 핵무기에 접목할 수 있다. 중국은 러시아와 달리 이러한 노력을 전개하는 데 충분한 기술 및 경제력도 보유하고 있다.

4. AI-핵 넥서스와 사이버 안보

AI-핵 넥서스의 등장은 기존의 사이버-핵 넥서스에 어떠한 영향을 주었는가에 대해서 생각해볼 수 있다. 즉, 사이버-핵 넥서스가 핵억제 및 관리체계의 사이버 안보 문제를 지칭하던 것이라고 할 때, AI-핵 넥서스의 부상은 기존 핵분야의 사이버 안보 문제의 범위를 다시 확대시켰을 수 있다. 앞서 사이버-핵 넥서스는 주로 지휘통제, 조기경보, 무기체계, 보관시설 등 인프라 분야에서 사이버위협으로 인해 핵무기 관리나 안정성이 침해되는 경우를 일컬었다. 반면, AI-핵 넥서스에서 핵무기 보관시설의 보안문제는 새롭

게 다루어지지 않지만, 감시정찰 및 미사일방어 분야의 AI활용은 주목되는 추가적 영역이다. 이러한 AI-핵 넥서스의 추가 영역 역시 사이버공격에 취약하다고 할 때, AI-핵 넥서스의 등장은 사이버공격에 취약한 핵억제체계의 영역이 더욱 확대되었음을 의미할 수 있다. 이러한 함의는 AI의 도입으로 군의 사이버공격에 대한 취약성이 높아졌다는 다른 전문가들의 지적과 맥을 같이 한다(Johnson 2019: 446). 자율무기체계의 사용이 확대됨에 따라, 사이버공격은 전통적인 해킹만이 아니라 스푸핑, 재밍, 데이터포이즈닝(data-poisoning)의 확대된 형태로 나타나고 있다. 그렇다면, 핵억제에 관련된 감시정찰과 미사일방어 분야의 자율무기체계에 대한 스푸핑, 데이터포이즈닝의 위협도 존재하게 된다.

〈그림 13-2〉 사이버-AI-핵 넥서스



여기에 더해, (AI-핵 넥서스 외에) AI-사이버 넥서스도 존재한다. 이 넥서스에서는, AI가 사이버 공격 및 방어 능력 모두를 강화시킨다. 먼저, 사이버공격의 측면에서, APT(Automated Persistent Threat) 공격작전팀들은 인력을 아끼고 기술적 수준을 높이기 위해 머신러닝과 AI를 활용할 수 있다. 기술이 낮고 자본이 적은 사이버공격팀들도 AI 기반 사이버 수단으로 상대의

사이버방어를 돌파하고 APT 도구를 사용할 수 있다(Johnson 2019: 448). 다음으로, AI는 사이버 방어도 강화시켜줄 수 있다. AI 방어 도구들이 소프트웨어의 취약점을 식별하는 데 쓰일 수 있고, 머신러닝 도구들은 정상 네트워크 활동과 다른 이상징후를 포착하는 데 활용된다(Johnson 2019: 446).

AI-핵 넥서스와 AI-사이버 넥서스가 만날 때의 주요 이슈로 생각해볼 문제로는 우발적 핵확전가능성이 있다. 예를 들어, AI 기반 사이버공격 무기가 상대국 센서나 자동 표적인식체계를 공격하는 경우에, 민간인 활동을 군사활동으로 오인하게 될 수 있다. 문제는 AI의 정보처리과정을 담당자가 검토하기 어려워, 잘못된 정보에 기반한 민간시설 공격까지 이루어질 수 있다는 점이다. 그 결과로, 공격을 받는 나라가 다시 맞보복을 한다면, 당사국들 간에는 점진적인 확전이 아니라, 갑자기 대규모 충돌이 일어나는 위기가 올 수 있다(Johnson 2019: 448-449).

이 대목에서, 주요 강대국들이 AI 기술과 핵억제체계를 결합하는 데 있어 서로 다른 모습을 보여주고 있다는 점을 고려해서, 미국, 러시아, 중국의 AI-핵 넥서스 유형에 따라 더욱 구체적인 사이버 취약성의 영향을 그려볼 수 있을 것이다. 우선, 미국과 같은 거부 위주의 AI-핵 넥서스의 경우에는 감시정찰이나 조기경보 분야에 대한 해킹, 스푸핑이나 대군사공격에 쓰일 수 있는 자율무기체계에 대한 스푸핑, 재밍, 데이터포이즈닝이 주로 예상된다. 이러한 공격은 주로 군사활동을 숨기는 데 목적을 둘 것이므로, 미국의 대응 속도를 지연시킬 것이다. 또한, 잘못된 정보로 인한 오폭을 야기할 수도 있다. 그러한 오폭은 확전 사다리의 몇 단계를 건너뛰는 형태로 분쟁을 확대시킬 수 있을 것이다.

그리고 러시아와 같은 보복 위주의 AI-핵 넥서스에서는 지휘통제나 무인핵무기체계에 대한 해킹이 이루어질 수 있다. 최악의 경우, 이는 도발되

지 않은 핵보복공격 개시라는 재앙적 결과로 이어질 수 있다. 또는, 핵운반용 무인체계가 탈취되는 경우도 상상해볼 수 있다.

중국의 경우, 거부와 보복 모두에 AI 기술을 도입한다면, 미국과 러시아의 경우에 발생할 수 있는 두 가지 현상이 모두 나타날 수 있다. 즉, 재밍, 스푸핑, 데이터 공격으로 AI 기반 감시정찰 및 조기경보체계가 정책결정자에게 잘못된 정보와 정책권고를 제공할 수도 있고, 사이버 공격으로 핵분야의 무인체계가 해킹될 수도 있다는 것이다. 이상의 논의는 사이버-AI-핵 넥서스 상의 위험에는 우발적인 확전 가능성뿐만 아니라, 대응지연에 따른 억제실패, 무인체계 탈취에 따른 핵확산 가능성도 있다는 점을 알려준다.

5. 나아가며

이 글에서는 미국, 중국, 러시아 별로 핵억제체계를 이루는 감시정찰, 조기경보, 지휘통제, 미사일 방어 및 타격 분야에 AI 기술을 어떻게 접목하고 있는지 살펴보았다. 그에 따르면, 미국은 C4ISR에 AI를 적극 활용하는 모습을 보여주었으며, 러시아는 보복체계를 자동화할 가능성과 핵탑재 무인체계를 개발하는 동향을 드러냈고, 중국은 보복체계에 무게를 두면서 거부전력을 증강하고 있는 상황에서 AI를 거부와 억제 모두에 복합적으로 활용해갈 것으로 보인다. 이글에서는 이러한 주요 핵보유국들의 AI-핵 넥서스를 거부형 넥서스(미국), 보복형 넥서스(러시아), 거부와 보복의 복합형 넥서스(중국)로 각각 분류하였다.

이어서, 이 글은 AI-핵 넥서스와 사이버의 관계를 살핌으로써, 사이

버-AI-핵 넥서스의 영향을 함께 제시했다. 각국은 AI를 활용하여 AI-핵 넥서스를 구축함으로써 핵억제체계는 강화했지만, AI의 결합으로 사이버에 대한 핵억제체계의 취약성은 증대되었다. AI 기술의 활용을 위해, 전투장비와 타격체계가 사물인터넷으로 연결되게 되었기 때문에, 사이버공격의 대상이 감시정찰 및 미사일 방어 체계로까지 확대될 수 있게 된 것이다.

그리고 AI-핵 넥서스의 거부형, 보복형, 복합형 유형에 따라 사이버-AI-핵 넥서스에서 발생할 수 있는 문제가 제시되었다. 먼저, 거부형의 AI-핵 넥서스에서는 사이버공격으로 군사적 위협에 적시에 대응하지 못하는 억제실패, 민간표적을 오폭하여 발생할 수 있는 확전가능성의 문제가 존재한다. 핵긴장고조를 관리하기 위해서는 각국은 비례적 대응의 원칙에 따라 확전을 통제하고자 하지만, 민간표적을 군사표적으로 오인하여 타격하게 된다면 그러한 확전통제에서 실패할 수밖에 없다. 상대국은 선제공격을 받았다고 생각해서, 그에 상응한 대응을 가할 수 있다. 결과적으로 확전은 몇 단계를 건너뛰는 형태로 급격히 확전될 수 있다. 한편, 보복형의 넥서스에서는 지휘통제가 침해되어 확전가능성이 발생하거나, 자동화한 핵보복수단이 사이버공격이나 스푸핑으로 탈취되거나 통제불능 상태에 빠질 우려가 존재한다. 그리고 복합형 넥서스에서는 거부 위주 넥서스의 문제와 보복 위주 넥서스의 문제가 모두 발생할 수 있다.

이러한 사이버-AI-핵 넥서스 논의로부터 군사영역의 공격과 방어 균형, 핵억제관계에 대한 영향, 북핵문제에 대한 함의도 도출할 수 있다. 우선, AI-핵 넥서스가 공격과 방어의 균형에서 어느 쪽을 유리하게 하느냐의 문제이다. 미국, 중국, 러시아 등 주요 강대국들은 핵억제체계의 거부와 보복 측면 중 자국의 역량과 핵전략에 따라, 상이하게 도입하고 있다. 그러한 양상을 보면, 주요 핵강대국들은 서로 쫓고 쫓기는 싸움을 벌이고 있는 것으

로 보인다. 미국이 거부 분야에 AI를 도입하면, 러시아와 같은 나라들은 핵보복능력의 신뢰성을 높이기 위해 보복 분야에 AI를 도입하려는 모습이다. 물론, 미국이 AI 기반 군사혁신의 선두주자이므로, 거부형 혁신이 앞서 보이기도 한다. AI 도입이 2격능력(보복능력)을 약화시킨다는 논의도 전개되고 있다. 그러나 중국과 러시아도 대응전략을 세우고 있고, 보복의 축에 AI를 도입할 수 있다. 그에 따라, 거부와 보복의 영역에서, 각국이 서로 응수하는 AI-핵 넥서스 군비경쟁이 계속될 전망이다.

다음으로, 사이버-AI-핵 넥서스가 핵억제관계를 어떻게 바꾸느냐에 대해서도 생각해볼 수 있다. 이글은, AI-핵 넥서스를 거부형, 보복형, 복합형 넥서스로 나누어보았을 때, 사이버-AI-핵 넥서스의 등장으로 기존의 핵억제관계에 나타날 영향은 더욱 다양해질 수 있다는 점을 보였다. 통상 사이버-AI-핵 넥서스는 외부의 사이버 공격으로 상황을 잘못 탐지·해석할 수 있고, 그에 따라 우발적인 확전이 이루어지는 핵안정성 저하의 상황에 직면할 수 있다고 논의되었다. 그런데, 그뿐만이 아니라, 거부형 AI-핵 넥서스에 대해서는, 사이버 혹은 AI-사이버 공격이 해당국이 공격에 대응할 적절한 시점을 놓치게 하는 억제실패를 야기할 수 있다(억제실패의 가능성). 나아가, 보복 위주의 AI-핵 넥서스에서 사이버-인지 공격을 받을 경우, 자국이 공격을 받은 것으로 오인하여 핵보복 실행의 문턱까지 갈 위험까지도 존재한다(핵안정성의 추가적 약화). 그리고, 핵무기가 무인체계에 실릴 경우에도, 사이버공격으로 무기체계가 탈취당할 수도 있다(핵확산의 위험).

끝으로, 이글에서 살펴본 사이버-AI-핵 넥서스 논의가 북핵문제에 주는 함의는, 북한이 AI-핵 넥서스를 구축한다면, 보복형 넥서스를 구축할 가능성이 있다는 것이다. 북한은 한정된 자원과 미국에 대한 대응의 필요에서 러시아처럼 보복 분야에 부분적으로라도 AI를 활용하려고 생각할 가능성

이 크기 때문이다. 북한은 이미 핵무력법령에서 지도부가 공격을 받을 경우 자동보복을 실행하겠다며 러시아의 '패러미터'와 유사한 아이디어를 제시한 바 있고, 핵무인잠수정인 '해일'도 개발 중이다. 이러한 점에서, 북한의 보복형 사이버-AI-핵 넥서스에서 나타날 수 있는 핵무기 오인발사와 통제실패의 가능성에 대해서도 대비가 필요하다.

제13장

사이버-우주 안보 넥서스

이수연 | 서울대학교 외교학 전공 박사과정

제13장

사이버-우주 안보 넥서스

이수연 | 서울대학교 외교학 전공 박사과정

1. 머리말

인류 첫 인공위성이 발사된 시점부터 우주는 사실상 제4의 전장으로서 안보에서 중요한 영역이 되었다. 사이버 공간은 2004년 〈국가 군사 전략(National Military Strategy)〉과 2006년 미국의 〈사이버 공간 작전을 위한 국가 군사 전략(The National Military Strategy for Cyberspace Operations)〉에서 육, 해, 공, 우주 등과 마찬가지로 독립적인 군사 작전 영역으로서 전략적 중요성이 있음을 강조함에 따라 제5의 전장으로 인식되기 시작했다. 해당 보고서에 따르면, 사이버 공간의 특성은 "육, 해, 공, 우주 영역 전반에 걸친 작전을 가능하게 해준다(enables operations across the domains of air, land, maritime, and space)"(Department of Defense, 2006, p. 3). 미국의 〈우주군을 위한 교리(Doctrine for Space Forces)〉에서도 우주 시스템이 데이터 전송 속도에 영향을 미치는 상당한 양의 글로벌 대역폭(bandwidth)을 제공한다는 이유에서 우주와 사이버 영역의 운영이 공생 관계에 있음을 강조하고 있다(Klein, 2024). 이렇듯 사이버 공간과 우주 영역은 긴밀하게 연결된 공간으로, 일상

생활뿐 아니라 안보의 관점에서도 두 영역은 별개로 다루어지기보다는 사이버-우주 넥서스의 관점에서 접근할 필요가 있다.

러시아-우크라이나 전쟁 발발 초기 러시아에 의해 사이버 공격을 받아 통신이 마비되었던 우크라이나가 위기를 극복하고 반격에 나설 수 있었던 결정적인 이유는 미국의 스페이스X사가 제공한 스타링크(Starlink) 서비스 덕분이었다. 우크라이나의 통신을 담당하던 비아샛(Viasat) 위성이 러시아에 의해 공격받았던 것도, 스페이스X의 위성을 통해 우크라이나의 통신을 복구한 것도, 사이버와 우주가 어떻게 연계되어 있는지를 잘 보여준다. 이 사례는 우주에 쏘아 올린 인공위성과 같은 전략적 자산이 사이버 공격의 대상이 될 수 있으며, 공격이 실현되었을 때 다시 사이버 공간에 영향을 미치면서 유발되는 피해가 어느 정도인지 확인할 수 있게 해주었다. 즉, 지상에서의 전투에 앞서 우주와 사이버 공간과 같이 영토적 개념이 불명확한 영역에서 분쟁이 시작될 수 있으며, 사이버와 우주 영역의 통합된 작전을 통해 실질적인 군사적 효과를 달성할 수 있다는 사실을 확인해 준 것이다(Klein, 2024). 동시에 민간 기업의 서비스 제공 여부가 전쟁 수행 능력에 직접적인 영향을 미칠 수 있음을 보임으로써, 국가안보와 민간 기업의 이해관계가 충돌할 때 발생할 잠재적 위험성도 드러나게 되었다.

또한 사이버 공간의 데이터 이동이 우주에 있는 인공위성과 같은 통신 인프라와 밀접한 관련이 있다는 점에서 데이터 안보가 사이버-우주 넥서스를 관통하는 중요한 이슈 중 하나임을 명확히 보여주었다(이수연, 2023). 데이터는 안보의 관점에서 굉장히 중요한 자원이자 자산으로, 데이터를 원료로 하여 개발되고 발전하는 인공지능 기술이 첨단무기와 결합하고 사이버, 우주 같은 전장과 결합하는 데 있어서도 중요한 연결고리를 제공한다. 따라서 이 글에서는 사이버-우주 안보 넥서스를 데이터 안보의 관점에서

살펴보고자 하며, 이를 정보의 흐름, 즉 데이터의 흐름과 가장 강력하게 연결된 중요한 우주 자산인 저궤도 군집위성을 중심으로 확인할 것이다. 뉴스페이스 시대가 열리며 저궤도 군집위성을 생산, 발사, 운용하는 주체가 국가가 아닌 민간 기업이 된 점 역시 중요하게 살펴보아야 할 지점이다. 정보, 데이터는 안보의 핵심이므로 사이버-우주 안보 넥서스는 통신 주권, 데이터 주권과도 연결된다. 정리하자면, 본문에서는 왜 데이터 안보가 사이버-우주 안보 넥서스의 핵심이고, 왜 통신 인프라에 초점을 맞춰야 하는지, 사이버-우주 안보 넥서스에 대한 위협이 무엇인지 그리고 인공지능 기술이 도입되게 되면서 직면하게 되는 도전과제는 무엇인지 등에 대해 구체적으로 다뤄볼 것이다.

2. 사이버-우주 안보 넥서스의 개념과 현황

1) 사이버-우주 안보 넥서스의 개념과 데이터 안보

사이버-우주 안보 넥서스에 대한 학술적 정의는 명확하게 존재하지 않는다. 논의의 편의를 위해 사이버-우주 안보 넥서스에 대해서 다음과 같이 개념을 정리하고자 한다. 사이버-우주 안보 넥서스의 개념을 정의하기 위해서는 정의를 구성하는 요소가 무엇인지부터 파악해야 한다. 여기서는 공간, 기능, 전략 등 세 가지 요소를 중심으로 정의한다.

먼저 공간적 요소를 통한 접근이다. 사이버 영역은 정보통신기술에 의해 형성되는 인위적인 공간이다. 반면, 우주 영역은 자연적으로 존재하지만,

육해공과 같이 물리적으로 쉽게 접근할 수 있는 공간은 아니며, 인간의 물리적 한계를 넘어 경험하는 공간이다. 두 영역의 공통점은 근대적 영토 주권 개념이 통용되기 어렵다는 데 있다. 공간의 경계를 나누기 어려우며 특정 주체에 의해 소유되지 않고 공간 그 자체 역시 제한적이지 않고 확장될 수 있다(이수연·윤정현, 2024). 이러한 유사성을 가진 사이버 영역과 우주 영역은 두 개의 공간으로 구분되어 있긴 하지만, 완전히 독립된 영역은 아니다. 사이버 공간의 확장을 위해서는 우주 기반의 통신 인프라가 필요하고, 우주 인프라의 정상적인 운용을 위해서는 사이버 공간을 통하는 것이 필수적이다. 즉, 공간적으로 사이버 영역과 우주 영역은 독립적으로 분리된 공간이 아닌 양방향의 상호작용이 발생하는 복합 공간인 것이다.

다음은 기능적 요소를 통한 접근이다. 사이버 영역의 기능과 우주 영역의 기능은 상호 의존성을 가진다. 다시 말해, 한 영역에 대한 공격이 그 영역 안에서만 영향을 미치고 끝나는 것이 아니라, 다른 영역으로까지 전이됨에 따라 기능의 수행에 있어 직접적인 문제가 발생한다. 러시아-우크라이나 전쟁에서 우크라이나가 사용하는 통신 인프라인 비아샛 위성에 러시아가 가한 사이버 공격으로 인해 우크라이나의 통신이 장애를 일으켜 사이버 영역을 통한 작전 활동을 원활하게 할 수 없게 되었다. 이는 사이버와 우주의 양 영역 간 기능적 연계를 잘 보여주는 사례라고 할 수 있다.

마지막으로 전략적 요소를 통한 접근이다. 사이버, 우주 영역에 대한 전략을 수립하는 데 있어서 통합이 일어나고 있다. 각 영역이 연계됨으로 인해 발생하는 위협 요소를 파악하고 이를 동시에 해결하기 위한 전략을 수립하는 것이다. 예를 들어, 미군이 제시한 다영역 작전(Multi-Domain Operation, MDO) 역시 사이버 영역과 우주 영역에서의 전략적 연계를 상정하고 있다.

따라서 공간, 기능, 전략이라는 세 가지 요소를 통해 사이버-우주 안보 넥서스는, '국가안보에 필수적인 통신, 감시, 정찰 등을 위한 우주 자산을 보호하기 위해 사이버 영역의 안전이 보장되어야 하고, 동시에 사이버 영역 내 활동의 안정성을 확보하기 위해 우주 기반 인프라를 보호해야 하는 상황에서 두 영역의 전략적 연계가 이루어질 수밖에 없는 안보 구조 또는 환경'으로 정의할 수 있다. 이러한 사이버-우주 안보 넥서스의 정의에 따르면, 사이버 안보가 없는 우주 활동은 존재할 수 없다(Department of Defense, 2006, p. 3; Klein, 2024; The White House, 2020). 반대로 우주 인프라에 대한 안전보장 없이 안정적인 사이버 활동도 존재할 수 없다. 즉, 어느 한 영역이 일방적으로 영향을 미치는 것이 아닌, 두 영역이 상호 의존성을 가지고 서로 영향을 주고받는다. 한 영역에 대한 위협이나 취약성이 그 영역 내에서 그치는 것이 아니고, 다른 영역으로 전이되고, 그것이 되돌아와서 부정적인 피드백을 주게 되는 복합적인 안보 환경을 설명하는 개념이라고 할 수 있다.

사이버-우주 안보 넥서스에 대한 모든 위협과 공격은 데이터 유출, 조작, 삭제 등 데이터 안보의 중요한 세 가지 요소인 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 침해하는 것으로 귀결된다고 할 수 있다. 따라서 사이버-우주 안보 넥서스의 궁극적인 목표는 사이버 영역이나 우주 영역의 시스템 또는 물리적 자산 그 자체가 아니라, 데이터 안보에 있다. 5G에서 6G로 차세대 통신 기술이 이행하는 과정에서 확인할 수 있다시피, 이제는 지상에서 통신의 트래픽을 모두 감당할 수 없는 초연결 사회에 진입했기 때문에 우주에 대한 통신 인프라의 의존은 더욱 심화되고 있으며, 사이버-우주 안보 넥서스의 핵심인 데이터 안보를 위해서는 우주 기반 통신 인프라에 초점을 맞추지 않을 수 없다(이수연, 2023).

특히, 사물인터넷, 인공지능 등이 중심이 되는 초연결, 초지능 사회에서 통신 기술에 요구되는 것은, '초고속·초저지연'으로 표현할 수 있는 속도와 회복탄력성이다. 기존 정지궤도에 있는 통신 위성들은 하나의 위성이 넓은 영역을 커버할 수 있다는 점에서 지금도 중요한 통신 인프라이긴 하지만, 지상과의 거리가 멀기 때문에 속도에서의 요구 조건을 충족시키는 데에 한계가 있다. '초고속'뿐만 아니라 '초저지연'이 중요한 현재의 상황에서, 정지궤도의 통신 인프라보다 주목을 받을 수밖에 없는 것은, 저궤도에 형성된 통신 인프라인 저궤도 군집위성이다. 저궤도 군집위성은 지상과의 거리가 가까우므로 특히 '초저지연'을 실현하기에 적합한 기술이다. 물론 지구와의 가까운 거리로 인해 하나의 위성이 커버할 수 있는 영역이 감소한다는 한계가 있긴 하지만, 이는 다수의 위성으로 군집을 이루는 것을 통해 극복할 수 있다. 또한 위성 군집의 형성은 분산된 다수의 위성에 의해 통신이 이루어진다는 점에서 공격에 대한 회복탄력성을 확보할 수 있다. 사이버-우주 안보 넥서스의 핵심은 데이터 안보에 있다는 점과 데이터 안보를 위해 필수적으로 살펴봐야 하는 것이 바로 통신 인프라인 저궤도 군집위성임을 확인하였으므로, 다음 절에서는 저궤도 군집위성을 중심으로 주요 국가들의 사이버-우주 안보 넥서스 현황에 대해 알아보고자 한다.

2) 사이버-우주 안보 넥서스의 현황: 저궤도 군집위성을 중심으로

사이버-우주 안보 넥서스에서 저궤도 군집위성이 지니는 전략적 중요성에 대해서는 러시아-우크라이나 전쟁을 통해 전 세계 국가들이 확인하였다. 사이버-우주 안보 넥서스를 관통하는 데이터 안보의 관점에서 저궤도 군집위성에 초점을 맞춰 가장 잘 접근하고 있는 국가는 미국인 것으로 보

인다. 미 육군은 2010년대 중반부터 다영역 작전 개념을 선제적으로 제시하고 발전시켜 오고 있다. 이는 미국이 사이버 영역과 우주 영역 간 전략적 연계의 중요성에 대하여 제대로 인지하고 대비해 왔음을 확인시켜 준다(설인효·신민석, 2024, p. 9). 또한 2020년 9월 4일, 트럼프 1기 행정부는 〈우주 정책 지침 5호(Space Policy Directive 5, SPD-5)〉를 발표하였다. 이 지침에서는 글로벌 통신, 위치·항법·시간, 과학적 관측, 국가안보에 중요한 여러 응용 프로그램 등의 기능을 가능하게 해주는 우주 시스템(지상 시스템, 센서 네트워크, 우주 차량을 모두 포함)에 대한 사이버 보안 원칙들을 다루고 있다(The White House, 2020).

SPD-5에서 제시하고 있는 원칙은 구체적으로 다음의 다섯 가지가 있다. 첫째, 우주 시스템과 소프트웨어를 포함한 지원 인프라는 위험 기반 사이버 보안에 최적화된 공학 기술을 사용하여 개발되고 운영되어야 한다(The White House, 2020). 이는 설계, 개발, 생산, 시험, 발사, 운영, 폐기 등 우주 시스템 수명의 전 주기에 걸쳐 지속적으로 사이버 보안 위험을 평가하고 관리해야 한다는 것과 이를 통해 회복탄력성을 확보해야 한다는 것을 의미한다. 둘째, 우주 시스템의 소유자와 운영자는 기능을 통합한 사이버 보안 계획을 개발하고 실행해야 한다. 셋째, 규칙, 규정, 지침에 더하여 사이버 보안 모범 사례와 행위 규범에 대한 고려 및 채택을 통해 이러한 원칙을 실행하는 것은, 우주 시스템에 대한 사이버 보안 측면에서도 강화해야 한다. 넷째, 우주 시스템의 소유자와 운영자는 모범 사례 개발을 촉진하는 데 협력해야 하며, 정보 공유 및 분석센터와 같은 장소를 활용하여 우주 산업에서의 위협, 경고, 사건에 대한 정보를 공유해야 한다. 다섯째, 보안 조치는 적절한 위험 허용 오차를 관리하고 과도한 부담을 최소화할 수 있도록 효과적으로 설계되어야 하며, 미국의 국가안보, 국가의 중요 기능, 우주 차량 크기, 임무 지속 기간, 기동성, 해당 궤도의 체제 등에 부합하여야 한다. 우주

자산에 대한 사이버 보안이 필수적이라는 문제의식에서 출발한 SPD-5는 우주 자산 및 이를 지원하는 인프라를 보호하기 위한 노력의 강화와 더불어 사이버 공격에 대한 회복탄력성(resilience)을 강화하기 위해 산업계뿐만 아니라 국제적인 파트너들과 협력할 것임을 밝히고 있다(The White House, 2020).

미국은 사이버-우주 안보 넥서스의 관점을 반영하여 전략과 정책에 반영하는 동시에, 실질적으로 실행할 수 있는 기술 및 체계 역시 마련해 놓았다. 러시아-우크라이나 전쟁 당시 러시아의 사이버 공격으로 우크라이나의 우주 기반 통신 인프라가 파괴되었을 때, 미국의 스페이스X는 우크라이나에 스타링크 서비스를 사용할 수 있도록 신속하게 지원해 준 바 있다. 이는 미국이 이미 민간 기업인 스페이스X를 통해 저궤도 군집위성을 통한 통신 인프라를 구축해 놓았으며, 실제 전장에서 언제든지 안정적으로 활용할 수 있을 정도의 수준을 갖추고 있다는 것을 보여준다.

