Institute For National Security Strategy
www.inss.re.kr

June 2026
No. 399

INSS 전략보고

북한 AI 역량 평가와 안보적 함의
음성 AI 기술과 연산 환경을 중심으로

김민정
mkim@inss.re.kr

국가안보전략연구원

June 2026
No. 399

CONTENTS

북한 AI 역량 평가와 안보적 함의: 음성 AI 기술과 연산 환경을 중심으로

북한 AI 역량 평가와 안보적 함의: 음성 AI 기술과 연산 환경을 중심으로

저자 | 김민정

국문 초록

북한의 인공지능 역량 평가는 공개 논문 수와 초거대 모형 보유 여부에 한정될 경우 군사·치안·사이버 분야의 실제 활용 가능성을 충분히 반영하기 어렵다. 본 고는 북한 연구자가 공개한 음성 인공지능 논문과 연산 장비 활용 정황을 분석하여 제한된 자료와 구세대 장비 조건에서 특정 임무용 기능을 구현하려는 북한 인공지능 연구의 특성을 평가하였다. 분석 결과, 호출어 식별 연구는 공개 음성자료와 휴대 단말급 연산칩을 활용하여 대기 장비의 명령어 호출 기능을 구현한 응용 연구 성격을 보였다. 음성합성 연구는 제한된 한국어 음성자료와 서버급 그래픽처리장치를 활용하여 합성음 생성 속도와 자연성 개선을 시도하였다. 억양 식별 연구와 음성 활동 탐지 연구는 방송·웹 영상 추출 자료와 잡음 음성자료를 활용하여 발화 특성 판별 및 현장 음성 구간 선별 기능을 검증하였다. 해당 논문들에서는 엔비디아 테슬라 P100과 지포스 RTX 2070가 활용되었는데 이는 북한 인공지능 연구가 중소형 모델 학습과 민수용 그래픽카드 실험에 집중되어 있음을 보여준다. 또한 퀄컴 스냅드래곤 820 활용 정황은 연구실 수준의 학습 결과를 소형 장비 탑재 환경에서 검증하려는 시도를 보여준다. 이러한 양상은 북한이 자체 연산 자원 제약에도 외부 모형 접속과 공개 가중치 모델을 병행할 경우 감시·식별·기만 기능을 보강할 가능성을 제기한다. 따라서 북한 인공지능 역량 평가는 연구 규모와 장비 세대에 대한 정량적인 판단을 보완하여, 자료 처리 능력과 실행 환경을 종합 검토할 필요가 있다. 또한 장비 활용 정황과 군사·공작 분야 적용 가능성도 병행 검토하여 제한 자원 조건에서의 임무형 인공지능 운용 가능성을 조기에 식별할 필요가 있다.

주제어: 북한 인공지능, 음성 AI, 딥러닝, 경량 모델, 연산 장비, 감시·식별 기술, 대북 제재, 북·중·러·이란 공조, CRINK

Ⅰ 문제 제기

- 조선로동당 제9차 당대회에서 김정은 위원장은 인공지능을 ICBM 계열 전력과 동일한 군사 기술력 과업 안에 포함하여, 전략무기 보강과 전력 증강에 활용할 비대칭 전력으로 간주
  - 핵 무력 확대 언급 직후 대륙간탄도미사일, 인공지능 도입 공격체계, 무인 공격수단, 적 위성 타격 수단 개발 과업 제시

- 최근 인공지능 모형의 제공 양상은 북한 역량 평가에서 독자 모형 보유 여부보다 외부 모형 호출·공개 기술 재사용·탈취 계정 활용 능력 검토의 필요성을 제기
  - 외부 접속 경로(API) 제공형이 주요 인공지능 모형 공개 사례에서 약 절반을 차지하고 학습 코드 미공개 사례도 다수 확인되면서, 북한의 실질 운용 역량은 자체 초거대 모형 유무만으로는 판단 제한
    ※ API[1]는 AI 모형 미보유 조건에서도 계정·인증키를 통해 외부 서버의 모형 기능을 프로그램으로 호출하는 기술 접속 수단이며, 북한은 고성능 AI 모형을 직접 확보하지 못한 경우에도 계정, 인증키, 제3국 서버를 이용해 번역·문서 작성·코드 보조·취약점 조사 기능 활용
- 특히 북한은 첨단 반도체 수출통제로 대규모 연산 인프라 확보가 구조적으로 차단된 조건에서, 제한된 연산 자원을 전제로 한 경량화·최적화 기법에 연구 역량을 집중해 온 것으로 평가
  - 경량화·최적화 기술 경로는 동일 모델의 민생용 단말과 군사·정보용 내장형 장비 전용을 뒷받침할 수 있어 이중용도 가능성 배제 곤란

- 북한의 AI 관련 공개 논문은 2024년 기준 세계 145위 수준이었으나 이후 해당 정량 지표에 반영되지 않은 질적 변화 정황이 관찰되어 자료 처리 능력·실행 환경·임무 적용 가능성을 포괄한 종합 평가 필요

- 이에 본 고에서는 북한 연구자가 발표한 인공지능 연구 산출물 일부를 분석하고, 해당 연구를 통해 확인되는 북한의 AI 기술 수준과 감시·식별·통제 영역의 안보적 함의를 검토
  - 다만 공개 논문 수는 폐쇄적 연구 환경이나 군사 분야 비공개 개발, 혹은 제재 회피형 기술 활용이나 외부 모형 접속을 통한 운용 가능성 등을 미반영하므로 논문 수와 실제 안보상 함의 분리 요망

1 Application Programming Interface의 약자

Ⅱ 공개 자료 기반 북한 AI 기술·운용 여건

1. 공개 자료 기반 기술 여건

가. 공개 자료를 통한 음성 AI 기술 연구 변화[2]

- 공개된 북한 AI 관련 자료 중 연도, 저자·소속, 장비·환경, 연구 내용 등이 동시에 확인되는 사례가 제한되어 접근 가능한 공개 자료를 기준으로 기술 변화 양상 검토(〈표 1〉)
  - △신경망 연구(2026), △음성합성연구(2025) △억양식별 연구(2025) 및 △음성 활동 탐지 연구(2023)

- 대규모 연산 인프라 확보가 제한된 조건에서, 공개 논문상 모델 경량화와 연산 최적화, 내장형 장비 탑재 검증을 지향한 북한 인공지능 연구 사례 확인
  - 네 편 모두 제한된 학습자료와 공개 음성자료를 활용해 음성 선별·생성·판별·호출 기능의 성능 개선을 시도한 사례
  - 공개 음성자료, 중급 그래픽처리장치, 휴대전화급 연산칩, 저전력 장비용 실행환경을 조합하여 특정 임무용 음성 기능을 구현한 자원 제약형 응용 연구로 평가
  - 호출어 식별연구는 소형 장비 실측 검증에, 음성합성연구는 저성능 장비의 생성 속도 개선에, 억양식별연구는 제한된 자료 보강에, 음성 활동 탐지 연구는 잡음 환경 하 음성 구간 선별에 각각 초점.

