

www.eai.or.kr

EAI 워킹페이퍼

북한의 AI 현황

오인환(동아시아연구원; 서울대학교)

북한의 AI 현황

오인환

EAI 수석연구원; 서울대학교 강사

I. 북한의 AI 관련 정책과 기술 발전 동향

북한의 인공지능(AI) 정책은 독립된 기술 어젠다라기보다 김정은 정권이 표방해 온 "과학기술강국 건설"과 "경제의 정보화" 노선의 하위 범주로 배태(胚胎)되어 왔다. 북한은 1960~70년대 '기술혁명', 1990년대 '정보화혁명', 2000년대 '새 세기 산업혁명', 2010년대 이후 '수자경제(數字經濟, 디지털경제)'로 이어지는 일련의 사회주의 경제성장 방법론 속에서 AI를 인식하였으며, 이를 노동의 절약과 생산의 자동화, 지능화, 무인화를 달성하기 위한 기술적 수단으로 자리매김하려 한다. 이러한 계보 속에서 AI는 '인민경제의 CNC화'와 '경제의 정보화'를 완성하는 단계의 기술로, 기존 디지털전환(DT)의 토대 위에서 추가적 가치를 창출하는 연속선상의 도구로 호명된다.

정책 및 법제 측면에서 북한의 AI 추진은 2019년을 분기점으로 본격화되었다. 북한은 2019년 헌법 제26조의 경제발전 원칙에 기존의 "주체화·현대화·과학화"에 더하여 '정보화'를 추가하였고, 같은 해 동법 제40조에 '전민과학기술인재화'를 명시함으로써 첨단기술 발전을 위한 헌법적 근거를 정비하였다. 다만 미국, 중국 등 주요국과 달리 북한은 AI의 육성 및 활용을 직접 규율하는 단행 법률을 제정하거나 국가 차원의 AI 발전전략을 공식화하는 단계에는 이르지 못한 것으로 평가된다. 대신 「이동통신법」, 「과학기술성과도입법」, 「소프트웨어보호법」 등 ICT 일반 법제를 2020년 전후로 연달아 정비하여 정보산업의 제도적 틀을 마련하는 방식으로 접근하였다.

조직 측면에서는 2021년 IT 및 정보화산업을 총괄하는 '정보산업성'을 신설하였고, 2013년 설립되었던 인공지능연구소를 정보산업성 산하로 편입 및 승격한 것이 핵심 변화이다. 신설된 정보산업성은 기존의 전자공업성을 확대 개편한 것으로, 체신성(방송·통신), 국가정보화국(소프트웨어),

전자공업성(하드웨어)을 통합하여 정보산업 거버넌스의 구심점 역할을 수행하는 것으로 추정된다. 이와 함께 북한은 평양컴퓨터기술대학의 프로그램공학부를 지능정보공학부로 전환(2019년)하고 김책공업종합대학 등에 인공지능학과를 개설(2021년)하는 등 전문인력 양성 체계를 정비하였으며, 초·중등 교원을 대상으로 한 AI 관련 과목 신설, 전국 단위 프로그래밍 경진대회와 코딩 교육 확대를 통해 수직적 인재 양성 체계를 구축해 왔다. 아울러, 2019년부터 매년 ‘전국정보화성과전람회’를 개최하여 연구소, 기업 및 기관의 AI 프로그램과 제품을 대내외에 홍보하며, 김일성종합대학 등을 통해 딥러닝 적용 음성인식 등 다수의 연구논문을 발표하고 있다.