사실 스페이스X가 스타링크 서비스를 위해 구축한 저궤도 군집위성 시스템은 군사적 이용을 위한 것이 아니다. 민간의 통신을 위해 제공되는 서비스이다. 그렇다 보니 스타링크 서비스는 보안이 상대적으로 취약할 수밖에 없다. 스타쉴드(Starshield)는 이러한 스타링크의 통신 보안 취약성을 극복함으로써 정부, 정보기관, 군 등에서 활용할 수 있게 만든 우주 기반 통신 인프라 혹은 시스템이라고 할 수 있다. 스페이스X의 설명에 따르면, 스타링크도 이미 사용자 데이터에 대하여 종단 간 암호화를 제공하고 있지만 스타쉴드는 여기에 더 높은 성능의 암호화 기능을 추가하여 기밀 데이터를 안전하게 처리할 수 있다고 한다(Space X, n.d.). 미국 정부는 스페이스X의 스타쉴드를 조달하여 2029년까지 정부가 소유하고 통제하는 스타쉴드 위성군을 확보할 계획이 있는 것으로 보인다(Erwin, 2024/6/11).

미국 스페이스X의 저궤도 군집위성이 커버하는 범위가 전 세계 120개가 넘는 국가에 달할 정도로 압도적인 데 비해, 중국은 아직 후발주자이다. 미국 스타링크에 의한 데이터 주권 침해를 우려하던 중국은(O'Loughlin, 2025), 크게 세 개의 저궤도 군집위성 구축 프로젝트를 계획하였다(Xinhua, 2024/8/9). 먼저, 중국은 2021년에 국가 차원의 프로젝트를 발표하였다. 일명 '궈왕(國網)'이라고 불리는 중국판 스타링크 통신망을 구축한다는 계획으로, 이를 주도하는 것은 '중국위성망락집단'이라고 하는 기업이다. 이 기업은 미국의 스페이스X와 달리, 중국 정부가 전액 출자하여 세운 기업으로, 민간이 설립한 기업이 아닌 국영기업이다. 중국판 스타링크를 꿈꾸는 만큼, 2035년까지 1만 3천 개 이상의 위성을 저궤도에 발사하여 궈왕이 커버하고자 하는 범위는 전 세계이다(최용석, 2024/2/7; O'Loughlin, 2025). 이를 위한 첫 번째 발사는 2024년 12월에 이루어졌고, 이때 10개의 위성을 발사하였다(O'Loughlin, 2025).

중국의 두 번째 계획은 상하이시가 주도하고 있다. 이 프로젝트는 '첸판(Qianfan)'으로 천 개의 돛을 의미하며, 'G60 스타링크'라는 별칭으로도 불린다. 2030년까지 1만 5천 개의 위성을 저궤도에 쏘아 올려 저궤도 통신망을 구축할 계획이며, 2025년까지 648개의 위성을 통해 지역 차원의 커버리지를 제공할 예정이다(Xinhua, 2024/8/9; O'Loughlin, 2025). 첸판 프로젝트는 상하이스페이스콤위성기술(Shanghai Spacecom Satellite Technology, SSST)이라는 국영기업이 중국과학원의 산하에 있는 소형위성혁신아카데미(the Innovation Academy for Microsatellites under the Chinese Academy of Sciences, IAMCAS)와 함께 진행하는 것으로 알려져 있다(Jones, 2024/6/27). SSST는 현재까지 구축한 저궤도 군집위성을 통해 이미 태국, 말레이시아, 브라질 등과 서비스 계약을 맺으며 미국의 스타링크 서비스에 대항하고자 노력 중이

다(O'Loughlin, 2025).

중국이 구상하는 세 번째 계획은 홍칭(Hongqing)이라는 기업을 통해 진행되고 있다. 홍칭은 저궤도에 1만 개의 위성을 배치하고자 하며, 이 위성 군집은 '홍후-3'이다. 2024년 5월 24일에 국제전기통신연합(ITU)에 계획을 공식적으로 제출한 바 있으며, 첫 발사는 2025년 중으로 예정하고 있다(박시수, 2024/6/4). 저궤도 위성통신 인프라를 자체적으로 구축함으로써 데이터 안보를 확보하려는 노력을 보이는 동시에 중국은 군 병종 체계를 개편하기도 하였다. 기존에 우주시스템부와 네트워크시스템부로 구성되어 있던 전략지원부대를 폐지하고, 정보지원부대, 군사우주부대, 사이버부대를 새로 창설하였다. 우주 영역을 담당하는 부대와 사이버 영역을 담당하는 부대를 분리했다는 점에서 단순히 중국이 사이버-우주 안보 넥서스의 시각을 가지지 못한 것으로 해석할 수도 있지만, 네트워크 정보 체계의 구축과 합동을 통한 승리를 강조하였다는 점을 고려한다면(정성조, 2024/4/19), 중국 역시 두 영역의 안보를 넥서스의 시각에서 바라보고 있으며, 정보 혹은 데이터의 흐름에 방점을 두고 있음을 확인할 수 있다.

중국과 전쟁 가능성이 있는 대만은 약 14개의 해저 케이블에 데이터 안보를 의존하고 있다(O'Loughlin, 2025). 이러한 상황에서 대만은 중국이 해저 케이블을 절단할 경우를 대비해야 할 필요가 있다. 2025년에만 해도 4건 이상의 케이블 절단 사례가 확인되었으며, 그중 2건은 중국 선박에 의한 것으로 추정된다. 러시아는 우크라이나를 빠르게 무력화하기 위하여 통신 인프라에 대해 사이버 공격을 가하였고, 우크라이나는 재빠르게 미국의 우주 기반 통신 인프라인 스타링크를 지원받아 데이터의 흐름을 복원하여 러시아에 맞선 바 있다. 우크라이나의 사례는 대만에 주는 함의가 있다.

대만 역시 중국에 의한 해협 봉쇄나 침공과 같은 비상사태를 경험할 수

있고, 이때 중국은 대만이 적절한 대응을 할 수 없게 만들기 위해 대만이 의존하고 있는 통신 인프라인 해저 케이블을 절단할 수 있다. 이때 만약 우주 기반 통신 시스템을 대만이 갖추고 있다면 해저 케이블 절단으로 인해 끊긴 데이터의 흐름을 복구할 수 있게 된다(Molock, 2025). 대만이 현재 가진 기술력으로는 저궤도에 위성 군집을 형성하여 통신 인프라의 회복탄력성을 확보하는 데 어려움이 있다. 이러한 이유에서 대만은 미국의 스페이스X와 협상하였으나 이해관계를 조정하는 데 실패함에 따라 대안으로 유럽의 저궤도 위성통신 시스템인 유텔샛원웹의 도움을 받게 되었다(김철문, 2025/3/31). 이와 동시에 대만은 자체적인 기술 개발에도 나서는 모습을 보이는 중이다. 대만 우주청(TASA)은 2030년까지 대만의 인공위성을 통한 저궤도 위성통신망 구축을 목표로 하고 있다(채제우 2024/12/26).

유럽연합 역시 스타링크와 같은 글로벌 저궤도 위성통신망에 대한 의존에 대해 국가안보, 주권의 차원에서 우려하고 있다(O'Loughlin, 2025). 디지털 전환이 이루어지는 과정에서 사이버 안보에 대한 위협이 증가하면서 안전성과 탄력성이 보장되는 글로벌 연결의 필요성을 인지하였다(EUSPA, 2025). 유럽연합은 2024년 12월에 아이리스2 프로젝트를 공식적으로 발표하였다. 이 프로젝트는 2030년까지 저궤도와 중궤도에 290개의 위성을 배치하여 다중 궤도 위성 군집을 형성하는 것을 목표로 한다(EUSPA, 2025; 박정한, 2024/12/19). 유럽이 미국으로부터 전략적 자율성을 확보하기 위해 시작한 아이리스2 프로젝트는 사이버-우주 안보 넥서스의 관점에서 우주 기반 인프라에 대한 사이버 보안 강화의 중요성에 초점을 맞추고 있다. 유럽 양자 통신 인프라(EuroQCI)의 양자 암호를 활용하여 설계에서부터 사이버 보안 강화에 신경 쓰는 모습을 보이고 있다(EUSPA, 2025).

유럽연합 사이버보안국(European Union Agency for Cybersecurity, ENISA)은

저궤도에 주로 배치되는 상업용 위성 시스템이 직면할 수 있는 사이버 보안 취약성을 식별하고 위협 환경을 평가하는 내용의 보고서 〈우주 위협 지형(Space Threat Landscape)〉를 발표하였다(ENISA, 2025/3/26). 이 보고서는 데이터의 흐름이 이루어지는 사이버 영역의 우주 영역에 대한 의존도가 증가함에 따라 위성에 대한 공격 빈도도 증가할 것으로 예측한다. 우주 기반 인프라에 가해지는 다양한 위협을 유형화함으로써 사이버-우주 안보 넥서스의 위협에 대해 식별해 내고 있다(ENISA, 2025, pp. 29-36).

3. 사이버-우주 안보 넥서스에 대한 위협과 도전과제

일반적으로 우주 안보에 대한 위협은 우주 자산에 대한 위협으로 설명할 수 있으며, 다음의 〈표〉와 같이 공격이 물리성을 갖느냐에 따라 물리적 위협과 비물리적 위협으로, 공격이 어디에서 시작돼서 어디에서 끝나는지에 따라 지상-우주, 우주-우주, 우주-지상으로 나누어 정리해 볼 수 있다.

〈표 14-1〉 우주 자산에 대한 위협 유형 구분

	지상 → 우주	우주 → 우주	우주 → 지상
물리적 위협 (kinetic)	직상승 ASAT 지상 기반 미사일	궤도상 ASAT 우주 기반 미사일 방어 요격	우주 기반 지상 공격
비물리적 위협 (non-kinetic)	업링크 재밍 레이저 간섭 스푸핑	궤도상 교차 재밍 궤도상 HPM	우주 기반 다운링크 재밍 레이저 EMP(핵폭발, 재래식) 데이저 절취, 변조

출처: 이성훈(2023), p. 3.

이 글에서는 〈표 14-1〉의 우주 안보에 대한 포괄적인 위협에 대한 구분을 참고하여, 사이버와 우주 영역을 매개하는 데이터의 흐름을 중심으로 사이버-우주 안보 넥서스에 대한 위협을 논하고자 한다. 두 영역을 오가는 데이터의 흐름은 통신 인프라가 얼마나 안정적인가에 좌우된다. 다시 말해, 지상에서 우주로, 우주에서 우주로, 우주에서 지상으로 흐르는 데이터에 어떠한 위협이 발생할 수 있는가를 중심으로 사이버-우주 안보 넥서스에 대해 발생할 수 있는 위협을 확인해 볼 수 있다. 통신 인프라에 대한 단순한 물리적 공격은 사이버와의 넥서스가 고려되지 않으므로 논의에서 배제한다. 예를 들어, 직상승 ASAT 발사를 통한 저궤도 군집위성 파괴는 지상에서 우주로 향하는 위협이자 공격이지만 이 자체에는 사이버 영역이 연계되지 않으므로 이 글에서는 제외하고자 한다. 대신, 사이버 공격을 통해 물리적 공격까지 전이시키는 경우는 사이버-우주 안보 넥서스에 대한 위협에 포함한다.

앞서 사이버-우주 안보 넥서스에 대한 위협의 본질은 데이터 안보라고 강조하였는데, 이는 데이터를 생성하고 전송, 처리, 활용하는 모든 단계에서 발생할 수 있는 취약성이 무엇인지 검토해야 함을 의미한다. 먼저 지상에서 우주를 향하는 위협이다. 우주 기반 통신 인프라인 저궤도 위성 군집과 실시간으로 원활한 연결성을 유지하기 위해서 지상에는 수많은 지상국이 존재한다. 이 지상국이 사이버 공격의 일차적인 침입 경로를 제공한다. 지상에서 우주로 향하는 위협은 업링크를 교란(uplink jamming)하는 것, 인공위성 시스템에 조작된 명령을 보내는 스푸핑(spoofing), 지상국 시스템의 통제권을 해킹하여 위성의 궤도를 변경하거나 데이터를 오염 또는 삭제하는 것 등이 있다. 이는 데이터가 출발하는 곳에서부터 신뢰성의 문제를 일으킬 수 있으므로, 데이터의 무결성을 침해할 수 있다. 저궤도 군집위성은

다수의 위성을 지구 저궤도에 촘촘하게 분산 배치함으로써 통신의 속도, 회복탄력성을 확보한다는 장점이 있지만, 공격받을 수 있는 표면적이 증가하게 된다는 단점도 동시에 생긴다. 애초에 사이버 공격을 시도해 볼 수 있는 위성의 수가 많이 있기도 하고, 촘촘하게 분산 배치되어 있기 때문에 사이버 공격을 통해 소수의 위성만 통제를 벗어나게 되어도 저궤도에 있는 위성 간 연쇄적인 충돌 가능성이 올라갈 수 있다. 지상에서 우주를 향하는 사이버-우주 안보 넥서스 위협의 가장 대표적인 사례로는 2022년 러시아가 우크라이나 침공 전 수행했던 비아샛에 대한 사이버 공격이 있다.

다음은 우주에서 우주로의 위협이다. 우주-우주 위협은 기본적으로 데이터 전송에 대한 취약성을 노리는 것이라고 할 수 있다. 저궤도에 형성되어 있는 수많은 인공위성 간의 네트워크에서는 데이터 릴레이(스위칭)가 일어난다. 이러한 활동은 저궤도 군집위성의 강점인 빠르고 분산된 통신을 가능하게 해주지만 그만큼 전파 교란과 같은 공격에 취약할 수밖에 없다. 주된 위협으로는 전송되는 데이터를 중간에 탈취하거나 도청·감청하는 것이 있다. 우주-우주 위협은 데이터가 이동하는 경로에 대한 신뢰성을 침해할 수 있으므로 최종적으로 지상에서 수신하는 데이터에 대한 기밀성, 무결성 등에 문제가 발생할 수 있다. 최근에는 이러한 위협에 대응하기 위한 데이터 전송 기술이 개발되고 있다. 광통신 기술이 바로 그것인데, 기존에는 위성 간 통신이 전파에 의해 이루어졌다면 광통신 기술은 데이터 송수신에 빛을 이용하는 방식이다. 일명 레이저 통신이라고 불리는 이 기술은 기존의 전파 통신보다 도청·감청이 어렵다는 점에서 보안성을 높인다. 또한 저궤도에 배치된 위성 간 연결(Inter-Satellite Link, ISL)을 기존보다 더 빠르고 안정적으로 할 수 있게 해줌으로써 단말기가 지상국을 통하지 않고 직접 위성과 연결될 수 있게 해주어 저궤도 군집위성을 통한 통신의 효율성을

극대화할 수 있다(강충구, 2025/2/11; 윤현성, 2024/11/19).

데이터가 이동하는 공간을 중심으로 한 위협의 마지막은 우주에서 지상으로 향하는 위협이다. 우주에서 위성을 통해 생성, 수집된 데이터는 지상으로 보내져 사이버 공간에서 저장, 분석, 활용된다. 이때 데이터가 위조되거나 변조될 수 있고, 허위 신호를 발신할 수 있으며, 이렇게 왜곡된 데이터가 지상에서 활용되는 과정에서 의사결정에 중대한 문제를 일으키게 만들 수도 있다는 점에서 역시 신뢰성을 해칠 가능성이 발생한다.

통신 인프라를 통해 데이터가 지상-우주, 우주-우주, 우주-지상을 오가면서 발생할 수 있는 사이버-우주 안보 넥서스 위협 외에도 뉴스페이스 시대가 도래하면서 나타날 수 있는 위협도 존재한다. 뉴스페이스 시대는 올드스페이스 시대와 달리 우주 영역이 군사적인 이유에서보다는 상업적인 이유에서 활용되는 경향이 있다. 이것이 가능한 이유는 3D 프린팅, 발사체의 재활용 등을 통해 비용을 획기적으로 낮출 수 있게 되었기 때문이고, 이를 통해 수익을 창출할 수 있게 되었기 때문이다. 이러한 이유에서 과거 우주 공간에서 주된 행위자는 국력의 과시를 위해 상징적으로 경쟁하던 국가들이었지만 현재는 우주 산업을 통해 수익을 창출하고자 하는 민간 기업들이 국가 행위자만큼 혹은 그 이상으로 적극적인 행보를 보인다.

사이버-우주 안보 넥서스에 뉴스페이스 시대가 불러올 위협은 민간에 대한 의존도 증가가 가져오는 불확실성에 있다. 민간 기업에 의해 저궤도에 형성된 인공위성 군집들은 앞서 살펴본 것처럼 사이버 공격을 당할 수 있는 표면적을 넓혔다. 대체로 이러한 인공위성들은 군사적인 목적에서 설계된 것이 아니라, 상업적 이유에서 만들어진 것이기 때문에 사이버 공격에 더 취약할 수 있다. 인공위성, 우주선 등에 대한 공급 역시 비용 효율 측면에서 민간 기업에 의존하고 있는데, 민간 기업의 협조가 잘 이루어지지

않는다면 우주 자산 또는 우주 인프라의 확보, 유지 자체에서부터 문제가 발생할 수 있다. 또한 국가 간 거버넌스가 부재한 상황에서 민간 기업이 우주에 쏘아 올린 수많은 위성 간 문제가 발생하게 된다면 타국과의 관계에서 외교 안보적 불안정성이 증가할 수도 있다. 이에 더하여, 거버넌스 부재의 관점에서 보았을 때, 사이버 영역과 우주 영역에 대한 독립된 거버넌스도 완전하지 않은 상황에서 두 영역이 넥서스 되면서 발생하게 되는 거버넌스, 규범, 제도의 공백은 통신 주권, 데이터 주권 등과 같은 논쟁을 끊임없이 등장시키고 증폭시킬 수도 있을 것으로 보인다.

지금까지 우주 기반 통신 인프라인 저궤도 군집위성과 데이터 안보를 중심으로 사이버-우주 안보 넥서스 위협을 살펴보았다. 데이터 안보를 불안정하게 만드는 사이버-우주 안보 넥서스 위협들은 데이터의 생성 및 수집에서부터 활용에 이르기까지 전 단계에 걸쳐 문제를 일으킨다. 최근 주목받는 인공지능 기술은 데이터를 중요한 자원으로 하여 성장하는 기술로, 사이버와 우주 영역에 접목되어 활용되는 과정에서 이 역시 데이터 안보를 매개로 상호 영향을 미치는 넥서스를 형성할 수 있게 된다. 즉, 사이버-우주-인공지능 안보 넥서스라는 삼각 넥서스가 만들어지는 것이다. 인공지능 기술은 어느 영역에나 결합하여 응용될 수 있는 기술로, 사이버 공간에서의 공격이나 방어에 활용되기도 하며, 우주 공간에서 인공위성의 데이터 분류, 식별, 분석 등에 도입되기도 한다. 만약 인공지능에 의해 인공위성에 사이버 공격이 이루어지고, 그 여파로 수집되어 전송되는 데이터에 왜곡이 발생하였다고 해보자. 이렇게 왜곡된 데이터는 인공지능을 학습하는 데이터로 활용될 수 있으며, 이 경우 인공지능에 의한 의사결정에 오류가 발생하여 안보적 문제가 발생할 수 있다. 사이버와 우주 그리고 인공지능은 이와 같은 방식으로 안보적인 차원에서 상호 영향을 주고받을 수 있다는 점

에서 넥서스를 이루게 된다. 이것이 바로 사이버-우주 안보 넥서스가 직면하게 되는 도전과제이다.

사이버, 우주(위성), 인공지능을 안보적으로 매개하는 것은 데이터이며, 이를 기술적으로 엮어낼 수 있는 것은 반도체이다. 반도체는 데이터를 기반으로 하는 디지털 기술들에 필수적인 것으로, 반도체를 통해 위성과 관련된 비용을 줄일 수 있으며, 이를 통해 더 많은 위성을 자산으로 가지게 된다면 통신을 통한 사이버 공간의 확장이 가능해지고, 이를 통해 얻게 되는 양질의 데이터를 원료로 하여 발전하는 인공지능이 모두 넥서스 된다. 이러한 삼각 넥서스는 공급망의 관점에서도 복잡성을 증가시켜 취약성이 올라갈 수 있다. 즉, 사이버-우주 넥서스에 인공지능까지 결합하면서 사이버 공급망, 우주 공급망, 인공지능 공급망이 복잡하게 얽히게 되고, 어느 하나라도 어긋나게 되면 사이버-우주-인공지능에 연쇄적으로 차질을 일으켜 취약성이 증가하게 되는 것이다. 사이버, 우주, 인공지능 세 영역에 있어 민간 기업에 대한 의존도가 모두 높다는 점에서 안보에 불확실성이 더 증가할 가능성도 존재한다는 것을 간과해서는 안 된다.

4. 맺음말

한국은 차세대 통신 기술의 핵심인 저궤도 군집위성과 같은 우주 기반 인프라의 구축에 있어 경쟁력 있는 자체 기술을 가지고 있지 않다. 스페이스X와 같은 글로벌 저궤도 위성통신 사업자들이 한국 시장에 진출하게 되면 데이터와 통신의 주권이 위협을 받을 가능성이 있다. 자체적인 기술을

보유하지 않고 전적으로 해외 사업자에 의존하는 구조를 갖추게 되면 통신 주권과 그 통신을 통해 수집되는 데이터에 대한 주권 역시 완전히 포기하는 것이다. 현재 한국은 2030년까지 6G를 위한 저궤도 통신 위성을 발사하는 사업을 진행하고 있다. 위성 군집을 형성할 정도의 기술력이 부족하고, 예산 규모도 상대적으로 작다는 점에서 한계가 있지만, 자체적인 역량을 기르려는 노력을 지속한다는 측면에서는 주목할 필요가 있다. 역량의 측면에서 혼자의 힘으로 미국, 중국과 같은 국가를 따라잡는 것은 어려우므로 선진 기술을 가진 미국과의 협력을 강화하면서도 중심추를 유지하기 위해 비슷한 처지에 있는 국가들과의 협력도 지속할 필요가 있다. 대만의 경우, 양안 관계의 불안정으로 인한 중국으로부터의 위협이 항시 존재하며, 미국에 안보를 의존하고 있으면서도, 동시에 첨단기술, 특히 반도체 기술력을 중심으로 한 협력으로 긴밀하게 연계되어 있다. 이처럼 한국과 매우 유사한 구조적 환경을 가진 대만 역시 독자 위성통신망을 구축하려는 노력을 진행 중이다. 한국은 이러한 국가들과의 협력을 적극적으로 추진할 필요가 있다. 한국의 사이버-우주 안보 넥서스를 안정적으로 유지하기 위해서는 우주 역량 강화만 필요한 것은 아니다. 최근 SKT, KT 해킹 사례에서 볼 수 있다시피, 여러 사이버 공격으로 인한 피해 사례가 국민적 주목을 받는 상황인 만큼, 민간 기업들의 사이버 보안 능력의 향상과 더불어 국가적 차원의 사이버 안보 역량 강화 역시 함께 이루어질 필요가 있다.

제14장

사이버-AI 넥서스와 미국의 동맹외교: 변화와 쟁점

신승휴 | 서울대학교 외교학 전공 박사과정

제14장

사이버-AI 넥서스와 미국의 동맹외교: 변화와 쟁점

신승휴 | 서울대학교 외교학 전공 박사과정

1. 서론

인공지능(AI)의 급격한 발전과 확산은 사이버 안보 분야에서 그간 주목해 온 다양한 초국적 위협을 한층 더 심화시키는 요인이 되고 있다. 사이버 안보를 둘러싼 국제정치의 구조와 동학이 AI 기술의 개입으로 인해 변화하고 있음은 물론이다. 이처럼 사이버와 AI의 결합을 의미하는 '사이버-AI 넥서스(cyber-AI nexus)'는 국가가 해결해야 할 사이버 위협의 양적·질적 변화를 초래하여 그 파급력을 키우고(Lohn 2025), 사이버 안보와 여타 안보 이슈 간 연계 가능성을 확대하며, 디지털 환경에서 발생하는 기술 차원의 문제가 지정학적 갈등과 경쟁으로 이어지게끔 하는(김상배 2025, 101-132), 그야말로 '신흥안보(emerging security)'의 문제로 부상하고 있다.

그동안 사이버와 AI의 결합을 둘러싼 학계의 논의는 주로 AI의 발전이 사이버 작전의 효과성, 사이버 억제와 위기관리 역량, 정보전에서의 공수 균형, 그리고 핵무기나 자율무기체계의 취약성 등에 어떠한 변화를 가져오는지에 초점을 두어 전개되어왔다(Johnson 2019; Khan, Khurshid & Cifuent-

es-Faura 2024). 그러나 오늘날 사이버-AI 넥서스는 군사 영역과 비군사 영역의 경계를 넘나들며 안보 문제를 심화하는 변수가 되고 있다. 여전히 'AI 기반 사이버 작전(AI-enabled cyber operations)'은 중요하지만, 국가를 지탱하는 핵심 인프라 전반에서 AI가 범용기술로 활용되는 가운데 AI 기반 시스템이 사이버 공격의 대상이 되면서 발생하는 정치적·사회적 안보 문제도 주목할 만하다. 온라인상 악의적 콘텐츠를 탐지·차단·예방하는 수단으로 AI가 도입됨에 따라 발생하는 윤리적 문제와 주권 침해도 관찰된다.

이렇듯 AI가 사이버 위협을 심화함과 동시에 사이버 위협의 표적이 되고, 또 사이버 공격을 차단하는 효과적인 수단으로도 활용되는 상황에서 사이버-AI 넥서스에 대한 국가적 대응은 총체적이고 유기적이며 초국적인 접근을 요구하고 있다. 그중에서도 특히 공통의 위협인식과 가치를 공유하는 동맹국 및 우방국들과의 협력은 사이버-AI 넥서스 대응의 가장 중요한 부분을 차지한다. AI의 기반이 되는 데이터와 알고리즘을 체계적으로 관리하는 일부터, AI 기반 사이버 공격이 국가안보 위협으로 이어지지 않도록 그 연결고리를 차단하는 문제에 이르기까지, 모든 단계에서 국제협력이 필수적일 수밖에 없기 때문이다. 이는 초강대국 미국에도 예외 없이 적용되는 조건이다.

바이든 행정부 출범 이후로 지금까지 미국은 사이버 안보와 AI를 위한 국가전략을 구분 지어 수립하고 그 안에서 국제협력을 모색하는 노력을 기울여왔다. 바이든 행정부는 사이버 위협 대응을 위한 글로벌 공조체계를 구축하고, 기술 표준화를 선도하며, 디지털 환경에서 핵심 가치를 보호하기 위해 민주주의 동맹 기반의 국제협력을 중시하는 모습을 보였다. 그와 마찬가지로 AI 분야에서도 기술의 윤리적 개발과 활용을 촉진하는 일련의 규칙과 표준을 마련함과 동시에 AI를 악용한 권위주의 국가의 위협을 차단

하려는 목적에서 동맹국과의 연대를 중시하였다. 그에 따라 미국의 사이버 안보 전략과 AI 전략은 민주주의와 규칙기반 질서(rules-based order) 그리고 다중이해당사자주의(multistakeholderism)를 표방하는 다양한 (소)다자협력 네트워크를 플랫폼으로 삼아 사이버 위협과 AI의 잠재적 위험, 더 나아가 기술지정학 위기에 공동으로 대응하는 동맹외교(alliance diplomacy)를 전개하였다(신승휴 2025, 6-7).

