WTIS V4.0

Secure AI 기술·시장·규제 동향 — LG U+ 전략 관점

2026-02-25 | 신뢰도: HIGH | 출처 2건 | completed

경영진 요약

2025년 국내 통신 3사 연쇄 해킹(SKT 유심 2,500만 건, KT·LGU+ 포함)이 촉발한 보안 패러다임 전환으로, LG U+는 5년간 7,000억 원 투자와 2027년 Zero Trust 완성을 목표로 '보안퍼스트' 전략을 공식화했다. 글로벌 AI 보안 시장은 2026년 약 354억 달러, 2030년 863억 달러로 성장하며, Agentic SOC와 Privacy-Preserving AI가 2026년 핵심 트렌드로 부상한다. LG U+가 MWC 2025에서 공개한 Anti-DeepVoice + PQC(양자내성암호) 기술은 통신사 차별적 포지션을 확보할 수 있는 선점 기회이나, SKT 7,000억·KT 1조 원 투자 대비 절대 규모에서 불리하다. 2026년 1월 시행된 한국 AI 기본법은 고영향 AI 사업자 의무를 부과하며, 2027년 1월 과태료 시행 전 거버넌스 체계 정비가 시급하다. 신뢰도: 주요 사실 [A/B] 수준, 시장 규모 예측 [B] 수준.

분석일	신뢰도	상태
2026-02-25	HIGH	completed

연구 질문

LG U+ 기술전략 관점에서 2025~2026년 Secure AI 분야의 기술 성숙도, 시장 기회, 경쟁 구도, 규제 리스크를 어떻게 평가하고, 어떤 포지션을 취해야 하는가?

1 기술 현황

1.1 AI 시스템 보안 (AI-as-Target)

적대적 공격 (Adversarial Attacks)

NIST는 2025년 `NIST.AI.100-2e2025` 보고서[1]를 통해 적대적 머신러닝 공격을 체계적으로 분류했다. 공격 유형은 크게 훈련 단계(Training-time)와 배포 단계(Inference-time)로 구분된다:

- **Poisoning Attack**: 훈련 데이터를 오염시켜 모델 내부에 백도어를 삽입. 2025년 의료기기 제조사 사례에서 실제 피해 확인[2].
- **Evasion Attack**: 배포된 모델이 악성 입력을 정상으로 판단하도록 유도. 통신 네트워크 이상 탐지 모델에 직접 위협.
- **Model Extraction/Inversion**: 모델 파라미터나 훈련 데이터를 역공학으로 추출. 통신사 고객 데이터 프라이버시 위협.

LLM 보안 위협 (2025년 현황)

OWASP LLM Top 10 2025 기준[3]:

- **Prompt Injection (LLM01)**: 2년 연속 1위. 롤플레이 기반 공격 성공률 89.6%, 적응형 공격은 가드레일 100% 우회 가능.
- **Model Poisoning**: 공급망 전반에서 위협 급증. ExtraHop은 2025년 AI 공급망을 "가장 위험한 공격 벡터"로 지목[4].
- **Jailbreak**: Generative Adversarial 기법을 활용한 CAVGAN 등 새로운 공격 기법 지속 등장.

기술 성숙도 (TRL): LLM 보안 방어 기술 TRL 4~6. 공격 기법이 방어 기법을 앞서는 비대칭 구조.

1.2 AI 활용 보안 기술 (AI-as-Defender)

AI SOC (Security Operations Center) 자동화

2025년은 Agentic SOC의 실증 원년으로 평가된다[5]. 2026년에는 이를 표준 도입으로 전환하는 전환점이 될 전망:

- 자율적 알람 트리아지(Triage), 위협 상관분석, 인시던트 대응을 AI 에이전트가 수행.
- Seceon 플랫폼: 하루 수십억 이벤트 처리, 95~99% 탐지 정확도, 서브초(sub-second) 상관관계 분석[6].
- Airtel(인도 통신사): Elastic AI 도입으로 SOC 효율 40% 향상, 조사 속도 30% 단축[6].
- 글로벌 AI 사이버보안 지출: 2024년 248억 달러 → 2034년 1,465억 달러 예상[5].

멀티 레이어 아키텍처: 엔드포인트, 네트워크, 클라우드, 신원(Identity)에 걸친 협력형 AI 에이전트 메시(Mesh) 구조가 2026년 선도 플랫폼의 핵심 특징.