기술 발전 동향을 학술 문헌의 추이로 살펴보면, 북한의 AI 연구는 응용 지향성과 점진적 심화라는 특징을 보인다. 김일성종합대학학보(정보과학), 정보과학, 정보과학과 기술 등 주요 ICT 학술지에 2020년부터 2024년까지 수록된 논문은 연간 400여 건에 이르며, 이 가운데 인공지능 분야는 2020년 전후 딥러닝의 도입을 계기로 신경망 응용 연구가 증가하였고, 2021~22년에는 모델의 경량화·최적화 연구가, 2023~24년에는 도메인별 특화 응용과 융합기술(퍼지+신경망, 진화연산+제어 결합 등) 연구가 두드러진다. 자연어처리·기계번역(특히 조선어 기반 신경기계번역), 음성인식·합성, 컴퓨터 비전 및 영상처리(얼굴·차량 인식, 의료영상 진단보조)는 북한이 상대적으로 특화된 영역으로 꼽힌다. 주목할 점은 북한이 챗GPT 유사 모델을 ‘생성식 인공지능’으로 소개하며 그 활용 가능성을 높이 평가하는 등, 글로벌 추세에 대한 인지(認知)와 담론적 추수(追隨)가 확인된다는 사실이다.

종합하면, 북한의 AI 정책은 (가) 헌법 개정과 조직 신설을 통한 제도적 기반 정비, (나) 교육·인재 양성 체계의 수직적 정비, (다) 머신러닝 기반 인식기술을 중심으로 한 연구개발의 점진적 확대, (라) 러시아, 중국 등과의 대외 기술협력 모색이라는 네 축으로 전개되어 왔다. 그러나 이러한 추진의 근저에는 AI를 독자적 프런티어 기술이 아닌 ‘경제의 정보화’를 위한 보완적·수단적 기술로 인식하는 일관된 정책 기조가 자리하고 있다. 이 점에서 북한의 AI 인식은, AI를 또 하나의 신기술로 간주하여 기존 하드웨어 및 생산력 강화에 접목하려 한다는 점에서 중국의 ‘구신지능(具身智能, embodied AI)’ 노선과 유사하나, 산업, 시장 및 생태계의 기초 체력과 성공 경험이 부재하다는 점에서 그와 결정적으로 구분된다. 이러한 정책 기조는 후술하는 북한 AI의 활용 양상과 한계를 규정하는 출발점이 된다.

II. 북한의 AI 활용 현황과 분야별 특징: 군사, 경제, 지식 및 거버넌스

북한의 AI 활용은 군사, 경제(산업·생산), 지식 및 거버넌스의 세 영역에 걸쳐 비균질적으로 전개되고 있다. 각 영역은 자원 제약과 단기적 성과 가시화 가능성, 그리고 체제 유지라는 정권의 우선순위에 따라 상이한 추진 강도와 양상을 보인다.

1. 군사

군사는 북한이 AI 군사화의 잠재력에 가장 높은 전략적 우선순위를 두는 영역이다. 북한은 AI 군사기술의 개발 및 전력화 실태를 핵·미사일 시험과 달리 외부에 공개하지 않아 ‘블랙박스’와 같이 세부 파악이 어려우나, 최근의 연구 동향과 정책 발언을 통해 그 지향점을 추론할 수 있다. 김정은 위원장은 2025년 정찰 및 자살형 AI 드론 시험을 직접 지도하며 "무인 장비와 인공지능을 군 현대화 계획의 우선순위로 삼을 것"을 강조하였고, 군 총참모부는 모든 군종에 걸친 "AI 기반 유무인 다목적 전투체계" 구축을 지시한 것으로 알려져 있다. 이는 AI가 북한의 군사 무기체계에 통합되는 전략적 전환의 신호로 해석된다.

북한의 군사 AI를 평가할 때는 그 수준을 과대평가하여 불필요한 공포를 조장하는 것, 이미 실전에서 활용되고 있는 위협을 과소평가하여 놓치는 것 모두 경계해야 한다. 위협의 본질은 기술의 고급성이 아닌 ‘전용 가능성’과 ‘전술적 결합’에 있다. 즉, 북한은 글로벌 AI 전략 경쟁의 주자가 아니라, 체제 유지, 군사, 감시, 사이버 목적에 특화된 실용 AI를 보유한 국가로 규정하는 것이 사실에 가깝다. 군사 AI의 역량을 플랫폼(연산 인프라)·알고리즘·데이터의 세 요소로 나누어 보면 이 점이 분명해진다.