〈표 1〉 북한 연구자들의 최근 음성 AI 기술 연구

연도	주제/제목	저자·소속	장비·환경	내용
2026	신경망 연구/Design of an Efficient Convolutional[3] Neural Network Based on Temporal Convolution for Wake-up Spotting[4]	김장수 (김일성종합대학 항공우주학부), 리기성 (김일성종합대학 항공우주학부), 엄철남 (김일성종합대학 첨단기술개발센터 정보기술연구소), 김명진 (김일성종합대학 물리학부)	Qualcomm MSM8996 Snapdragon 820 휴대전화급 연산칩 탑재 실험용 내장형 장비, 내장형 리눅스 운영체제, 저전력 장비용 실행환경 사용	Google Speech Commands 64,727개 음성 파일을 활용해 대기 장비의 호출어 식별 속도와 정확도를 평가한 연구로, 무인장비·은닉 감시장비·현장 명령 수신 장치의 음성 기반 운용 여지와 관련

2 지면 제약상 구체적 기술 분석은 별도 학술 논문으로 작성하여 학술지 게재 예정

3 Convolutional("합성곱")은 영상·음성 자료에 포함된 사람, 사물, 소리의 반복적 특징을 자동 식별하는 AI 연산 기법을 의미

4 Jang Su Kim, Ki Song Ri, Chol Nam Om and Myong Jin Kim, "Design of an Efficient Convolutional Neural

연도	주제/제목	저자·소속	장비·환경	내용
2025	음성합성 연구/A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis[5]	송진혁, 정성철, 김태명, 김국철, 홍학호 (국가과학원 수학연구소)	학습은 단일 NVIDIA Tesla P100 그래픽처리장치, 실행은 AArch64 1.8GHz 휴대전화급 연산칩 사용	25시간 분량 한국어 음성 자료로 학습하고 모바일급 장비에서 합성음성 생성 속도와 자연성을 개선한 연구로, 음성 안내·기만·심리전·자동응답 장비 활용 여지와 관련
2025	억양 식별 연구/Korean Spoken Accent Identification Using T-vector Embeddings[6]	엄영수, 김학성 (리과대학 인공지능기술연구소)	GeForce RTX 2070 그래픽처리장치 사용, NVIDIA NeMo 활용	조선중앙TV와 웹 영상에서 추출한 70.9시간, 162명 발화자, 25,948개 음성 구간을 활용하고 합성음성으로 부족한 지역 억양 자료 보강
2023	음성 활동 탐지 연구/A Gated Recurrent Unit Based Robust Voice Activity Detector[7]	한일, 엄철남, Om), 김은일, 김장수 (김일성종합대학 첨단기술개발센터 정보기술연구소)	구체 장비 미기재, TensorFlow 학습환경과 MATLAB 잡음자료 생성만 확인	저신호대잡비 환경에서 음성과 비음성 구간을 판별하는 연구로, 잡음이 포함된 현장 음성자료의 선별·정리 역량 축적에 해당

▪ 과제 성격과 활용 자료가 상이하여 일률 비교에는 한계가 있으나, 동일 평가 항목 적용 시 신경망 연구(2026)는 제한된 장비 환경에서의 실행 검증 측면에서 상대적 우위 확인

- 신경망 연구(2026)는 구글 음성 명령자료 6만 4,727개를 활용해 호출어 식별 모델을 설계하고 스냅드래곤(Snapdragon) 820 개발보드에서 실행시간을 측정한 사례로, 대기 장비가 특정 음성 명령을 빠르게 식별하는 소형 장비 탑재형 연구
- 억양식별 연구(2025)는 조선중앙TV와 웹 영상에서 추출한 70.9시간 분량의 음성자료와 합성음성 보강 자료를 활용하여, 표준말·남부·서북·동북 억양을 구분하기 위한 발화 특성 판별

Network Based on Temporal Convolution for Wake-up Spotting," International Journal of Advanced Networking and Applications Vol. 17, No. 5 (2026), pp.7094-7100.

5 Jin-Hyok Song, Song-Chol Jong, Thae-Myong Kim, Guk-Chol Kim and Hakho Hong, "A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis," American Journal of Neural Networks and Applications Vol. 11, No. 1 (2025), pp.28-34.

6 Yong Su Om and Hak Sung Kim, "Korean Spoken Accent Identification Using T-vector Embeddings," Science Research Vol. 13, No. 2 (2025), pp.13-20.

7 Il Han, Chol Nam Om, Un Il Kim and Jang Su Kim, "A Gated Recurrent Unit Based Robust Voice Activity Detector," International Journal of Advanced Networking and Applications Vol. 15, No. 2 (2023), pp.5831-5836.

- 음성합성 연구(2025)는 25시간 분량의 한국어 음성자료로 학습한 모델을 모바일급 연산칩에서 시험하여, 낮은 성능의 장비에서도 합성음성 생성 속도와 자연성 개선
- 음성 활동 탐지 연구(2023)는 잡음이 섞인 음성자료에서 실제 발화 구간과 비발화 구간을 구분하는 모델을 시험하여, 현장 음성자료 선별·정리에 필요한 전처리 연구

▪ 학술기관 소속 연구자의 단일 자료라는 한계에도, 공개 자료를 통해 음성자료 처리, 경량 모델 설계, 소형 장비 실측 평가를 병행한 정황은 북한 내부 AI 연구 수준을 판단하는 참고 근거로 활용 가능

- 특히 신경망 연구(2026)는 제한된 전력·연산 여건에서 호출어를 즉시 식별하는 소형 장비 탑재형 연구까지 진입했음을 시사
- 내장형 리눅스, 퀄컴 스냅드래곤820, 텐서플로 라이트를 활용해 실행시간을 측정한 사례로, 제한된 장비 환경에서의 실측 검증까지 포함한 연구로 평가[8]
- 다만 순환 신경망 표현과 잔차 신경망 인용 혼재, 구글 음성 명령자료 설명 부족, 문장 오류,[9] 참고문헌 오류 등 학술적 완성도 측면의 한계도 병존

나. 공개 논문 게재 학술지의 신뢰도 평가

▪ 해당 논문들의 게재 학술지는 국제 핵심 인용색인 등재와 엄격한 동료심사 체계가 미확인되어 학술지 평판과 심사 신뢰도 제한(〈표 2〉)

〈표 2〉 게재 학술지 명단

연도	논문명	게재 학술지	저자 소속
2026	Design of an Efficient Convolutional Neural Network Based on Temporal Convolution for Wake-up Spotting[10]	International Journal of Advanced Networking and Applications, Vol. 17, No. 5, 2026, pp.7094-7100	김일성종합대학

8 Jang Su Kim 외, “Design of an Efficient Convolutional Neural Network Based on Temporal Convolution for Wake-up Spotting,” pp. 7098-7099.