1.3 통신 인프라 AI 보안

5G 네트워크 이상 탐지

Springer Nature 2025년 리뷰 논문[7]에 따르면, 통신 네트워크 이상 탐지에서 AI 적용이 급격히 증가:

- **Hybrid Deep Learning**: Autoencoder + LSTM + CNN 결합으로 공간·시간·재구성 이상을 동시 탐지. 탐지율 최대 97.6%[8].
- **Reinforcement Learning (RL)**: 실시간 네트워크 환경 변화에 자기 적응하는 탐지 모델. 5G/6G의 고동적 환경에 최적.
- **Federated Learning**: 분산 IoT/엣지 노드에서 프라이버시를 보존하며 공동 학습. GDPR 준수 관점에서 EU가 권고하는 Privacy-by-Design 접근법[9].

위협 행위자 변화

Salt Typhoon, Volt Typhoon, Flax Typhoon 등 국가급 APT(Advanced Persistent Threat) 그룹이 통신사 와이어탭 시스템에 침투, 다년간 지속성 유지, 가입자 및 민감 네트워크 데이터 유출 사례 발생[6]. 전통적인 규칙 기반 방어로는 대응 불가능한 수준.

1.4 양자내성암호 (PQC) 기술 현황

NIST가 선정한 PQC 표준 알고리즘:

- **키 캡슐화**: ML-KEM (구 CRYSTALS-Kyber), HQC
- **전자서명**: ML-DSA, FALCON, SPHINCS+

3GPP는 5G-Advanced 및 6G 규격에 PQC 통합을 연구 중이나, 공식 배포 전까지는 임시 해결책(Hybrid 방식) 사용[10].

실증 사례: SKT + Thales — 양자 내성 SIM 카드(CRYSTALS-Kyber)로 SUPI(가입자 식별자) 암호화 실증. SoftBank — 4G/5G 트래픽에 Hybrid PQC 파일럿[10].

TRL 평가: PQC 알고리즘 자체 TRL 7~8 (표준화 완료). 5G 네트워크 통합 TRL 5~6 (파일럿 단계). 전면 배포 TRL 4~5.

---

2 시장 동향

2.1 글로벌 AI 보안 시장

지표	수치	출처	신뢰도
2024 AI 사이버보안 시장	$248억	Gartner/업계 추정	[B]
2026년 AI 사이버보안 시장	$354억	Precedence Research	[B]
2030년 AI 사이버보안 시장	$863억	Precedence Research	[B]
CAGR (2024~2034)	~19%	복수 리서치 추정	[B]
연방학습 시장 (2024)	$1.386억	업계 추정	[C]
연방학습 시장 (2030)	$2.975억	업계 추정	[C]
연방학습 성장률	>40% YoY	업계 추정	[C]

국내 시장 특징: 국내 기업 AI 보안 성숙도 3%에 불과(2025년 기준) → 미충족 수요(Unmet Demand) 대규모 존재.

2.2 성장 드라이버

1. **규제 압박**: 한국 AI 기본법 시행(2026.1.22), EU AI Act 고위험 AI 조항 발효(2026.8.2)
2. **위협 진화**: 국가급 APT의 통신 인프라 공격 증가, LLM 기반 자동화 공격 도구 확산
3. **Agentic AI 도입**: 보안 인력 부족 + 알람 과부하(Alert Fatigue) 문제를 자율 AI 에이전트로 해소
4. **양자 컴퓨팅 위협**: "Harvest Now, Decrypt Later" 공격 현실화 우려로 PQC 수요 가속

---

3 경쟁사 동향

3.1 국내 통신사 비교

항목	LG U+	SKT	KT
5년 보안 투자	7,000억 원	7,000억 원	1조 원
2024년 실제 투자	828억 원 (IT대비 7.4%)	600억 원 (8.7% 증가)	1,218억 원
주요 AI 보안 기술	Anti-DeepVoice, PQC, On-Device AI	스캠뱅가드(Scam Vanguard), Zero Trust	AI 보이스피싱 탐지 2.0, AI 사이버 센터
Zero Trust 목표	2027년 완성	2026년 추진	국내 최초 통신+IT 통합 AI 사이버 센터
보안 인력	292.9명 (전년 대비 +86%)	미공개	300명 확대 계획
MWC 2025 발표	Anti-DeepVoice + PQC + On-Device AI	스캠뱅가드 CES 수상	-

출처: 보안뉴스, 파이낸셜뉴스, 보안뉴스 정보보호 공시 데이터[11][12][13]

LG U+ 상대적 강점: IT 투자 대비 보안 투자 비율(7.4%)이 3사 중 최고. Anti-DeepVoice + PQC의 기술적 선도성.