플랫폼 측면에서 북한은 구조적 한계에 직면해 있다. 대북제재로 NVIDIA A100·H100 등 엔터프라이즈급 AI 칩셋의 공식 확보가 불가능하여, GeForce RTX 계열 소비자용 그래픽 카드를 병렬 연결하거나 중국산 상용 드론 및 스마트폰의 칩셋을 분리하여 무기체계에 이식하는 방식으로 엣지(edge)용 연산 자원을 충당하는 것으로 추정된다. 하드웨어 획득은 중국 내 위장회사를 통한 부품 밀반입, 제3국 파견 연구원을 통한 현지 대학 및 클라우드 자원의 원격 활용, 암호화폐 탈취 자금의 세탁을 통한 직접 구매 등 우회 경로에 의존한다. 더 결정적인 제약은 전력 수급이다. 과도한 수력 발전 의존에 따른 계절적 편차와 전압·주파수 불안정은 24시간 연속 가동이 필수인 대형 모델 학습을 사실상

불가능하게 하며, 평양 과학기술전당 및 국방과학원 등 극소수 핵심 시설만 안정적으로 전력을 공급받는 우선공급 구조가 이를 더욱 심화시킨다. 이러한 한계로 인해 북한에는 하이퍼 스케일 데이터센터가 부재하며, ‘과학기술전당’을 허브로 하는 중앙집중형 인트라넷(광명망) 파일 서버가 그 역할을 대신하되 기관 간 연동성 부족으로 데이터 통합 활용에는 이르지 못한 것으로 평가된다.

알고리즘 측면에서 북한은 GPT-4 수준의 자체 파운데이션 모델을 보유했다는 증거가 없으며, 대신 저사양 환경에서도 구동 가능한 경량 특화 모델(SLM) 개발과 검증된 오픈 웨이트(open weights) 모델의 도입 및 운용 전략을 취하는 것으로 보인다. 김일성종합대학이 개발한 음성인식·번역 소프트웨어 ‘룡남산’, 세계대회 우승 경력의 바둑 AI ‘은별’ 등은 군사 위게임 및 드론 제어에 전용될 잠재력을 지닌 기반 기술로 거론된다. 특히 주목할 위험은, 인터넷이 차단된 내부망에서도 독자 운용이 가능한 Meta LLaMA, Alibaba Qwen 등의 오픈 웨이트 모델을 LoRA(Low-Rank Adaptation)와 같은 적은 자원으로 가능한 미세조정 기법을 활용하여 군사 교리 데이터 등으로 특화할 수 있다는 점이다. 이 경우 최첨단 모델 없이도 사이버 공격의 자동화(악성코드 변종 생성, 취약점 탐지 스크립트 작성)와 심리전 문구 생성 등 비대칭적 효용이 큰 영역에서 즉각적인 위협이 발생할 수 있다. 실제로 해외 정보기관은 북한 해커 조직이 LLM을 활용하여 피싱 문구를 정교화하고 악성 스크립트를 생성하는 정황을 포착한 바 있다.

데이터 측면에서 북한은 거대 모델 학습에 필요한 ‘오픈 인터넷 데이터’가 부재한 대신, 국가 주도 특수목적 데이터 확보에 역량을 집중하는 것으로 분석된다. 주민 통제 목적으로 강제 수집된 전 국민의 지문 및 안면 데이터는 감시용 안면인식 AI의 토대가 되며, 사이버 탈취를 통해 확보한 한국의 방산, 의료 및 포털 데이터셋은 한국어 자연어 학습과 군사 교리 분석에 활용될 수 있다. 즉, 북한은 ‘데이터 빈곤’을 불법적인 정보 수집과 국가 통제력으로 상쇄하여 특정 군사 및 감시 분야에서의 비대칭적 데이터셋을 구축해 가고 있는 것으로 평가된다.