그러나 2025년 초 트럼프 2기 행정부가 출범하면서 이러한 전략 기조는 점차 변화하는 양상을 보이고 있다. 트럼프 행정부는 출범 직후 사이버 위협의 대상을 이전보다 더 구체화하면서도 또 다른 한편으로 사이버 안보를 군사안보의 맥락에서 범주화하는 이중적 접근을 취하고 있다. 그에 따라 국제협력은 사안별 이익을 위한 단편적 협력으로 귀결되는 결과가 발생하고 있다. AI 분야에서는 역시 동맹국들과 협력하여 글로벌 차원에서 합의된 원칙과 규범에 근거한 질서를 만들어가는 일보다 기술 혁신과 견제를 통해 글로벌 AI 경쟁의 무대에서 전략적 우위를 확고히 하는 데 더 높은 이해관계를 표출하고 있다. 물론 여전히 동맹국 및 유사입장 국가들과의 협력이 중요하다는 원칙을 표방하고는 있지만, 미국우선주의(America First) 기조로의 회귀가 기정사실화된 가운데 AI를 위한 국제협력은 공유된 이익과 가치보다는 국익 극대화를 목표로 거래적인 맥락에서 이루어져야 한다는 논리를 내세우고 있는 것이다.

사이버-AI 넥서스로 인해 여느 때보다 국제협력의 중요성이 커지는 상황에도 불구하고 사이버 안보와 AI 분야 미국의 전략이 이익 중심의 단편적이고 거래적인 협력을 선호하는 방향으로 나아가고 있음에 주목하여 이 글은 사이버-AI 넥서스에 대한 미국의 대응 역시 가치 중심의 동맹 협력에서 점점 더 멀어지고 있음을 주장한다. 이러한 시각을 뒷받침하기 위해 본

연구는 사이버 안보와 AI에 대한 트럼프 2기 행정부의 전략이 국제협력에 어떻게 접근해왔는지 살펴보았다. 구체적으로 사이버 안보 전략과 AI 전략에 담긴 국제협력의 기조, 이니셔티브, 플랫폼 그리고 추진체계의 내용을 검토하여 그 안에서 발견되는 시기별 특징을 이해하고 이를 토대로 변화의 추이를 포착하였다. 이에 기반하여 AI에 의한 사이버 작전의 양·질적 변화, AI 생성 허위정보를 토대로 이루어지는 영향력 공작, AI 기반 콘텐츠 검열에 따른 데이터 안보와 주권 침해 등 사이버-AI 넥서스 차원에서 최근 주목받고 있는 문제들에 미국이 어떻게 접근하고 있으며, 그러한 접근이 동맹외교에 미치는 영향은 무엇인지 분석하였다.

2. 미국의 사이버 안보 국제전략

바이든 행정부 시기 사이버 안보를 위한 미국의 전략은 초국적 사이버 위협을 관리할 수 있는 글로벌 거버넌스를 구축하고 디지털 기술 표준화를 선도함으로써 사이버 공간에서도 민주주의, 자유, 인권, 규칙기반 질서 등 핵심 가치를 보호하는 것을 목표로 하였다. 당시 미국은 '동맹의 복원과 다자주의'를 표방한 대외정책을 추진하였으며, 그와 같은 맥락에서 사이버 안보 전략 역시 민주주의 가치 중심의 동맹외교를 통해 자국의 리더십에 기초한 연대를 형성하고 이를 기반으로 패권의 회복을 도모하는 데에 집중되었다(Fontaine, 2025/01/20). 그러나 2025년 1월 트럼프 행정부가 재출범에 성공하면서 미국의 사이버 안보 국제전략은 빠르게 변화하고 있다.

아직 사이버 안보를 위한 새로운 국가전략이 수립되진 않았으나, 2025년 6월 6일 트럼프 대통령은 사이버 안보 우선순위를 재설정하는 것을 목표로 「행정명령 제143061호(국가 사이버보안 강화를 위한 선별된 노력 유지)」를 발표하였다. 「행정명령 제143061호」는 사이버 안보를 위해 오바마 행정부가 2015년 발표한 「행정명령 제13694호(중대한 악의적 사이버 행위에 관여하는 특정인의 재산 차단)」과 바이든 행정부가 집권 말기인 2025년 1월 마련한 「행정명령 제14144호(국가 사이버보안 강화 및 혁신 촉진)」을 일부 수정·철회하여 위협 대상 명확화, 차세대 디지털 기술 도입 가속화, 정부 규제 완화 등을 목표로 하는 것으로 알려졌다. 특히 중국에만 국한되었던 사이버 위협국의 범위를 러시아, 이란, 북한 등으로 확대하는 조치와 더불어 사이버 보안을 위한 정부의 규제보다 기업의 자체적인 대응을 독려하는 조치가 주된 변화로 평가된다(The White House, 2025b).

그러나 트럼프 행정부는 사이버 위협의 대상을 이전보다 더 구체화하면서도 정작 사이버 안보를 군사안보의 맥락에서 범주화함으로써 사이버 안보 국제협력이 사안별 국익에 집중된 단편적 협력으로 이어지는 결과를 초래하고 있다. 그에 따라 바이든 행정부 시기에 추진되던 포괄적이고 통합적인 협력 이니셔티브들이 지속되기 어려울 것이라는 전망도 제기되는 상황이다. 무엇보다 러시아에 대한 선제적인 사이버 작전이 중단되었다는 의혹이 확산하면서 그동안 미국이 주도해 온 민주주의 가치 기반의 디지털 연대나 사이버 안보협력의 네트워크가 더는 효과적으로 작동하기 어려울 것을 우려하는 목소리도 작지 않다(Magee, 2025/04/15). 당장 「행정명령 제143061호」가 선거개입 위협과 같은 사회안보 이슈와 사이버 안보 간 상관성을 사실상 부인하는 원칙을 담아냄에 따라 민주주의 동맹국과의 공조를 바탕으로 허위정보 확산과 영향력 공작에 공세적으로 대응하는 사이버 작

전의 영역도 축소될 여지가 있다(Ortega, 2025/04/09).

전략의 기조와 이니셔티브에서 발견되는 이 같은 변화의 조짐은 미국이 중심이 되어 운영해 온 국제협력의 플랫폼 자체를 약화하는 요인이 되고 있다. 이는 비단 사이버 안보에 대한 미국의 접근이 변화하였기 때문만은 아니다. 동맹 중심의 국제협력에 대한 미국의 접근이 가치보다는 배타적 국익을 우선시하는 거래적인 방식을 선호하게 되면서 나타나는 현상으로 볼 수 있다. 대표적으로 파이브 아이즈의 공조체계가 흔들리는 사례를 예로 들 수 있다. 미국과 캐나다의 외교적 갈등은 차치하더라도 트럼프 행정부가 사이버 안보 국제협력을 위한 이니셔티브에 소극적인 모습을 보이면서 중국과 러시아의 사이버 위협에 공동으로 대응해온 파이브 아이즈 차원의 협력도 약화하고 있는 것으로 파악된다(Miller & Roussi, 2025/02/12). 바이든 행정부의 대외정책에서 핵심적인 부분을 담당하던 AUKUS 협정 역시 트럼프 행정부의 재검토 대상에 포함되면서 사이버 및 첨단기술 부문 3국 협력이 지속될 수 있을지 장담하기 어려운 상황이다(Roughead, et al, 2025/09/02).

전략의 추진체계에서 발견되는 변화에도 주목할 필요가 있다. 트럼프 행정부는 출범과 동시에 그동안 국무부와 함께 국제협력을 추동해온 사이버 인프라보안국(CISA)의 권한을 재검토하는 등 추진체계를 새롭게 정비하기 시작하였다(Cassidy, 2025/03/11). 트럼프 대통령은 당선 이전부터 CISA의 폐지를 논할 만큼 그 기능과 역할에 강한 회의를 드러냈으며 당선 이후 곧바로 CISA에 대한 인력 감축과 예산 삭감을 단행하였다(Rundle, 2025/06/02). 또한 국무부의 CDP도 구조적으로 분할·재편됨에 따라 사실상 일원화된 사이버 외교 전담지원기관의 기능을 상실하게 되었다. 허위정보 확산과 내정간섭 위협 대응을 전담해온 국무부 산하의 해외정보조작·

간섭대응허브(R-FIMI)[73]를 폐쇄하는 조치 역시 주목할만 하다. R-FIMI의 폐쇄는 트럼프 행정부가 언론을 감시하는 정부의 과도한 권한을 축소하려는 목적에서 내린 결정으로 알려졌지만(Gegeon, 2025/04/16), 해당 조치가 사이버상 영향력 공작을 목적으로 하는 악의적 사이버 활동에 대한 미국의 자체적인 대응 역량과 동맹 협력의 실효성을 약화하는 결과로 이어지고 있다는 비판도 제기되고 있다(Psaledakis, 2025/04/17).

물론 최근 트럼프 대통령은 CISA를 이끌 신임 국장에 사이버 보안 전문가를 지명하였고, 이에 대한 민간 부문의 긍정적 평가가 이어지면서 기존에 제기되던 CISA 폐지론은 사실상 수그러들었다. 미국의 통신망과 핵심 인프라의 사이버 보안을 책임져 온 기관이 예산 삭감과 인력 감축의 위기에서 부침을 겪고 있는 상황에 대한 공화당과 민주당의 우려로 앞으로도 미국의 사이버 안보 전략에서 CISA의 역할은 중요할 것으로 전망된다(Ribeiro, 2025/07/28). 실제로 2025년 5월 CISA는 NSA와 FBI 그리고 파이브아이즈 동맹국 관련 기관들과 합동으로 새로운 'AI 데이터 보안 모범 사례 가이드'를 내놓는 등 사이버 안보와 AI가 융합되는 지점에서 발생하는 문제들에 대응을 이어오고 있다(CISA, 2025/05/22). 그러나 동맹 협력 부문에서 CISA의 역할은 바이든 행정부 집권기 수준을 유지하긴 어려울 것으로 보이는데, 이는 트럼프 행정부와 공화당이 CISA의 역할을 대내적 사이버 보안과 민관협력에 국한하려는 모습을 보이고 있기 때문이다. 이렇듯 트럼프 행정부는 사이버 안보를 위한 국제협력에서 중요한 역할을 담당했던 기

73) R-FIMI는 2016년 설립된 글로벌관여센터(GEC: Global Engagement Center)가 2024년 12월 명칭을 변경하면서 출범하였다가 2025년 4월 공식적으로 폐쇄되었다.

관들의 권한과 역할을 축소하거나 거두어들이고 있다는 점에서 바이든 행정부와는 뚜렷한 차이를 드러낸다.

3. 미국의 인공지능 국제전략

바이든 행정부 시기 AI에 대한 미국의 전략은 기술의 안전성 확보와 위험성 관리를 위한 규범을 마련하는 것을 목표로 하였다. 따라서 AI 분야 국제협력을 모색하는 노력 역시 AI의 윤리적 개발과 활용을 촉진하는 일련의 규칙과 표준을 마련하고, 나아가 AI를 악용한 권위주의 국가의 위협을 차단하는 데에 집중되었다. 2023년 11월 30일 발표된 「행정명령 제14110호(안전하고 신뢰할 수 있는 인공지능 개발 및 활용)」은 정부의 기술 규제를 강화하기 위해 마련된 조치였지만, 대외적 차원에서는 동맹국을 포함한 유사입장 국가들과 협력하여 AI 규제 거버넌스 구축을 주도하고, AI 표준의 개발과 구현을 촉진하며, 안전한 AI 시스템의 확산을 도모하는 것을 목표로 하였다(The White House, 2023). 물론 바이든 행정부가 AI에 대한 윤리와 규제의 원칙을 마련하는 국제적 노력을 주도하고자 한 것은 AI의 잠재적 위험성에 대한 경각심 때문만은 아니었다. 다른 한편으로는 미국에 "유리한 국제기술질서(a favorable international technology order)"를 확립하여 핵심 가치를 보호하고 더 나아가 패권을 강화하고자 하는 이해관계도 강하게 작용하였다(NSCAI, 2021, p. 13).

바이든 행정부와 마찬가지로 트럼프 행정부도 1차 집권기인 2019년 백악관 산하에 'AI국가안보위원회(NSCAI)'를 설립하고 퇴임 직전인 2021년 1

월 「국가AI이니셔티브법 2020」을 제정하는 등 일찍이 AI가 미국의 안보와 경제에 미치는 영향에 대해 높은 관심을 드러냈다. 그러나 2차 집권 시작과 동시에 「행정명령 제14148호(위험 행정명령과 조치에 대한 1차 취소)」를 발효하여 바이든 행정부의 「행정명령 제14110호」를 폐지함과 동시에 「행정명령 제14179호(미국 인공지능 주도에 대한 장벽 제거)」에 서명함으로써 AI 전략의 초점을 규제보다는 혁신과 성장에 맞추는 방향으로 수정하였다. 「행정명령 제14179호」는 미국의 AI 혁신을 저해하거나 제약한다고 판단되는 기존의 규정을 철회하는 것을 목적으로 하며, 규범보다는 혁신을 통해 글로벌 AI 경쟁 구조에서 미국의 주도권을 공고히 하려는 의도를 반영한다(The White House, 2025a). AI에 대한 트럼프 행정부의 전략도 큰 틀에서는 다중이해당사자주의 접근을 취하고 있지만, 민간 부문 행위자들에 윤리적이고 책임 있는 참여를 유도한 바이든 행정부와 달리 트럼프 행정부는 민간 주도 혁신을 강조하고자 민간 부문, 특히 미국 기업에 확대된 역할을 부과한다는 점에서 뚜렷한 차이를 보인다.

이렇게 변화된 전략 기조를 바탕으로 미국은 2025년 7월 새로운 『미국의 AI 행동계획』을 수립하여 세부적인 목표와 정책 과제 및 실행 방안을 소개하였다(The White House, 2025c). 여기서도 트럼프 행정부는 'AI 경쟁(AI Race)'에서의 승리가 혁신의 가속화, 인프라 구축, 국제 리더십 확보에 달려 있음을 명확히 하였다. 책임 있는 AI 개발 원칙에 근거한 국제협력이 세부적인 목표로 언급되긴 하였으나, 전략의 무게중심과 초점은 혁신에 맞춰졌다. 그에 따라 현재 미국이 AI 분야에서 추진하는 국제협력의 이니셔티브는 공유된 가치나 규범보다는 배타적 국익 증진을 위한 거래적 협력을 선호하는 방향으로 계획·시행되고 있다. 당장 2025년 7월 시행된 「행정명령 제14320호(미국 AI 기술 수출 촉진)」만 보더라도 미국은 자국 AI 기술을 패키

지화하여 수출함으로써 미국산 AI에 대한 동맹국 및 파트너국의 도입을 더욱 적극적으로 유도하는 것을 목표로 한다. 또한 『미국의 AI 행동계획』 역시 동맹국 및 파트너국에 대한 미국산 AI 수출 촉진, AI 관련 기술의 해외 유출 통제 등 보호주의적이고 일방적인 대외 조치를 다수 포함하고 있다. AI 규범과 표준을 확립하기 위한 협력마저도 공유된 가치보다는 중국이 관련 국제기구나 다자협의체 안에서 영향력을 더 키우지 못하도록 견제하는 데 초점을 맞추고 있다(Mok, 2025/08/08).

물론 바이든 행정부도 2022년 이른바 'CHIPS법'으로 알려진 「반도체칩과 과학법」을 도입하여 대중국 견제를 위한 기술 수출 통제를 강화하는 한편, 반도체 공급망의 안정성을 확보하고자 일본·한국·대만과의 협력을 모색하는 '칩4동맹' 구상을 내놓은 바 있지만, 트럼프 행정부는 여기서 한발 더 나아가 동맹국에 미국산 AI 도입을 강요하는 행보를 보인다는 점에서 차이를 가진다. 따라서 협력의 플랫폼도 이전보다 그 활기를 잃게 될 가능성이 커졌다. 일차적으로 미국이 AI 규제 거버넌스 구축을 위한 다자협의체나 국제기구에 적극적으로 참여할 동기가 줄어들면서 G7, OECD, GPAI, CoE 등을 통해 이루어지던 규범 협력이 부침을 겪게 될 여지가 있다. 미국의 빅테크 기업이 유럽에서 규제법을 두고 역내 정부들과 갈등하는 국면에서 트럼프 행정부의 AI 전략이 기업의 혁신 활동에 힘을 실어주면서 안전한 AI 개발 및 확산을 위한 미국과 EU 간 협력에도 비상등이 커졌다는 평가가 나온다(Kroet, 2025/05/08). 한편 AUKUS에 대한 미국의 검토가 진행 중인 가운데 AI를 포함한 첨단기술 부문 AUKUS의 필러-2 협력도 현재는 표류하고 있다. 물론 미 의회를 중심으로 AUKUS에 대한 긍정적인 여론이 점차 커지고 있다는 분석도 있지만, 트럼프 행정부가 거래적 동맹 협력 기조를 유지하는 한 의미 있는 협력이 이루어질 수 있을지도 미지수이다

(Motwani, 2025/09/03).

전략 추진체계에서 나타나는 변화 역시 눈길을 끈다. 미국의 관심이 AI에 대한 규제보다는 혁신과 성장으로 옮겨감에 따라 정부 내부적으로 국제협력에 참여하는 주체도 자연스럽게 제한되는 경향을 보인다. 이는 바이든 행정부 집권기에 AI의 윤리원칙과 규범을 확립하기 위해 국제협력에 적극적으로 참여하던 정부부처와 기관의 기능이 약화하는 현상을 통해 가장 명확히 드러난다. 가장 대표적인 예로 국무부의 역할이 축소된 것을 들 수 있다. 2025년 7월 국무부는 CDP 안에서 사이버, AI, 양자컴퓨팅 등 첨단기술 관련 업무에 종사하던 인력을 대폭 감축하는 개편을 단행하였고, 그중에서도 디지털자유를 전담하던 부서는 아예 해체되기에 이르렀다. 이로 인해 국무부의 기술 전문성이 크게 훼손되었다는 지적과 함께 미국의 AI 분야 기술외교가 가치 중심에서 국익 중심으로 완전히 돌아섰다는 평가가 잇따랐다(Miller, 2025/07/17). 상무부의 표준기술연구소(NIST)와 그 산하의 AI표준혁신센터(CAISI)도 상황은 비슷하다. NIST는 AI 위험관리를 위한 자율적 프레임워크(AI RMF)를 통해 AI 생성 허위정보 대응을 위한 국제협력에 참여해왔지만, 트럼프 행정부의 결정에 따라 AI RMF에서 "허위정보(misinformation)"라는 표현이 삭제되면서 해당 이슈 분야에서의 국제협력도 미온해질 가능성이 커졌다. 그보다 더 큰 변화는 CAISI와 관련한 것인데, 트럼프 행정부는 AI 안정성 증진을 위한 국제협력에 큰 관심을 드러내지 않고 있을뿐더러 2025년 2월 파리 'AI 안정성 정상회의'에 참석한 미국 대표단에 CAISI 관계자가 포함되지 않았다는 점에서 해당 기관의 활동도 더욱 제한될 것으로 보인다(Dastin, 2025/02/07).

4. 사이버-AI 넥서스와 미국의 동맹외교

이상에서 살펴본 바와 같이, 트럼프 행정부 재출범 이후로 사이버 안보와 AI를 위한 미국의 전략은 각각 '사안별 이익 중심의 단편적 협력'과 배타적 국익 우선의 거래적 협력'을 선호하는 방향으로 나아가고 있다. 그렇다면 사이버-AI 넥서스 시대에 미국의 사이버 안보 전략과 AI 전략은 어떠한 내용의 국제협력을 모색하게 될까? 사이버-AI 넥서스가 초래하는 다양한 안보 문제를 바라보는 트럼프 행정부의 시각은 바이든 행정부의 그것과 어떠한 차이를 가지는가? 좀 더 구체적으로, 트럼프 행정부는 사이버 위협이 AI로 인해 날로 진화하는 상황을 어떻게 인지하고 있는가? 또는 AI 시스템에 대한 사이버 공격을 효과적으로 탐지하고 예방하기 위해 트럼프 행정부가 추진하고자 하는 동맹외교는 무엇인가?

물론 '사이버-AI 넥서스'를 위한 별도의 전략이 마련되지 않은 상태에서 이상의 질문에 대한 답을 찾기 위해서는 최근 트럼프 행정부가 사이버 안보와 AI가 융합되는 지점에서 발생하는 문제들에 어떻게 대응하고 있는가를 좀 더 자세히 들여다볼 필요가 있다. 따라서 이 글은 다음의 세 가지 사이버-AI 넥서스 문제에 주목하였다. 첫째, AI가 사이버 작전에 활용됨으로써 증폭되는 위협과 그러한 위협에 대응하는 방법을 모색하는 군사·정보 영역의 문제이다. 둘째, AI를 통해 생성되는 허위정보 및 오정보가 선거개입이나 내정간섭으로 이어지는 정치·사회 영역의 문제이다. 셋째, 온라인상 악의적 콘텐츠를 탐지·차단하는 수단으로 AI가 도입됨에 따라 발생하는 데이터·주권 영역의 문제이다. 이 세 가지 영역의 안보 문제는 트럼프 행정부의 사이버 안보 전략과 AI 전략이 규제에서 멀어져감에 따라 그 심

각성을 더해갈 것으로 예상되는 사이버-AI 넥서스 차원의 위협이라 할 수 있다.

1) 군사·정보 영역

군사·정보 영역에서 최근 미국이 예의주시하고 있는 사이버-AI 넥서스 문제는 AI가 사이버 작전에 활용됨으로써 증폭되는 사이버 위협과 그러한 위협에 대응하는 방법을 모색하는 일이다. 자동화된 사이버 공격을 대규모로 수행하는 작전이나 정보전의 효율성을 높이기 위해 봇(bot) 계정과 AI 생성 텍스트·이미지·영상을 활용하는 과정에서 AI가 사용되는 사례가 증가하고 있다. 특히 미국과 전략적 경쟁 구도에 있는 중국의 경우, '군민융합(軍民融合)' 전략 아래 무인 시스템, 전장 상황 인식, 다영역 작전 등에 AI를 점진적으로 적용하고 있는 것으로 파악된다. 중국이 AI를 타깃 네트워크에 대한 사전 침투(pre-positioning)의 도구로 이용하고 있다는 분석도 있다. 즉 AI 기술을 통해 특정 네트워크에 대한 지속적이고 일상적인 자동화 접속을 수행함으로써 네트워크 방어자가 접속자를 특정하거나 비정상적 활동을 쉽게 식별하지 못하게끔 하는 전략을 수행하고 있음을 뜻한다. 이러한 공격은 단기적 차원의 성과를 위한 것이라기보다 중장기적인 차원에서 서서히 공격 대상 네트워크에 침투·잠입하여 적당한 때에 막대한 피해를 초래한다는 점에서 더욱 위협적인 것으로 평가된다(Lesser 2025/06/12).

AI를 기반으로 한 중국의 사이버 작전은 그 공격 주체를 식별하기 어렵다는 점에서 미국에 큰 위기로 다가온다. 현재 중국은 민간 부문 기업과 대학 등 '비전통 방산기관'들의 사이버·AI 자원을 군이나 정보기관의 활동과 연계함으로써 제로데이 공격과 같은 침투형 사이버 작전을 활성화하고 있

다. 2017년 중국 정부가 도입한 「국가정보법(中华人民共和国国家情报法)」 등 국내법에 따라 중국 기업은 정보기관의 요청이 있을 시 사실상 협력을 거부할 수 없는 위치에 있다. 이로 인해 ICT와 AI 관련 기업과 플랫폼들은 잠재적 트로이 목마가 될 수 있다는 경고가 지속해서 제기되고 있는 것이다. 특히 최근에는 딥시크의 데이터와 알고리즘이 중국 정부의 선전 도구로 활용되고 있다는 지적도 나오고 있는데, 사용자 로그를 정부에 제공하거나 소프트웨어에 백도어를 숨기는 방식, 또는 중국 정부의 이익을 위해 AI 생성 정보를 필터링하도록 강제되고 있는 것으로 추정된다(Grealy 2025).

현재 트럼프 행정부는 군사작전의 맥락에서 사이버와 AI가 결합되는 현상에 다소 이중적인 시각을 내비치고 있다. 2025년 7월 트럼프 행정부는 「AI 행동계획」을 통해 AI가 사이버 공격과 방어 양쪽에서 그 역할을 확대해가고 있다고 경고하며 미국을 대상으로 이루어지는 적대적 사이버 작전과 AI 기술 간 연관성을 강조하였다. 그러나 또 한편으로는 대러시아 관계와 국내정치적 갈등 상황을 고려하여 사이버 안보를 영향력 공작, 선거개입, 내정간섭 등 정치안보 문제와 분리함으로써 그 범위를 군사안보 영역에 제한하려는 의도 역시 내비치고 있다. 사이버 안보 전략에서 핵심적인 역할을 담당했던 기관들의 기능을 대폭 축소한 결정은 이러한 의도에서 비롯된 것이다. AI를 매개로 중국의 기업과 대학들이 제로데이 공격과 같은 정보기관의 '침투형' 사이버 작전을 지원하는 상황에서 사이버 안보의 이슈 범위를 축소하는 이 같은 행보는 국제협력의 지평을 좁히는 결과로 이어질 수 있다는 점에서 우려를 낳는다(Chin 2025/09/03).

물론 최근 미국은 군사 분야에서 핵심 동맹국들과 사이버 안보 및 AI 관련 협력을 지속하는 움직임을 보이고 있기는 하다. 대표적으로 AUKUS 첨단기술 부문에서 영국, 호주와 사이버 및 AI를 위한 동맹 협력을 유지하고

있다. AUKUS는 트럼프 행정부의 재검토 대상 중 하나로 지목되며 그 지속 가능성이 불분명했지만, 2025년 10월 미호 정상회담을 통해 트럼프 대통령의 지지 의사가 확인됨으로써 당분간은 협력이 지속될 것으로 전망되고 있다(Caisley 2025/10/21). 또한 미국은 최근 능동적 사이버 방어체계를 구축하기 위해 「사이버대응능력강화법(サイバー対処能力強化法)」을 도입한 일본과도 협력을 증진하는 한편 공동연구를 통해 AI 기반 사이버 공격을 차단하는 방법을 함께 모색해나갈 계획임을 밝히기도 하였다. 이는 동맹국 간 정보공유, 전장 인식 및 기타 작전에 사용되는 AI 시스템을 공동으로 개발하고 또 도입함으로써 빠르게 전산화되고 있는 지휘통제통신 체계의 상호 운용성을 끌어올리려는 의도를 반영한다.

다만 이 같은 협력은 어디까지나 미국의 배타적 이익을 극대화하는 조건 아래에서만 지속되고 있으며, 그 결과 공유된 가치 기반의 협력은 점차 그 동력을 잃어가고 있다. 이는 '공세적 사이버 작전(OCO: Offensive Cyber Operations)'을 둘러싼 미국의 접근을 통해 명확히 드러난다. 2025년 7월 트럼프 행정부는 「하나의 크고 아름다운 법(One Big Beautiful Bill Act)」을 발효하였으며, 그 일부로 OCO 역량 강화를 위해 향후 4년간 10억 달러 규모의 예산을 투입할 계획을 발표하였다(Brewster 2025/7/15). 아직은 능동적 위협 차단을 위한 사이버 작전에 AI를 적용하여 그 효율성을 끌어올릴지 명확히 밝혀진 바 없지만, 진화하는 사이버 위협을 고려할 때 트럼프 행정부는 앞으로 AI를 OCO에 적극적으로 활용해나갈 것으로 전망된다. 실제로 국방 분야에서는 사이버 작전 교육 및 훈련(시뮬레이션)을 위해 AI가 이미 도입되고 있는 것으로 알려지기도 하였다.