9 신경망 종류를 혼동한 문장, 학습자료 설명과 실제 분류 대상 수가 맞지 않는 대목 등 존재

10 Jang Su Kim, Ki Song Ri, Chol Nam Om and Myong Jin Kim, “Design of an Efficient Convolutional Neural Network Based on Temporal Convolution for Wake-up Spotting,” International Journal of Advanced Networking and Applications Vol. 17, No. 5 (2026), pp.7094-7100.

연도	논문명	게재 학술지	저자 소속
2025	An Improved Adaptive Angular Margin Loss Function for Deep Face Recognition[11]	American Journal of Neural Networks and Applications, Vol. 11, No. 1, 2025, pp.1-10	국립과학원
	A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis[12]	American Journal of Neural Networks and Applications, Vol. 11, No. 1, 2025, pp.28-34	
	A Study on the Incremental Text-to-speech Synthesis Taking into Account Intermediate Feature-level Context[13]	American Journal of Engineering and Technology Management, Vol. 10, No. 6, 2025, pp.94-100	
	Korean Spoken Accent Identification Using T-vector Embeddings[14]	Science Research, Vol. 13, No. 2, 2025, pp.13-20	리과대학
	Research on Multi-player Tracking in Soccer Videos by Combining Tracking-Prediction-Detection[15]	Science Research, Vol. 13, No. 4, 2025, pp.90-100	
2023	A Gated Recurrent Unit Based Robust Voice Activity Detector[16]	International Journal of Advanced Networking and Applications, Vol. 15, No. 2, 2023, pp.5831-5836.	김일성종합대학

11 Kwang-Uk Han, Song-Jun Yun, Chol Song, Kwang-Min Kim and Chol-Jun O, "An Improved Adaptive Angular Margin Loss Function for Deep Face Recognition," American Journal of Neural Networks and Applications Vol. 11, No. 1 (2025), pp.1-10.

12 Song et al., "A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis," pp.28-34.

13 Song-Yun Kim, Jin-Hyok Song, Dae-Hun Pak, Dong-Song Pak, Myong-Hyok Won and Hakho Hong, "A Study on the Incremental Text-to-speech Synthesis Taking into Account Intermediate Feature-level Context," American Journal of Engineering and Technology Management Vol. 10, No. 6 (2025), pp.94-100.

14 Yong Su Om and Hak Sung Kim, "Korean Spoken Accent Identification Using T-vector Embeddings," Science Research Vol. 13, No. 2 (2025), pp.13-20.

15 Gyong-Jun So, Hak-Song Kim, Man-Chol Ho and Jin-Song Ri, "Research on Multi-player Tracking in Soccer Videos by Combining Tracking-Prediction-Detection," Science Research Vol. 13, No. 4 (2025), pp.90-100.

16 Il Han, Chol Nam Om, Un Il Kim and Jang Su Kim, "A Gated Recurrent Unit Based Robust Voice Activity Detector," International Journal of Advanced Networking and Applications Vol. 15, No. 2 (2023), pp.5831-5836.

▪ Science Publishing Group(SPG)은 Beall's List의 '잠재적 약탈 오픈액세스 학술 출판사 목록'[17]에 포함

- Beall's List는 별도 예외 표시가 없는 한 약탈 출판사가 발행한 모든 학술지를 '잠재적 약탈 학술지'로 취급한다고 규정

▪ SPG 계열 학술지와 IJANA는 홈페이지에서 다수 색인·식별 경로를 제시하나, 이는 논문 검색과 문헌 식별을 위한 기초 요건이며 동료 심사 품질을 보증하는 주요 인용색인 등재와 구분 필요

- SPG 계열 학술지는 Crossref·WorldCat·WanFang·J-Gate·Scilit·OpenAlex 등을, IJANA는 Google Scholar·ORCID·Crossref 등을 제시하나, 검토 대상 학술지의 Web of Science Core Collection 및 Scopus 등재 여부 미확인

▪ 이러한 학술지 평판상 제약에도 불구하고 논문에 기재된 장비명, 실행 환경, 활용 자료, 저자 소속, 연구진 반복 등장, 공개 모형 활용 정황은 기술 추적 자료로 활용 가능

- 학술성과의 신뢰도 검토와 별도로, 반복 확인되는 연산 장비와 실행 환경을 중심으로 북한의 제한된 장비 기반 응용 연구 동향 추적 要

다. 공개 논문 기준 북한의 AI 기술 연구 수준

▪ 2017~2023년 공개된 논문 기준 북한은 AI 관련 논문 161편으로 Scopus 기준 세계 145위[18]

- 해당 수치는 여타 국제기관의 최신 갱신 자료가 부재한 상황에서 여전히 국제적으로 통용되는 정량 기준
- 동일 기간 중국 연구자의 AI 관련 공개 논문은 약 86만 건으로 세계 최상위권 연구 규모를 형성한 반면, 북한 연구자의 공개 논문은 161건에 그쳐 토고와 에스와티니 등 연구량이 제한된 소규모 국가와 유사한 수준으로 집계[19]

▪ 그러나 2024년 이후 김일성종합대학 인공지능기술연구소 위상 변화, 생성형 AI 연구 착수, 그래픽처리장치 활용 사례 등 질적 변화가 누적되어 해당 정량 지표만으로 현 시점 역량을 평가하는 데 한계 존재

17 'Potential predatory scholarly open-access publishers'

18 Hyuk Kim, "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications," 38 North, January 23, 2024.

19 토고와 에스와티니 비교는 북한의 공개 AI 연구량이 주요 기술국과 큰 격차를 보이며 국제 논문 수 기준으로는 최하위권에 근접한다는 점을 보여주기 위한 정량 비교

- 본 고가 검토한 논문들 외에도, 김일성종합대학 인공지능기술연구소의 "2025년 10대 최우수정보기술기업" 선정[20] 및 동 연구소장 주도 생성형 AI 강습,[21] 김일성종합대학 연구진의 엔비디아 Titan XP 그래픽처리장치 4기 활용 연구[22] 등 AI 연구 변화 정황 추가 관찰
- 다만 동 사례들은 단편적 관찰에 해당하므로 북한 AI 연구 전반의 추세로 일반화하기보다 자원 제약형 응용 연구 양상과 이중용도 위험을 보강하는 단서로 활용이 적절

2. 공개 자료 기반 운용 여건

- 스냅드래곤 820은 휴대전화 급 연산칩으로, 북한 인공지능 연구가 서버 장비 학습 이외에도 소형 장비 검증 단계에 진입했음 시사
- 엔비디아 P100은 대규모 데이터 처리와 복잡한 AI 학습에 적합하여, 음성처리·영상추적 기능의 군사·사이버 응용 가능성 배제 곤란
- 지포스 RTX 2070은 중고품 접근성이 높아, 제재 下 우회 조달 여지 존재

■ 본 고가 검토한 공개 논문을 기준으로, 북한 AI 장비·환경은 구세대 GPU, 민수용 그래픽카드, 휴대 단말기급 연산 칩을 활용한 특정 임무형 AI 기능 구현 단계로 평가

- 구세대 서버용 GPU와 민수용 그래픽카드를 이용해 안면인식, 음성합성, 억양식별, 영상추적 등 특정 임무형 기능 구현

■ 국립과학원 연구진 논문들에서는 美 엔비디아 테슬라 P100이, 리과대학 연구진 논문들에서는 美 엔비디아 지포스 RTX 2070[23]이 김일성종합대학 연구진 논문에서는 美 퀄컴 스냅드래곤 820 연산칩 사용(〈표 3〉)

20 "2025년 10대 최우수정보기술기업의 경험 - 인재양성에서 이론과 실천을 잘 배합하였다," 『로동신문』 2026년 1월 5일자.