이러한 세 요소를 종합하면, 북한의 AI 군사화는 자국이 비교우위를 지닌 비대칭 전략무기체계를 중심으로 전개될 가능성이 높다. 첫째, 사이버 작전은 AI 군사화 적용 가능성이 가장 높은 분야로 평가된다. 북한은 1990년대부터 사이버 전사를 체계적으로 육성하여 2024년 기준 약 8,400명 규모로 추정되는 사이버 작전 인력을 보유한 것으로 알려져 있으며, AI 도구를 활용한 악성코드 개발, 가짜 면접을 통한 IT 인력 침투, 암호화폐 탈취 등 공세적 사이버 활동을 외화벌이 및 정보수집 수단으로 적극 활용하고 있다. 둘째, 미사일 운용통제체계 분야에서 북한은 적의 미사일 방어망을 탐지·회피하고 궤적을 자율 변경하는 지능형 미사일 기술에 관심을 가질 것으로 예측된다.

셋째, 무인 전투체계 분야에서는 개별 무기의 지능화(on-device) 전략에 따라 드론 및 순항미사일 등 종말 타격수단에 경량 AI 모델을 탑재하여 타격 정확도를 높이는 데 집중할 가능성이 크며, UAV(무인기)의 소형화와 더불어 UUV(무인잠수정) 개발도 제기된다. 객체 인식(YOLO 등) 및 군집 비행 제어(PX4·ArduPilot 계열) 오픈소스의 변형 및 활용 정황은 이러한 방향을 뒷받침하는 식별 지표로 지목된다.

요컨대 한국이 플랫폼, 데이터, 알고리즘을 두루 갖춘 ‘시스템의 지능화’(full-stack)로 나아가는 반면, 북한은 ‘재래식 타격 수단의 정밀화’라는 파편화된(fragmented) 경로를 밟는다. 이는 단순한 우열의 문제가 아닌 서로 다른 차원의 위협이 맞물리는 비대칭적 경쟁 구도를 형성하며, 좁은 중심의 한반도에서 위기 시 오판과 확전의 위험을 증폭시킬 수 있다. 다만, 외부 연구기관들은 북한의 AI 군사화 기술 수준이 아직 낮은 단계에 머물러 있으며, 국제사회의 제재와 폐쇄성으로 인해 단기간 내 핵심기술의 전력화에는 제약이 따른다고 평가한다.

2. 경제 (산업 및 생산)

경제 분야에서 북한 AI 활용의 본질은 ‘경제의 정보화’를 위한 생산공정의 자동화 및 지능화이며, 그 기술적 실체는 CNC(컴퓨터 수치제어) 기술과 분산조종체계(DCS)의 진화 과정에 있다. 북한은 1995~2009년 ‘CNC공작기계 국산화’를 거쳐 2009년 컨트롤러(‘열린조종체계’) 국산화를 선언하였고, 2010년대 이후 이 컨트롤러 기술을 매개로 CNC를 개별 공작기계의 제어에서 센서 및 설비 데이터를 통합하는 공장 전체의 분산조종체제로 확장해 왔다. 이 과정에서 산업용 사물인터넷(IIoT) 플랫폼 성격을 지닌 공업정보체계 개발환경이 ‘미래 1.0’에서 ‘미래 4.0’으로 단계적으로 고도화되었으며, 2024~25년 북한 매체는 ‘미래102’와 같은 환경을 “체계들 사이의 정보통합을 능동적으로 분산시켜 전반적 생산공정을 진행하는 인공지능프로그램”으로 규정하기에 이르렀다. 즉, 북한에서 AI는 데이터의 축적과 활용을 매개로 기존 디지털전환의 토대 위에 적용되는 ‘임베디드(embedded) AI’로 자리하며, 신포시·락원군 바다가양식사업소의 통합생산체계 개발이나 국가통합전력관리체계 운영 등 구체적 사업장 단위의 적용 사례가 보고되고 있다.