OCO의 개발과 활용에 대한 트럼프 대통령의 이해관계는 1차 집권기에 이미 명확히 드러난 바 있는데, 당시 트럼프 행정부는 적대 세력의 사이버

공격을 원천적으로 차단하기 위해 역으로 OCO를 수행할 필요가 있음을 줄곧 강조하였다. 그 과정에서 사이버 방어의 개념을 적의 사이버 공격을 사전에 탐지하고 차단하는 선제적 방어(defend forward)와 지속적 개입(persistent engagement) 능력으로 확대하는 등 OCO의 제도적·전략적 기반을 마련한 것으로도 평가된다(김소정 2025). 트럼프 1기 행정부의 OCO 정책은 바이든 행정부 시기에도 지속되었는데, 바이든 행정부는 특히 파이브 아이즈 동맹국들과 협력하여 OCO가 국제법의 울타리 안에서 이루어질 수 있다는 인식을 대외적으로 확산시킴으로써 그 당위성을 마련해가고자 노력하였다.

문제는 현재 OCO에 대한 트럼프 2기 행정부의 접근이 그 적용 대상과 범위 측면에서 명확하지 않다는 데 있다. 앞서 언급한 것처럼, 트럼프 행정부는 정치적 이해관계에 따라 사이버 안보의 이슈연계 가능성을 의도적으로 외면하거나, 사이버 안보를 군사안보 문제로 축소하여 접근하려는 경향을 보인다. 특히 OCO의 주된 대상이 되어야 할 러시아발 사이버 공격에 대해 모호한 해석을 내놓고 있다. 그에 따라 사이버 안보 협력 역시 사안별 이익 중심의 단편적 협력의 형태로만 이루어지고 있어 동맹국과의 긴밀하고 장기적인 공조를 보장하기 어려운 상황이다. AI로 인해 사이버 위협이 양·질적으로 심화하는 가운데 미국이 보이는 이 같은 행보는 오히려 OCO를 둘러싼 동맹 중심의 협력이 제대로 이루어지지 못하게끔 하는 요인으로 작용할 수 있다. 무엇보다 중국, 러시아 등 권위주의 국가들의 사이버 위협을 염두에 두고 그동안 파이브 아이즈 동맹 차원에서 추진되어온 OCO 공조의 역할 분담, 기술협력, 규범화 담론 등이 점차 동력을 상실할 가능성도 배제하기 어렵다.

2) 정치·사회 영역

정치·사회 영역에서 미국의 안보를 위협하는 사이버-AI 넥서스는 AI 생성 허위정보를 통해 이루어지는 영향력 공작의 형태로 나타난다(Mchangama & White 2024/02/26). AI 기반 영향력 공작은 자유로운 인터넷 환경을 지향하는 민주주의 국가들의 내재적 취약점을 효과적으로 공격하여 정부에 대한 불신과 사회적 불안정을 단기간 내에 초래할 수 있다. 특히 AI 학습에 사용되는 데이터를 악의적으로 조작하는 데이터 오염(data poisoning)과 AI 모델에 대한 탈옥(jail-break) 공격이 이러한 정치·사회안보적 위협을 심화하는 원인이 되고 있다. 실제로 중국이 상업용 AI를 정보원 포섭 전략의 도구로 활용하고 있다는 분석도 제기된 바 있다. 그동안 중국은 소셜미디어 플랫폼을 활용하여 외국의 정부 관계자, 군인, 학자 등을 정보원으로 포섭하는 전략을 취해왔는데, 상업용 AI 모델이 이러한 작전의 속도와 규모 그리고 성공 가능성을 높이는 데에 도움을 제공하고 있는 것으로 알려져 있다. 이러한 전략은 정보수집(intelligence gathering)과 지식공유(knowledge sharing) 사이의 모호한 경계를 착취하는 방식으로 이루어진다는 점에서 대응이 더욱 어려운 것으로 평가된다.

바이든 행정부 집권기 미국은 AI 영향력 공작이 군사·기술·사회·경제 분야에서 국가안보 위기를 심화하고 있으며, 특히 권위주의 국가들이 AI를 악용해 생성하는 허위정보가 민주주의 기반을 위협한다고 보았다. 일례로 ODNI가 2023년 발간한 『연례위협평가』 보고서는 머신러닝과 (빅)데이터 분석 기술이 급격히 발달하면서 미국 정부와 기업 그리고 국민의 중요 데이터가 정치적 담론을 형성하는 전략 자원으로 악용되고 있다고 밝혔다. 2024년도 보고서 역시 AI를 활용한 중국과 러시아의 영향력 공작 활동이

미국의 선거를 위협하고 민주주의를 훼손할 수 있음을 경고하였다(ODNI 2024). 그러나, 재차 강조하듯, 현재 트럼프 행정부는 선거에 대한 위협을 사이버 안보와 분리하여 인식하는 경향을 보이고 있으며, 이는 AI 기반 영향력 공작 위협을 의도치 않게 탈안보화(de-securitisation)하는 결과로 이어지고 있다.

물론 2025년 3월 ODNI가 발간한 『연례위협평가』 보고서에도 중국과 러시아의 AI 기반 사이버 공격과 영향력 공작에 대한 위협인식이 담겼지만, 트럼프 행정부의 정책은 그러한 인식과는 일치하지 않는 방향으로 나아가고 있다. 트럼프 대통령은 당선 직후 CISA의 영향력 공작 및 선거 안보 관련 활동을 중단시키는 한편 ODNI 산하에 설치된 해외악성영향센터(FMIC: Foreign Malign Influence Center)의 해체 및 기능 통합을 예고하였다(Madhani, Tucker & Swenson 2025/08/21). FBI의 해외위협 전담팀 역시 해체 절차를 밟게 되었다. 이들 기관은 바이든 행정부 집권기에 영향력 공작에 대한 범정부 대응을 총괄하거나 지원하는 기관이었다는 점에서 안보적 공백을 경고하는 목소리가 작지 않다(Itkowitz, et al 2025/02/08). 이에 더하여 트럼프 대통령이 러시아에 대한 OCO 수행을 중단하도록 지시하면서 AI 영향력 공작 대응을 위한 동맹 차원의 협력도 약화될 것이라는 우려 섞인 전망도 제기된다(Nakashima & Menn 2025/03/01).

한편 NIST가 AI 시스템의 설계·개발·도입·활용 과정에서 발생할 수 있는 위험을 관리하기 위해 공공기관, 기업, 연구기관 등에 제공한 AI RMF에서 허위정보 항목이 빠지게 된 것 역시 사이버-AI 넥서스 대응을 위한 국제협력에 부정적인 영향을 미칠 우려가 있다. 바이든 행정부 시기 NIST는 EU, 일본 등 파트너국들과 AI 규제 표준 및 지침의 호환성을 높이기 위해 AI RMF를 지속해서 조율하고 맞춰나갈 계획을 내놓은 바 있다. 하지만 AI

를 활용한 영향력 공작 위협이 심화되는 상황에서 미국이 허위정보 문제를 안보 위협이 아니라 정치적으로 쟁점화하면서(Knight 2025/03/14), AI가 생성한 허위정보를 여전히 중대한 위험으로 받아들이는 동맹국 및 파트너국들과의 협력 범위가 축소될 가능성이 크다. G7의 '히로시마 AI 프로세스', EU의 「AI법」, OECD의 「AI 권고안」 등이 AI 생성 허위정보, 오정보, 딥페이크 등에 공동으로 대응할 필요성을 강조한다는 점에서 미국의 동맹외교가 전개될 공간이 줄어들 수 있다.

정치·사회 영역에서 발생하는 또 다른 사이버-AI 넥서스는 AI 학습 데이터가 오염되거나 AI 모델에 대한 탈옥 공격이 이루어지면서 유해하고 악의적인 결과물이 생성되는 문제이다. 이는 앞서 조명한 AI 기반 영향력 공작과도 밀접한 관련이 있는데, AI 시스템이 학습하는 데이터를 의도적으로 오염시켜 정치적·문화적 편향성을 키우거나, AI 안전장치를 우회하여 윤리적으로 적절하지 않은 악의적 허위정보를 생성·확산함으로써 선거개입, 내정간섭, 사회분열 등을 초래할 수 있기 때문이다. 데이터 오염과 AI 탈옥 공격은 최근 트럼프 행정부가 AI 전략의 초점을 혁신과 성장에 맞춤에 따라 더욱 심화할 가능성이 있다. 트럼프 대통령은 경제 성장에 대한 자신감의 원천으로 자신의 행정부와 기업 간 긴밀한 관계를 강조하며, 기업 친화적이고 시장 주도적인 기술 정책을 선호하고 있다. 크라치오스(Michael Kratsios) OSTP 실장 역시 "바이든 행정부는 (AI) 기술이 국가에 가져올 수 있는 피해를 분석하고 예측하는 등 약속보다는 두려움의 정신으로 이끌었다"고 비판하며 AI 규제 완화와 시장 주도 혁신을 지향하는 트럼프 행정부의 접근을 치켜세웠다(Moynihan 2025/05/08). 정부의 규제에 부담을 느끼는 산업계도 이러한 변화를 긍정적으로 평가한다(Zakrzewski & Natanson 2025/07/24).

이 같은 상황은 데이터 오염과 AI 탈옥에 대한 미국의 대응이 효과적으로 이루어지기 어려운 환경적 조건이 될 수 있다. 기업에 대한 규제를 완화하는 조치가 데이터 품질 관리 규제의 약화로 이어질 가능성을 배제하기 어렵기 때문이다. 신속한 기술 개발과 상용화에 높은 이해관계를 가지는 기업이 AI 탈옥 방어를 위한 메커니즘을 충분히 검증하지 않은 채로 기술을 제공할 위험도 크다. 탈옥은 미시적인 차원에서 반복적으로 이루어지는 기술 안전의 문제라는 점에서 이를 관리하기 위해서는 그 개발 주체인 기업의 역할이 특히 중요한데, 기업은 정부와 달리 공익을 추구할 의무가 없으므로 상황에 따라 안정성 검증에 소극적일 수 있기 때문이다.

더 큰 문제는 미국과 동맹국 간 AI 시스템과 데이터의 신뢰성·안전성·책임성에 대한 정합성이 감소하여 데이터 오염과 AI 탈옥에 대한 공동대응이 원활히 이루어지지 못하는 상황이 발생하는 것이다. 트럼프 행정부의 AI 국제전략은 기본적으로 미국의 배타적 국익을 극대화하는 거래적 협력만을 고집하는 경향을 보인다는 점에서 자국에 대한 직접적인 경제적 손실이나 안보적 피해가 발생하지 않는 이상 AI 시스템과 데이터 품질을 관리하고 규제하는 국제협력에 적극적으로 나서지 않을 가능성이 작지 않다. 이는 결국 AI 규제 거버넌스에 대한 미국의 리더십이 동맹국들의 지지를 확보하는 데 실패하게 될 위험으로 이어지며, 종국에는 다중이해당사자주의와 민주주의 등 핵심 가치에 기초한 AI 거버넌스 구축을 저해하는 결과를 초래할 수도 있다.

3) 데이터·주권 영역

끝으로, 콘텐츠를 검열하는 기술로서 AI가 도입됨에 따라 발생하게 되는

데이터 안보 문제도 미국이 당면한 사이버-AI 넥서스 차원의 위협이다(Goldstein & DiResta 2023). AI 기반 검열은 AI 산업 진흥과 치안 강화의 측면에서 분명 혜택을 제공하지만, 그와 동시에 사회적 분열과 국제적 갈등을 초래하는 양날의 검이 되고 있다. AI는 그 기술적 특성으로 인해 내재적인 편향과 환각(hallucination)에서 자유롭지 않기 때문에 콘텐츠 검열 수단으로 AI가 활용될 경우 방대한 데이터를 수집하는 과정에서 프라이버시 침해와 표현의 자유 억압 등이 발생할 수 있다. 더 큰 문제는 AI의 자동화된 데이터 수집 활동이 국경을 넘어 이루어지게 되면서 타국의 '데이터 주권(data sovereignty)'을 위협하는 문제로 이어질 수 있다는 것이다. 물론 데이터 부문에서 선두를 달리는 미국의 입장에서는 이러한 문제가 언뜻 보기에 심각하지 않은 것으로 비칠 수 있다. 하지만 미국 정부나 기업의 AI 기반 데이터 수집과 콘텐츠 검열 활동이 동맹국 및 파트너국을 대상으로 이루어진다면 이는 데이터 주권 침해나 디지털 식민주의(digital colonialism) 위협으로 인식되면서 데이터의 자유로운 이동을 옹호하는 미국 주도의 연대에 부정적인 영향을 미칠 여지가 있다. 데이터 안보 분야 미국의 리더십이 약화할 수 있음은 물론이다.

이미 미국은 사이버 위협 탐지와 콘텐츠 검열을 위해 AI를 활용하고 있는데, 2025년 1월 바이든 행정부는 사이버 안보에 대한 마지막 조치로 백악관을 통해 「행정명령 제14144호」를 발표하여 사이버 공격자에 대한 제재의 실효성 강화와 사이버 범죄 대응을 위해 AI를 활용할 필요성을 강조한 바 있다. 그리고 트럼프 행정부도 「행정명령 제143061호」에서 AI가 "사이버 취약점을 신속하게 식별하고, 위협 탐지 기술의 규모를 늘리며, 방어를 자동화함으로써 사이버 방어를 혁신할 수 있는 잠재력을 가지고 있다"고 명시하였다. 더 나아가 2025년 5월에는 플랫폼 기업에 딥페이크 콘텐츠

삭제를 요구하는 「테이크잇다운법(Take It Down Act)」이 발효되기도 하였다. 일각에서는 동 법률의 조치가 종단간 암호화(E2EE) 해체를 강요할 여지가 있으며, 동시에 공정한 논평부터 뉴스 보도에 이르기까지 합법적인 콘텐츠도 삭제 대상으로 인식하는 자동화 필터링 기술에 의존한다는 점에서 표현의 자유를 억압할 위험이 크다고 경고하고 있다(Ortutay 2025/05/21).

물론 「테이크잇다운법」처럼 AI 생성 악의적 콘텐츠의 확산을 저지하려는 조치는 EU의 「AI법」이나 영국의 「온라인안전법(Online Safety Act)」처럼 딥페이크 규제를 강화하는 한편 소셜미디어와 플랫폼 기업의 윤리적·법적 책임을 강조한다는 점에서 글로벌 AI 규범을 선도하는 미국의 위치를 확고히 하는 데 기여하는 바가 분명히 크다. 또한 파이브 아이즈와 같은 동맹 네트워크 차원에서 딥페이크 대응 공조체계를 마련하고 법제적 협력을 추진하는 과정에도 도움이 될 수 있다. 그러나 다른 한편으로 미국 기업이 악의적 콘텐츠 검열 규제를 준수하기 위해 자국 밖에서 생산·보관되는 데이터까지 감시의 대상으로 삼게 될 시, 이는 데이터 주권 위협과 같은 의도치 않은 역외적 효과를 낳을 여지가 있다. 더욱이 2018년 트럼프 행정부 1차 집권 시기에 도입된 「클라우드법(CLOUD Act)」이 이미 해외 데이터에 대한 미국 수사기관의 접근을 허용하는 근거가 되고 있다는 점에서 AI 기반 검열과 데이터 주권 침해 간 상관관계를 외면하기 어렵다(Mellor 2025/03/27). 이러한 우려는 현재 트럼프 행정부의 사이버 안보와 AI 전략이 동맹국의 사정에는 별다른 관심을 보이지 않은 채 미국의 배타적 이익을 우선하는 방향으로만 작동하고 있다는 점을 고려할 때 더욱 분명해진다.

설상가상으로 최근 중국이 자국의 값싼 AI 모델을 글로벌 사우스 국가들에 수출하며 점차 중국형 데이터 안보 거버넌스 모델을 확산하는 추세는 데이터·주권 영역에서 미국의 동맹외교를 더욱 어렵게 만드는 요인이 되고 있

다. 그동안 중국은 개별 국가의 데이터 통제 권리를 강조하는 국가주권 중심의 데이터 안보 거버넌스를 추구하며 서방 세계와 끊임없이 충돌해왔다. 2020년 중국이 발표한 「글로벌 데이터 보안 이니셔티브(全球数据安全倡议)」 역시 표면상 진영을 따지지 않는 협력을 표방하지만, 실제로는 데이터 국지화와 정부 통제를 정당화하는 논리를 담고 있다(Webster & Triolo 2020/09/07). 따라서 중국이 강조하는 데이터 주권 보호 원칙은 자국에만 적용되는 기준일 뿐 중국산 AI 모델을 수용하는 국가들의 데이터 주권을 보호하는 데에는 사실상 적용되지 않는다고 봐야 할 것이다. 앞서 언급한 것처럼 중국산 AI 모델은 국내 법령에 따라 정부의 요구가 있을 경우 사용자 정보와 데이터를 제공할 수밖에 없기 때문이다. 딥시크의 경우에도 개인정보취급방침에 사용자 데이터를 "중화인민공화국 내 보안서버"에 저장할 수 있다는 조항을 포함하고 있다(장은지 2025/01/30). 그럼에도 불구하고, 당장 프라이버시 침해나 데이터 착취를 돌아볼 여유가 없는 글로벌 사우스 국가들은 값싼 중국산 AI 모델의 실용성만을 고려하여 이를 도입하는 데 거리낌이 없다.

이처럼 중국산 AI 모델의 확산에 힘입어 데이터 주권 담론이 이전보다 더 힘을 얻고 있는 상황은 미국의 AI 기반 데이터 검열 조치가 동맹국 및 우방국의 데이터 주권을 침해할 수 있다는 우려와 맞물리면서 결과적으로 미국에 불리하게 작용할 가능성이 크다. 더 큰 문제는 바이든 행정부 시기 상당한 수준의 성과를 거둬온 민주주의 기반의 글로벌 데이터 안보협력이 축소되거나 와해될 수 있다는 점이다. 트럼프 행정부는 1차 집권기에 해당하는 2019년 일본 정부와 함께 데이터의 자유로운 흐름과 반(反)국지화(data localisation)를 촉구하는 「오사카 트랙(Osaka Track)」을 발족시켰고, '신뢰할 수 있는 데이터 유통론'을 강조했던 바이든 행정부도 이에 협력적 자

세를 유지하였다. 현재 트럼프 2기 행정부 역시 여전히 데이터 국지화에 반대하며 디지털 무역 확대를 위한 자유로운 데이터의 유통을 옹호한다는 점에서 정책적 지속성을 보이고 있지만, AI 기반 데이터 검열 조치로 인해 미국의 데이터 유통론은 데이터 식민주의와 디지털 기술 봉건주의를 위한 수단으로 곡해될 위험에 놓여있다. 이는 결국 민주주의와 인권 등 공유된 가치에 근거한 데이터 안보 거버넌스를 창출하고자 그동안 미국이 주도해 온 국제협력에 걸림돌이 될 수밖에 없다.

5. 결론

이상에서 본 바와 같이, 현재 트럼프 행정부는 기술에 대한 규제보다는 혁신과 산업적 이익을 우선함에 따라 거래적인 국제협력을 선호하고 있다. 그로 인해 사이버 안보와 AI를 위한 미국의 전략은 국제협력의 이니셔티브와 플랫폼 그리고 추진체계 면에서 빠르게 변화하고 있으며, 사이버-AI 넥서스 차원에서 발생하는 문제들에 대응하는 과정에서 동맹외교가 전개될 공간이 점점 줄어들고 있다.

물론 트럼프 행정부가 재출범 이후 첫해를 보내고 있는 지금, 미국의 사이버 안보 전략과 AI 전략은 과도기를 거치고 있다는 점에서 이 글에 담긴 분석과 전망을 기정사실로 여기는 것은 시기상조일 수 있다. 또한 사이버-AI 넥서스에 대한 동맹 중심의 국제협력도 지금보다 더 적극적으로 모색될 가능성을 완전히 배제하긴 어렵다. 트럼프 대통령의 「행정명령 제143061호」도 악의적 사이버 활동을 수행하는 국가로 중국뿐만 아니라 러

시아, 이란, 북한 등 전통적인 적대국들을 지목함으로써 바이든 행정부 집권기 사이버 안보 국제협력을 뒷받침했던 '권위주의에 대항하는 민주주의 연대' 기조가 유지될 여지를 남겨두었기 때문이다. 앞서 소개한 사이버-AI 넥서스 위협이 만약 2018년 발발한 이른바 '화웨이 사태'처럼 권위주의 국가가 연관된 특정 이슈를 계기로 쟁점화된다면, 트럼프 행정부도 민주주의 동맹 네트워크를 다시금 적극적으로 활용할 수밖에 없을 것이다.

미국과 동맹 관계에 있는 한국은 앞으로의 변화 양상을 더욱 주시해야만 한다. 사이버-AI 넥서스가 군사, 정보, 정치, 사회, 데이터, 주권 등 다양한 영역에서 초래하는 문제들은 북한과 마주한 한국에게 특히 위협적일 수밖에 없는데, 첨단기술에 대한 미국의 접근이 규제보다 혁신을, 규범보다 국익을 우선시하는 상황은 한국이 위협 대응을 위한 동맹 차원의 협력을 기대하기 어렵게 만들기 때문이다. 당장 선거개입과 허위정보 문제를 사이버 안보 분야에서 분리하려는 미국의 움직임은 북한발 대남 영향력 공작이 갈수록 심화하는 상황을 고려할 때 한국에게는 여러모로 이롭지 않다. 미국의 AI 기반 콘텐츠 검열 조치가 글로벌 플랫폼과 AI 모델을 매개로 데이터 주권을 위협하는 상황도 우리에게 부담스럽긴 마찬가지이다. 결국 사이버-AI 넥서스의 불확실성 속에서 한국에게 주어진 과제는 미국의 전략적 변화가 동맹국들에게 전가할 수 있는 비용과 위험을 면밀히 검토하는 일이라 할 수 있다.

제15장

사이버-AI 넥서스와 중국의 연대외교

박병광 | 국가안보전략연구원 수석연구위원

제15장

사이버-AI 넥서스와 중국의 연대외교

박병광 | 국가안보전략연구원 수석연구위원

1. 머리말

시진핑 주석 집권 이후 중국은 세계적 영향력을 확대하기 위해 일대일로(一帶一路, Belt and Road Initiative, BRI) 전략을 국가 핵심 프로젝트로 추진해 왔다. 시진핑은 2013년 9월과 10월 카자흐스탄과 인도네시아를 잇달아 순방하면서 일대일로 구상을 처음 제안했다. 일대일로는 시진핑이 제시한 국가발전전략 구상 중의 하나로 중국 서부-중앙아시아-러시아-유럽을 잇는 '실크로드 경제벨트'와 중국 남부-동남아시아-중동-아프리카-유럽을 연결하는 '21세기 해상 실크로드'를 건설하는 것을 일컫는다(中华人民共和国国务院新闻办公室 2023/10). 2023년 6월 말까지 150여 개 국가와 30여 개 국제기구가 일대일로에 참여하고 있으며 3회의 국제협력 정상포럼 개최를 통해 200여 건의 협력 문서가 체결되어 수많은 프로젝트와 민생에 도움이 되는 '작지만 아름다운(小而美)' 프로젝트가 형성되었다(中国经济时报 2023/10/16). 다만 최근 2023년 12월 이탈리아는 일대일로 구상에 참여한 지 4년 만에 공식 탈퇴했다.

일대일로는 초기에 육상과 해상 네트워크를 통한 교통·물류·에너지 인프라 중심의 연결 전략이었으나, 시간이 지남에 따라 점차 디지털·기술 차원으로 확장되었다. 중국은 일대일로 구상의 핵심 축으로서 '디지털 실크로드(數字丝绸之路, Digital Silk Road)' 건설을 적극 추진하고 있다(유현정 2020, 8-9). 이는 단순한 정보통신 인프라 확충에 그치지 않고 5G 통신망, 데이터센터, 인공지능 등 첨단 디지털 인프라를 구축하고 보급하여 일대일로 연선 국가들과의 디지털 연계성을 강화하고 중국 중심의 디지털 생태계를 구축하려는 전략이다. 이를 통해 기술 패권 경쟁에서 우위를 확보하고 글로벌 디지털 시장에서의 지배력을 강화하는 것을 목표로 한다.

특히 중국은 디지털 경제와 사이버·인공지능(AI) 기술을 결합하여, 일대일로 협력국의 디지털 전환과 경제 현대화를 지원한다는 점에서 주목된다. 이는 단순히 철도와 항만, 송유관 건설에 국한된 것이 아니라, 사이버 공간과 인공지능(AI)을 새로운 전장으로 삼아 중국이 세계 질서 속에서 디지털 패권을 확보하려는 시도라 할 수 있다. 중국은 자국 기업들의 기술을 해외에 보급하고, 자국식 규범과 표준을 확산함으로써 국제사회에서 미국·서방 중심의 질서에 도전하고자 한다. 중국이 추진하는 사이버 보안·데이터 통제·인공지능(AI) 감시 기술을 중심으로 한 협력은, 일대일로 참여국들에게 단순한 경제 협력을 넘어 정치·안보적 파급력을 가진다. 예를 들어 중국은 피지(Fiji)와의 치안 협력에서 차량, 통신 및 감시 장비를 제공하였으며, 파키스탄과 사우디아라비아 역시 중국의 감시·AI기술 이전·현지화 등에 대한 협력 문서를 체결한 상태이다(The Guardian, 15 Mar 2024).

이 글에서는 중국의 디지털 실크로드 전략이 사이버 및 인공지능(AI) 영역에서 어떠한 방식으로 전개되고 있는지를 분석하고자 한다. 또한 이 과정에서 나타나는 다양한 쟁점과 도전 요인을 살펴보고자 한다. 아울러 이

러한 도전과제를 해결하기 위한 중국의 전략적 선택, 예컨대 다자무대에서의 규범 경쟁, 개도국과의 정치·경제적 연대, 그리고 서방과의 협력 가능성 등을 구체적으로 평가할 것이다. 나아가 이 글은 향후 중국의 사이버-AI 전략이 어떠한 방향으로 전개될지 전망하는 동시에 한국의 입장에서 이러한 흐름에 어떻게 대응할 것인지도 중요한 과제로 제시한다.

2. 중국의 사이버-AI 연대 외교 현황과 쟁점, 도전, 과제

1) 중국의 디지털 실크로드와 사이버-AI 넥서스

중국의 디지털 실크로드 전략은 2015년부터 등장하기 시작했으며, 국제사회를 향해 공식적으로 천명된 것은 2017년에 개최된 일대일로 국제협력 정상회의이다. 동 회의에서 시진핑은 일대일로 참여국과 21세기형 네트워크 연결, 즉 정보통신기술(ICT), 전자상거래, 스마트 도시, 위성항법체계, 스마트 시티를 포괄하는 디지털 실크로드 건설을 역설했다(新华社 2015/05/15). 이후 중국은 라오스, 사우디, UAE, 헝가리, 터키 등 16개국과 디지털 실크로드 구축 양해각서 서명(2019), 카자흐스탄, 우즈베키스탄 등 중앙아시아 5개국과의 디지털 실크로드 추진 외교부 장관 회의(2020), 아세안과의 디지털 경제협력 원년 선언(2020) 등 외교적 이니셔티브를 통하여 중국 기술기업들의 해외 진출을 지원했다. 중국은 이를 통해 물리적 인프라를 넘어 데이터와 기술 표준의 글로벌 질서를 주도하려는 야심을 드러냈다.

최근 중국은 디지털 실크로드를 통해 사이버와 인공지능(AI) 분야를 전

략적 핵심 축으로 삼고 있다. 첫째, 중국은 우선 5G, 해저 케이블, 데이터센터와 같은 디지털 인프라 건설을 추진하며 파트너 국가들의 정보통신망을 자국 기술로 연결하고 있다. 글로벌 디지털 인프라에서 영향력을 확대하고 있는 것이다. 이러한 인프라는 단순한 기술 지원을 넘어, 중국의 사이버 보안 규범과 네트워크 관리 모델을 수용하도록 유도하는 효과를 낳는다. 둘째, 인공지능(AI) 분야에서도 중국은 스마트시티, 안면인식 시스템, 전자정부 플랫폼을 중심으로 신흥국에 기술을 공급하고 있다. 중국의 기술은 효율성과 편리성을 제공하는 동시에, 데이터 관리와 감시, 사회적 통제에 관한 중국식 디지털 거버넌스 모델을 내재하고 있다. 결과적으로 중국은 기술 수출과 함께 자국의 규범과 가치가 해외에 정착되도록 유도한다.