21 위의 글

22 "북한의 인공지능 연구 개발 현황과 발전 전망," 『NK경제』 2026년 2월 2일, https://www.nkeconomy.com/news/articleView.html?idxno=15921 (검색일: 2026년 5월 25일).

23 'RTL 2070'로 표기된 부분들이 다수 확인되나 RTX 2070의 오기로 판단

〈표 3〉 인공지능 장비·환경이 명시된 공개 연구 논문(선별)

연도	논문명	장비·환경	저자 소속
2026	Design of an Efficient Convolutional Neural Network Based on Temporal Convolution for Wake-up Spotting[24]	Snapdragon 820[25]	김일성종합대학
2025	An Improved Adaptive Angular Margin Loss Function for Deep Face Recognition[26]	엔비디아 테슬라 P100	국립과학원
	A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis[27]		
	A Study on the Incremental Text-to-speech Synthesis Taking into Account Intermediate Feature-level Context[28]		
	Korean Spoken Accent Identification Using T-vector Embeddings[29]	엔비디아 지포스 RTX 2070	리과대학
	Research on Multi-player Tracking in Soccer Videos by Combining Tracking-Prediction-Detection[30]		

24 Jang Su Kim, Ki Song Ri, Chol Nam Om and Myong Jin Kim, “Design of an Efficient Convolutional Neural Network Based on Temporal Convolution for Wake-up Spotting,” International Journal of Advanced Networking and Applications Vol. 17, No. 5 (2026), pp.7094-7100.

25 호출어 탐지 연구는 학습용 NVIDIA GPU를 활용한 2025년도 발간 타 인공지능 연구들과 성격이 구분됨. 해당 연구는 TC-ResNet-8·TC-ResNet-14 호출어 탐지 모델의 현장형 장비 적용 가능성을 확인하기 위해 휴대전화급 Qualcomm MSM8996 Snapdragon 820 칩을 탑재한 개발보드에 Embedded Linux 3.0과 TensorFlow Lite 1.13을 설치해 실행 시간 측정

26 Han et al., "An Improved Adaptive Angular Margin Loss Function for Deep Face Recognition,."

27 Jin-Hyok Song, Song-Chol Jong, Thae-Myong Kim, Guk-Chol Kim and Hakho Hong, “A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis,” American Journal of Neural Networks and Applications Vol. 11, No. 1 (2025), pp.28-34.

28 Song-Yun Kim, Jin-Hyok Song, Dae-Hun Pak, Dong-Song Pak, Myong-Hyok Won and Hakho Hong, “A Study on the Incremental Text-to-speech Synthesis Taking into Account Intermediate Feature-level Context,” American Journal of Engineering and Technology Management Vol. 10, No. 6 (2025), pp.94-100.

29 Yong Su Om and Hak Sung Kim, “Korean Spoken Accent Identification Using T-vector Embeddings,” Science Research Vol. 13, No. 2 (2025), pp.13-20.

30 Gyong-Jun So, Hak-Song Kim, Man-Chol Ho and Jin-Song Ri, “Research on Multi-player Tracking in Soccer Videos by Combining Tracking-Prediction-Detection,” Science Research Vol. 13, No. 4 (2025), pp.90-100.

▪ P100은 연구소급 서버에서 중소 규모 학습에, RTX 2070은 개인·업무용 컴퓨터에서 음성·영상 실험에, 스냅드래곤 820은 소형 단말에서 AI 기능 실행 여부 검증 용도로 사용(〈표4〉)

- P100은 고대역폭 메모리(HBM2)를 탑재한 2016년 공개 초기 데이터센터용 서버급 그래픽처리장치로[31] H100·B200 계열 대비 성능 격차가 크나 중소 규모 음성·안면 인식 연구에는 충분한 연산 자산
- 지포스 RTX 2070은 2018년 출시된 민수용 그래픽카드[32]로 중고품 접근성이 높아, 서버급 장비 확보 부담을 낮추면서 음성·영상 AI 반복 실험과 제재 下 우회 조달이 가능한 저비용 연산 장비
  ※ 중국 중고거래 시장에서 상위 제품인 RTX 2070 Super도 1,000위안 미만 거래 가능
- 스냅드래곤 820은 퀄컴이 설계한 MSM8996 계열 휴대전화용 통합 연산칩(SoC)으로, 2016년 전후 고급 스마트폰에 탑재되었고 소형 장비에서의 AI 기능 실행 검증에 활용된 구세대 모바일 연산 자산

〈표4〉 AI 연산 장비 세대별 성격 비교

구분	테슬라 P100	지포스 RTX 2070	H100·B200 계열
공개	2016년	2018년	2023년 이후
적합 분야	데이터센터용 GPU로 중소규모 딥러닝 학습, 고성능 계산	소비자용 그래픽카드로 영상·음성 AI 실험, 중소규모 학습·추론	최신 데이터센터용 AI 가속기로 초거대 AI 학습·추론과 대규모 데이터센터 활용
북한 논문 활용	연구소급 학습 장비 활용 정황	민수용 GPU 활용 정황	사용 정황 미확인
평가	구세대 서버급 연산 자산	조달 용이성이 높은 민수용 연산 자산	수출통제와 대규모 전력·인프라 소요 장비

▪ 특히 올해 2월 게재된 스냅드래곤 820 기반 연구는 연구실 학습 결과를 소형 내장형 장비에서 실행시간까지 측정한 사례로, 북한 AI 연구가 저전력 장비 탑재 검증 단계까지 일부 진전되었음 시사

31 P100은 16비트 정밀도 기준 초당 약 21조 회 부동소수점 연산과 초당 732GB 자료 전송을 처리하는 FP16 21테라플롭스급 구세대 데이터센터용 그래픽처리장치로, 최신 H100·B200 계열 대비 세대·성능 격차가 커 대규모 인공지능 경쟁 자산이라기보다 제한 자료 조건의 음성·영상 인식 실험용 연산 자산으로 평가

