

해외는 위성 동맹 뭉치는데… 한국은 저궤도 경쟁 ‘뒷걸음’

스페이스X, 모바일 진출 기반 마련
유럽·日 등 해외 통신사 합종연횡
한국은 해외 위성망 판매에 그쳐

저궤도 위성 통신 서비스 확보를 위해 해외 통신사들이 직접 연합 전선을 구축하는 등 대응에 나서고 있다. 반면 국내 기업은 정부 주도의 사업 진척이 더뎠다. 국제 경쟁력을 상실할 수 있다는 우려가 나온다.

11일 통신업계에 따르면, 일론 머스크가 이끄는 스페이스X는 최근 위성통신 스타링크의 저궤도 주파수(800MHz)를 현지 투자사로부터 인수했다. 정부 당국의 승인이 마무리 되면, 기지국 없이도 저궤도 위성에서 쏘는 신호를 통해 미국 전역에서 통신 서비스가 가능해진다. 글로벌 통신 인프라 독점에 한발짝 다가간 셈이다.

현재 전 세계의 저궤도 위성 시장 경쟁은 스페이스X의 독점에 대항하는 구도다. 올해 10월 기준 저궤도에서 작동 중인



글로벌 통신사들이 연합 전선을 구축하며 저궤도 위성통신 경쟁에 나서고 있다. /KT SAT

1만5800기 중 1만1100기가 스타링크로 알려졌다. 이는 전체 활성 위성 중 약 67%에 달하는 규모다.

중국 정부는 비지상망 위성 사업 '위

왕-첸판' 프로젝트를 2024년 시작했지만, 현재까지 운영하는 위성은 약 460기에 그친다. 유럽연합(EU)은 아이리스2 프로젝트를, 일본 총무성은 J-LEO를 가동 중으

로, 아직까지 쏘아올린 위성은 없다.

이에 해외 통신사들은 직접 연합 전선 구축에 나선 상황이다. 미국 대표 통신사인 AT&T·T모바일·버라이즌은 이달 스타링크를 견제할 라이벌 기업들을 포섭하기 위해 위성통신 합작 법인을 출범했다.

일본 통신사 라쿠텐은 미국의 AST 스페이스모바일 설립 초기부터 기술 동맹을 맺고 현지에서 700MHz 저궤도 주파수를 공급 중이다. 유럽의 유텔셋 원웹의 경우 650기의 저궤도 위성을 직접 운영해 국방 등 공공 시장을 선점했다.

반면, 국내 기업의 독자망 구축은 상대적으로 더뎠다. 주도권 상실이 우려된다. 현재 KT SAT(셋)과 SK텔링크 등 국내 기업이 스타링크와 원웹 등의 서비스 판매권을 국내로 들여와 수익 모델로 활용하는 정도다. 또한 통신 3사 중 국내 위성통신 사업자는 KT의 완전 자회사인 KT 셋이 유일하지만, 저궤도 보다 고도가 높은 정지궤도 위성만을 운영한다.

이에 정부가 핵심 자원 선점 등 글로벌 시장 변화에 빠르게 대응해야 한다는 목소리가 나온다. 이 사업의 민간 서비스 운용 총괄을 맡은 KT 셋은 최근 공식 석상에서 정부가 위성체 개발에만 집중할 것이 아니라 국제기구에 궤도·주파수 사용 권리를 선제적으로 확보해야 한다는 입장을 밝힌 바 있다. 현재 과기정통부는 2035년까지 저궤도 위성 512기를 구축하는 것을 목표로 'K-LEO'를 출범하고 민관협력의 한국형 저궤도 위성통신망 구축 사업을 추진 중이다.

국내 6세대 이동통신(6G) 상용화는 안정적인 저궤도 위성 인프라 구축에 달려 있다. 지상망과 비지상망(NTN) 간 초저지연 연결이 핵심인 6G 시대에는 저궤도 위성 확보가 필수다. 통신 3사는 2030년 상용화를 목표로 위성 전송 효율을 높이는 기술 시연과 국제 표준화 기구에 참여해 기술 개발을 추진 중이다.

msjo@metroseoul.co.kr



metro

AI로 빨라진 해킹… 금융권 보안 사각지대 ‘비상’

오늘 AI

금융사 7곳, 6.8만건 개인정보 유출
정부, 내년 AI 분야 약 9.4조 투자
“안전성 검증·보안 역량 강화” 목소리

인공지능(AI)을 활용한 사이버 공격이 국내 금융권을 겨냥하면서 정부의 보안 대응 체계가 시험대에 올랐다. 정부가 내년 AI 분야에 9조4000억원을 투입하기로 한 가운데 기술 경쟁력 확보뿐 아니라 고도화하는 해킹에 대응할 보안 역량 강화도 시급한 과제로 떠오르고 있다.