LG U+ 상대적 약점: 절대 투자 금액 기준 KT 대비 열위. SKT와 동급이나 가입자 기반이 작아 규모의 경제 불리.

3.2 글로벌 빅테크 동향

기업	AI 보안 동향	통신사 영향
Microsoft	Security Copilot 11개 에이전트 출시 (2025 Q1)	B2B 솔루션 경쟁 상대
Cisco	Robust Intelligence 인수($400M, 2025)	AI 네트워크 보안 포트폴리오 강화
AWS	IAM Policy Autopilot, re:Invent 2025 AI 보안 발표	클라우드 이전 고객 확보 위협
Palo Alto Networks	Cortex XSIAM (Agentic SOC) 시장 선도	기업 SOC 시장 잠식
Google + PwC	AI 보안 감사·컨설팅 협력	엔터프라이즈 고객 접근

출처: Microsoft Blog, AWS Blog, The Register[14]

3.3 글로벌 통신사 벤치마크

- **Airtel (인도)**: Elastic AI SOC 도입으로 효율 40% 향상 — 통신사 AI SOC 성공 선례[6]
- **SKT + Thales**: 양자내성 SIM 실증 (CRYSTALS-Kyber, 5G SA 환경)[10]
- **SoftBank**: 4G/5G Hybrid PQC 파일럿[10]
- **Seceon**: 통신사 전용 AI 보안 플랫폼 (aiSIEM + aiXDR + aiCompliance) 공급[6]

---

4 학술 동향

4.1 주요 연구 방향 (2025년)

통신 네트워크 이상 탐지

- *"Artificial intelligence advances in anomaly detection for telecom networks"* (Springer Nature, 2025)[7]: GAN·RL 기반 적응형 이상 탐지 체계화. 5G/6G 환경에서 RL의 자기 적응 특성을 핵심 차별화 요소로 제시.
- *"AI-enabled cybersecurity framework for future 5G wireless infrastructures"* (Nature/Scientific Reports, 2025)[8]: 97.6% 탐지율, 저지연 고부하 환경 실증.
- *"Security and Privacy Challenges in 5G Core AI-Powered Threat Detection"* (Wiley Internet Technology Letters, 2025)[15]: 5G 코어망 AI 위협 탐지와 완화 전략 체계화.

Privacy-Preserving AI

- *"Federated Learning: A Survey on Privacy-Preserving Collaborative Intelligence"* (arXiv, 2025)[9]: FL 아키텍처 분류, Differential Privacy + Blockchain 검증 결합.
- *"A hybrid federated learning framework with generative AI"* (Nature/Scientific Reports, 2025)[16]: IoT 스마트 환경에서 GenAI + FL 결합으로 프라이버시·보안 동시 해결.
- *"Enhanced IoT security: privacy-preserving federated learning model"* (ScienceDirect, 2025)[17]: 실시간 침입 탐지 + 연방학습 결합 실증.

LLM·적대적 공격

- *"Security Concerns for Large Language Models: A Survey"* (arXiv, 2025)[18]: Prompt Injection, Jailbreak, 데이터 포이즈닝, 오용 시나리오 분류.
- *"Forewarned is Forearmed: LLM-based Agents in Autonomous Cyberattacks"* (arXiv, 2025)[19]: LLM이 기존 위협 모델을 증폭시키는 메커니즘 분석.
- *"Adversarial ML Problems Are Getting Harder to Solve"* (IEEE S&P Workshop, 2025)[1]: 방어 기법 평가의 어려움 증가, 비대칭 위협 구조 심화.

양자내성암호 + 5G

- *"Post-Quantum Cryptography in the 5G Core"* (arXiv, 2025.12)[20]: 5G 코어가 기술적으로 PQC 통합 가능함을 입증. 성능 저하 소폭(서비스 영향 미미).
- ATIS 백서 *"Preparing 5G for the Quantum Era"* (2025.02)[10]: 3GPP 아키텍처 PQC 통합 로드맵 제시.