32 NVIDIA, “GeForce RTX 2070 Graphics Card,” NVIDIA; TechSpot, “Nvidia GeForce RTX 2070 Specs,” 2025. NVIDIA,

Ⅲ 북한 AI 기술의 안보적 함의

1. 자체 기술 축적과 외부 모델 운용 병행

가. 북한 내부 AI 연구 역량판별의 필요성

▪ 북한 인공지능 기술 현황 평가는 외부 모델 활용에 따른 역량 변화와 자체 개발 수준을 구분해 확인할 필요

- 해킹·피싱, 가상자산 절취, 영상·음성 기반 신원 위장 등은 고성능 자체 모델 없이도 외부 상용 모델, 공개 가중치 모델, 공개 소스 도구, 제3국 서버, 탈취 계정과 결합해 단기간 운용 효과 향상 가능
- 외부 접속 경로(API)를 통해 계정·인증키로 외부 서버의 모델 기능 호출이 가능하므로[33] 서버 침투 없이도 반복 질의, 프롬프트 자동화, 접속키 절취, 공개소스 접속 도구 결합을 통한 모델 역량 활용 가능
- 주요 모형의 API 제공과 학습 코드 미공개 확산은 공격 절차가 외부 모형 기능으로 보강되는 반면 방어 기술 축적은 제한되는 북한식 비대칭 운용 여건을 보여주는 단서

▪ 외부 모델 활용 능력만으로 식별하기 어려운 실제 운용 가능 범위와 대응 소요 판단을 위해 자체 개발 수준 확인 병행 필요

- 북한은 독자 방어 기술을 충분히 축적하지 못한 조건에서도 문서 작성, 번역, 악성코드 보조, 취약점 조사, 사회공학 문안 제작 기능을 외부에서 확보할 수 있어 안보상 파급 가능성 지대
- 공개된 AI 관련 자료 분석을 통해 자체 모델 설계 이해도와 데이터 확보·처리 능력 및 학습·검증 절차, 또한 제한된 장비 기반 구현 수준을 확인해야 군사·공작 분야 활용 가능성에 대한 종합 판단 가능

▪ 다만 공개 자료에 나타난 AI 역량은 북한의 해당 분야 인력 수준, 모델 활용, 외부 접촉 현황을 판단하기 위한 참고 자료로 한정되며, 비공개 AI 역량 추정에는 한계 존재

- 폐쇄성, 제재 환경, 공개 매체 관리 관행, 국내 학술지 검색 제한으로 공개 연구만으로 전체 AI 기술 수준 확인이 어려우며, 군사·안보 분야 기술은 비공개 개발 가능성 배제 곤란
- 장비 결합, 현장 데이터, 운용 절차, 반복 사용 기록이 확인되기 전까지 연구 논문에 나타난 기술을 실제 북한 보유 AI 기술로 확정하는 판단은 유보 要

33 Google Threat Intelligence Group, “GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use,” Google Cloud Blog, 2026년 2월 12일, https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use(검색일: 2026년 4월 26일).

나. 경량화·최적화 기반 AI 운용 양상의 반영

▪ 이와 동시에, 제한된 자원 여건에서 특정 임무에 필요한 기능만 선별·개조·결합하는 북한식 비대칭 활용 양상을 별도 검토할 필요

- 북한은 군사·사이버 분야에서 장기간 비대칭 수단을 우선 개발해 왔으며 AI 기술도 감시·식별·음성처리·문서작성·코딩보조·취약점 조사·신원기만 등 특정 임무 수행에 필요한 기능 단위로 활용 중
- 북한 AI 수준 파악 기준을 공개 논문 수, 고성능 연산 장비 보유, 초거대 모델 개발 여부 등으로 한정 시 실제 위협을 낮게 평가할 가능성 존재

▪ 기술 선진국과 동일한 첨단 모델 개발 경쟁 관점과 함께, 제재와 장비 부족을 전제로 한 모델 경량화, 연산 최적화, 외부 모델 접속, 현장 적용, 임무별 기능 보강, 비대칭 피해 유발 가능성도 동시 반영

- 경량 모델만으로도 실제 감시망 운용과 보안 자동화 수행이 가능하므로, 북한은 제한된 자원 여건 아래에서도 실용적 감시 체계 고도화가 가능한 것으로 판단

▪ 최근 세계 AI 산업에서는 고성능 모형의 외부 접속 경로(API) 제공이 늘고 학습 코드 비공개 사례가 다수를 차지하면서, 독자 학습 역량과 외부 모형 호출 역량을 구분해 평가해야 할 필요성 증가

- 작년 주목할 만한 AI 모델 중 API 접근형 공개가 가장 큰 비중을 차지하고 학습 코드 비공개 모델이 대다수
- 스탠퍼드대 인공지능 지표에 따르면 최근 주목할 만한 인공지능 모형 95개 가운데 45개가 외부 접속 경로(API) 형태였고 80개는 학습 코드가 공개되지 않은 것으로 확인

  ※ 학습 코드 비공개는 최상위 모델 재현을 제약하나, API 또는 원격 접속이 제공될 경우 내부 학습 절차를 알지 못해도 출력 기능 활용이 가능하여 모델 투명성 저하와 안전성 검증 한계 유발[34]

- 이는 북한 AI 역량 평가에서, 제한된 연산 환경에서 외부 모델 기능을 활용·변형하거나 모델 경량화·연산 최적화·임무별 기능 구현을 시도한 연구 논문 분석이 실질적 판단 근거가 될 수 있음을 의미
- 학습 코드 비공개는 최상위 모형의 재현을 어렵게 하나, 외부 접속 경로(API)가 제공될 경우 내부 학습 절차를 알지 못해도 출력 기능 활용이 가능하여 모형 투명성 저하와 안전성 검증의 한계 초래

34 Nestor Maslej 외, The AI Index 2026 Annual Report, Stanford Institute for Human-Centered Artificial Intelligence, 2026, p. 20, https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf(검색일: 2026년 4월 26일).