다만 북한 매체가 보여주는 산업 AI 활용은 대규모 인프라와 자본이 요구되는 영역보다는, 기존 정보화 역량을 활용할 수 있고 단기적 성과 발현이 가능한 분야에 집중되는 경향이 뚜렷하다. 북한은 시장성, 성능, 품질보다 ‘구현 자체’의 성과와 속도에 무게를 두며, 생성형 AI 등 대규모

컴퓨팅을 전제로 하는 영역에서는 상대적으로 소극적인 양상을 보인다. 이는 북한 산업 AI가 ‘구조적 체질 개선’보다 기존 생산의 ‘정상화’를 보조하는 수준에 머물러 있음을 시사한다.

3. 지식 및 거버넌스

지식 및 거버넌스 분야에서 북한의 AI는 낮은 위험과 단기적 정책 성과를 거둘 수 있는 공공서비스 영역에서의 가시적 활용이 확인된다. 교육 분야에서는 AI 기반 학생 영어·수학 학습프로그램(‘무지개’, ‘날개’)과 중등교육 시험지 채점 소프트웨어, 의료 분야에서는 종합약국에 배치된 AI 로봇과 질병 예측 및 진단 보조 모델, 행정 분야에서는 행정정보망 고도화와 안면인식 기반 출입통제시스템 등이 보고된다. 자연어처리 분야의 7개국어 상호번역 시스템 ‘룡마’(2021년)와 음성인식 프로그램 ‘룡남산’은 학술·번역 영역에서 지식 처리 역량을 보여주는 대표 사례이다.

거버넌스의 관점에서 더욱 주목할 점은 AI가 북한의 사회 통제 기제와 결합하는 양상이다. 외부 연구들은 북한이 기존의 대규모 인적 감시망(인민반, 직장 관리자 등)에 더하여 바이오 인식, CCTV, 전자결제, 네트워크 통제를 통한 디지털 감시 기술을 지속적으로 고도화하고 있으며, 디지털 감시가 인적 감시를 ‘대체’하기보다 ‘보완’하는 방식으로 발전하고 있다고 분석한다. 즉, 권위주의 체제로서 북한은 심각한 자원 제약 속에서도 AI를 권력 강화와 정보 통제의 수단으로 전용(轉用)하기 위한 유인을 지니며, 이는 향후 러시아와의 협력 확대를 통해 인지전, 감시 분야의 전문지식이 유입될 경우 한층 심화될 수 있는 위험으로 지적된다.

세 영역을 종합하면, 북한의 AI 활용은 정권의 위험 회피적 자원 배분 논리에 따라 ‘낮은 위험·단기 성과’ 영역(공공서비스, 산업 정상화 보조)에서 가시적 성과를 내는 한편, ‘높은 전략적 가치’ 영역(사이버·군사, 사회 통제)에서는 잠재력 확보에 집중하는 이원적 구조를 보인다. 이러한 분야별 비 균질성 자체가 북한 AI의 자원적·기술적 제약을 방증하는 동시에, 향후 남북 협력 및 역내 안보 환경을 설계할 때 고려해야 할 핵심 변수가 된다.

III. 북한 AI 발전의 한계, 주체 AI의 한계와 북한의 전략적 선택방안

1. 북한 AI의 개념적·구조적 한계: ‘주체 AI’의 한계

북한 AI의 가장 본질적인 한계는 자원 및 인프라의 제약에 앞서, AI를 인식하는 개념적 틀 자체에 내재한다. 북한의 인공지능은 통상적인 AI와 지향성이 근본적으로 다르다. 통상적인 AI가 인간의 사고, 추론 및 학습을 모방하며 자율성과 데이터 기반 학습을 핵심으로 하는 데 비해, 북한의 AI는 "기계가 사람의 사고활동을 일정하게 대신하는 기술"로 정의되며 자동화, 최적화, 인간노동 대체를 핵심 초점으로 삼는다. 과학적 범위 또한, 통계학, 심층신경망, 대규모언어모델(LLM), 강화학습 등 데이터 중심 AI가 아닌 지식공학, 탐색이론, 전문가체계, 패턴인식, 기계번역 등 고전적 AI 범주에 머무는 경향이 있다. 이를 두고 일부 전문가는 북한의 AI가 "AI적 요소는 있으나 AI적 수준은 아니"며, 세계가 4세대(LLM, GenAI, 멀티모달) 단계에 진입한 가운데 북한은 2세대(규칙기반)에서 3세대(기계학, 딥러닝)로 전이되는 단계에 있다고 평가한다.