4.2 연구 기관 현황

기관	연구 포커스	주목 이유
NIST	AI RMF, 적대적 ML 분류 체계, PQC 표준화	국제 규제 기준 형성
IEEE/Springer	5G 네트워크 이상 탐지, 연방학습	실용화 연구
arXiv	LLM 보안, Agentic AI 위협	최신 공격/방어 트렌드
3GPP	PQC 5G 통합 표준화	통신사 직접 영향
OWASP	LLM Top 10, 프롬프트 인젝션 가이드	실무 보안 기준

5 특허 동향

> ***주의***: *patent-intel MCP 도구 미작동으로 WebSearch 데이터로 대체. 정확한 특허 건수는 별도 patent-intel 호출로 검증 필요.*

5.1 AI 보안 특허 전반

- 중국 기업 주도: Huawei + Alibaba + Tencent가 AI 관련 특허 80% 이상 보유[21].
- Huawei 네트워킹 특허: 164,088건 이상. AI 기반 통신 보안이 핵심 클러스터[21].

5.2 5G 표준특허 (SEP) 현황

기업	선언 5G SEP 수	비고
Huawei	1위	정확 수치 미공개
Samsung	8,164건	
LG (전체 LG)	7,917건	통신 계열 포함
ZTE	7,802건	
Ericsson	7,285건	

출처: Parola Analytics 5G SEP 분석[22]. AI 보안 특허 세부 분류는 데이터 공백.

5.3 시사점

국내 통신사(SKT·KT·LGU+)의 AI 보안 특허 포트폴리오는 공개 데이터 부재. 기술 차별화 검증을 위해 KIPRIS 특허 검색 및 patent-intel MCP 가동 후 재분석 권고.

---

6 전략적 시사점

6.1 기회 (Opportunities)

O1. Anti-DeepVoice + PQC 선점 포지션 강화 LG U+가 MWC 2025에서 공개한 Anti-DeepVoice(딥페이크 음성 탐지)와 SW 형태 PQC는 국내 통신사 중 유일한 결합 기술. Exio AI 에이전트에 통합해 B2C 서비스로 차별화 가능[23].

O2. AI SOC-as-a-Service 신규 B2B 수익 창출 국내 AI 보안 성숙도 3%라는 극단적인 낮은 수준은 미충족 수요를 의미. 통신 인프라를 보유한 LG U+가 SOC 자동화 플랫폼을 중견·중소기업 대상으로 제공하면 경쟁사 대비 네트워크 연동 강점 활용 가능.

O3. 연방학습(FL) 기반 프라이버시 보안 서비스 2026년 한국 AI 기본법 고영향 AI 의무 이행을 지원하는 FL 기반 익명화·프라이버시 분석 플랫폼을 기업 고객에 공급. 규제 컴플라이언스 서비스는 고객 락인(Lock-in) 효과 강함.

O4. PQC 표준화 선행 참여 3GPP Release 19 이후 PQC 통합이 구체화되기 전, 5G SA 환경에서 선행 파일럿을 통해 표준 기여 및 특허 포트폴리오 구축.

6.2 위협 (Threats)

T1. 경쟁사 투자 규모 격차 KT 1조 원 > SKT·LGU+ 각 7,000억 원 계획이지만, 2024년 실제 집행액 기준 KT 1,218억 vs LGU+ 828억. KT가 선언한 국내 최초 통신+IT 통합 AI 사이버 센터 구축 시 B2B 보안 레퍼런스 독점 위험.

T2. 빅테크 AI 보안 시장 잠식 Microsoft Security Copilot, Palo Alto Cortex XSIAM 등 글로벌 플랫폼이 B2B 엔터프라이즈 시장 선점. 통신사가 솔루션 공급자보다 구매자로 전락할 위험.

T3. AI 공급망 공격 취약성 LG U+ 내부 ML 시스템(네트워크 최적화, 고객 추천, 부정 탐지) 자체가 Poisoning·Backdoor 공격 대상. 2025년 의료·물류 분야 AI 공급망 공격 사례처럼 통신 인프라도 표적이 될 수 있음[4].

T4. 규제 대응 부담 한국 AI 기본법 고영향 AI 의무(2026.1 시행, 과태료 2027.1 부과) + EU AI Act (2026.8 고위험 AI 조항 발효) 동시 대응. 거버넌스 체계 미비 시 과태료 및 평판 리스크.