2. 북한의 AI 기술 인식과 대외 협력 변수

가. 북한 정권의 AI 기술 인식

- 제9차 당대회에서 김정은 위원장은 새 5개년 계획 기간 군사 기술력 강화 과업으로 대륙간탄도미사일과 인공지능 무인 공격 종합체를 함께 제시하며, AI 기술을 전략무기 보강 및 전력 증강 과업에 포함
  - "군사 기술력을 세계 최강의 수준에 올려세우기" 위한 "새로운 비밀 병기, 특수한 전략 자산" 과업 설명에서 대륙간 탄도 미사일 종합체와 인공지능 무인 공격 종합체를 가장 먼저 언급[35]

> "김정은 동지께서는…새로운 비밀 병기, 특수한 전략 자산들을 우리 군대에 취역 시킬데 대한 중대한 과제들을 제시하고…지상 및 수중 발사형의 대륙간 탄도 미싸일 종합체와 각이한 인공지능 무인 공격 종합체들, 유사시 적국의 위성을 공격하기 위한 특수 자산과 적의 지휘 중추를 마비시키기 위한 매우 강력한 전자전 무기 체계들, 더욱 진화된 정찰위성들이 포함될 것"

  - 이는 AI 기술을 전략무기 보강과 전력 증강에 활용할 ICBM 계열 전력에 준하는 비대칭 군사자산으로 인식하고 있음을 표출

- 북한 AI 기술은 1990년대 후반 정보기술 강화와 「은별」 개발로 가시화[36] 된 이후 최근에는 최고지도부의 승인 아래 군사 분야에 적극 활용 되어온 것으로 평가
  - 기타 공개 자료에서도 AI 기반 자폭 드론과 전략 정찰드론을 전력 현대화 과제로 반복 제시[37]

2021.1. 군사 장비의 지능화·정밀화·무인화를 군수공업의 우선 목표로 제시하고 정찰드론과 각종 무인 타격장비 개발을 과업으로 상정
2024.8. 자폭 무인기와 전략정찰 및 다목적 공격 드론 개발, 수중 자폭 공격 드론 개발, 드론 개발에 AI 기술 도입을 지시하고 11월 자폭 무인기 전면 양산 주문
2025.3. 최신 AI 기술이 도입된 자폭 드론과 전략 정찰 드론의 군사적 효용을 공개적으로 평가
2025.3. 무인항공기 시험에서 무인장비와 AI 분야를 무력 현대화의 최우선 과업으로 천명하고 국가 장기 계획 수립 지시
2025.9. AI 기술 개발과 드론 양산 능력 증대 재차 요구

35 노동신문, 2026년 2월 26일, 제57호(루계 제28853호), p.6.

36 김민정, "북한의 인공지능 기술을 활용한 인권 침해 가능성 및 우리의 대응 방안," 국가안보전략연구원, 「전략보고」 통권 303호 (2024), p.7.

37 Lami Kim, "Assessing North Korea's AI ambitions"), International Institute for Strategic Studies, 2026년 3월 20일, https://www.iiss.org/online-analysis/online-analysis/2026/03/assessing-north-koreas-ai-ambitions/ (검색일: 2026년 4월 26일).

▪ 북한이 인공지능 부문에 자원을 우선 투입하고 연구·교육 체계를 지속 정비해 온 점을 고려할 때, 제약된 정보 여건에서는 공개 연구 결과를 북한 AI 역량과 활용 방향 판단의 근거로 활용 가능

- 2013. 정보산업지도국 산하에 인공지능연구소를 설치하고, 2021년 이후에는 이를 정보산업성 체계로 편입하여 관련 부문의 위상 제고
- 2014. 김일성종합대학은 첨단기술개발센터를 설치해 음성·문자 인식, 동시통역, 빅데이터 분석을 연구하였고, 2018년 이후 여러 대학이 인공지능 전공 과정 도입
- 기업 부문에서도 만경대정보기술사는 2020년 지문·음성·안면·문자 인식 기능을 탑재한 휴대전화를 선전하였고 압록강기술개발회사는 딥신경망을 보안감시체계와 지능형 카메라에 적용한다고 홍보

나. 북한 AI 역량의 CRINK 협력 증폭 가능성

▪ 북한의 AI 역량은 응용 연구와 일부 활용 사례가 확인되는 수준이나, 주요국 대비 연구량, 연산·학습자료가 모두 부족한 낮은 단계로 평가

- 대규모 AI 훈련에 필요한 GPU·데이터센터·전력·학습자료 확보 제약으로 고급 AI 개발 가능성 제한[38]
- 북한은 제한적 GPU 활용과 감시·식별·음성·영상·시계열·생명정보 분야 응용 연구를 통해 AI 기술을 지속 축적하고 있으나, 독자 초거대 모델이나 대규모 데이터센터를 보유하지 못한 것으로 판단

▪ 그러나 최근 북·중·러·이란(CRINK) 간 군사·기술·사이버 접촉 증가로 중국의 공개형 대규모 모델, 러시아의 국가 주도 AI 생태계, 이란의 사이버 운용 경험이 북한의 AI 역량 보강에 활용될 가능성 존재

- CRINK 국가 간 다자 AI 협력의 확인 증거는 제한적이나 중·러, 북·중, 북·러, 중국·이란, 러시아·이란 등 양자 접촉이 사이버·정보작전·감시·드론·위성·통신 분야에서 누적 중[39]
- 지난 3월 스탠포드대학은[40] 미·중 모델 성능 격차가 사실상 축소되고 중국이 논문·인용·특허·산업로봇 설치에서 우위를 보인다고 평가

38 Lami Kim, “Assessing North Korea’s AI ambitions,” International Institute for Strategic Studies, 2026년 3월 20일, https://www.iiss.org/online-analysis/online-analysis/2026/03/ assessing-north-koreas-ai-ambitions/ (검색일: 2026년 4월 26일).

39 Centre for Emerging Technology and Security, “AI Cooperation Trajectories: Adversaries and Geostrategic Competitors,” The Alan Turing Institute, 2026.

40 Stanford AI Index 2026

- 따라서 북한 AI 위협 평가는 북한 내부 연구 성과만이 아니라 CRINK 협력망을 통한 인력 양성이나 자료 공유, 상용 AI 도구 활용, 우회 조달, 해외 IT 노동자 네트워크 등을 종합 판단할 필요
  - 다만 북·중·러·이란 간 다자 AI 협력 확인 자료가 제한적인 만큼, 현 단계에서는 기술 이전을 확정하기보다 양자 접촉, 공개 모형 접근, 우회 조달을 통한 간접 보강 가능성으로 평가하는 것이 적절
  - 특히 중국의 영상감시·안면인식·음성인식 기술, 러시아의 전장 자료와 드론·대드론 운용 경험, 기가챗·스베르 기반 AI 생태계, 이란의 무인기·사회공학·사이버 운용 경험 반영 가능

Ⅳ 전략적 고려 사항

1. 북한 AI 응용 가능성의 조기 식별과 대응체계 구축

▪ 국제 학술지 색인 등재 여부와 학술적 평판만으로 북한 인공지능(AI) 연구의 안보상 함의를 낮게 평가하기 어려우며, 학술적 완성도와 감시·추적 수단 활용 가능성을 구분 검토할 필요

- 약탈적 학술지는 게재료 수취와 논문 노출을 우선하는 경우가 많아 동료 심사와 연구 윤리 점검이 충분하지 않은 사례가 다수
- 북한 연구자는 약탈적 학술지를 국제 학술 활동 외양 확보, 연구 성과 축적 및 외부 노출, 기관 연구 역량 과시 수단으로 활용 가능
- 안면인식·음성합성·영상추적 연구는 검증 절차가 취약한 학술지에 게재되었음에도 감시·추적 절차에 필요한 식별 정확도, 자료 처리, 실행 속도 개선을 겨냥한 응용 연구에 해당