중국은 사이버와 AI를 둘러싼 국제규범 형성에도 적극 개입하고 있다. 국제전기통신연합(ITU)이나 인공지능 거버넌스 관련 다자 회의에서 '국가주권 기반의 사이버 질서'와 'AI 윤리의 국가별 차별성 존중'을 강조하며, 서구식 개방·자유·투명 모델과는 다른 접근법을 확산하려 하고 있다. 이는 단순한 기술 표준 경쟁을 넘어, 미래 사이버 공간과 AI 활용 질서에서 주도권을 차지하기 위한 전략적 행보다. 결국 디지털 실크로드에서 드러나는 사이버-AI 넥서스(Nexus)는 경제와 안보, 기술과 규범이 복합적으로 얽힌 중국의 글로벌 영향력 확장 전략의 핵심이다. 중국은 디지털 인프라 수출과 함께 사이버 규범, AI 기술, 데이터 거버넌스를 패키지로 결합하여 '중국식 디지털 질서'를 구축하려 하고 있다. 이러한 움직임은 개발 도상국에게는 새로운 발전의 기회로 다가올 수 있지만, 동시에 국제사회에서는 디지털 권위주의 모델 확산과 글로벌 거버넌스의 양극화라는 우려를 불러일으키고 있다.

2) 중국의 사이버 연대 외교 넥서스

중국은 21세기 국제질서에서 사이버 공간을 단순한 기술 기반이나 경제 활동의 장을 넘어, 국가 안보·정치 체제·사회 안정과 직결된 전략적 자산으로 인식하고 있다. 사이버 공간은 글로벌 권력 경쟁의 핵심 무대가 되었으며, 이러한 맥락에서 중국은 사이버 주도권 확보를 외교적 영향력 확대와 국제 전략경쟁에서 필수적인 요소로 간주하고 있다. 이를 위해 중국은 '사이버 연대 외교'를 적극적으로 전개하며, 기술력, 규범, 외교력을 결합한 복합 전략을 구사한다.

첫째, 중국은 국제규범 형성 과정에 적극적으로 개입하며 '국가 주권 기반 사이버 질서'를 확산시키려 한다. 이는 서구가 주장하는 개방적·자율적 인터넷 모델과 대비되는 것으로, 각국 정부가 인터넷과 데이터 흐름을 통제할 권리를 갖는다는 원칙을 강조한다. 중국은 국제전기통신연합(ITU), 유엔(UN) 산하 협의체 등 다자간 회의를 무대로 이러한 규범을 제도화하고, 사이버 공간의 새로운 질서를 주도하려는 전략을 지속적으로 추진한다. 대표적인 사례로 2022년 ITU 사무총장 선거를 들 수 있다. 비록 미국 후보가 당선되었지만, 중국은 러시아와 협력하여 기존의 다자 참여형 거버넌스 모델(multi-stakeholder model)을 다자간 정부 주도 모델(multilateral model)로 전환하려는 시도를 지속하였다(중앙일보 2023/10/24). 이러한 접근은 국제 규범의 '정치적 설계권'을 확보하려는 중국의 전략적 야심을 보여준다.

둘째, 중국은 2020년 '글로벌 데이터 안보 이니셔티브(全球数据安全倡议)'를 통해 각국이 데이터 보안을 보장받으면서 개방적이고 안정적인 디지털 공급망을 유지해야 한다고 주장하였다(新华社 2020/09/08). 이를 통해 중국은 국제 사이버 안보 및 데이터 관리 담론에서 '규범 제공자'로서의 입지를

강화하고 있다. 그러나 실제 정책을 들여다보면, 중국식 데이터 보호주의와 디지털 주권 개념을 정당화하는 성격이 강하다. 중국은 데이터 국지화와 국가 주도의 강력한 통제를 옹호하면서도, 동시에 디지털 무역과 데이터 흐름을 통한 기술 혁신을 추구하는 모순된 목표를 추구한다. 외국 기업에는 중국 내 데이터 규제를 엄격히 적용하면서도, 자국 기업은 해외에서 상대적으로 자유로운 데이터 활용을 허용하는 이중적 구조를 갖고 있다. 이는 중국의 사이버 외교가 단순한 협력이나 기술 수출에 그치지 않고, 전략적 이해관계와 권력 구조 재편을 동시에 겨냥함을 보여준다.

셋째, 중국은 양자 및 지역 차원의 연대 외교를 통해 국제적 영향력을 확장하고 있다. 대표적 사례는 일대일로(一带一路)의 디지털 실크로드 프로젝트다. 중국은 아시아, 아프리카, 중동, 중남미 국가들과 사이버 인프라, 데이터 관리, AI 기술 협력을 추진하며, 통신 장비, 스마트시티 시스템, 전자정부 플랫폼 등을 제공한다. 이를 통해 단순한 기술 수출을 넘어, 중국식 디지털 거버넌스 모델을 이식하고, 글로벌 표준과 규범에 대한 간접적 영향력을 확대한다. 특히 개발도상국들은 경제 발전과 디지털 안보를 동시에 확보할 수 있다는 점에서 중국의 접근을 전략적 대안으로 받아들이며, 결과적으로 중국의 사이버 외교 네트워크가 확대되는 계기가 된다(김영석 2024, 175-193).

넷째, 중국은 국제사회에서 '협력적 파트너' 이미지를 전략적으로 활용한다. 2022년 발표한 백서에서 중국 정부는 '사이버 공간의 운명공동체(网络空间命运共同体)' 개념을 강조하며, 사이버 범죄 대응, 테러 방지, 디지털 격차 해소 등 글로벌 의제에서 책임 있는 협력국 이미지를 부각시켰다(中华人民共和国国务院新闻办公室 2022/11). 그러나 이러한 협력적 제스처는 단순한 외교적 이미지 구축을 넘어, 서구 중심의 규범 질서에 균열을 내고

중국 중심의 연대 네트워크를 확대하려는 전략적 포석으로 해석된다.

결과적으로 중국의 사이버 연대 외교는 기술적 주도권 확보, 규범 재편, 개발도상국 연대 확대, 글로벌 디지털 질서 재구성 등 다층적 목표를 포괄하며, 국제사회는 이러한 전략이 디지털 권위주의의 확산으로 이어질지, 아니면 보다 다원적이고 균형 잡힌 사이버 협력 질서로 발전할지를 면밀히 관찰해야 한다. 중국의 사이버 외교는 단순한 기술 경쟁을 넘어 국제정치, 경제, 안보를 아우르는 새로운 게임 체인저로서, 앞으로 글로벌 질서 재편 과정에서 핵심 변수로 작용할 전망이다.

3) 중국의 인공지능(AI) 연대 외교 넥서스

중국은 인공지능(AI)을 자국의 미래 성장 동력이자 국제정치·경제 질서에서 영향력을 확대하기 위한 전략적 자산으로 인식하고 있다. 시진핑 정부는 AI 기술 개발을 국가 발전의 핵심 의제로 격상시키며, 이를 국제 협력과 외교의 새로운 의제로 적극 활용하고 있다. 이러한 움직임은 단순히 기술 경쟁력을 확보하는 차원을 넘어, 중국이 글로벌 거버넌스 구조 속에서 규범과 표준을 선도하려는 외교적 전략과 맞닿아 있다.

중국의 인공지능(AI) 연대 외교는 크게 세 가지 차원에서 전개된다.

첫째, 글로벌 파트너십의 확장이다. 2023년 10월 시진핑 주석이 '제3회 일대일로 국제협력 정상포럼'에서 '글로벌 인공지능 거버넌스 이니셔티브(全球人工智能治理倡议)'를 제안한 것도 이러한 노력의 일환이다(中國外交部 2023/10/20). 중국은 '인공지능 개발·이용 원칙'과 같은 정책적 가이드라인을 다자무대에서 제시하며, 개발도상국을 중심으로 AI 인프라 구축, 인재 양성, 데이터 협력 프로젝트를 지원한다. 이는 중국식 AI 발전 모델을 전파

하는 동시에, 중국에 우호적인 디지털 협력 네트워크를 형성하는 효과를 낳는다. 일례로 화웨이, 하이크비전, ZTE 등 중국 기술 기업들은 인공지능 기반 모니터링 시스템을 전 세계 63개국에 수출하고 있으며, 그중 36개국은 일대일로 참여국이다. 이와 함께 중국이 글로벌 파트너십을 확장하는 과정에서 일대일로(BRI) 연선 국가들과 함께 주요 대상으로 삼고 있는 것은 브릭스(BRICS) 국가들, 상하이협력기구(SCO) 참여국들이다(中國外交部 May 01, 2025).

중국은 최근 상하이에서 개최한 '세계 인공지능대회(WAIC)'에서 리창(李强) 총리가 개막식 연사로 나서 시진핑 주석이 제창한 '글로벌 AI 거버넌스 이니셔티브'를 다시금 강조하고, 중국이 선진국들뿐만 아니라 '글로벌 사우스'의 개발도상국들을 모두 아우르는 AI 발전을 이끌겠다는 포부를 밝혔다. 또한 그는 "인공지능은 소수 국가와 기업의 독점적 게임이 돼서는 안 된다"며 국가 간 기술·인재 협력과 공유를 위한 '세계인공지능협력기구' 설립을 제안했다(新華通信 2025/07/27). 이처럼 중국은 글로벌 사우스의 요구에 부응하여 디지털 격차 해소를 돕고, AI 기술이 소수 국가의 전유물이 되지 않도록 해야 함을 강조하면서 적극적으로 글로벌 파트너십을 확장하고자 한다.

둘째, 규범과 표준의 제도화이다. 중국은 AI 표준과 규범을 국제적으로 선도하려는 노력을 꾸준히 강화하고 있다. 2017년 「차세대 인공지능 발전 계획」을 발표한 이후, 중국은 자국 내 AI 산업 생태계를 육성하는 것에 그치지 않고, 국제 전기통신연합(ITU)과 국제표준화기구(ISO), 경제협력개발기구(OECD) 등 다양한 국제기구에서 AI 관련 기술 표준과 윤리 규범 논의에 적극적으로 참여해 왔다. 이러한 활동은 단순히 기술적 표준을 제정하는 수준을 넘어, 국제사회에서 중국의 영향력을 제도적으로 확대하고, 자

국의 정책 기조와 개발 이익을 국제규범 체계에 반영하려는 의도와 맞닿아 있다.

중국이 강조하는 핵심은 '책임 있는 AI(responsible AI)'라는 국제 담론 속에서도 '디지털 주권(digital sovereignty)'이라는 원칙을 중심에 두는 것이다. 즉, 각국이 AI 데이터 관리, 알고리즘 설계, 윤리 규범 수립에서 독자적인 결정권을 가져야 한다고 주장하며, 데이터와 AI 기술의 통제권을 국가별 주권 하에 두려는 입장을 일관되게 견지하고 있다. 이는 중국 내에서 이미 확립된 데이터 보안법, 개인정보보호법, 그리고 인터넷 관리 규제 체계와도 긴밀히 연결되어 있으며, 해외 협력에서도 동일한 논리를 확산하려는 모습으로 나타난다. 중국은 이러한 규범적 접근을 통해 '중국식 AI 질서'를 확산시키려 하고 있다.

셋째, AI 안보와 거버넌스 담론 주도이다. 중국은 국제안보 차원에서 AI의 군사적 활용과 사회적 안정 관리 가능성을 중시하며, '책임 있는 AI 개발'을 내세운다. 그리고 AI의 잠재적 위험에 대한 논의를 선점함으로써 향후 글로벌 거버넌스 규범 형성에서 발언권을 강화하려 한다. 일례로 최근 중국군 기관지인 『해방군보』는 휴머노이드 로봇의 무차별 살인 가능성을 경고하며, 군이 도덕적 함정을 피하기 위해 휴머노이드 로봇의 사용을 규제하고, 휴머노이드 로봇에 대한 윤리적, 법적 연구를 수행해야 한다는 취지의 주장을 펼쳤다(解放軍報 2025/07/10).

중국은 AI 윤리와 거버넌스를 둘러싼 국제 담론에서 미국과 서구 진영에 대한 대안을 제시하고 있다. 중국의 글로벌 담론은 언제나 인권과 같은 서구식 '보편가치'보다는 주권국 간의 동등한 권리와 기회를 강조해 왔다. 중국과학기술부는 2021년 「차세대 AI 윤리 규범(新一代人工智能伦理规范)」을 발표하였다(中华人民共和国科学技术部 2021/09). 그러나 중국이 제시하는

「차세대 AI 윤리 규범」은 서구가 강조하는 개인 자유와 데이터 프라이버시보다는 집단적 이익과 국가 중심의 관리 기조를 부각한다. 이는 AI가 국가의 통치 역량 강화와 국제적 협력 도구로 활용될 수 있음을 보여준다.

이처럼 중국의 AI 연대 외교 넥서스는 기술적 협력과 제도적 규범, 안보 담론을 포괄하는 종합적 접근으로 요약할 수 있다. 이는 단순한 기술협력 차원을 넘어, AI를 매개로 한 글로벌 영향력 확대와 외교적 연대 강화의 전략적 수단이다. 향후 중국은 디지털 실크로드와 AI 연대 외교를 결합하여, 국제질서 속에서 새로운 '중국식 디지털 질서'를 구축하려는 시도를 지속할 것으로 보인다. 또한 중국은 AI 기술 수출, 표준 설정, 윤리 담론, 개발협력 등을 통해 글로벌 AI 네트워크에서 영향력을 확대하고 있으며, 이는 향후 국제사회에서 미중 간 AI 주도권 경쟁의 중요한 축으로 작용할 전망이다.

4) 중국의 사이버-AI 연대 외교 넥서스의 쟁점, 도전, 과제

중국은 디지털 실크로드 전략을 확대하며 사이버 공간과 인공지능(AI)을 글로벌 외교 자산으로 적극 활용하고 있다. 특히 '연대 외교'를 통해 개발도상국과의 협력망을 강화하고, 데이터 및 AI 규범을 선도함으로써 국제질서에서 주도권을 확보하려는 시도가 본격화되고 있다. 그러나 이러한 과정은 순탄치 않으며, 기회 못지않게 여러 쟁점과 도전을 동반한다.

우선 가장 뚜렷한 쟁점은 '디지털 주권과 글로벌 규범의 충돌'이다. 중국은 국가가 데이터와 인터넷을 통제할 권리를 강조하며, 이를 기반으로 국제적 규범을 형성하려 한다. 반면 미국과 유럽은 자유로운 데이터 흐름과 개방적 디지털 환경을 중시한다. 결과적으로 국제사회는 두 모델 간 균열

을 경험하게 되며, 중국의 접근은 일부 개발도상국에는 매력적이나, 서구권 국가들에는 규범적 저항과 신뢰 부족을 초래한다.

또 다른 민감한 쟁점은 'AI의 군사적 활용'이다. 중국은 '군민융합' 전략 아래 AI를 안보·군사 영역에 적극 적용하며, 미래전을 지능화 전쟁(Intelligentized Warfare)으로 전망하고 있다. 2017년 시진핑 주석의 19차 당대회 연설에서 강조된 이 전략은 AI, 우주, 사이버 역량을 집중적으로 발전시키는 데 초점을 맞춘다. 중국군은 AI와 무인체계를 활용하여 지능화 군대로 거듭나려는 의지를 표출하며, 이를 통해 전투 효율성과 정보우위 확보를 꾀한다(나호영·최근대 2020, 91-118). 그러나 국제사회는 이를 군비 경쟁과 안보 긴장 확산의 불씨로 바라보며, '책임 있는 AI 개발'이라는 중국의 공식 입장과 실제 군사적 활용 간 괴리를 문제 삼는다.

여기에 더해, 중국의 AI 및 사이버 외교는 기술 표준과 산업 경쟁의 영역에서도 논란을 일으킨다. 중국은 자국 기업을 중심으로 글로벌 AI 플랫폼과 데이터 관리 체계를 확산하며, 표준화 과정에서 우위를 확보하려 한다. 이는 개발도상국과의 기술협력을 매개로 영향력을 확대하는 한편, 미국·유럽과의 산업·규범 경쟁을 심화시키는 요인이 된다. 나아가 개인정보 보호, 데이터 이동 자유, AI 윤리 등 국제 규범의 조화 문제 역시 불거지며, 글로벌 사이버-AI 연대 외교의 신뢰성과 지속 가능성에 의문을 남기고 있다.

이 과정에서 중국이 직면하는 도전도 뚜렷하다. 중국에 대한 '기술 신뢰성 문제'는 여전히 발목을 잡는다. 특히 중국산 장비에 대한 국제적인 신뢰 우려는 중국 정부의 정보 접근 및 사이버 보안 위협 가능성에서 비롯되며, 특히 통신 및 네트워크 장비에서 이러한 우려가 크다. 주요 쟁점은 중국 정부가 자국 기업 장비를 통해 데이터에 접근하거나 조작할 수 있다는 점과, 해커 공격의 통로로 악용될 수 있다는 점이다. 이에 따라 미국, 독일 등 여

러 국가에서 중국산 통신 장비 사용을 제한하거나 퇴출하는 정책을 추진하고 있으며, 이는 국가안보 및 사이버 안보 강화 목적의 규제 강화로 이어지고 있다.

영국은 5G 네트워크에 중국 통신장비(화웨이 등) 사용을 전면 금지했고, 독일도 핵심 부문의 중국산 장비 의존도를 낮추고, 네트워크 장비 내 중국산 부품에 대한 전면 조사를 진행하며 신뢰할 수 있는 다른 기술로 전환하려는 움직임을 보이고 있다(연합뉴스 2025/07/17). 미국 역시 연방통신위원회(FCC)가 중국 기술이 포함된 해저 통신 케이블의 미국 연결을 금지하는 규정을 도입하고, 중국산 인터넷 공유기 판매를 금지하는 방안을 검토하는 등 중국산 장비에 대한 규제를 강화하고 있다(중앙일보 2024/12/18). 한국의 경우도 한국인터넷진흥원(KISA)의 로봇청소기 보안 조사 결과에서 드러난 허술한 인증 체계 및 암호화되지 않은 데이터 전송과 같은 실질적인 보안 리스크 사례를 통해 중국산 기기에 대한 신뢰성 문제가 제기되고 있다.

사이버와 AI 분야에서 중국에 대한 국제사회의 '정치적 신뢰 부족'도 부담이다. 중국의 모델은 종종 '디지털 권위주의'로 불리며, 민주주의 국가들과의 협력 기반을 약화시키고 있다. 중국이 강조하는 거버넌스의 주요 원칙에는 개인정보 보호는 물론이고 각국의 주권, 법체계를 존중해야 하며 모든 국가가 그 규모나 국력, 사회체제와 무관하게 인공지능의 개발 및 이용에서 동등한 권리를 가져야 한다는 점도 강조하고 있다. 그러나 중국은 국가안보를 명분으로 공안이 특별한 제동장치 없이 개인정보나 알고리즘에 언제나 접근, 간여할 수 있는 나라이다. 중국에서는 개인을 보호하기 위한 원칙의 실현이 어려우며, 모든 국가가 인공지능의 운용에 있어서 독자성을 인정받아야 한다는 것은 사실상 인공지능의 남용을 '주권'이라는 이름 하에 허용해야 함을 의미하는 것이다(중앙일보 2023/11/09).

여기에 더해 반도체와 첨단 칩 같은 핵심 부품에서 '미국의 규제와 압박'을 받는 것은 중국의 장기 전략에 구조적 한계를 드러낸다. 미국은 첨단 반도체와 칩의 중국 유출을 막기 위해 2022년부터 수출을 금지하고, 2024년 이후에는 알리바바 같은 중국 기업의 블랙리스트 등재와 우회 수출 차단을 위한 위치 추적기 도입 등 규제를 강화하며, 삼성전자와 SK하이닉스 같은 동맹국 기업의 중국 공장 장비 수출에도 개별 허가제를 적용하는 등 압박을 지속하고 있다(조선일보 2025/08/14). 미국은 첨단 반도체가 중국의 군사 기술 발전에 사용될 수 있다는 점을 우려하여, 이를 차단하기 위해 규제를 강화하는 것이다. 또한 미국은 중국의 첨단기술 자립 시도에 대응하고, 자국 반도체 산업의 경쟁력을 강화하며 공급망을 재편하려는 목적으로 중국에 대해 강력한 규제를 시행하고 있다.

그렇다면 중국의 과제는 무엇일까. 중국의 사이버와 인공지능 연대외교에서 당면한 과제는 단순히 기술 경쟁을 넘어 국제규범과 신뢰 구축의 문제로 귀결된다. 첫째, 국제규범 조율 능력을 키우는 것이 무엇보다 필요하다. 지금까지 중국은 사이버 주권과 데이터 안보를 강조하며 '중국식 모델'을 제시해 왔지만, 이는 종종 폐쇄적이고 국가 통제적이라는 비판을 받아왔다. 글로벌 거버넌스 무대에서는 일방적 강요보다는 다양한 이해관계자들과의 협력과 타협이 필수적이다. 예컨대 유엔 산하 인공지능 윤리 논의, OECD의 디지털 거버넌스 협의체 등에서 중국이 적극적으로 다자협력의 모습을 보여야 규범 형성 과정에서 배제되지 않을 수 있다.

둘째, 투명성과 개방성 강화가 시급하다. 중국식 AI 모델이 불투명하고 정치적 목적에 따라 설계되었다는 국제적 인식은 이미 광범위하게 퍼져 있다. AI 알고리즘의 신뢰성과 데이터 활용의 투명성을 확보하지 못한다면, 글로벌 파트너십 구축은 물론 국제 표준 경쟁에서도 불리한 위치에 설 수

밖에 없다. 중국이 주도하는 '디지털 실크로드' 프로젝트가 일부 국가에서 신뢰 부족으로 저항을 받는 것도 같은 맥락이다. 따라서 중국은 국제 사회가 납득할 수 있는 수준의 데이터 관리 기준, 알고리즘 감사 체계, AI 윤리 규범을 일정 부분 수용할 필요가 있다.

셋째, 균형 외교가 필수적이다. 중국은 그동안 글로벌 사우스 국가들과의 디지털 협력, 즉 개발도상국을 중심으로 한 연대 구축에 힘써 왔다. 이는 단기적으로는 지지 세력을 확대하는 효과가 있지만, 장기적으로는 서구와의 최소한의 협력 없이는 규범 경쟁에서 승리하기 어렵다. 특히 AI 기술의 핵심은 반도체, 클라우드, 초거대 모델 등에서 여전히 미국과 유럽의 강력한 영향력이 작동하고 있다는 점에서, 중국이 완전히 대체적 체제를 구축하기는 쉽지 않다. 따라서 서구와 일정 수준의 협력과 기술 교류를 병행하면서도, 개발도상국과의 연대를 통해 다극적 질서를 지향하는 '투트랙 전략'이 요구된다.

중국의 사이버-AI-연대 외교 넥서스는 분명 기회와 위험을 동시에 안고 있다. 기회의 측면에서 보자면, 중국은 세계 최대의 데이터 시장과 빠른 AI 상용화 능력을 무기로 글로벌 디지털 질서의 강력한 축으로 자리 잡을 잠재력이 크다. 만약 중국이 개방성과 협력을 일정 부분 수용하고, 자국의 디지털 인프라 경험을 국제 공공재로 제공한다면, 아시아·아프리카·중남미 지역에서 '디지털 리더십'을 공고히 할 수 있다. 그러나 위험의 측면도 만만치 않다. 강압적이고 배타적인 접근을 고수한다면 국제사회에서 불신이 커지고, 이는 곧 중국이 스스로 고립을 심화시키는 결과를 초래할 것이다.

결국 중국의 선택이 향후 글로벌 디지털 질서의 향방을 좌우하게 될 것이다. 규범 경쟁과 기술 패권 경쟁이 동시에 전개되는 현 시점에서, 중국이 협력과 개방을 전략적으로 활용할 수 있을지, 아니면 안보 논리와 폐쇄성

에 갇힐지는 국제사회의 주목을 받는 대목이다. 디지털 질서의 미래는 단순히 기술의 문제가 아니라, 국제정치적 신뢰와 규범적 정당성 확보의 문제라는 점에서, 중국의 행보는 향후 수십 년간 국제사회의 구조적 변화를 결정짓는 중요한 변수로 작용할 것이다.

3. 맺음말 : 전망과 대응 방안

중국의 사이버-AI 연대 외교는 기술·규범·외교가 유기적으로 결합된 전략으로 더 정교해질 것이다. 중국은 디지털 실크로드와 국가데이터국 등 제도적 기반을 바탕으로 기술 수출(5G·데이터센터·스마트시티)과 규범 제안(데이터 주권·글로벌 데이터 보안 이니셔티브)을 병행하며 영향력을 확장해 왔다. 앞으로는 단순한 인프라 제공에서 더 나아가 AI 표준·윤리·거버넌스 분야에서 주도권을 노리는 단계로 진화할 가능성이 크다. 최근 중국이 AI 표준화 기구와 글로벌 거버넌스 구상을 적극적으로 제시하는 움직임은 이러한 방향성을 뒷받침한다. 결과적으로 중국의 사이버-AI 연대 외교는 기술적·군사적·규범적 차원을 동시에 아우르는 복합 전략으로, 국제사회는 이를 기회로 볼지, 아니면 디지털 권위주의 확산과 군비 경쟁으로 이어지는 위험으로 평가할지를 면밀히 가늠해야 하는 상황이다.

중국이 사이버-AI 연대 외교의 넥서스 주도권 확보를 위한 기술·제도·외교의 결합은 다음의 몇 가지 방식으로 나타날 것이다.

첫째, 중국은 파트너국들에 자국 기술(감시·스마트시티·전자정부)을 수출하면서 그 활용 규범(데이터 국지화·국가 주권 우선 규범)을 함께 전수하는 '패키

지형' 접근을 계속할 것이다. 이는 파트너국의 정책·운영 모델을 중국 쪽으로 기울게 만드는 구조적 영향력을 만든다(Joshua Kurlantzick December 18, 2020). 이는 기술적 협력만이 아니라 거버넌스 모델까지 확산되는 형태로, 중국이 국제사회에서 디지털 권위주의의 주요 공급자로 자리매김할 수 있음을 보여준다.

둘째, 국제규범 경쟁은 격화될 것이다. 중국은 ITU·UN 등 다자무대와 독자적 포럼을 통해 '국가 주권'과 '데이터 보안' 명목으로 규범을 확산하려 하고, 서구의 개방·다중 이해관계자 모델과의 충돌은 지속될 전망이다. 이 경쟁은 규범의 '지역화·분절화'를 초래할 수 있다(Chaeri Park March 31, 2022). 중국식 모델과 규범은 개도국·비동맹국에서는 확산될 수 있으나, 선진국 블록과의 협력에서는 구조적인 한계를 지닐 수밖에 없다.

셋째, 중국식 모델을 받아들이는 국가가 늘어날 가능성이 있다. 특히 디지털 인프라와 자금, 그리고 기술적 역량에 대한 수요가 큰 개발도상국에서는 중국의 제안이 상당히 매력적으로 작용할 수 있다. 중국은 '일대일로(一帶一路)' 구상과 연계하여 통신망, 데이터 센터, 클라우드 서비스, 인공지능 응용 기술 등을 패키지 형태로 제공하고 있으며, 여기에 장기 저리 대출이나 재정 지원을 결합함으로써 수용국 정부의 부담을 완화시킨다. 이러한 접근은 선진국 기업이 제공하는 고비용·고규제 모델에 비해 상대적으로 '저비용·고속도·정책 일관성'을 보장하기 때문에, 빠른 디지털 전환을 추구하는 개도국 정부 입장에서는 현실적인 대안으로 인식될 수 있다. 더 나아가 중국식 모델은 정치·사회적 통제 역량을 강화하려는 일부 권위주의적 성향의 국가들에게도 유용하게 받아들여질 가능성이 크다.