11일 보안업계와 금융당국 등에 따르면 최근 국내 금융사들을 겨냥한 연쇄 해킹에서 AI 기반 자동화 공격 도구가 활용된 정황이 드러났다. 공격자들은 핵심 금융 거래 시스템보다 상대적으로 관리가 취약한 대출모집인 시스템과 영업지원 플랫폼 등을 집중 공격한 것으로 분석됐다. 지난 8일 국회 정부위원회 국정감사에서는 금융사 7곳에서 약 6만8000건의 개인정보가 유출됐다는 지적도 나왔다.



AI가 만든 이미지.

정부도 대응 수위를 높이고 있다. 이재명 대통령은 지난 6일 국무회의에서 일부 해킹에 AI가 활용된 정황을 언급하며 신속한 경위 파악과 피해 최소화를 지시했다. 특히 사고 발생 이후 수습하는 방식에서 벗어나 공격을 사전에 탐지하고 차단하는 보안 역량 확보를 강조했다.

금융당국은 금융권 보안 점검과 함께 AI 보안 기술 활용을 확대하기 위한 망분리 규제 완화도 추진하고 있다. 기존 규제

를 제한하면서 공격 기술과 방어 역량 사이의 격차를 키울 수 있다는 우려에 따른 것이다.

◆AI가 공격 속도 증폭…보안 사각지대 집중 공략

SK윌더스가 최근 공개한 침해사고 분석 자료에 따르면 공격자들은 AI 침투 테스트 도구 '아르텍스'에 답시크 등 AI 모델을 결합해 취약점 탐색과 공격 과정을 자동화한 것으로 분석됐다.

특히 보안 조직의 관리에서 누락되거나 점점 우선순위에 밀린 '새도 IT'가 주요 공격 대상으로 지목됐다. AI가 새로운 해킹 기법을 만들어냈다기보다 기존 공격의 속도와 규모를 증폭시켰다는 설명이다.

국내 민간 정보통신 환경에서도 취약점이 다수 확인됐다. 국회에 제출된 과학기술정보통신부 자료에 따르면 민간 주요 정보통신 기반시설과 상용 소프트웨어, 오픈소스에서 총 523건의 보안 취약점이 발견됐다.

주요 정보통신 기반시설 16곳에서 304건, 상용 소프트웨어 5곳에서 135건, 오픈

소스 144종에서 84건이 각각 확인됐다.

◆정부 AI 투자 확대…보안 역량 확보 관련

정부는 2027년 AI 분야에 약 9조4000억원을 투자할 계획이다. 독자AI 모델 개발과 컴퓨팅 인프라 확보 등에 대규모 예산이 투입되는 가운데 AI 안전성 검증과 사이버 보안 역량을 함께 강화해야 한다는 지적이 나온다.

내년 AI안전연구소 관련 예산은 약 159억원으로 올해보다 늘었지만, 실제 AI 모델 평가와 위협 대응 등을 위한 비연구개발 예산 증가율은 1.7%에 그쳤다. 다만 AI 모델의 안전성 평가와 금융권 사이버 보안은 구분되는 영역인 만큼 관련 투자의 실효성을 종합적으로 점검할 필요가 있다.

민간에서도 AI 방어 기술 확보에 속도를 내고 있다. SK텔레콤과 엽스테이지, SK윌더스, 인텔 등은 대학과 함께 독자 AI 사이버 보안 협의체를 출범시키고 취약점 분석과 실시간 보안관제 기술 개발에 나섰다.

/최빛나 기자 vitna@

LGU+

기지국 접속 기록으로 산악지역 조난자 찾는다

기존 방식보다 수색 범위 99% 축소

LG유플러스가 통신 정보를 활용해 긴급구조 지원에 나선다.

LG유플러스는 전파 분석 전문기업 솔빛시스템과 산악 지역의 조난자 수색 범위를 좁히는 기술을 실증했다고 11일 밝혔다.

이는 이동통신 기지국 정보와 휴대전화 접속 기록을 활용한 기술이다. 국방 분야 전파를 분석하고 시뮬레이션을 맡는 솔빛시스템과 LG유플러스의 통신 데이터를 기반으로 조난자 수색 지원 기술을 실증했다.

실증은 전북특별자치도 진안군 운장산 일대에서 실시했다. 산악 지역에서 GPS 신호가 잡히지 않거나 휴대전화가 꺼져 정확한 위치를 확인하기 어려운 상황을 가정했다.