T5. LLM Jailbreak 내부 위협 LG U+가 도입하거나 개발 중인 LLM 기반 서비스(Exio 등)에 Prompt Injection 공격이 성공할 경우 고객 데이터 노출 및 서비스 무결성 훼손.

6.3 권고사항

우선순위	과제	기한	예상 효과
P1	AI 거버넌스 체계 구축 (AI 기본법 준수 로드맵)	2026 Q2	규제 리스크 제거
P2	Anti-DeepVoice + PQC를 Exio 상용화 및 B2B 라이선싱	2026 Q3	차별적 매출 창출
P3	AI SOC 자동화 솔루션 중소기업 대상 서비스화	2026 Q4	신규 B2B 수익원
P4	5G SA 환경 PQC 파일럿 → 3GPP 표준 기여	2027 Q1	IP 포트폴리오 강화
P5	내부 ML 시스템 AI 공급망 보안 감사	상시	내부 리스크 통제

신뢰도 평가

높은 확신 [A/B]:

- LG U+ 보안퍼스트 전략·7,000억 투자: 공식 보도자료 및 복수 언론 확인 [A]
- SKT/KT 투자 규모: 2025년 정보보호 공시 데이터 기반 [A]
- NIST PQC 표준 알고리즘(ML-KEM, ML-DSA 등): 공식 NIST 문서 [A]
- EU AI Act 타임라인(2025.8, 2026.8 발효 기준): 공식 EU 디지털 전략 페이지 [A]
- 한국 AI 기본법 시행(2026.1.22): 국가법령정보센터 확인 [A]
- Airtel AI SOC 40% 효율 향상: Elastic 공식 케이스스터디 [B]
- LLM Top 10 Prompt Injection 1위·공격 성공률 89.6%: OWASP 공식 발표 [B]

추가 검증 필요 [C/D]:

- AI 보안 시장 규모(354억, 863억 달러): Precedence Research 단일 소스 [C]
- 연방학습 시장 규모($138.6M, $297.5M): 단일 업계 추정 [C]
- 국내 AI 보안 성숙도 3%: 출처 불명확 [C]
- Huawei AI 특허 10,000건+: 복수 소스이나 정의 불명확 [C]

데이터 공백:

- patent-intel MCP 미작동으로 Secure AI 세부 특허 분류 미확인
- research-hub MCP 미작동으로 피인용 수·연구 영향력 정량 분석 불가
- trend-tracker MCP 미작동으로 시계열 뉴스 트렌드 변화 분석 불가
- LG U+ 내부 AI 시스템 현황 (Exio 기술 스택, 내부 보안 체계) 비공개
- 국내 Secure AI 특허 현황 (KIPRIS 기반 분석 필요)

부록: MCP 도구 미작동 제약 명시

본 보고서는 VSCode 확장 환경에서 MCP 도구(`research-hub` , `patent-intel` , `trend-tracker`) 호출이 불가능함에 따라, 아래와 같이 WebSearch + 기존 보고서 폴백으로 작성되었다:

- `research-hub.search_papers` : 대체 → WebSearch로 arXiv, Springer, Nature, IEEE 논문 직접 검색
- `patent-intel.search_patents` : 대체 → WebSearch로 Lumenci, PatentPC, Parola Analytics 데이터 활용 (정확도 [C])
- `trend-tracker.search_news` : 대체 → WebSearch로 보안뉴스, 파이낸셜뉴스 등 언론 직접 검색
- 기존 보고서 참조: `2026-02-23_wtis-standard-secureai-skill4.md` 내용 교차 확인 및 반영