우리는 단순히 중국의 사이버-AI 연대외교 넥서스에서 그들의 영향력 확산을 저지하는 데만 집중해서는 곤란하다. 동시에 한국의 기술·거버넌

스 역량을 키워 국제규범 경쟁에서 실질적 대안을 제시하는 것이 필요하다. 이를 위해 다음 네 가지 축을 균형 있게 추진할 필요가 있다. 첫째, 국제규범과 표준경쟁에 적극 참여하여 다자무대에서의 영향력과 주도권을 일정 부분 확보한다. 둘째, 핵심 반도체·AI 칩·고성능 컴퓨팅 등 필수 기술의 국산화와 다변화를 추진하고, 우방국과 안정적인 공급망 협력체(안전벨트)를 구축한다. 셋째, 아프리카·아세안·중앙아시아 등에서 디지털 인프라 구축, 인재 양성, 표준 교육, 사이버 보안 지원 등을 통해 중국의 제안과 경쟁할 수 있는 '가치동맹'을 확장한다. 넷째, 규범·거버넌스·보안 분야에서 동맹국 및 파트너와 공동 원칙을 마련하고, 기초연구·표준화·인력 교류 등 공동사업을 추진해 중국의 규범 공세에 대응한다. 이러한 방향으로 준비할 때, 한국은 다가오는 디지털 규범 경쟁에서 유의미한 행위자가 될 수 있을 것이다.

제16장

사이버-AI 넥서스와 국제규범 형성

유준구 | 세종연구소 안보전략센터장

제16장

사이버-AI 넥서스와 국제규범 형성

유준구 | 세종연구소 안보전략센터장

1. 머리말

국제안보 맥락에서의 사이버안보 논의는 2000년대 초반부터 유엔정보안보전문가 그룹(UNGGE)를 중심으로 비교적 오랜 기간 지속되었다. 반면 AI에 대한 글로벌 거버넌스 및 관련 국제규범 논의는 2020년대 OECD가 AI의 윤리적 원칙을 제시한 이후 최근에 논의가 본격적으로 진행되고 있다. 이는 관련 신기술 발전에 시간적 차이로 인한 당연한 결과이지만 사이버와 AI는 컴퓨팅, 네트워크, 소프트웨어 등 여러 부분에서 기술적 토대와 적용이 유사하다. 또한 AI의 범용성으로 인해 AI는 사이버 활동에 다양한 형태로 활용되고 있는 바, 이에 따른 새로운 형태의 위협이 증대되고 있다. 따라서 사이버-AI를 연계·융합하여 이러한 위협에 대응하기 위한 국제규범 논의가 필요하다는 것은 일견 당연한 과제일 것이다.

그럼에도 불구하고 사이버-AI 넥서스 국제규범 형성 시 양 기술의 속성 및 규범 구조의 차이로 인해 상당히 복잡한 난제를 해결해야 한다. 우선 기술적 속성의 경우 AI가 도구적 성격이 강한 기술인 반면 사이버는 ICT라는

보다 범위가 큰 섹터적 관점에서 접근하는 경향이 현저하다. 이는 AI가 사이버에 포함되어 다루어질 수 있다는 의미이며 실제 그러한 방향으로 국제규범 논의가 진행되고 있다. 규범 구조와 관련해서는 사이버의 경우 다양한 사이버 활동으로 인한 위협 및 취약성을 해결하는 것이 국제규범 논의의 핵심 과제인 반면, AI는 현재 위협 관점에서 접근하기보다 AI의 내재적 혹은 활용 시 발생되는 위험을 중심으로 논의가 시작되고 있다. 이러한 논의 수준의 시간적 격차와 접근 방식의 차이는 양 기술의 연계·융합적 규범 논의를 어렵게 하는 주요한 원인이기도 하다. 또한 이중용도성이라는 난제를 해결하는 것도 어려운 과제이다. 즉 사이버는 위협에 대응한다는 차원에서 국제안보 맥락에서 범주화하여 논의가 진행되고 있지만, AI는 상업적 활용과 군사적 활용을 명확히 구분하여 거버넌스 및 규범 논의가 전개되고 있어서 현재로서는 범주화를 통한 논의가 이루어지지 않는 상황이다. 물론 AI의 위협이 본격적으로 가시화될 경우 범주화 문제는 어느 정도 해결될 수 있으며 AI의 역시 사이버안보와 같이 국제안보 맥락의 접근이 가능할 것으로 예상된다. 또한 AI는 "자율살상무기체계(Lethal Autonomous Weapon Systems)"에 대한 규제를 중심으로 무기체계 논의가 먼저 시작된 관계로 군사적 이용과 관련해서도 논의의 범위(scope)를 결정해야 하는 과제도 남아 있다.

끝으로 '규범의 파편화'라는 국제법의 '고전적' 문제도 발생할 수 있다. 특히 AI를 구성하는 데이터, 컴퓨팅, 알고리듬/모델의 경우 각기 다른 현안을 바탕으로 논의가 개별적으로 진행되고 있다. 또한 각각의 현안에 대해 국가·진영 및 다중이해관계자간 이해관계가 상당히 대립되고 있어서 이러한 분절적·파편적 논의가 지속·심화될 가능성이 높다. 이러한 상황에서 사이버-AI의 연계·융합적인 국제규범 형성 논의는 더더욱 어려운 것도 사실

이다. 다만 AI 기술을 활용한 사이버 위협이 고도화하는 상황은 이에 대한 대응 역시 시급할 수 밖에 없다. 이러한 현실적 필요로 인해 종국적으로 사이버-AI 넥서스 국제규범 논의를 추동할 것이며 향후 국제안보 맥락에서 논의가 수렴될 가능성이 높다. 이에 본고는 우선 사이버-AI 넥서스 국제규범 논의의 배경 및 특성의 분석을 통해 관련 쟁점과 현안 및 과제를 평가한다. 이에 대한 논의를 바탕으로 향후 국제규범 형성의 방향을 전망하고 끝으로 한국이 고려해야 할 정책적 시사점과 고려 사안을 제시해 보고자 한다.

2. 사이버-AI 넥서스 국제규범 형성 논의의 배경과 특성

최근 사이버, 우주, AI 등 신기술의 급속한 발전에 따라 특정 신기술에 대한 글로벌 거버넌스 논의가 심화되고 있으며 관련 국제규범 형성 논의 또한 글로벌, 지역, 국가 차원에서 빠르게 제안되고 있다. 즉 글로벌 거버넌스 기구 신설, 표준 설정 및 규범 창설이 핵심 의제로 논의되는 상황에서 향후 국제법 및 규범 논의에 대한 대응이 필요한 시점이다. 또한 개별 국가 차원의 법안 수립이 빠르게 추진되고 있으며 미국, EU 등 개별국가 및 지역 차원의 법을 다자화하고 있다. AI 거버넌스 논의 이면에는 미·중 및 주요국 간 기술패권 경쟁이 있는 바, 기술 강국들은 자국의 기술혁신을 촉진하면서 경쟁국의 기술 습득은 제한하는 수단으로서 표준 및 규범경쟁을 가속화하는 경향이 현저하다(김상배, 2025). 국제표준 및 규범 설정 문제는 신기술이 보편적으로 확대될 경우 나타나는 일반적 현상이기도 한데, 인류에 혜

택을 제공함과 동시에 안보 및 군사분야의 적용 시 기술의 내재적인 파괴적 속성이라는 신기술의 양면성에 기인한다(유준구, 2024).

문제는 신기술의 경우 군사안보 및 경제산업에 적용되는 이중용도 특성으로 인해 즉각적인 융합이 가능함은 물론 최근에는 신기술 간 연계·융합되어 활용된다는 점이다. 특히 이러한 기술 간 융합 현상의 경우, 국제규범 논의에 있어서 여러 복잡한 문제가 발생하는 바, 개별 신기술의 국제규범이 응고 과정에 있는 상황에서 자칫 규범 형성이 지체되는 결과를 초래할 수 있다. 이러한 점을 감안하여 UN GGE 논의 당시 다른 신기술과의 연계의 경우 emerging technologies를 통칭하여 규정하였으며 AI를 포함할지에 대해서 국가 간 입장이 상이하였다(유준구, 2020). 신기술 분야에서 비교적 일찍 논의가 시작된 사이버의 경우 20여 년이 지난 현재 글로벌 차원에서 다수의 국제법 및 국제규범 문서가 도출되었다. 물론 사이버의 경우도 ICT 기술의 발전에 따른 새로운 위협 형태 등도 계속해서 진화·발전됨에 따라 규범의 대상, 양태, 이행 및 대응이 점차 확대되고 있다. 반면, AI는 비교적 최근에 거버넌스 논의가 시작된 관계로 국제규범 논의는 특정재래식무기협약(CCW)상 자율살상무기체계 논의를 제외하고는 원론적 수준에 머물러 있었다. 그러나, 2020년 이후 주요 기술강국들이 앞다투어 AI 전략 및 정책을 발표하고 법제 정비를 시작하면서 글로벌 차원의 거버넌스 및 규범 형성 논의가 급속히 진행되고 있는 상황이다. 즉 LAWS GGE는 조약 성안을 전제로 논의가 진행중에 있으며, 지역적 차원의 EU AI Regulation, 최초의 다자조약인 2024년 Framework Convention on AI(Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law)이 채택되었다.

사이버와 AI 공히 컴퓨팅 및 소프트웨어 기반 기술이라는 점에서 기술적

유사성이 크며, 정보 및 데이터가 투입·산출된다는 점에서도 기술적 목적 역시 동일할 수 있다. 다만 인공지능을 인간지능과 비교하여 접근하는 것에 대한 문제점이 제기되고 있는 바, 기존 인공지능의 정의 방식은 미국의 '정치적 선언'에서 처럼 AI를 인간지능을 필요로 하는 작업을 수행하는 기계의 능력을 의미하는 것으로 이해하고 있다. 또한, 자율성의 경우, 활성화 후 추가적인 인간 개입 없이도 시스템이 동작하는 것으로 개념화하고 있다(Political Declaration, 2023). 반면 최근 업데이트된 OECD AI시스템 정의의 경우 인간지능 요소와 무관하게 투입(input)을 통한 결과물의 산출(ouput)과 관련한 '기계기반 시스템'(machine-based system)으로 정의하고 있으며 상기 정의 방식은 미국 국가인공지능구상법(NAIIA, 2020)의 AI 정의를 준용한 것이다(OECD, 2024). 중요한 점은 AI 기술은 매우 다양한 분야에서 특정화된 목적을 위해 활용·적용될 수 있는 점에서 기술적 범용성 및 확장성이 크고 사이버와 같은 도메인이나 섹터가 아닌 도구로서의 기술 차원에서 그 의미가 크다. 따라서, 상기 관점에서 보면, AI 시스템과 기술은 cross-cutting 하기보다는 다른 도메인이나 섹터로 통합될 가능성이 높으며 규범적 방향성도 범주화되거나 다른 분야 및 도메인으로 파편화되어 논의될 가능성이 상당하다. 사이버, 우주, AI의 기술적 범위를 규정하려는 논의와 관련 도구(tool), 도메인(domain), 분야(sector)로 각기 분류하려는 경향이 있는 바, AI는 tool, 우주는 domain, 사이버는 sector 관점에서 보고 있다. 상기 이슈는 주요기반시설 지정 및 보호와 연계되는 문제이다.

3. 연계 규범 형성 시 현안 및 쟁점

사이버 AI 규범 넥서스의 경우 우선 고려해야 할 점은 각기 규범 구조의 강조점이 다르다는 것이다. 사이버 규범 체계는 오랜 논의 끝에 사이버 공간이 '무법적(lawless)'이지 않다는 전제로 국제법의 적용을 강조하면서, 사이버 공간 및 인프라에 대한 위협요인을 확인하고 이를 방지·완화하기 위한 이행을 중시하는 규범을 채택하였다. UNGGE 논의 초기에는 사이버 안보 관점에서 위험(risks), 위협(threats), 취약성(vulnerability)을 통합하여 논의하였으나, 이후 사이버 공간의 위험과, 취약성에 대한 공통의 인식이 확립된 이후부터는 위험을 초래하는 현존·잠재하는 위협을 중심으로 논의하였다(The 4rd UNGGE Report, 2015). 반면 AI는 기술 활용에 있어 발생할 위험을 중심(risk-based approach)으로 의미 있는 인간통제를 강조(human centered approach)하면서 금지 v. 규제 중심의 규범 구조가 형성되었다. AI의 상업적 활용의 경우, EU AI Act처럼 AI가 적용 시 발생가능한 위험 수준을 고려하여 금지되는 영역과 규제되는 영역을 구분하여 규율하고 있다. 반면 군사적 활용과 관련하여서는 LAWS GGE에서 "의미 있는 인간통제(meaningful human control)" 여부에 따라 완전자율무기(금지) 부분자율무기(규제) 방식의 규범 구조를 유지하고 있다(유준구, 2019). 이러한 접근 방식은 AI 분야는 기술의 이중용도성에도 불구하고 규범 구조가 다르며 아직 위협을 논의하는 수준에 이르지 못하고 있다는 것을 시사한다. 향후 AI 기술을 활용한 다양한 방식의 위협이 구체화되는 상황에서 위협에 대한 논의가 이루어질 수 있다는 의미이다. 따라서 사이버-AI 연계 시 규범 구조의 목적 차원에서 위협과 위험을 통합하여 다루어야 하는 문제가 발생한다. 현 단계에서는 사

이버 안보로 cross-cutting 돼서 논의가 이루어지는 만큼, "AI에 기반한 사이버 위협(AI driven cyber threats)"을 중심으로 논의되는 경향이 뚜렷하다.

사이버-AI 규범 넥서스에서 고려할 또 다른 쟁점은 AI의 규범화가 파편화되어 형성된다는 점이다. AI는 상업적 이용과 군사적 이용을 분리해서 규범화가 논의되고 있으며 군사적 이용의 경우도 무기체계 논의가 별도로 논의되고 있다. 다만 최근 논의 동향은 점차 상업적 안전-국제안보-군사안보의 스펙트럼에서 점차 국제안보로 수렴화되는 경향이 있으며 머지않아 사이버 안보 규범 논의와 일정한 유사성을 보일 것으로 전망된다. 따라서 현재로서는 AI 논의의 규범의 범위 설정이 주요한 쟁점으로 부상하고 있다. 같은 맥락에서 AI 시스템의 구성 부분이 컴퓨팅, 알고리즘/모델, 데이터의 세 부분인바, 규범 형성 역시 세 분야로 구분되어 각기 다른 법규범 레짐이 구체화되고 있다(유준구, 2025-10).

우선, 데이터의 경우 개별국가 혹은 양자, 소다자 지역협정에서 데이터 이전, 데이터 안보 관련 국제법이 성안되고 있으며 OEWG에서도 최종보고서에 데이터 안보의 중요성을 강조하고 있다(OEWG Report, A/AC.292/2025/CRP.1). AI 관련 데이터 거버넌스의 경우 상대적으로 여타 쟁점보다 지속적인 논의가 있었던 쟁점인 바, △데이터의 자유로운 이동과 활용을 강조하는 미국, △주권에 따른 데이터 통제를 중시하는 중국과 개도국, △인권 및 개인정보보호차원의 규범을 선도하는 유럽 간 입장이 상이하다. 상기 데이터 이동과 별도로 데이터 자체의 안전성 및 데이터 처리로부터 데이터의 오염 및 위험 완화, 데이터가 외부로부터 훼손될 수 있는 가능성 등 데이터 안전 및 안보의 문제가 최근 AI와 연계되어 논의되고 있다(김상배, 2024). 특히 데이터 처리 시 위험 문제의 경우 GDPR 제35조 4항에서 규정하고 있는데, 데이터 처리의 위험성 여부를 판단하여 관련 기업들

을 블랙리스트 분류를 하고 있다. 이에 대해서는 인도 등 많은 신흥국들이 동 조치가 일종의 규제 장벽으로서 기능한다고 비판한다. 동 사안은 데이터가 결국 알고리즘을 통한 처리 문제로 AI와 ICT가 연계되는 핵심 이슈이기도 하다.

컴퓨팅의 규범 논의는 기존 수출통제 등 경제안보 이슈로 미중 간 이해가 첨예하게 대립되는 영역으로 글로벌 공급망 논의와 긴밀히 연계되어 있다. 또한, 미·중 AI 패권경쟁에서 미국이 우월적인 지위를 누리고 있는 영역으로 미·중 공히 국가전략의 핵심 의제로 접근하고 있으며 트럼프 2기 행정부에서 발표한 AI 행동계획에서도 강조되고 있다(유준구, 2025). AI 시스템 구성 요소로 컴퓨팅 분야는 데이터나 알고리듬과 달리 '경쟁적인 유형재화(rivalrous tangible good)'로 상당히 배제적인 특성을 지니고 있으며 글로벌 거버넌스 및 규범 차원에서는 기술 및 수출통제 적용, 공급망 안전성, 기술표준화 등이 주요 쟁점이다. 이와 관련 미국은 자국 정책 및 법제의 다자화 작업을 적극적으로 추진하고 있는 반면, 중국은 미국의 기술통제에 대한 대응 전략을 강화하면서 미국의 글로벌 거버넌스 리더쉽이 소극적인 상황을 이용하여 거버넌스 주도권 확보에 적극적이다. 최근 AI 거버넌스 논의에서 핵레짐을 모델로 하는 AI 컴퓨팅 거버넌스 구상이 주목되고 있다. 기본 발상은 우라늄 원료 채굴 → 우라늄 정광 → 원심분리기를 통한 농축 → 저농축, 고농축 우라늄 추출 과정을 chip 물질 → 반도체 소자 제조 → 반도체(마이크로칩) → 데이터센터 훈련 → 저사양, 고사양 AI 모델 구축 과정과 비교되어 거버넌스 논의를 구상하는 경향이 있다. 즉 생산, 이전, 제조 전 단계에서 핵비확산 레짐의 테스트, 검증, 공급망 관리가 AI 컴퓨팅 거버넌스의 주요 의제로 논의되고 있으며, 국제기구 설립 구상도 이를 반영하여 IAEA를 고려하고 있다(UN Adivisory Report on AI, 2024). 상당한 유사성에

도 불구하고 IAEA 모델 적용을 위해서는 우라늄 추출 전과정에서 적용되는 검증체계를 컴퓨팅 주기 전체 검증체계에 적용하는 것은 여러 난제가 존재하고 있다. 그럼에도 불구하고 여하한 형태의 위험성 평가 및 검증 모델에 기반한 컴퓨팅 거버넌스 구축은 현실화 되고 있는 상황이다.

알고리즘/모델 거버넌스의 경우 개방형 모델과 폐쇄형 모델 경쟁이 주요 쟁점인 바, 상대적으로 미국은 폐쇄형, 중국은 개방형 전략을 추진하고 있으나 동 이슈는 빅테크 기업의 선호는 국가 내에서도 차이가 있다. 실제 트럼프 행정부 AI 행동계획에서도 미국 역시 오픈소스에 대한 중요성을 강조하며 지원 정책을 강화하고 있는데, 폐쇄형 모델이 일부 기업 이윤을 극대화할 뿐 전체적인 AI 혁신을 저해할 수 있다는 우려를 지적하였다(AI Action Plan, 2025). 개방형 vs. 폐쇄형 경쟁은 최근 ChatGPT와 DeepSeek의 경쟁을 통해 확인할 수 있듯이 중국과 같은 후발주자는 하이브리드 혹은 개방형 모델을 선호하고 있다(김상배, 2025). 동 이슈 관련 거버넌스는 민간 빅테크 기업이 주도하고 이를 국가 정책을 통해 뒷받침되고 있으며 개별 기업, 국가의 거버넌스가 글로벌 차원으로 확산되는 상황이다. 생성형 AI가 높은 부가가치를 창출할 것으로 예상됨에 따라 기존에 오픈소스를 기반으로 활성화되었던 AI 기술들이 점차 비공개화되고 있다. 알고리즘의 안정성, 투명성 강화 수준 및 적정성 관련 논의가 글로벌 차원에서 국가 진영은 물론 빅테크 기업 간에도 이견이 상존한다. 동 이슈는 AI의 설명성 부재로 인해, 오작동시 의도치 않은 임무 수행시 여러 문제가 발생하는 바, 이를 완화하기 위해 설명가능성(white box)을 제고하는 일련의 규제 도입과 연계되어 있다.

사이버 안보 국제규범의 경우 초창기 위험, 위협, 취약성을 식별하는데 초점을 두었고 신기술의 발전과 연계융합되는 과장에서 추가적인 요소들

을 추가하여 왔다. 즉 AI 기술을 사이버 안보 논의에 포함할지에 대해 논란 끝에 결국 최종 OEWG 보고서 "현존, 잠재하는 위협(Existing and Potential threats)"파트에 반영하였다. ICT 외 다른 신기술로부터의 위협의 경우 IoT, 개별 소프트웨어 기술, 데이터 등으로 추가되어 왔고 이번에 AI, 양자(Quantum), 거대언어모델(LLM) 기술로부터의 위협을 추가하였다(2025, A/AC.292/2025/CRP.1). 또한 LLM 및 생성형 모델에 기반한 말웨어나 딥페이크 활용 가능성에 대한 우려를 강조하였고 신기술간 연계를 통한 위험의 증가 가능성을 지적하였다. 특히 AI 시스템과 AI 모델을 훈련시키는 데이터의 안전 및 보안을 확립해야 한다는 점을 지적한 바, 상기 언급한 AI 시스템을 구성하는 세 가지 구성요소 모두 사이버 논의의 포함시킨 것이다.

사이버-AI 넥서스 맥락에서 국제규범 논의는 일차적으로 위험 및 위협 요인을 식별하고 이를 감소하는데 초점을 두고 있는 바, 문제는 사이버와 AI 논의의 숙성도 및 주안점이 차이가 있다는 점이다. 사이버 규범 논의의 경우 위험 및 취약성에 대한 논의가 어느 정도 일단락된 후 구체적인 위협을 중심으로 규범이 형성되고 있는 반면 AI는 위험을 인식하고 위험의 정도에 따라 금지 혹은 규제를 도입하는 차원에서 규범이 형성되고 있다. 또한 두 기술의 유사성에도 불구하고 AI 기술의 범용성, 목적의 특정성, 도구성으로 인해 사이버와 AI를 통합하여 규범 형성이 이루어지는 데 한계가 있다.

4. 사이버-AI 넥서스 국제규범 형성 논의의 평가 및 전망

사이버-AI 넥서스 국제규범 논의는 초기 단계로 현 단계에서는 사이버, AI가 각각의 영역에서 규범 형성이 독자적으로 진행되면서 일부 요소들을 "크로스 커팅(cross-cutting)"하는 방향으로 전개될 가능성이 높다. 이 경우 우선적으로 AI와 사이버안보의 교차점에서 발생하는 위험을 완화하고 위협에 대응하는 차원에서 국제규범 논의가 전개될 것이다. 이러한 전망은 사이버와 AI는 기술적 유사성이 높은 것도 하나의 요인인 바, 두 기술 분야는 네트워크, 데이터 처리·전송, 컴퓨팅 하드웨어, 소프트웨어 등 공통된 기반 기술을 이용하고 있다. 또한 비국가 행위자의 위협에 대응 차원에서도 사이버-AI 넥서스 국제규범 논의가 촉진될 수 있다. 특히 정보조작과 같은 위협은 대표적인 AI 기술을 활용한 사이버 위협인 바, 국가 혹은 비국가 행위자의 AI 기술의 악용은 사이버-AI 넥서스 논의에 주요한 현안으로 부상하고 있는 상황이다.

개별 국가 차원에서 적대적 AI 활용에 대응하는 국가 정책 및 법제가 글로벌 차원에서 조율된 대응을 추진하는 과정이 주요한 규범 논의의 시발점이 될 것이다. 우선 미국 및 EU가 자국의 사이버-AI 국가 전략·정책들을 통해 사이버-AI 연계되는 위협요인들을 식별하고 이에 대한 대응 방안들을 제시할 것이다. 이를 바탕으로 글로벌, 지역 기구에서 이를 구체화하는 과정이 전개될 것이다. 실제 미국의 여러 사이버 및 AI 전략보고서(Rand Report, 2024)에서는 사이버-AI 특히 AI 기반한 사이버위협에 대한 논의가 활발히 진행되고 있다. 이러한 전망 하에 현재 파편적으로 논의되는 글로벌 AI 이니셔티브들이 점차 국제안보 맥락에서 수렴되고 있고 특히, 2024년

한국이 주도하여 채택된 결의안(A/C.1/79/L.43, 2024)은 주목할 만하다.

사이버 안보 논의에서 주요 기반시설의 취약성을 보호 및 완화하는 의제가 규범 형성 논의의 주된 쟁점으로 다루어진 것처럼, AI 분야도 향후 AI 침해, 취약성, 적대적 활용에 대한 대응이 주된 규범 논의의 쟁점이 될 것이다. 현재 AI 거버넌스는 주로 예측에 의존하며 개발자에 집중하는 반면 최종 사용자 규제는 크게 다루어지지 않았다. 그러나 최근 위협 정보 분석 기술의 발전은 적대적 AI 사용 축적이 불가능하지 않음을 보여주며, 개발자와 최종 사용자 간 책임을 균형 있게 조정하는 거버넌스 접근법의 단초를 제공하였다. 이러한 상황에서 해로운 AI 위협이라는 시급한 현실에 대응하기 위한 기본적 지침과 플랫폼 창설이 단기적으로 논의될 전망이다.

또한 AI는 침해, 취약성 관리, 위협 탐지, 사고 대응을 개선하며 사이버 방어 역량이 급속히 발전시킬 수 있는 반면, 역으로 AI의 내재적 불안정성, 사이버 인프라의 분절성 등 AI와 사이버 연계를 통합적 관리하는 한계가 있다. 이는 사이버-AI 넥서스 규범 설계의 난제이기도 하다. 그러나 AI 활용이 급속히 증대하는 것에 비례하여 AI에 대한 규범 형성이 속출하고 있으며, 글로벌 차원에서도 국제규범 형성이 기존 사이버 안보 규범형성에 비해 빠르게 진행될 것으로 전망된다. 같은 맥락에서 글로벌 AI 거버넌스 및 규범 논의가 우주, 화학, 원자력 거버넌스와 자주 비교되지만, 사이버와 매우 유사한 특성(인프라, 알고리즘, 데이터)을 보유하는 바, 양 기술의 규범 연계는 필연적인 수순이다(Morse J., 2024). 결국 현 단계에서는 사이버와 AI가 국제규범 형성이 별개로 진행될 가능성이 높은 만큼, 사이버에서 AI 위협, AI에서 사이버 보안을 관리하는 방식의 논의가 주를 이룰 것이다. 가령 디지털 트윈(digital twin) 같은 기술은 ICT, IoT, 데이터, 컴퓨팅, 블록체인, AI 등 매우 다양한 신기술들이 연계·융합된 기술 시스템이다. 또한 디지털 트윈은 사이버-AI 넥

서스를 통한 안보위협의 대응 기술로도 유용하게 활용될 수 있다. 그리고 글로벌 차원의 기술혁신은 파편적이고 중첩적인 기준 및 규범과 정책을 유인할 수 밖에 없기 때문에 최소한의 공통 기준의 부재는 중첩, 상충, 일관성의 결여를 야기할 것이다. 이러한 관점에서는 EU의 사이버복원법 및 AI 기본법은 여러 시사점을 제공한다(Irene Kamara, 2025). 상기 법안에서는 다양한 신기술과 연계된 사이버 위협 대응 및 복원력 강화를 강조하고 있다.