  ※ P100 활용 논문들은 「American Journal of Neural Networks and Applications」에, RTX 2070 활용 논문들은 「Science Research」에 각각 게재

▪ 제한 장비 환경에서의 실행 검증 사례는 북한 AI의 현장 적용 능력과 소형 감시·추적 장비 활용 가능성을 판단하는 별도 추적 대상

- 2024~2025년 게재 사례가 주로 그래픽처리장치 기반 학습·실험 정황을 보여주는 데 비해, 2026년 호출어 탐지 연구는 휴대전화급 연산칩, 내장형 리눅스, 텐서플로 라이트 실행환경을 제시하고 실제 실행시간을 측정했다는 점에서 소형 장비 탑재 검증 사례로 분류 가능
- 올해 발간된 호출어 탐지 연구는 신경망 명칭 혼용, 학습자료 설명 부족, 참고문헌 오류 등 학술적 한계가 확인된바, 연구 품질 평가는 유보하되 제한 장비 기반 실행 검증 정황은 별도 추적 필요
- 엔비디아 활용 연구는 초거대 연산 자원과 방대한 학습자료를 동원하는 미·중·유럽 AI 기술에는 못 미치나, 제한 장비 환경에서 특정 임무형 AI 기능을 구현하려는 북한의 기술 추진 양상을 확인한 사례
- 2024~2025년 발간된 인공지능(AI) 기술 연구 가운데 공신력 있는 저널 게재 사례도 다수 확인되나,[41] 해당 연구들은 대규모 연산 처리 등 현대 심층학습 구현 단계에는 미진

41 Hakjin Choe, Kukhuan Jang, Kyonghyok Ham, Chunghyok Kang, "A cascade control scheme with T-S fuzzy model-assisted linear active disturbance rejection controller for position tracking of cart inverted pendulum," 『International Journal of Dynamics and Control』(Springer, ISSN 2198-6061), 2025; Unjin Pak, Ho Kim, UnHui Jong, Ri Guang Hyon, Jang Hak Kim, Kukchol Kim, Kwangho Kim, "A deep learning

- 초거대 연산 자원과 방대한 학습자료를 동원하는 미·중·유럽 기술과 비교하면 1~2세대 후행 양상

2. 제한 장비 기반 기술 진전의 안보 함의 식별

▪ 북한 AI 연구에서 확인되는 주요 고려 사항은 초거대 모형 개발보다 제한된 자료·연산 여건에서도 음성 선별이나 합성음 생성, 또는 억양 판별 등 기능을 특정 임무에 맞게 구현하는 응용 능력에 있음

- 테슬라 P100과 RTX 2070 활용 정황은 대규모 AI 기반 시설 보유를 의미하지 않으나, 연구소급 서버와 민수용 그래픽카드를 통해 감시·식별·음성처리·영상추적 기능을 반복 실험할 수 있는 최소 연산 여건 확보 시사
- 스냅드래곤 820 기반 호출어 탐지 연구는 소형 장비에서 음성 명령 식별을 검증한 사례로 무인장비나 은닉 감시장비, 또는 현장 명령 수신 장치에 탑재 가능한 경량 AI 연구의 일부 추진 정황

▪ 따라서 최신 데이터센터급 그래픽처리장치 반입 차단 외에도 구세대 그래픽처리장치이나 민수용 그래픽카드, 혹은 단말기 급 연산칩이나 공개 음성·영상자료, 외부 모형 접속 경로까지 포함한 추적 필요

3. 민수 영역 데이터·응용 기술의 군수 활용 경계

▪ 북한 AI 기술은 민간 문장 생성·번역보다 전술 상황 판단, 교전 모의, 화력 운용 효율화 분야에 우선 활용될 가능성이 큰 것으로 판단

- 북한 학술지 『정보과학』에 강화학습을 적용한 전투 유희 지능대행체 연구가 수록됐으며 전투 승패, 포탄 명중률, 생존 시간 비율을 보상 항목으로 설정해 교전 조건에서의 전투 모의 가능성 검토[42]
- 해당 분석 보고서는 북한 연구진이 중국 군 관련 연구자의 공중전 모의 논문을 참고하였고 이전 학술 이력에는 전이학습과 같은 적은 자원 소모형 기법도 보인다고 지적
- 해당 연구는 중국 군 관련 연구자의 공중전 모의 연구를 참고하는 등, 제한된 자료·연산 여건에서 기존 모델을 특정 군사 과제에 재학습하는 기술 접근 가능성 확인

approach via multifractal detrended fluctuation analysis for PM2.5 prediction," 『Journal of Atmospheric and Solar-Terrestrial Physics』(Elsevier, ISSN 1364-6826), 2025; Gum-Chol Jong, Jong-Chol Choe, Un-Ryong Rim, Un-Song Ri, "Acoustic sediment classification using MLP-KNN model on single-beam echosounder data from shallow water," 『Marine Systems & Ocean Technology』(Springer, ISSN 2523-0857), 2025.

42 Kim, 2024.

▪ 북한은 연산 자원이 충분하지 않은 조건에서도 사전 학습을 마친 외부 모형과 공개 지식을 도입하여 군사용 과업에 맞게 다시 학습시키는 우회 경로를 찾을 개연성

- 2025년 3월 조선중앙통신은 새 전략정찰드론이 지상과 해상의 각종 전략 목표와 적군 활동을 추적·감시할 수 있다고 주장하고 같은 날 자폭드론의 전술 공격 임무 수행 능력을 선전, 김정은은 이를 토대로 무인체계와 인공지능 기술을 결합한 장기 계획 수립 지시

4. CRINK 공조 대응 및 제재 실효성 제고

▪ 북한은 우방국들의 군사용 AI 성과를 적극 수용 중으로, 미사일 유도·표적획득·무인체계에 딥러닝 등 최신 AI 기법을 적용하여 군사적 임계능력 상승 가능성 배제 곤란

- 북한 연구자들은 강화학습 활용 워게임 시뮬레이션 연구를 통해 포병 전투와 전술훈련 과정에 AI 기술 접목을 시도하였으며 해당 논문에 중국 군사과학원 연구진의 미사일 방어 시뮬레이션 논문 인용
- 2024년 6월 러·북 포괄적 동반자 조약은 우주·생물·평화적 원자력·인공지능·정보기술 분야 교류와 공동연구 촉진을 명문화하였고 국제 정보·안보 협력 병기

▪ 이에 AI 기술의 부정 활용에 대응하기 위해 국내 규제 강화와 우방국과의 기술 공조 및 공급망 보안 협력 등을 통해 혁신 역량을 유지하며 안보상 위해 가능성의 선제적 관리 요망

- 북한의 의료·정부·통신 등 광범위 표적 대상 첩보 행태는 미 정부 기소·제재 자료에서도 확인되며[43] GPU 병렬 가속 결합 시 내부 계정·문서 체계를 신속 식별·분석하여 접근권 탈취 소요 시간 단축

43 U.S. Cybersecurity and Infrastructure Security Agency(CISA), “FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity,” 2024.7.25.