이러한 개념적 한계는 ‘주체(主體) AI’의 한계로 요약될 수 있다. 즉, 북한은 ‘우리식’, ‘주체적’ 기술을 강조하는 자립 노선 속에서 AI를 사회주의 경제건설과 생산현장 응용이라는 목표 지향성에 종속시키며, 이로 인해 (가) 데이터 및 컴퓨팅의 규모를 전제로 하는 현대 AI의 발전 경로에서 구조적으로 이탈하고, (나) 시장성과 성능보다 ‘구현 자체’의 정치적 성과를 우선하는 왜곡을 낳는다. 다만 흥미로운 점은, 최근 북한이 ‘우리식, 주체적’ 기술에 대한 강조를 다소 약화시키고 글로벌 추세와의 이격(離隔) 축소를 의식하는 담론적 변화를 보인다는 사실이다. 이는 자립 이데올로기와 기술적 현실 사이의 긴장을 시사한다.

2. 구조적·환경적 제약

개념적 한계에 더하여, 북한 AI는 다음과 같은 구조적·환경적 제약에 직면해 있다. 첫째, 국제사회의 대북제재와 경제난에 따른 고성능 컴퓨팅 및 반도체 등 선진 인프라 도입의 제한이다. AI 산업은 반도체(GPU와 HBM), 클라우드, 시스템 소프트웨어, 모델·데이터에 이르는 풀스택(full-stack)에서 각 레이어가 하위 레이어에 의존하는 ‘기술적 락인(lock-in)’ 구조를 지니는데, 북한은 그 출발점인 컴퓨팅 인프라에 대한 접근이 봉쇄되어 있다. 둘째, 글로벌 기술 트렌드와의 단절 및 국제

공동연구, 시험개발의 부재이다. 북한내 다수 연구는 외국의 선행 연구를 모방하는 수준에 있으며, 이미 상용화 및 보편화된 기술을 재현하는 데 머무는 경우가 많다. 셋째, 원료·연료·자재의 부족과 설비 노후화, 경제 하부구조(SOC)의 열악함 등 산업 전반의 미성숙이 AI가 실제 생산공정에 안착할 토양을 제약한다. 넷째, 소수 정예 연구집단 중심의 운영으로 인한 인재 저변의 협소함이다. 특히, AI의 급속한 발전으로 초·중급 지식노동의 상당 부분이 자동화되면서, 그간 북한이 비교우위로 여겨 온 소프트웨어 인력의 가치 자체가 잠식될 위험이 있다. 대규모 모델을 실제로 개발해 본 극소수의 최상위 인재만이 유의미해지는 경쟁 구조에서, 폐쇄적 환경의 북한이 그러한 자질을 확보하기는 사실상 불가능하다. 결과적으로 북한의 AI는 프로그램 기반의 공공, 교육, 농업, 일부 제조업에 응용이 집중되어, 인민경제 전반의 ‘생산 정상화’와 경제적 효과 창출은 제한적이며 구조적 체질 개선 수준에는 이르지 못하고 있다.