한편 국제법의 적용 이슈는 사이버안보 논의에서 현재까지도 핵심 쟁점이었는데, 개별 국제법 원칙 및 범위와 관련이 있다. 유엔 헌장의 적용의 경우 사이버안보 논의에서 "전체로서(in its entirety)" 유엔 헌장의 적용이 미서방과 중러 간 대립이 첨예하게 대립되었다. 전체로서의 적용에서 문제가 되는 것이 자위권의 적용인 바, 물리적 피해가 부재할 수 있는 상황에서 자위권의 적용에 유보적인 중러 및 글로벌 사우스 국가들의 거부감이 있다. 따라서 사이버-AI 넥서스 논의에서도 이에 대한 대립은 지속될 것이다. 또한 국제규범의 기본 전제가 평시 규범일지 평시·전시를 포괄할지도 공통의 합의가 어려운 쟁점이다. 상기 이슈는 AI 규범 형성의 범위와도 연계되는 문제로 특히 AI의 군사적 적용 시 무기체계를 포함하여 규율할지와 관련되어 있다. 한편 적용되는 개별 국제법 분야의 경우, 기술의 대상 및 속성상 국제인도법 및 국제인권법이 우선적으로 적용될 것이다. AI의 운영과 인프라 구축 시 막대한 양의 에너지가 필요한 관계로 이에 따른 환경의 파괴 및 기후변화의 영향이 상당한 관계로 국제환경법의 적용을 주장하는 견해가 제기되고 있다. 특히 AI의 위험성 평가는 기후변화의 영향평가 모델을 차용할 수도 있다. 그럼에도 불구하고 사이버-AI 연계시에는 지나치게 논의를 복잡하게 할 수 있고 관련 논의가 초기라는 점을 감안하면 가장 시급한 분야를 중심으로 논의가 시작될 가능성이 높다.

5. 맺음말

사이버-AI 넥서스 국제규범 형성 논의가 진행되는 상황에서 한국도 이에 대응하기 위해서는 포괄적 국가전략 차원의 신기술 안보전략 수립이 필요하다. 기존 한국의 AI 전략은 기술개발 및 혁신 전략에 치우쳐 있었으나 동 전략을 지속적으로 강화하면서도 변화하는 신기술 간 연계·융합되는 현실에 효율적인 대응을 위해서는 신기술안보 전략 수립이 필요하다. 새로운 국가전략 수립 시 전반적인 신기술 생태계 구축을 위한 기술혁신의 수준, 가용자원 배분의 방향성, 변화된 신기술 간 연계·융합하는 환경에 대한 대응, 관련 거버넌스 및 국제규범에 대한 한국의 기본입장 및 국제협력 등을 포괄하는 국가전략의 수립이 필요하다.

사이버-AI 국제규범 형성의 경우 AI 기술발전 및 파급력, 국내 대응 능력 수준을 고려해서 신중한 입장이 요구되지만, 향후 논의가 빠르게 전개될 가능성이 있어서 관련 위협에 대한 확인, 대응 수단 및 방법 등 기본적인 사안에 대해서는 선제적인 메뉴얼 작업이 필요하다. 이를 바탕으로 국제규범 형성 논의에서 한국이 배제되지 않으면서 일정한 국가이익을 관철하기 위해서는 주요 쟁점에 대한 입장 정립은 필수적이라 할 수 있다. 이를 전제로 효율적이고 적극적인 신기술외교를 수행하기 위한 Diplomacy Tool-kit 마련이 필요하다. 상기 툴킷은 한국의 책임외교를 위한 최소한의 수단이기도 하다. 실제 EU, 캐나다, 호주 등은 신기술 거버넌스 및 국제규범 형성 논의에 대응하기 위해 자국의 신기술 전략·정책, 자국 법제에 대한 홍보, 안전성 강화를 위한 이행조치, 글로벌 거버넌스를 위한 국제협력의 기조 등을 설명하는 개별 신기술에 대한 diplomacy 툴킷을 구비하여 글로벌 아웃

리치를 강화하고 있다. 또한 Diplomacy tool-kit은 관련 글로벌 거버넌스 및 국제규범의 핵심 의제인 신뢰구축조치, 투명성 강화조치의 일환으로 활용이 가능하다.

사이버-AI 넥서스 국제규범 형성 논의를 주도하고 책임 있는 외교를 전개하기 위해서는 국제적 추세를 반영한 국내 정책 수립과 이를 뒷받침할 수 있는 국내적 정책 차원의 역량 강화가 필요하다. 정책적 역량 강화의 경우 관련 정책 실무자 및 이해관계자에 대한 아웃리치를 통한 인식 공유를 전제로 학제 간 연구를 강화할 수 있는 전문가 네트워크 및 연구기관 간 컨소시엄 구축이 필수적이다. 최근 중국이 신기술 혁신 전략의 추진을 위해 학제 간 장벽을 제거하는 것을 핵심 과제로 추진하는 사례는 중대한 시사점을 제공한다. 유엔 역시 특정 신기술 위협에 대한 대응과 관련 거버넌스 논의 시 학제 간 장벽의 제거를 최우선 과제로 다루고 있다. 학제 간 장벽의 경우 대부분 학제 간 인식 격차에서 기인하는 경우가 많은데 이는 상시적이고 실질적인 연구·논의의 플랫폼이 부재한 것이 주요 원인이다. 한국도 학제 간 연구·논의의 플랫폼 구축이 시급하고 이를 위해 정부가 관련 전문가 풀 구성 및 연구기관 간 컨소시엄 구축을 지원하고 이를 위해 기존 모범 사례 발굴이 시급하다.

〈참고문헌〉

〈국내 문헌〉

"AI 시대 국가 사이버 보안 근본적인 강화대책 절실하다." 국방혁신기술보안협회. 2024년 3월 27일. https://ksaem.or.kr/ai-%EC%8B%9C%EB%8C%80-%EA%B5%AD%EA%B0%80-%EC%82%AC%EC%9D%B4%EB%B2%84-%EB%B3%B4%EC%95%88-%EA%B7%BC%EB%B3%B8%EC%A0%81%EC%9D%B8-%EA%B0%95%ED%99%94%EB%8C%80%EC%B1%85-%EC%A0%88%EC%8B%A4%ED%95%98%EB%8B%A4/ (검색일: 2025년 10월 31일)

『KIDET Podium』 2023, MAY 제9호. 한국국방기술학회. https://www.kidet.or.kr/file/KIDET_Podium_09.pdf (검색일: 2025년 10월 31일)

『S&T DATA』. 2024 Fall vol.7. 2024년 9월 30일. 한국과학기술정보연구원(KISIT). https://m.kisti.re.kr/post/stdata/6531;jsessionid=irIgeiHPETTkV15B-1FaboK8GxPmI9ZcaWhHdcZLUbLJDMfVovaEtg4uCmkE4OsGV.al211_servlet_engine23?t=1743552000066# (검색일: 2025년 10월 31일)

『연합뉴스』 2025년 7월 17일.

『조선일보』 2025년 8월 14일.

『중앙일보』 2024년 12월 18일.

KOTRA. 2025. "일본, 사이버보안산업 육성전략 발표…시장규모 3조 엔 목표." https://dream.kotra.or.kr/kotranews/cms/news/actionKotraBoardDetail.do?SITE_NO=3&MENU_ID=80&CONTENTS_NO=2&bbsGbn=242&bbsSn=242&pNttSn=226579 (검색일; 2025.10.31.)

강충구. 2025. "우주를 연결하는 한 줄기 빛, 레이저 통신 기술과 ISL." 『한화(Hanwha)』 (2025년 2월 11일), https://www.hanwha.co.kr/newsroom/media_center/news/article.

do?seq=13975.
개인정보보호위원회. 2025.『2025년 개인정보보호위원회 주요 정책 추진계획』.
국제반도체장비재료협회. 2025.
https://www.semi.org/ko (검색일; 2025.10.31.)
국토교통부. 2020. 자동차 사이버보안 가이드라인.
국토교통부. 2024.「자동차관리법」·「공항시설법」 개정안 국회 본회의 의결. [보도자료].
김민국. 2024 "일본 라인야후, 앨범 섬네일 유출로 25만명 피해."『조선일보』(12월 6일).
김민석. "글로벌 AI 기업 '팔란티어', 한국 방산시장 진출 타진." Target@Biz 2024년 4월 3일.
https://www.bizhankook.com/bk/article/27392 (검색일: 2025년 10월 31일)
김상배. 2024. 이제는 '데이터 지정학' 지평 속에서 안보·외교의 숨은 코드 읽어낼 때. 나라경제, 404, 20-21. KDI경제정보센터.
김상배. 2016. "신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해."『한국정치학회보』50(1), pp.75-102.
김상배. 2018.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』. 한울.
김상배. 2022.『미중 디지털 패권경쟁』. 한울아카데미.
김상배. 2023. "신흥평화의 개념적 탐색: '창발(emergence)'의 시각에서 본 평화연구의 새로운 지평,"『한국정치학회보』57(1), pp.225-248.
김상배. 2024. "데이터 안보의 복합지정학: 새로운 이론적 시각의 모색." 김상배 역음,『데이터 안보의 복합지정학』서울: 한울아카데미, 8-39.
김상배. 2025. "미중 인공지능 패권경쟁과 한국: 국제정치의 전환과 중견국의 국가전략."『국가전략』제31권 2호, pp. 101-132.
김소정. 2025. "미국 사이버공간의 선제적 방어 전략과 한국에의 시사점."『평화학연구』제26권 2호, pp. 7-30.
김영석. "중국의 대중남미 디지털 실크로드 프로젝트에 관한 고찰," Journal of Global and Area Studies, Vol.8, No.1, 2024.
김주완. "국방에도 치명적인 'AI 데이터 오염'…"방어막·신뢰성 평가 필수"."『한국경제』2024년 7월 22일.

https://www.hankyung.com/article/202407207204i (검색일: 2025년 10월 31일)

김철문. 2025. "'대만판 스타링크' 2029년 구축…1천100억 들여 위성 4개 발사." 『연합뉴스』 (2025년 3월 31일),
https://www.yna.co.kr/view/AKR20250331102500009.

나호영·최근대. "인공지능에 기반한 중국의 군사혁신: 지능화군 건설을 중심으로," 『한국군사학논집』 Vol 76, No. 3(2020).

민한빛. 2019. 자율주행차와 통상규범: 국경 간 데이터이전 문제에 관한 소고(小考). 국제경제법연구, 17(2), 43-78.

박, 페르. 2012. 『자연은 어떻게 움직이는가?: 복잡계로 설명하는 자연의 원리』. 한승.

박소영·이강복, "스마트 헬멧 기술 동향: 국방·안전 분야를 중심으로" 정부조달우수제품협회(2023).
https://www.ppta.or.kr/webzine/2023_06/a2.html.

박시수. 2024. "중국, 대규모 위성 군집화 추진 '홍후-3' 프로젝트 발표." 『산경투데이』 (2024년 6월 4일),
https://www.sankyungtoday.com/news/articleView.html?idxno=46311.

박정한. 2024. "EU, 스타링크에 맞서 106억 유로 위성통신망 '아이리스2' 구축." 『글로벌이코노믹』 (2024년 12월 19일),
https://www.g-enews.com/article/Global-Biz/2024/12/202412190726225877fbbec65dfb_1.

배성수. ""국방 분야 AI 근본 변화 없인 '국방혁신 4.0'은 이상일 뿐"." 『한국경제』 2023년 5월 14일.
https://www.hankyung.com/article/202305143590i (검색일: 2025년 10월 31일)

설인효, 신민석. 2024. "다영역 작전과 사이버전: 사이버전의 역할과 양상의 변화를 중심으로." 『사이버안보연구』 제1집 1호, 1-41.

송태은. 2022. "현대 전면전에서의 사이버전의 역할과 전개양상: 2022년 러시아-우크라이나 전쟁사례" 『국방연구』제65권 3호, 215-236.

스티븐 로치. 2022. 『우발적 충돌: 미국과 중국은 왜 갈등하는가』 한국경제신문.

신범식·양정윤. 2024. “우크라이나 전쟁과 사이버전: 러시아의 사이버 공격 및 NATO의 우크라이나 지원 영향에 대한 고찰.” 『러시아연구』제34권 1호, 129-165.

신승휴. 2025. “파이브 아이즈 국가의 사이버 안보 전략 동조화: 정책지향성과 추진체계를 중심으로.” 『국제지역연구』 제20권 2호, pp. 3-36.

심우현·박정원. 2021. 커넥티드 카 분야 규제합리화를 위한 위험평가 활용 방안 연구. 융합사회와 공공정책, 15(2), 35-65.

심혜인·김지영. 2025. “일본의 능동적 사이버 방어 전략의 형성과 전개” 『국가전략』제35집, 147-183.

엄도영. 2024. 미국의 커넥티드 차량 규제: 주요 내용, 쟁점 및 시사점. 주요국제문제분석 2024-35. 국립외교원 외교안보연구소.

엄도영. 2025. 첨단 자동차와 안보: 주요국의 대응 및 한국에 주는 시사점. 모빌리티연구, 5(1), 83-114.

오승희. 2024. “구마모토(熊本) 관찰기: ‘반도체 부활’을 향한 도전과 과제.” 『IJS 일본리뷰』 제43호.

외교부 경제안보센터. 2023. “경제안보 Review.” 경제안보센터.

외교안보연구소. 2024. 데이터 안보와 국제통상: 현안과 시사점.

원병철. “2025년, AI 기반 사이버 위협과 보안 기술 모두 확대된다.” 『보안뉴스』 2025년 1월 6일. https://www.boannews.com/media/view.asp?idx=135475 (검색일: 2025년 10월 31일)

유인태. 2024. “데이터 안보와 공급망 안보” 김상배 역음, 『데이터 안보의 복합지정학』서울: 한울아카데미, 136-172.

유준구. 2019. “자율살상무기체계의 논의 동향과 쟁점”, 『정책연구시리즈』, 2019-18, 1-32.

유준구. 2020. “유엔정보안보 개방형작업반(OEWG) 최종보고서 채택의 의의와 시사점”, 『주요국제문제분석』, 2020-59, 1-19.

유준구. 2021. “국제안보 차원의 데이터 주권 논의의 이중성과 시사점”, 『국가전략』, 제27권 2호(여름호), 115-136.

유준구. 2023. “파괴적 신기술로서 인공지능의 책임 있는 군사적 이용 논의 동향과 시사점”, 『주요국제문제분석』, 2023-33, 1-18.

유준구. 2025. “미중경쟁 맥락에서 본 글로벌 AI 거버넌스 현황과 전망”, 『세종정책브리프』, No. 2025-10, 1-20.

유준구. 2025. “트럼프 제2기 행정부 AI 전략의 쟁점과 시사점: AI 행동계획(Action Plan) 및 행정명령을 중심으로” 『세종정책연구』, No. 2025-04, 1-50.

유현정.『중국의 디지털 실크로드』 국가안보전략연구원 연구보고서(2020.12).

윤대엽. 2024. “한국과 일본의 데이터 규제와 통상정책: 디지털 상호의존의 정치경제.” 『아세아연구』제67권 3호, 7-33.

윤정현. 2024. “데이터 안보 이슈의 부상과 사이버공격의 진화.” 김상배 역음, 『데이터 안보의 복합지정학』서울: 한울아카데미, 174-211.

윤정현. 2025. “딥시크: AI 시대의 스푸트니크 쇼크인가?” 『ISSUE BRIEF』, 제665호 (2025. 3. 4.).

윤정현. 2025. “미중 강대국 AI 질서와 한국의 중견국 외교전략” 『21세기 정치학회보』, (2025년 9월), 제35집 3호. pp. 133-163.

윤현성. 2024. “스타링크 韓 상륙 앞두고…국산 위성 레이저 통신 기술 날개 편다.” 『뉴시스』 (2024년 11월 19일), https://mobile.newsis.com/view/NISX20241118_0002963531#_PA.

이성훈. 2023. “우주자산 위협 양상과 주변국의 대응 정책 및 시사점.” 『INSS 전략보고』 228호.

이수연, 윤정현. 2024. “사이버 공간의 평화 개념 모색과 실천적 접근 방향.” 『국가전략』 제30권 1호, 165-198.

이수연. 2023. “미일 동맹과 일본의 구조적 공백 모색: 사이버-우주 넥서스로서의 데이터 안보.” 『국제정치논총』 제63집 4호, 125-160.

이승신 외.『중국의 디지털 통상 발전 전략과 시사점』 세종: 대외경제정책연구원, 2024.

이승주, 2017. “일본 사이버안보 전략의 변화: 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화,” 『국가안보와 전략』 17.1.

이정구. “HD현대·대한항공, 美 AI 방산 안두릴과 無. 기술 개발하기로.” 『조선일보』 2025년 8월 8일.
https://www.chosun.com/economy/industry-company/2025/08/08/VRTRW3BSZVBERFYKNMLZQOIWLY/ (검색일: 2025년 10월 31일)

이정환. 2024. “일본의 ‘능동적 사이버 방어(ACD)’ 수용과 전수방위 원칙.” 일본공간 35, 147-183.

이중구, “AI와 국방전략의 연계: 미국의 국방혁신구상을 통해 본 한국의 미래전 대비,” 『안보전략 포커스』(2025. 7. 24).

임해정. “국방 AI 효과적으로 활용하려면…”데이터 공유 제한·망 분리 정책 등 규제 완화해야.” ‘『팍스경제TV』 2025년 2월 25일.
https://www.paxetv.com/news/articleView.html?idxno=224666 (검색일: 2025년 10월 31일)

장은지. 2025. ““딥시크, 중국내 서버에 개인정보 저장”…정보유출 우려 제기.” 『동아일보』 (1월 30일).
https://www.donga.com/news/It/article/all/20250130/130940412/1

장재규. 2023. “미 육군의 MDTF에 대한 이해와 함의.” 『신아세아』제30권 3호, 59-89.

전경운, 김정환. “숨겨왔던 軍데이터 … 펜타곤처럼 개방해 K방산 ‘레벨업’ 한다.” 『매일경제』 2025년 7월 9일.
https://www.mk.co.kr/news/economy/11363881 (검색일: 2025년 10월 31일)

정성조. 2024. “中 전략지원부대 폐지…정보지원·우주·사이버부대 각각 창설.” 『연합뉴스』 (2024년 4월 19일),
https://www.yna.co.kr/view/AKR20240419167100083.

정진용. “K방산 손잡고·亞 최초 법인 낸 안두릴…현지화 시동거는 배경은.” 『NATE뉴스』 2025년 7월 22일.
https://news.nate.com/view/20250722n01143 (검색일: 2025년 10월 31일)

정충신. “AI·드론 등 첨단무기체계 ‘신속획득’ 가능해진다…패스트트랙법 통과.” 『문화일보』

2023년 5월 9일.
https://www.munhwa.com/article/11359393 (검색일: 2025년 10월 31일)
조일섭. "KT, 207억원 규모 '국방 5G 인프라 구축 사업' 구축한다. AICT 기반 스마트 국방 앞장." 『뉴스 스페이스』 2025년 8월 13일.
https://www.newsspace.kr/news/article.html?no=8582 (검색일: 2025년 10월 31일)
중국 공신부. 2024. 중국 공업분야 데이터안보 능력 제고 실시방안(2024~2026).
채제우. 2024. "통신은 대만 안보의 생명...2030년까지 독자 위성통신망 구축." 『조선일보』 (2024년 12월 26일),
https://www.chosun.com/economy/weeklybiz/2024/12/26/LROP-KLH7MRCZHNHYRLTTGLTHSE/.
최계영. "디지털 실크로드와 디지털 패권" 『중앙일보』 2023년 10월 24일.
최용석. 2024. "중국의 저궤도 위성 '우주 굴기' 새로운 글로벌 안보 위협." 『글로벌이코노믹』 (2024년 2월 7일),
https://www.g-enews.com/article/Global-Biz/2024/02/20240206161421 9158b418061615_1.
하라리, 유발. 2024. 『넥서스(Nexus): 석기시대부터 AI까지 정보 네트워크로 보는 인류 역사』. 김영사.
하영선·김상배 편. 2006. 『네트워크 지식국가: 21세기 세계정치의 변환』. 을유문화사.

〈국외 문헌〉

Afifi-Sabet, K. 2020. 36 billion personal records exposed by hacks in 2020 so far. ITPro.
Arguilla, John and David Ronfeldt. 1993. "Cyberwar is Coming" RAND
https://www.rand.org/pubs/reprints/RP223.html (검색일: 2025.08.20.)
Backlinko. 2025.
https://backlinko.com/most-popular-apps

Barton Gellman. 2013. Edward Snowden: The whistleblower behind the NSA surveillance revelations. The Guardian.

Biancotti, Claudia. 2019. "The Growing Popularity of Chinese Social Media Outside China Poses New Risks in the West." Peterson Institute for International Economics.
https://www.piie.com/blogs/china-economic-watch/growing-popularity-chinese-social-media-outside-china-poses-new-risks.

Biddle, Stephen. 2023. "Back in the Trenches: Why New Technology Hasn't Revoultionized Warfare in Ukraine." Foreign Affairs 102. No.5, 153-164.

Birch, K., Cochrane, D. T., & Ward, C. 2021. Data as asset? The measurement, governance, and valuation of digital personal data.

Boak, Josh and Zeke Miller. "Trump highlights partnership investing $500 billion in AI." AP News, Jan 23, 2025.
https://apnews.com/article/trump-ai-openai-oracle-softbank-son-altman-ellison-be261f8a8ee07a0623d4170397348c41 (검색일: 2025년 10월 31일)

Bondar, Kateryna. 2025. "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare." CSIS (June 02)
https://www.csis.org/analysis/how- ukraines-spider-web-operation-redefines-asymmetric-warfare(검색일: 2025.08.25.).

Braun, D. 2025. Why "Artificial Intelligence" Should Not Be Regulated. Digital Government: Research and Practice, 6(2), 1-16.by Big Tech. Big Data & Society, 8(1), 20539517211017308.

Bruce, Bennett W. "Deterring North Korea from Using WMD in Future Conflicts and Crises," Strategic Studies Quarterly 6(4)(2012): 119-151.

Burdette, Zachary, et al. 2025. "An Ai Revolution in Military Affairs? How AI Could Reshape Future Warfare." RAND Working Paper (June)

https://www.rand.org/ pubs/working_papers/WRA4004-1.html (검색일: 2025.10.26.).

Caisley, Olivia. 2025. "Trump ends AUKUS uncertainty with firm backing for Albanese." ABC News (October 21). https://www.abc.net.au/news/2025-10-21/trump-aukus-albanese-firm-support-pact/105915668

Cassidy, Christina. 2025. "Trump administration halts funding for two cybersecurity efforts, including one for elections." AP News (March 11). https://apnews.com/article/election-security-cisa-trump-kristi-noem-6c437543f5d26d890704e5f2a8400502

Chaeri Park. "Knowledge Base: China's 'Global Data Security Initiative' 全球数据安全倡议," Stanford University DIGICHINA, March 31, 2022. https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/?utm_source=chatgpt.com

Chang Dong-woo, "Officials from U.S. defense tech firm Anduril in Seoul for partnership talks, office launch," Yonhap News Agency August 06, 2025. https://en.yna.co.kr/view/AEN20250806009700320 (검색일: 2025년 10월 31일)

Chappellet-Lanier, Tajha. "DARPA announces $2 billion in funding for 'AI Next' campaign." FEDSCOOP, Sep 7, 2018. https://fedscoop.com/darpa-announces-ai-next-campaign/ (검색일: 2025년 10월 31일)

Chernavskikh, Vladislay and Jules Palayer, "Impact of Military Aritificial Intelligence on Nuclear Escalation Risk," SIPRI Insight on Peace and Security No. 2025/06(June 2025).

Chernavskikh, Vladislay, "Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities," SIPRI Background Paper(September 2024).

Chief Digital and Artificial Intelligence Office. Artificial Intelligence Rapid Capabilities Cell. Dec 2024. https://www.ai.mil/Portals/137/Documents/Resources%20Page/2024-12-CDAO-Artificial-Intelligence-Rapid-Capabilities-Cell.pdf (검색일: 2025년 10월 31일)

Chief Digital and Artificial Intelligence Office. Department of Defense Metadata Guidance. Version 1.0. Jan 2023. https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Metadata%20Guidance.pdf (검색일: 2025년 10월 31일)

Chin, Josh. 2025. "China Is Using the Private Sector to Advance Military AI." The Wall Street Journal (September 3, 2025). https://www.wsj.com/world/china/china-military-ai-partners-7836a2bc

CISA. 2025. "AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems." (May 22).

Crampton, Jeremy, "Government must protect us from geolocational disinformation" Fulcrum(February 29, 2024).

Cunningham, Alan. 2024. "Integrated Warfare: How US SOF can Couter-AI Equipped Chinede SOF." Military Review Online Exclusive (April) https://www.armyupress. army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2024/Integrated-Warfare/cunningham-integrated-warfare-ole-UA.pdf (검색일: 2025.08.20.).

D'Innocenzio, A. 2024. Biden administration seeks to ban Chinese, Russian tech in US autonomous vehicles. Associated Press. https://apnews.com/article/commerce-autonomous-vehicles-national-security-chna-russia-a895bbbbe59ae915aad2f0980b7acf08

Dastin, Jeffrey. 2025. "Exclusive: Trump's Paris AI summit delegation won't include AI Safety Institute staff, sources say." Reuters (February 7).

https://www.reuters.com/technology/trumps-paris-ai-summit-delegation-not-include-ai-safety-institute-staff-sources-2025-02-06

David Omand, Jamie Bartlett, & Carl Miller. (2021). Principles for Data Intelligence. Intelligence and National Security, 36(1), 1-18.

Department of Defense. 2006. "The National Military Strategy for Cyberspace Operations." (December, 2006).

DoD. 2022. "Summary of the Joint All-Domain Command & Control Strategy." (March) (검색일: 2025.03.17.)
https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf (검색일: 2025.08.20.).

DoD. 2024. "Contracts for May 29, 2024"
https://www.defense.gov/News/ Contracts/Contract/Article/3790490// (검색일: 2025.08.20.).

Dylan, H., & Stivang, N. 2025. Emerging technologies and national security intelligence. Intelligence and National Security, 1-22.

Easley, Mikayla. "Palantir partners with data-labeling startup to improve accuracy of AI models." DEFENSESCOOP, Feb 5, 2025.
https://defensescoop.com/2025/02/05/palantir-enabled-intelligence-partnership-foundry/ (검색일: 2025년 10월 31일)

Elms, D. (January 21, 2025). Who is 'us'? Why a battle to define connected cars matters. Hinrich Foundation.
https://www.hinrichfoundation.com/research/article/trade-and-geopolitics/why-a-battle-to-define-connected-cars-matters/

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., and Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214.

ENISA. 2021. Recommendations for the security of CAM. European Union Agency for Cybersecurity.
https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam

ENISA. 2025. "From Cyber to Outer Space: A Guide to Securing Commercial Satellite Operations." Press Release (March 26, 2025), at
https://www.enisa.europa.eu/news/from-cyber-to-outer-space-a-guide-to-securing-commercial-satellite-operations.

ENISA. 2025. "Space Threat Landscape." ENISA (March, 2025).

Enkrypt AI, "DeepSeek R1: Red Teaming Report" (Jan 2025),

Erwin, Sandra. 2024. "Pentagon embracing SpaceX's Starshield for future military satcom." Space News (June 11, 2024), at
https://spacenews.com/pentagon-embracing-spacexs-starshield-for-future-military-satcom/.

European Parliament. 2023. Security concerns around Chinese electric vehicles.
https://www.europarl.europa.eu/doceo/document/E-9-2023-002806_EN.html#def3

EUSPA. 2025. "IRIS2." EUSPA (April 25, 2025), at
https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2.

Faverio, Michelle and Olivia Sidoti. 2024. "Teens, Social Media and Technology 2024." Pew Research Center.
https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/.