수색은 조난자의 휴대전화가 마지막으로 접속한 기지국부터 시작해 확장하는 방식으로 진행했다. 또 솔빛시스템의 지능형 수색지원 시스템 (iSAR)을 활용해 기지국의 전파 도달 범위와 시간대별 휴대전화 접속 기록을 추가로 분석했다.

이를 통해 기존 방식보다 수색 범위를 약 99% 축소할 수 있었다. 솔빛시스템과 협력한 시스템으로 시간에 따른 접속 기록과 지형별 전파 도달 범위를 분석해 조난자가 있을 가능성이 높은 지역을 추정할 수 있었다는 게 회사 측의 설명이다.

해당 기술이 실제 구조 현장에 활용되면 구조대가 수색해야 하는 지역을 빠르게 좁히는 데 도움이 될 것으로 기대된다. 넓은 산악 지역을 모두 살피는 대신 조난자가 있을 가능성이 높은 지역에 구조 인력과 장비를 집중 투입해 조난자 수색이 빨라진다.

향후 LG유플러스와 솔빛시스템은 관련 기술의 정확도와 활용성 검증을 통해 긴급구조기관의 수색 지원 체계에 적용할 수 있도록 방안을 마련할 계획이다.

/조민선 기자

AI 아침에 넘어갔다… 유도성 제안 수용률 77%

오늘 AI

美 MIT 등 'AI 위치독' 연구 결과
AI 다크패턴 10명 중 8명 신고 안 해

생성형 인공지능(AI)이 이용자의 판단과 선택에 미치는 영향이 커지는 가운데, AI와 대화한 이용자 10명 중 8명이 특정 선택을 교묘하게 유도하는 '다크패턴'을 신고하지 않았다는 연구 결과가 나왔다. 특히 AI가 이용자의 의견에 과도하게 동조하거나 칭찬할수록 유도성 제안을 따르는 경향이 두드러져 AI 서비스의 신뢰성과 이용자 보호 문제가 새로운 과제로 떠오르고 있다.

11일 미국 매사추세츠공과대학(MIT)

미디어랩과 태국 카시콘랩스 등이 참여한 공동 연구진의 'AI 위치독' 연구 결과에 따르면 실험 참가자 150명 중 120명인 80%가 AI와의 대화에 포함된 다크패턴을 한 차례도 신고하지 않았다.

다크패턴이란 이용자가 특정 선택을 하도록 정보 제공 방식이나 화면 구성을 교묘하게 설계하는 행위를 뜻한다. 기존에는 온라인 쇼핑물의 결제 유도 등에 주로 활용됐지만 생성형 AI에서는 특정 상품을 편향되게 추천하거나 이용자의 의견에 지나치게 동조하는 방식으로 나타날 수 있다.

연구진은 미국 성인 150명을 대상으로 GPT-4o 기반 AI와 대화하며 프랑스 파리 여행 일정을 세우거나 소셜미디어 관련 발표 자료를 준비하도록 했다. 일부 A

I 답변에는 의도적으로 다크패턴을 포함하고 참가자들이 이를 발견하면 신고하도록 했다.

그러나 참가자의 80%는 실험이 끝날 때까지 신고 기능을 한 차례도 사용하지 않았다. 다만 신고하지 않았다는 사실이 모든 참가자가 다크패턴을 인지하지 못했다는 의미는 아니다.

AI의 유도성 제안이 실제 선택으로 이어지는 경향도 확인됐다. 별도의 경고 없이 AI와 대화한 집단에서 유도성 제안을 따른 비율은 평균 71.7%에 달했다. 특히 AI가 이용자의 생각을 과도하게 칭찬하거나 동조하는 '아침성 응답'에서는 제안 수용률이 77%로 나타났다.

반면 대화 도중 의심스러운 표현을 알

려주는 실시간 경고를 제공하자 제안 수용률은 53.7%로 낮아졌다. 경고가 없는 집단보다 18%포인트 감소한 수치다.

연구진은 AI에 대한 신뢰도가 높은 이용자가일수록 유도성 제안을 따르는 경향이 강한 반면, 조작적인 표현에 대한 인식은 낮았다고 분석했다.

이번 연구는 생성형 AI의 위험이 잘못된 정보 제공을 넘어 이용자의 의사결정 과정에까지 영향을 미칠 수 있음을 보여준다. 특히 AI가 검색과 쇼핑, 금융 등 일상적인 서비스로 확산하면서 대화 과정에서 발생하는 선택 유도에 대한 감시와 대응 체계의 필요성도 커지고 있다.

연구진은 "AI가 점점 더 설득력 있는 방식으로 이용자와 상호작용하는 상황에서 적절한 시점에 제공되는 간단한 경고가 이용자의 자율적인 판단을 지키는 데 도움이 될 수 있다"고 설명했다.

/최빛나 기자