References

#	출처명	URL	발행일	접근일	신뢰도
1	NIST Adversarial ML (AI.100-2e2025)	https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf	2025	2026-02-25	[A]
2	LastPass: AI Model Poisoning 2026	https://blog.lastpass.com/posts/model-poisoning	2025	2026-02-25	[B]
3	OWASP LLM Top 10	https://owasp.org/www-project-top-10-for-large-language-model-applications/	2025	2026-02-25	[A]
4	ExtraHop: AI Supply Chain Attacks 2025	https://www.extrahop.com/blog/amid-rising-genai-hacking-hysteria-supply-chain-most-at-risk	2025	2026-02-25	[B]
5	Splunk: Security Predictions 2026	https://www.splunk.com/en_us/blog/leadership/security-predictions-2026-what-agentic-ai-means-for-the-people-running-the-soc.html	2025.12	2026-02-25	[B]
6	Seceon: Telecom APT Defense	https://seceon.com/telecommunications-network-security-defending-against-nation-state-apts-with-unified-ai-defense/	2025.11	2026-02-25	[B]
7	Springer: AI Anomaly Detection Telecom	https://link.springer.com/article/10.1007/s10462-025-11108-x	2025	2026-02-25	[A]
8	Nature/Scientific Reports: AI 5G Security	https://www.nature.com/articles/s41598-026-37444-8	2025-2026	2026-02-25	[A]
9	arXiv: Federated Learning Survey	https://arxiv.org/html/2504.17703v3	2025.04	2026-02-25	[B]
10	ATIS: 5G Quantum Era Whitepaper	https://cdn.atis.org/atis.org/2025/02/25152429/Preparing-5G-for-the-Quantum-Era-WP-V9.pdf	2025.02	2026-02-25	[A]
11	파이낸셜뉴스: LGU+ 보안퍼스트 전략	https://www.fnnews.com/news/202507291458075239	2025.07	2026-02-25	[B]
12	보안뉴스: SKT 정보보호 공시 2024	https://m.boannews.com/html/detail.html?tab_type=1&idx=137930	2025	2026-02-25	[B]
13	보안뉴스: 정보보호 공시 Top 3	https://m.boannews.com/html/detail.html?idx=137949	2025	2026-02-25	[B]
14	The Register: MS Security Copilot	https://www.theregister.com/	2025	2026-02-25	[B]
15	Wiley: 5G Core AI Threat Detection	https://onlinelibrary.wiley.com/doi/abs/10.1002/itl2.70070	2025	2026-02-25	[A]
16	Nature: Hybrid FL + GenAI	https://www.nature.com/articles/s41598-025-31769-6	2025	2026-02-25	[A]
17	ScienceDirect: IoT FL Intrusion Detection	https://www.sciencedirect.com/science/article/pii/S2090447925006070	2025	2026-02-25	[A]
18	arXiv: LLM Security Survey	https://arxiv.org/html/2505.18889v3	2025.05	2026-02-25	[B]
19	arXiv: LLM Autonomous Cyberattacks	https://arxiv.org/html/2505.12786v1	2025.05	2026-02-25	[B]
20	arXiv: PQC in 5G Core	https://arxiv.org/abs/2512.20243	2025.12	2026-02-25	[A]
21	PatentPC: AI Patent Race	https://patentpc.com/blog/whos-winning-the-ai-patent-race-a-data-driven-look-at-ai-ip-growth	2025	2026-02-25	[C]
22	Parola Analytics: 5G SEP 2025	https://parolaanalytics.com/blog/5g-standard-essential-patentskey-players-and-trends-in-2025/	2025	2026-02-25	[C]
23	LGU+ 공식: Anti-DeepVoice MWC 2025	https://www.lguplus.com/biz/insight/trend/513	2025.02	2026-02-25	[A]
24	EU AI Act 공식	https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai	2024-2026	2026-02-25	[A]
25	국가법령정보센터: AI 기본법	https://www.law.go.kr/lsInfoP.do?lsiSeq=268543	2026.01	2026-02-25	[A]

#	출처명	URL	발행일	접근일	신뢰도
26	피카부랩스: AI 기본법 완전 정리	https://peekaboolabs.ai/blog/ai-basic-law-guide	2026	2026-02-25	[B]
27	NIST AI RMF 2025 Updates	https://www.ispartnersllc.com/blog/nist-ai-rmf-2025-updates-what-you-need-to-know-about-the-latest-framework-changes/	2025	2026-02-25	[B]
28	Securiti: EU AI Act 2026	https://securiti.ai/whitepapers/eu-ai-act-what-changes-now-what-waits-2026/	2025	2026-02-25	[B]
29	보안뉴스: 통신3사 AI 보안 신사업	https://www.insightkorea.co.kr/news/articleView.html?idxno=241106	2025	2026-02-25	[B]
30	IEEE: AI for 5G/6G Taxonomy Survey	https://www.mdpi.com/2227-7080/13/12/559	2025	2026-02-25	[A]