참고문헌

1. 논문

Choe, Hakjin, Kukhuan Jang, Kyonghyok Ham and Chunghyok Kang. "A Cascade Control Scheme with T-S Fuzzy Model-assisted Linear Active Disturbance Rejection Controller for Position Tracking of Cart Inverted Pendulum." 『International Journal of Dynamics and Control』 (Springer, 2025).

Han, Il, Chol Nam Om, Un Il Kim and Jang Su Kim. "A Gated Recurrent Unit Based Robust Voice Activity Detector." International Journal of Advanced Networking and Applications. Vol. 15, No. 2 (2023), pp.5831-5836.

Han, Kwang-Uk, Song-Jun Yun, Chol Song, Kwang-Min Kim and Chol-Jun O. "An Improved Adaptive Angular Margin Loss Function for Deep Face Recognition." American Journal of Neural Networks and Applications. Vol. 11, No. 1 (2025), pp.1-10.

Jong, Gum-Chol, Jong-Chol Choe, Un-Ryong Rim and Un-Song Ri. "Acoustic Sediment Classification Using MLP-KNN Model on Single-beam Echosounder Data from Shallow Water." 『Marine Systems & Ocean Technology』 (Springer, 2025).

Kim, Jang Su, Ki Song Ri, Chol Nam Om and Myong Jin Kim. "Design of an Efficient Convolutional Neural Network Based on Temporal Convolution for Wake-up Spotting." International Journal of Advanced Networking and Applications. Vol. 17, No. 5 (2026), pp.7094-7100.

Kim, Song-Yun, Jin-Hyok Song, Dae-Hun Pak, Dong-Song Pak, Myong-Hyok Won and Hakho Hong. "A Study on the Incremental Text-to-speech Synthesis Taking into Account Intermediate Feature-level Context." American Journal of Engineering and Technology Management. Vol. 10, No. 6 (2025), pp.94-100.

Om, Yong Su and Hak Sung Kim. "Korean Spoken Accent Identification Using T-vector Embeddings." Science Research. Vol. 13, No. 2 (2025), pp.13-20.

Pak, Unjin, Ho Kim, UnHui Jong, Ri Guang Hyon, Jang Hak Kim, Kukchol Kim and Kwangho Kim. "A Deep Learning Approach via Multifractal Detrended Fluctuation Analysis for PM2.5 Prediction." 『Journal of Atmospheric and Solar-Terrestrial Physics』 (Elsevier, 2025).

So, Gyong-Jun, Hak-Song Kim, Man-Chol Ho and Jin-Song Ri. "Research on Multi-player Tracking in Soccer Videos by Combining Tracking-Prediction-Detection." Science Research. Vol. 13, No. 4 (2025), pp.90-100.

Song, Jin-Hyok, Song-Chol Jong, Thae-Myong Kim, Guk-Chol Kim and Hakho Hong. "A Fast Acoustic Model Based on Multi-Scale Feature Fusion Module for Text-To-Speech Synthesis." American Journal of Neural Networks and Applications. Vol. 11, No. 1 (2025), pp.28-34.

2. 보고서

Centre for Emerging Technology and Security. "AI Cooperation Trajectories: Adversaries and Geostrategic Competitors." The Alan Turing Institute (2026).

Maslej, Nestor 외. The AI Index 2026 Annual Report. Stanford Institute for Human-Centered Artificial Intelligence (2026).

김민정. "북한의 인공지능 기술을 활용한 인권 침해 가능성 및 우리의 대응 방안." 국가안보전략연구원. 「전략보고」 통권 303호 (2024).

3. 뉴스·기사 및 인터넷 자료

Google Threat Intelligence Group. "GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use." Google Cloud Blog. 2026년 2월 12일, https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use(검색일: 2026년 4월 26일).

Kim, Hyuk. "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications." 38 North. 2024년 1월 23일.

Kim, Hyuk. "North Korea's International Network for Artificial Intelligence Research." 38 North. 2024년 8월 21일, https://www.38north.org/2024/08/north-koreas-international-network-for-artificial-intelligence-research/(검색일: 2026년 4월 26일).

Kim, Lami. "Assessing North Korea's AI Ambitions." International Institute for Strategic Studies. 2026년 3월 20일, https://www.iiss.org/online-analysis/online-analysis/2026/03/assessing-north-koreas-ai-ambitions/(검색일: 2026년 4월 26일).

NVIDIA. "GeForce RTX 2070 Graphics Card." NVIDIA.

TechSpot. “Nvidia GeForce RTX 2070 Specs.” TechSpot (2025).
U.S. Cybersecurity and Infrastructure Security Agency. “FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity.” 2024년 7월 25일.
『노동신문』. 2026년 2월 26일, 제57호(루계 제28853호), p.6.

Abstract

Assessing North Korea's AI Capabilities and Security Implications: Focusing on Deep Learning and Intelligent Optimization Data Analysis

Minjung Kim
(Institute for National Security Strategy)

Evaluating North Korea's artificial intelligence capabilities solely through the number of publicly available papers or the possession of large-scale models risks overlooking practical applications in the military, public security, and cyber domains. This study examines North Korean researchers' published work on speech AI and observable computing environments to assess how North Korea seeks to implement task-specific AI functions under constraints in data availability and legacy hardware. Wake-up word spotting research shows an applied approach using open speech datasets and mobile-grade processors to enable voice-command activation in standby devices. Text-to-speech research demonstrates attempts to improve synthetic speech generation speed and naturalness using limited Korean speech data and server-grade graphics processing units. Accent identification and voice activity detection studies use broadcast, web-extracted, and noise-mixed speech data to classify speech characteristics and identify meaningful voice segments in field audio. The use of NVIDIA Tesla P100 and GeForce RTX 2070 indicates that North Korean AI research remains concentrated on small- and medium-scale model training and experiments with civilian graphics cards. The use of Qualcomm Snapdragon 820 also suggests attempts to validate laboratory-level models in compact device environments. These patterns raise the possibility that North Korea may reinforce surveillance, identification, and deception capabilities through external model access and open-weight models despite domestic computing constraints. North Korea's AI capabilities should therefore be assessed through

an integrated review of data processing capacity, execution environments, hardware use, and potential applications in military and covert operations, beyond quantitative judgments based on research scale or hardware generation.

Keywords: North Korean artificial intelligence, speech AI, deep learning, lightweight model, computing hardware, surveillance and identification technology, sanctions on North Korea, China–Russia–Iran–North Korea cooperation, CRINK

Institute For National Security Strategy

www.inss.re.kr

INSS 전략보고

June 2026
No. 399

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr

국가안보전략연구원