3. 자체 개발의 한계와 대중(對中) AI 종속 가능성

이상의 개념적·구조적 제약을 종합하면, 북한이 미국, 중국, 유럽의 프런티어 기업에 견줄 범용 AI 역량을 자체적으로 발전시킬 가능성은 사실상 희박하다. AI는 막대한 데이터, 컴퓨팅, 인재의 동시 투입을 요구하고, 네트워크 효과와 락인 효과가 강하게 작동하는 플랫폼 기술이기에, 후발주자의 자력 추격이 본질적으로 어렵고 대응이 늦을수록 완전한 소외로 귀결되는 성격을 지닌다. 이 때문에 북한의 현실적인 경로는 자체 개발이 아닌 외부 기술의 도입으로 수렴되며, 제재 환경과 정치적 조건을 감안할 때 그 통로는 사실상 중국으로 좁혀진다. 미국 기술의 도입은 북미 정상회담을 통한 정치적 돌파를, 한국 기술의 도입은 남북관계 개선을 각각 전제로 하는 반면, 오픈소스 기반의 높은 가성비를 갖춘 중국산 AI 소프트웨어 및 하드웨어는 이러한 정치적 문턱 없이도 접근 가능하기 때문이다. DeepSeek을 비롯한 중국산 오픈 웨이트 모델의 확산은 최고 성능의 GPU 없이도 일정 수준의 AI 역량을 구축할 수 있는 경로를 제공함으로써, 제재로 인한 컴퓨팅 봉쇄의 제약을 부분적으로 완화한다.

그러나 이러한 대중(對中) 종속 경로는 북한 AI 역량을 보완하는 동시에 새로운 전략적 위험을 수반한다. 첫째, 중국 플랫폼, 칩, 데이터 처리 방식 및 디지털 통치모델에 대한 의존은 북한의 기술주권을 중국에 종속시키고, 중국식 데이터·AI 거버넌스 및 표준에 대한 락인을 심화시킬 수 있다. 둘째, 북한이 중국식 감시 및 사회관리 기술을 부분적으로 수용할 경우 북한 체제의 디지털

권위주의적 성격이 한층 정교해질 수 있다. 셋째, 북한의 군사 및 사이버 AI가 중국 기술생태계와 연결될 경우 한반도 안보문제는 남북 간 사안을 넘어 미중 기술·군사경쟁의 하위 전선으로 편입될 수 있다. 북한 스스로도 중국에 대한 과도한 의존을 경계하는 것으로 보이나, 앞서 살펴본 자체 개발의 구조적 한계와 정치적 제약을 고려할 때 이 딜레마를 단기간에 해소하기는 어렵다.

4. 북한의 전략적 선택방안

이러한 한계는 역설적으로 북한의 합리적 전략 선택을 규정한다. 자원과 인프라가 제약된 후발주자로서 북한이 취할 수 있는 전략적 선택은 다음과 같이 정리된다.

첫째, **데이터 축적 토대 위의 선택적 적용**이다. 북한은 CNC, DCS 등 자체 디지털전환의 경험을 통해 데이터 축적이라는 ‘AI의 수용 토대’를 일정 부분 확보한 것으로 평가된다. 따라서, 대규모 투자가 필수적이지 않은 분야, 즉 기존 정보화 역량을 활용할 수 있는 영역을 중심으로 AI 적용을 점진적으로 확대하는 것이 합리적이다.

둘째, **후발자의 이점 활용과 외부 기술의 선택적 도입**이다. 일부 외부 연구는 북한이 최첨단 기술을 인프라에 통합하고 선례에서 얻은 교훈을 활용함으로써 후발주자의 이점을 누릴 수 있으며, 부족한 자원에도 불구하고 최첨단 알고리즘을 개발할 역량과 경험을 보유하고 있다고 본다. 특히, 2023년 이후 본격화된 러시아와의 과학기술 및 IT 협력은 제재 우회를 통한 기술 이전의 통로로 기능할 수 있으며, 북한은 이를 통해 AI 연구개발의 부분적·일시적 진전을 도모할 것으로 예상된다.