"Fiji to stick with China police deal after review, home affairs minister says," The Guardian, 15 Mar 2024;
https://www.article19.org/wp-content/uploads/2025/02/cybersecuri-

ty-with-chinese-characteristics.pdf?utm_source=chatgpt.com

Fontaine, Richard. 2025. "The Trump-Biden-Trump Foreign Policy: American Strategy's Strange Continuity." Foreign Affairs (January 20). https://www.foreignaffairs.com/trump-biden-trump-foreign-policy

Fukuda, M. 2022. "Japan-Taiwan cooperation in the area of economic security." 2022/45, European University Institute(EUI).

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth" International Security 38(2), 41-73.

Gegeon, Joseph. 2025. "Trump administration shutters US office countering foreign disinformation." The Guardian (April 16). https://www.theguardian.com/us-news/2025/apr/16/trump-state-department-foreign-disinformation

Goldstein, Josh A. and Renee DiResta. 2023. "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations." Cyber Policy Center Report, Stanford University (January 11).

Goncharuk, Vitaliy. 2025. "Ukraine Isn't the Model for Winning the Innovation War." War on the Rocks (Aug. 12) https://warontherocks.com/2025/08/ ukraine-isnt-the-model-for-winning-the-innovation-war/ (검색일: 2025.08.25.)

Goujon, R., and Sebastian, G. (October 8, 2024). Car Trouble: ICTS Rule Rewires Global Auto Supply Chains. Rhodium Group. https://rhg.com/research/car-trouble-icts-rule-rewires-global-autoꠓsupply-chain

Grealy, Andrew. 2025. "China's AI Surge: New Front in Cyber Warfare." Armis Labs.

Hersman, Rebecca K.C. and Reja Younis, "Surveillance, Situational Awareness, and Warning at the Conventional-Strategic Interface," Next Generation Nuclear Network, January 15, 2021.

Holland, Steve. “Trump announces private-sector $500 billion investment in AI infrastructure.” Reuters, Jan 22, 2025.
https://www.reuters.com/technology/artificial-intelligence/trump-announce-private-sector-ai-infrastructure-investment-cbs-reports-2025-01-21/ (검색일: 2025년 10월 31일)
https://access.redhat.com/ko/articles/2621341?utm
https://ax.dev/docs/why-ax/
https://biilmann.blog/articles/introducing-ax/
https://blog.humminglab.io/posts/tls-cryptography-3-block-cipher/
https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html
https://developer.android.com/privacy-and-security/risks/hardcoded-cryptographic-secrets?hl=ko
https://kanerika.com/blogs/multimodal-models/
https://m.boannews.com/html/detail.html?idx=121029
https://www.dailysecu.com
https://www.newsis.com/view/NISX20250107_0003024188
https://www.samsungsds.com/kr/insights/generative-ai-trends.html
https://www.theax.ai/blog/ushering-in-the-new-age-of-accelerated-experience-%28ax%29-driven-by-ai;
https://www.yna.co.kr/view/AKR20240830075200009

Irene Kamara, Marco Bassini. 2025. “AI Nexus in the EU Digital Acquis”, TILT, 312-326.

Itkowitz, Colby, Yvonne Wingett Sanchez, Sarah Ellison and Patrick Marley. 2025. “Trump administration cuts teams that fight foreign election interference.” The Washington Post (February 8).
https://www.washingtonpost.com/politics/2025/02/08/trump-adminis-

tration-cuts-election-security-teams

Ivanovska, Marija and Vitomir Struc, "On the Vulnerability of Deepfake Detectors to Attacks Generated by Denoising Diffusion Models" (2024). https://www.computer.org/csdl/proceedings-article/wacvw/2024/702800b051/1WbOU8Bt7uU.

Jaycox, M. M. 2021. No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333. Harvard National Security Journal, 12, 58.

Jessop, Bob. 2003. The Future of the Capitalist State. Cambridge, UK: Polity Press.

Johnson, James. 2019. "The AI-cyber nexus: implications for military escalation, deterrence and strategic stability," Journal of Cyber Policy 4(3): 442-460.

Jones, Andrew. 2024. "China to launch first satellites for megaconstellation in August." Space News (June 27, 2024), at https://spacenews.com/china-to-launch-first-satellites-for-megaconstellation-in-august/.

Joshua Kurlantzick. "Assessing China's Digital Silk Road: A Transformative Approach to Technology Financing or a Danger to Freedoms?" CFR, December 18, 2020. https://www.cfr.org/china-digital-silk-road/

Khan, Khalid, Khurshid, Adnan, and Cifuentes-Faura, Javier. 2024. "Is artificial intelligence a new battleground for cybersecurity?." Internet of Things. Vol. 28, 101428.

Kirichenko, David. 2025. "Why Ukraine's AI Drones are't a Breakthrough Yet." The Strategist (June 19) https://www.aspistrategist.org.au/why-ukraines-ai-drones- arent-a-breakthrough-yet/ (검색일: 2025.08.20.)

Kitishian, Dany. 2025. "Palantir's AI Strtegy: Path to AI Dominance from Defense to

Enterprise." (July 14)
https://www.klover.ai/palantir-ai-strategy-path- to-ai-dominance-from-defense-to-enterprise/ (검색일: 2025.08.20.)

Klein, John J. 2024. "Space and Cyber Warfare as One." CSIS (October 31, 2024), at https://www.csis.org/analysis/space-and-cyber-warfare-one.

Knight, Will, "Deepfake Maps Could Really Mess With Your Sense of the World" Wired (May 28, 2021).
https://www.wired.com/story/deepfake-maps-mess-sense-world.

Knight, Will. 2025. "Under Trump, AI Scientists Are Told to Remove 'Ideological Bias' From Powerful Models." Wired (March 14).
https://www.wired.com/story/ai-safety-institute-new-directive-america-first

Kokas, A. 2018. Platform patrol: China, the United States, and the global battle for data security. The Journal of Asian Studies, 77(4), 923-933.

Konkel, Frank. "A decade-old risk led to 'phenomenal partnership' between AWS and the intel community." NextGov, Dec 13, 2024.
https://www.nextgov.com/acquisition/2024/12/decades-old-risk-led-phenomenal-partnership-between-aws-and-intel-community/401649/ (검색일: 2025년 10월 31일)

Konkel, Frank. "Pentagon Awards $9B Cloud Contract to Amazon, Google, Microsoft, Oracle." NextGov, Dec 7, 2022.
https://www.nextgov.com/digital-government/2022/12/amazon-google-microsoft-oracle-awarded-9b-pentagon-cloud-contract/380596/ (검색일: 2025년 10월 31일)

Kroet, Cynthia. 2025. "US companies still engaging with AI Code despite Trump, says EU official." Euro News (May 8).
https://www.euronews.com/next/2025/05/08/us-companies-still-en-

gaging-with-ai-code-despite-trump-says-eu-official

Lesser, Max. 2025. "New Report Shows How China Uses AI to Augment its Online Intelligence Operations." Defense of Democracies (June 12). https://www.fdd.org/analysis/policy_briefs/2025/06/12/new-report-shows-how-china-uses-ai-to-augment-its-online-intelligence-operations

Lieber, Keir A. and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," International Security 41, no. 4 (Spring 2017): 37-46.

Lim, T. W. 2023. "Japanese semiconductor industry's collaboration with Taiwan semiconductor manufacturing company." East Asian Policy, 15(01), 47–59.

Lin, L. S. 2025. Organisational Challenges in US Law Enforcement's Response to AI-Driven Cybercrime and Deepfake Fraud. Laws, 14(4), 46.

Lohn, Andrew. 2025. "Anticipating AI's Impact on the Cyber Offense-Defense Balance." Centre for Security and Emerging Technology Policy Brief (May).

Machtiger, P. 2021. Updating the Fourth Amendment Analysis of US Person Communications Incidentally Collected Under FISA Section 702. Harvard National Security Journal Online.

Madhani, Aamer, Eric Tucker and Ai Swenson. 2025. "Gabbard slashing intelligence office workforce and cutting budget by over $700 million." AP News (August 21). https://apnews.com/article/gabbard-intelligence-cuts-trump-e982e5364481d41a058e2bd78be4060f

Magee, Tamlin. 2025. "Trump cyber cuts put US allies on guard." Raconteur (April 15). https://www.raconteur.net/technology/trump-admin-cyber-turbulence-rattles-allies

Mantua, Janna, "China's Focus on the Brain Gives it an Edge in Cognitive Warfare"

Irregular Warfare Initiative(July 6, 2023).
https://irregularwarfare.org/articles/chinas-focus-on-the-brain-gives-it-an-edge-in-cognitive-warfare/

Marcus, Ruth. 2025. "Opinion | The Head-Spinning Chutzpah of Trump's TikTok Brief." The Washington Post (Jan 3).
https://www.washingtonpost.com/opinions/2025/01/03/tik-tok-trump-china-sauer/.

Mchangama, Jacob and Jules White. 2024. "The Future of Censorship Is AI-Generated." Time (February 26).
https://time.com/6835213/the-future-of-censorship-is-ai-generated/

Mellor, Chris. 2025. "Data sovereignty in focus as Europe scrutinizes US cloud influence." Blocks & Files (March 27).
https://blocksandfiles.com/2025/03/27/eu-data-sovereignty-and-trumps-usa

Miller, C. 2022. Chip War: The fight for the world's most critical technology. New York: Scribner.

Miller, Maggie and Antoaneta Roussi. 2025. "Trump's return freezes Western cyber plans to counter Russia, China." Politico (February 12).
https://www.politico.eu/article/donald-trump-return-freeze-western-cyber-plan-counter-russia-china/

Miller, Maggie. 2025. "State Department cyber, tech cuts deeper than previously known." Politico (July 17).
https://www.politico.com/news/2025/07/17/cyber-tech-state-ai-00460679

Miller, R. G. 2019. FISA Section 702: Does Querying Incidentally Collected Information Constitute a Search Under the Fourth Amendment?. Notre Dame L. Rev. Reflection, 95, 139.

Minges, Madisoin. 2025. "National Security and the TikTok Ban." American University School of International Service News. https://www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm.

Mok, Charles. 2025. "The US Aims to Win the AI Race, But China Wants to Win Friends First." Tech Policy (August 8). https://www.techpolicy.press/the-us-aims-to-win-the-ai-race-but-china-wants-to-win-friends-first

Molock, Diarra. 2025. "A Plan B for PRC Cable-Cutting: Taiwan's Satellite Communications." Global Taiwan Brief 10(13), Global Taiwan Institute (July 2, 2025), at https://globaltaiwan.org/2025/07/a-plan-b-for-prc-cable-cutting/.

Momoko, K. 2022. "Taiwan's TSMC as a focal point of US-China high-tech conflict." Asia-Pacific Review 29(1), 5-12.

Morse J. 2024. "Frameworks and Outcomes for International AI Governance: Goals and Lessons for AI", Microsoft Publications.

Motwani, Nishank. 2025. "America Is Watching: AUKUS Needs More Than Rhetoric From Australia." The Diplomat (September 3). https://thediplomat.com/2025/09/america-is-watching-aukus-needs-more-than-rhetoric-from-australia/

Moynihan, Lydia. 2025. "Michael Kratsios-Trump's go-to tech policy guy-reveals how the US needs to step up its innovation plan." New York Post (May 8). https://nypost.com/2025/05/08/business/michael-kratsios-on-artificial-intelligence-and-tech-in-the-u-s

Mügge, Daniel. 2023. "The Securitization of the EU's Digital Tech Regulatiobn." Journal of European Public Policy 30(7), 1431-1446.

Nakashima, Ellen and Joseph Menn. 2025. "As Trump warms to Putin, U.S. halts offensive cyber operations against Moscow." The Washington Post (March 1).

https://www.washingtonpost.com/national-security/2025/03/01/trump-putin-russia-cyber-offense-cisa/

Nam, Hyun-woo, "KT signs strategic partnership with Palantir," The Korea Times, Mar 13, 2025. https://www.koreatimes.co.kr/business/tech-science/20250313/kt-signs-strategic-partnership-with-palantir (검색일: 2025년 10월 31일)

NIIS·NSR. 2023. "챗GPT 등 생성형 AI 활용 보안 가이드라인"

NSCAI. 2021. NSCAI Final Report. March.

O'Loughlin, Rex Fox. 2025. "Orbital ambitions: LEO satellite constellations and strategic competition." IISS (May 27, 2025), at https://www.iiss.org/online-analysis/six-analytic-blog/2025/05/orbital-ambitions-leo-satellite-constellations-and-strategic-competition/.

ODNI. 2023. Annual Threat Assessment of the U.S. Intelligence Community. February 6.

Oertel, J. 2024. Security recall: The risk of Chinese electric vehicles in Europe. European Council on Foreign Relations. https://ecfr.eu/article/security-recall-the-risk-of-chinese-electric-vehicles-in-europe

OEWG Report. 2025. A/AC.292/2025/CRP.1. https://docs.un.org/A/AC.292/2025/L.1 (검색일: 2025.10.20).

Office of the Director, Operational Test and Evaluation, "Integrated Visual Augmentation System(IVAS)"(2022).

Ortega, Bob. 2025. "Trump is dismantling election security networks. State officials are alarmed." CNN (April 9). https://edition.cnn.com/2025/04/09/politics/election-security-systems-trump-invs

Ortutay, Barbara. 2025. "President Trump signs Take It Down Act, addressing non-

consensual deepfakes. What is it?." AP News (May 21).
https://apnews.com/article/take-it-down-deepfake-trump-melania-first-amendment-741a6e525e81e5e3d8843aac20de8615

Palantir. "AIP Overview."
https://www.palantir.com/docs/foundry/aip/overview (검색일: 2025.08.20.).

Palantir. "Gotham"
https://www.palantir.com/platforms/gotham/(검색일: 2025.08.20.).

Palantir. "Palantir Foundry"
https://www.palantir.com/platforms/foundry/ (검색일: 2025.08.20.).

Palantir. "The Palantir Platform: The Platform for Informational Analysis"
https://nsarchive.gwu.edu/sites/default/files/documents/3891748/Palantir-The-Palantir-Platform-The-Platform-for.pdf (검색일: 2025.08.20.).

Park, Allyson. "JUST IN: Pentagon Establishes AI Rapid Capabilities Cell." National DEFENSE, Dec 11, 2024.
https://www.nationaldefensemagazine.org/articles/2024/12/11/pentagon-establishes-ai-rapid-capabilities-cell-to-advance-generative-ai-capabilities (검색일: 2025년 10월 31일)

Petit, J., and Shladover, S. E. 2015. Potential Cyberattacks on Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546-556.

Porcedda, M. G., & Wall, D. S. 2021. Modelling the cybercrime cascade effect of data theft. Proceedings of the IEEE Workshop on Attackers and Cyber-Crime Operations (WACCO), Montreal.

Psaledakis, Daphne. 2025. "US State Department closing office aimed at countering foreign disinformation." Reuters (April 17).
https://www.reuters.com/business/media-telecom/us-state-department-closing-office-aimed-countering-foreign-disinformation-2025-04-16/

Pusztaszeri, Aosheng. 2024. "Why China's UAV Supply Chain Restrctions Weaken Ukraine's Negotiating Power." CSIS (Dec. 16) https://www.csis.org/analysis/ why-chinas-uav-supply-chain-restrictions-weaken-ukraines-negotiating-power?utm_source=chatgpt.com (검색일: 2025.08.20.).

Pytlak, Allison. 2024. "False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War." Stimson Commentary (Feb. 22) https://www.stimson.org/ 2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/ (검색일: 2025.08.20.)

Radio Free Asia. 2024. "TikTok promotes pro-China bias on Tibet, Taiwan, Uyghurs: study." (Aug 16).

Raoul Ramirez, Zachary and Le, Tho V., 2024. "Semiconductor Supply Chain Resilience: Systematic Review, Conceptual Framework, Implementation Challenges, and Future Research Directions" Available at SSRN: https://ssrn.com/abstract=4994726 (검색일; 2025.10.31.)

Ribeiro, Anna. 2025. "Sean Plankey pledges to rebuild, refocus CISA as lawmakers warn of weakened cyber defense posture." Industrial Cyber (July 28). https://industrialcyber.co/cisa/sean-plankey-pledges-to-rebuild-refocus-cisa-as-lawmakers-warn-of-weakened-cyber-defense-posture/

Richter, Alex Lewis, "Experts See Risk and Reward to Integrating AI in Nuclear Weapons," China Brief 25(11)(2025).

Roughead, Gary, Marise Payne, Nicholas Carter, and James Mattis. 2025. "Don't Abandon AUKUS: The Case for Recommitting to-and Revitalizing-the Alliance." Foreign Affairs (September 2). https://www.foreignaffairs.com/united-states/dont-abandon-aukus-jim-mattis

Rundle, James. 2025. "Top U.S. Cyber Agency Faces Staff and Funding Cuts in

New Budget." The Wall Street Journal (June 2).
https://www.wsj.com/articles/top-u-s-cyber-agency-faces-staff-and-funding-cuts-in-new-budget-507e87f1

Russ-Eft, D. 2025. Strategic Planning by State Chief Information Officers. Journal of Leadership and Management, 11(1), 16.

Saalman, Lora ed., The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk (Sipri, 2019).

Scharre, Paul and Michael Depp, "Artificial Intelligence and Nuclear Stability," Center for New American Security, Jaunary 16, 2024,
https://www.cnas.org/publications/commentary/artificial-intelligence-and-nuclear-stability.

Schneier, B. 2015. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

Siegelman, J. 2021. Cambridge Analytica, Russia, and the 2016 U.S. Election. Harvard International Review, 42(3), 18-22.

Soroush Vosoughi, Deb Roy, Sinan Aral. 2018. "The spread of true and false news online." Science 359: 1146-1151.

Space X. n.d. "Starshield." at
https://www.spacex.com/starshield.

Starks, Tim, "Suspected Russian hacking, influence operations take aim at Ukrainian military recruiting" Cyberscoop (October 28, 2024).
https://cyberscoop.com/suspected-russian-hacking-influence-operations-take-aim-at-ukrainian-military-recruiting/

Stockholm Environment Institute(SEI), 2011. "The Water, Energy and Food Security Nexus: Solutions for the Green Economy." Bonn Conference.
https://uploads.water-energy-food.org/resources/bonn2011_nexussynopsis.pdf

Stokes, Jacob, Colin H. Kahl, Andrea Kendall-Taylor, and Nicholas Lokker, "Averting AI Amageddon: U.S.-China-Russia Rivalry at the Nexus of Nuclear Weapons and Artificial Intelligence," CNAS, February 2025.

Sutter, K. M., and Sayler, K. M. 2024. U.S.-China Competition in Emerging Technologies: LiDAR. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12473/6

Swanson, Ana, Paul Mozur, and Raymond Zhong. 2020. "Trump's Attacks on TikTok and WeChat Could Further Fracture the Internet." The New York Times, August 17, 2020, sec. Technology. https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html.

Sydney J. Freedberg Jr., "'OpenAI For Government' launches with $200M win from Pentagon CDAO," BreakingDefense, Jun 17, 2025. https://breakingdefense.com/2025/06/openai-for-government-launches-with-200m-win-from-pentagon-cdao/ (검색일: 2025년 10월 31일)

The White House. 2025a. America First Trade Policy. https://www.whitehouse.gov/presidential-actions/2025/01/america-first-trade-policy/

The White House. 2025b. Regulatory Freeze Pending Review. https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/

The White House. 2025c. Report to the President on the America First Trade Policy Executive Summary. https://www.whitehouse.gov/fact-sheets/2025/04/report-to-the-president-on-the-america-first-trade-policy-executive-summary/

The White House. 2020. "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems." (September 4, 2020), at

https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

The White House. 2023. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." (October 30). https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

The White House. 2024. "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." Federal Register.

The White House. 2025. "Winning the Race AMERICA'S AI ACTION PLAN", https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf?utm (검색일: 2025.10.20.).

The White House. 2025a. "Removing Barriers to American Leadership in Artificial Intelligence." (January 23). https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence

The White House. 2025b. "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144." (June 6). https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

The White House. 2025c. Winning the Race: America's AI Action Plan. July.

The White House. Executive Order-14141: Advancing United States Leadership in Artificial Intelligence Infrastructure. Jan 14, 2025.

https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/14/executive-order-on-advancing-united-states-leadership-in-artificial-intelligence-infrastructure/ (검색일: 2025년 10월 31일)

The White House. Winning the Race AMERICA'S AI ACTION PLAN. Jul 2025. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf (검색일: 2025년 10월 31일)

Tian, M., & Feirong, P. 2025. Geopolitical Data Barriers in Biomedicine: Resolving Sino-US Regulatory Conflicts and Compliance Challenges Under Executive Order 14117. Biotechnology Law Report.

Tierney, Kathleen and Michel Bruneau. 2007. "Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction." TR News 250, May-June, pp.14-17.

TIME. 2022. "The Chips That Make Taiwan the Center of the World." https://time.com/6219318/tsmc-taiwan-the-center-of-the-world/ (검색일; 2025.10.31.)

U.S. Department of Commerce. 2024. Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles. Federal Register, 89(187), 79088-79123. https://www.federalregister.gov/d/2024-21903

U.S. Department of Defense. Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage. Jun 27, 2023. https://media.defense.gov/2023/nov/02/2003333300/-1/-1/1/dod_data_analytics_ai_adoption_strategy.pdf (검색일: 2025년 10월 31일)

U.S. Department of Defense. DoD Artificial Intelligence Cybersecurity Risk Management Tailoring Guide. Version 2. Jul 14, 2025. https://dodcio.defense.gov/Portals/0/Documents/Library/AI-CybersecurityRMTailoringGuide.pdf (검색일: 2025년 10월 31일)

U.S. Department of Defense. Fact Sheet: 2018 DoD Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity. Feb 12, 2019. https://media.defense.gov/2019/Feb/12/2002088964/-1/-1/1/DOD-AI-STRATEGY-FACT-SHEET.PDF (검색일: 2025년 10월 31일)

U.S. Department of Defense. Responsible Artificial Intelligence Strategy and Implementation Pathway. Jun 2022. https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF (검색일: 2025년 10월 31일)

UN. 2024. "Governing AI for Humanity: Final Repor", (Sep. 2024). https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf (검색일: 2025.10.20.).

US Department of Homeland Security. 2020. "Data Security Business Advisory." https://www.dhs.gov/publication/data-security-business-advisory.

US Department of Justice. 2021. "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research" Press Release. https://www.justice.gov/archives/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

USGA(A/RES/79/239). 2024. "Artificial intelligence in the military domain and its implications for international peace and security : resolution / adopted by the General Assembly." Palantir Technologies Inc." (Dec. 31) https://digitallibrary.un.org/record/4071348?v=pdf (검색일: 2025.10.20).

US SEC. 2025. "Palantir Technologies Inc." (Feb. 18) https://www.sec.gov/ Archives/edgar/data/1321655/000132165525000022/pltr-20241231.htm#i3e102edc3e324d1d-

85b3af889db7f10b_16 (검색일: 2025.08.20.).

Vakulina, Sasha. 2024. "Lost and Spoofed: How Ukraine Redirects Russian Drones to Belarus." Euro News (April 12) https://www.euronews.com/my-europe/2024/ 12/04/lost-and-spoofed-how-ukraine-redirects-russian-drones-to-belarus (검색일: 2025.08.10.).

Vergun, David. "DOD, Partners Find Data Sharing Challenging." DoD News, Jun 26, 2024. https://www.war.gov/News/News-Stories/Article/Article/3818870/dod-partners-find-data-sharing-challenging/ (검색일: 2025년 10월 31일)

Wadhwani, S. 2022. Medibank confirms data leak following refusal to pay ransom. spiceworks.

Wall, D. S. 2018. How big data feeds big crime. Current History, 117(795), 29-34.

Wan, Wilfred, Andraz Kastelic, and Eleanor Krabill, The Cyber-Nuclear Nexus (Nuclear Risk Reduction: Friction Points Series Paper 2), (UNIDIR, 2021).

Wang, Luxuan, Galen Stokcing, Samuel Bestvater, Regina Widjaya. 2025. "A closer look at Americans' experiences with news on TikTok." Pew Research Center. https://www.pewresearch.org/short-reads/2025/01/17/a-closer-look-at-americans-experiences-with-news-on-tiktok/.

Webster, Graham and Paul Triolo. 2020. "Translation: China Proposes 'Global Data Security Initiative'." New America (September 7). https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative/

White House, "Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China," U.S. Emabassy and Consulates in China, November 17, 2024.

Xinhua. 2024. “China’s new mega-constellation marks milestone in satellite internet.” The State Council, The People’s Republic of China (August 9, 2024), at https://english.www.gov.cn/news/202408/09/content_WS66b55ad9c6d0868f4e8e9cf8.html.

Yeung, H.W.C. 2022. InterconnectedWorlds: Global Electronics and Production Networks in East Asia. Stanford,California: Stanford University Press.

Yuzue, N., & Sekiyama, T. 2025. Defining economic security through literature review. Frontiers in Political Science, 7, 1501986.

Zakrzewski, Cat and Hannah Natanson. 2025. “Silicon Valley’s bet on Trump starts to pay off.” The Washington Post (July 24). https://www.washingtonpost.com/politics/2025/07/23/trump-ai-action-plan-big-tech

Zuboff, S. 2019. Surveillance capitalism and the challenge of collective action. New Labor Forum, 28(1), 10-29.

《携手构建网络空间命运共同体》白皮书, (北京; 中华人民共和国国务院新闻办公室, 2022年 11月). http://www.scio.gov.cn/zfbps/ndhf/2022n/202303/t20230320_705522.html

『新一代人工智能伦理规范』(北京: 中华人民共和国科学技术部, 2021年 9月). https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html

“习近平在“一带一路”国际合作高峰论坛圆桌峰会上的开幕辞,“『新华社』2015年 5月 15日. https://www.gov.cn/xinwen/2017-05/15/content_5194130.htm

“一带一路”十年丰硕成果,“『中国经济时报』2023年 10月 16日.

“全球数据安全倡议(全文),”『新华社』2020年 9月 8日. https://www.gov.cn/xinwen/2020-09/08/content_5541579.htm

《共建“一带一路”：构建人类命运共同体的重大实践》白皮书, (北京; 中华人民共和国国务院新闻办公室, 2023年 10月). http://www.scio.gov.cn/zfbps/

zfbps_2279/202310/t20231010_773682.html

『新華通信』 2025年 7月 27.

『解放軍報』 2025年 7月 10日.

サイバーセキュリティ戦略本部. 2021. サイバーセキュリティ戦略.
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf (검색일; 2025.10.31.)

サイバーセキュリティ戦略本部. 2025. サイバーセキュリティ 2025.
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2025.pdf (검색일; 2025.10.31.)

国家サイバー統括室(NCO). 2025.
https://www.nisc.go.jp (검색일; 2025.10.31.)

熊本日日新開. 2025.
https://kumanichi.com (검색일; 2025.10.31.)

中國外交部, "Wang Yi on BRICS Cooperation on Counter-Terrorism and Cybersecurity"
https://www.mfa.gov.cn/eng/wjbzhd/202505/t20250504_11615432.html?utm_source=chatgpt.com (May 01, 2025).

中國外交部, "全球人工智能治理倡议," (2023年 10月 20日).
https://www.mfa.gov.cn/ziliao_674904/1179_674909/202310/t20231020_11164831.shtml.

2026 KACS 스페셜리포트

사이버 복합 넥서스:

최신 동향 파악과 대응 전략 모색

연구책임자: 김상배(서울대)

공동연구원: 윤정현(국가안보전략연구원)
오승희(국립외교원)
엄도영(국립외교원)
송태은(국립외교원)
이종진(서울대)
정태진(평택대)
이왕휘(아주대)
김주희(동덕여대)
김명하(서울대)
윤대엽(대전대)
이중구(한국국방연구원)
이수연(서울대)
신승휴(서울대)
박병광(국가안보전략연구원)
유준구(세종연구소)

연구보조원: 김명하(서울대)

발 간 일: 2026년 1월 16일

| 2026 KACS 스페셜리포트 |

사이버 복합 넥서스:

최신 동향 파악과 대응 전략 모색

한국사이버안보학회
KACS