

영토적 제재 VS 디지털 침투: 북한 IT 노동자의 유럽 확산이 던지는 경고

조은정(국가안보전략연구원)

이 글은 미국의 단속이 북한 IT 노동자의 위장취업을 종식시키기는 커녕 오히려 그 활동 공간을 재편하는 촉매로 작용해온 과정을 분석한다. 유럽에서 확인된 북한 IT 노동자의 구직·취업 시도와 이로 인한 기업 피해, 그리고 수사 협조 사례들은 북한의 네트워크가 원격노동과 가상신분을 활용해 미국 바깥의 노동시장으로까지 활동 범위를 넓히고 있음을 보여준다. 이 과정에서 노동은 '탈영토화'된 반면 제재 집행은 여전히 국가별 관할권을 따라 분절되어 있어, 구조적 불일치가 드러난다. 이에 이 글은 북한의 불법 수익 차단을 하나의 국가안보 의제로 통합하고, MSMT 참여국들의 기존 집행체계를 연계하며, '노트북 팜'과 같은 디지털 관문과 물리적 병목을 동시에 겨냥하는 다층적 대응을 제안한다.

‘11개국 공동주의보’와 북한의 반박

2026년 7월 31일, 한국·미국·일본·영국·프랑스·독일·이탈리아·네덜란드를 포함한 11개국 정부가 북한 정보기술(IT) 노동자를 겨냥한 '공동주의보'를 발표했다.¹ 이 '공동주의보'는 '다국적제재모니터링팀(MSMT)'에 참여하는 11개국 전체가 함께한 것으로, 발표 기관에는 외교당국뿐 아니라 수사·금융제재·사이버·경제 당국까지 포함되었다.² 그러나 우리가 주목해야 할 지점은 이들 국가가 설정한 대응 대상에 있다. 이번 공동주의보는 북한 IT 노동자의 물리적 이동을 추적하기보다, 허위신분·온라인 구직 플랫폼·원격접속·제3자 계정·암호화폐 결제·해외 조력자 등 국경을 넘나드는 취업 인프라 자체를 차단 대상으로 지목하였다.³ 이는 이제 북한 노동자가 고용국 영토 안에 발을 들이지 않고도 해당국 노동시장에 진입할 수 있기 때문이다. 바로 이 지점에서 기존 대북제재의 구조적 문제가 드러난다. 원격근무를 통해 노동은 '탈영토화'되었으나, 제재를 관장하는 법적 권한과 집행기관은 여전히 국가 영토와 관할권을 중심으로 조직되어 있다. 따라서 북한 IT 노동자의 유럽 확산은 단순히 새로운 위협 지역의 출현을 의미하지 않는다. 이는 미국 내 단속 강화가 유럽 등 다른 시장으로의 활동 확대로 이어지는 가운데 국경 기반의 제재체계가 국경을 넘지 않는 노동을 어떻게 통제할 수 있는가라는 보다 근본적인 질문을 제기한다.

¹ 외교부. 2026. “북한 IT 인력 관련 공동주의보 발표.” 7월 31일.

https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=377471

² Department of Foreign Affairs and Trade (Australia). 2025. “Multilateral Sanctions Monitoring Team (MSMT) Steering Committee Inaugural Meeting Joint Statement.” February 21.

<https://www.dfat.gov.au/news/media-release/multilateral-sanctions-monitoring-team-msmt-steering-committee-inaugural-meeting-joint-statement>.

³ Global Affairs Canada. 2026. “Alert to Countries, Companies and Other Entities Regarding North Korean IT Workers.” July 31. <https://www.canada.ca/en/global-affairs/news/2026/07/alert-to-countries-companies-and-other-entities-regarding-north-korean-it-workers.html>.

북한은 11개국의 전례 없는 전방위적 압박에 즉각적이고 민감하게 반응하였다. 공동주의보 발표로부터 불과 나흘 뒤인 2026년 8월 4일, 북한 외무성 대변인은 이를 "진부한 정치모략극"이라 비난하였다.⁴ 대변인은 나아가 다국적제재모니터링팀(MSMT)을 서방이 만들어낸 "신빙성 없는 거짓정보나 유포하는" "유령조직"이라 지칭하며 강하게 항의하였다.⁵ 북한은 이러한 서방의 조치가 사이버 공간에서의 부당한 주권 침해라고 주장한다. 이처럼 신속한 반응은 북한이 이번 다자적 대응을 정치적으로 민감한 사안으로 취급하고 있음을 보여준다.

이러한 집행의 비대칭성은 이미 유럽에서 관찰되고 있다. 구글 위협정보그룹(Google Threat Intelligence Group)은 미국 내 단속과 신원확인 절차 강화 이후 북한 IT 노동자의 활동이 유럽으로 확대되고 있다고 분석했고, 독일과 영국은 각각 자국 기업을 대상으로 별도의 경보를 발령한 바 있다.⁶ 유럽 기업들이 실제로 입은 피해와 폴란드, 네덜란드에서의 체포 및 인도 공조 역시 확인되었다. 그러나 공개적으로 확인된 주요 형사기소와 유죄판결은 여전히 미국 법원을 중심으로 이루어지고 있다.⁷ 문제의 핵심은 유럽의 대응이 미진한 데 있다기보다, 위협은 이미 탈영토화 되었음에도 집행권한은 여전히 국가별로 분절되어 있다는 데 있다.