셋째, **데이터의 자산화와 가치사슬 내 위치 설정**이다. 자체 모델 및 인프라 경쟁에서 우위를 점하기 어려운 조건에서, 북한이 AI 가치사슬에서 확보할 수 있는 현실적 역할은 데이터의 생산자·공급자이다. 북한만이 생산하거나 북한에서만 시험 및 실증할 수 있는 데이터(예: 특정 산업공정, 농업, 보건 도메인의 폐쇄 데이터)를 자산화하는 전략은, 제한된 자원으로 AI 가치사슬에 진입하는 합리적 진입점이 될 수 있다. 이는 생성형 AI 기반 설비의 파일럿 테스트 공간으로서 북한이 기능할 수 있다는 경제 협력 시나리오와도 맞닿아 있다.

넷째, **사이버 및 군사 분야로의 전략적 집중**이다. 자원 제약 하에서 가장 높은 비대칭적 효용을 기대할 수 있는 사이버 작전과 비대칭 전략무기체계에 AI 역량을 우선 투입하는 선택은, 비용 대비 효과와 체제 생존 논리에 부합한다.

다섯째, **체제 유지와 기술 발전의 트레이드오프** 관리이다. 북한 AI 발전의 근본적인 제약은 기술 자체가 아닌 개방과 협력을 통한 정상국가화가 체제 유지와 상충한다는 딜레마에 있다. 따라서 북한은 체제 안정성을 훼손하지 않는 범위 내에서 외부 협력을 선별적으로 수용하는, ‘제한된 개방’ 전략을 지속할 것으로 전망된다.

여섯째, **다자 호환성 확보를 통한 중국 의존 위험의 분산**이다. 자체 개발이 어려운 조건에서 중국 기술의 도입이 불가피하더라도, 중국식 데이터 및 AI 거버넌스와 표준에 대한 전면적 락인은 전략적 자율성을 결정적으로 잠식한다. 따라서 북한이 합리적 행위자로서 취할 수 있는 선택은, UN, APEC, RCEP 등 글로벌 및 지역 다자체제의 AI 생태계와 최소한의 호환성을 확보하여 대안적 기술·표준에 대한 접근 경로를 일부 열어 두는 것이다. 다만, 이러한 호환성 확보는 일정 수준의 대외 개방과 국제규범 수용을 전제로 하므로, 앞서 지적한 체제 유지의 딜레마와 다시 충돌한다. 결국 북한에게 다자 호환성 전략은 합리적 방향이되 정치적으로 제약된 선택지로 남는다.

요컨대 북한의 AI는 ‘주체 AI’라는 개념적 천장과 제재·자원이라는 구조적 바닥 사이에서, 디지털전환의 토대를 활용하여 선택적·점진적으로 발전하되, 자체 개발의 한계로 인해 상당 부분 중국 기술생태계에 의존하는 경로를 밟을 가능성이 크다. 이러한 진단은 AI 시대 남북 협력과 신통일구상을 설계함에 있어, 북한의 기존 디지털 리터러시를 활용할 것인가, 새로운 토대를 구축할 것인가, 상이한 표준(경영, 투자, 기술·설비, 사회 시스템)을 어떻게 합리적으로 절충할 것인가, 그리고 북한 AI의 대중(對中) 종속 심화를 어떻게 관리하면서 군사적 전용을 억제하고 민간 활용을 선별적으로 지원할 것인가라는 핵심 과제를 제기한다. ■

■ **오인환**_EAI 수석연구원; 서울대학교 강사.

■ **담당 및 편집: 임재현**_EAI 연구원

문의: 02-2277-0746 (ext. 209) jhim@eai.or.kr

인용할 때에는 반드시 출처를 밝혀주시기 바랍니다.
EAI는 어떠한 정파적 이해와도 무관한 독립 연구기관입니다.
EAI가 발행하는 보고서와 저널 및 단행본에 실린 주장과 의견은 EAI와는 무관하며 오로지 저자 개인의 견해를 밝힙니다.

발행일 2026년 9월 21일
979-11-7584-152-9 95340

재단법인 동아시아연구원
03028 서울특별시 종로구 사직로7길 1
Tel. 82 2 2277 1683 Fax 82 2 2277 1684

Email eai@eai.or.kr Website www.eai.or.kr