⁴ Spokesperson of the DPRK Ministry of Foreign Affairs. 2026. "DPRK Foreign Ministry Spokesperson on U.S. Groundless 'Theory of Cyber Threat'." *Korean Central News Agency (KCNA)*. August 4. <https://www.globalsecurity.org/wmd/library/news/dprk/2026/dprk-260804-kcna01.htm>.

⁵ Spokesperson of the DPRK Ministry of Foreign Affairs 2026. 유엔 안보리 전문가패널은 러시아의 거부권 행사로 현재 사실상 마비된 상태이나, MSMT는 이러한 제약에 구속되지 않는 유사입장국들의 연합체다.

⁶ Collier, Jamie. 2025. "DPRK IT Workers Expanding in Scope and Scale." Google Threat Intelligence Group. April 2. <https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale?hl=en>.

⁷ Multilateral Sanctions Monitoring Team (MSMT). 2025. "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities." October 22.

이러한 문제의식 위에서 이 글은 북한 IT 노동자의 유럽 확산을 대북제재 집행의 구조적 전환이라는 관점에서 살펴본다. 첫째, 미국의 단속 강화 이후 북한 IT 노동자의 활동이 유럽으로 확산된 경로와 방식을 검토한다. 둘째, 원격노동이 기존의 해외파견 노동자 제재가 전제해온 영토성과 관할권을 어떻게 흔드는지 분석한다. 셋째, 7월 31일 공동주의보를 계기로 정보와 정보공유의 다자화가 실제 집행의 다자화로 이어질 수 있는 조건을 검토한다. 마지막으로, 한국이 개별 사건 대응을 넘어 비확산·제재·사이버·금융·디지털 고용을 연결하는 국가 차원의 대북 불법 수익 차단 전략을 어떻게 설계해야 하는지를 제안한다.

미국의 단속 강화와 북한 IT 노동자의 유럽 활동 확대

북한 IT 노동자의 유럽 확산은 독자적으로 발생한 새로운 현상이라기보다 미국 내 집행 환경 변화와 맞물린 결과로 이해하는 편이 타당하다. 2024년 3월, 미국 법무부는 국가안보부(NSD)와 연방수사국(FBI)을 중심으로 "DPRK RevGen: 국내 조력자 이니셔티브(Domestic Enabler Initiative)"를 출범시키고 미국 내 북한 IT 노동자의 활동 기반을 집중적으로 차단하기 시작했다. 단속의 초점은 개별 북한 노동자 적발에 머물지 않았다. 미국 기업이 지급한 업무용 컴퓨터를 대신 보관하며 원격접속을 가능케 하는 이른바 '노트북 팜(laptop farm)'을 폐쇄하고, 미국 내 조력자들을 수사·기소하였다.⁸ 또한, 위장 웹사이트와 금융계좌를 폐쇄하고 피해 기업에 통보하는 한편, 온라인

⁸ U.S. Department of Justice, Office of Public Affairs. 2024. "Justice Department Announces Arrest, Premises Search, and Seizures of Multiple Website Domains to Disrupt Illicit Revenue Generation Efforts of Democratic People's Republic of Korea." May 16.

<https://www.justice.gov/archives/opa/pr/justice-department-announces-arrest-premises-search-and-seizures-multiple-website-domains>.

서비스 제공업체와 정보를 공유함으로써, 하나의 수사·집행 연결망으로 묶였다.⁹ 이후 단속은 지속적으로 확대되어, 2025년 6월에는 미국 14개 주 21곳에서 동시다발적인 수색을 통해 노트북 137대가 압수되었으며, 북한 IT 노동자를 뒷받침해온 미국 내 지원 인프라 자체가 법집행의 주요 대상이 되었다.¹⁰

그러나 이러한 압박도 북한 IT 노동자들의 불법 취업 활동을 멈추지는 못했다. 구글 위협정보그룹은 2025년 4월 북한 IT 노동자의 미국 내 취업이 어려워짐에 따라 이것이 오히려 북한 IT 노동자의 해외 취업이 유럽 등 세계 각지로 확대되는 계기가 되었다고 분석했다.¹¹ 역설적으로 미국 내 북한 IT 기술자에 대한 위장취업 단속 강화와 같은 집행 환경의 변화가 자리 잡으면서, 다른 고용시장으로의 구직활동 확대와 적발을 피하기 위한 위장취업 수법의 진화가 동시에 관찰된다. GTIG가 추적한 한 북한 IT 노동자는 2024년 말 기준 유럽과 미국에 걸쳐 최소 12개의 가짜 신원을 운용하며 이탈리아·일본·말레이시아·싱가포르·우크라이나·미국·베트남 등 여러 국적으로 위장했다.¹² GTIG는 또한 독일과 포르투갈에서의 구직 시도를 확인했으며, 영국에서는 웹 개발이나 블록체인·AI 애플리케이션 개발과 같은 실제 프로젝트 수행 사례를 포착했다.¹³ 구직에는 Upwork, Freelancer, Telegram과 같은 초국경 플랫폼이 활용되었고, 급여 지급에는 TransferWise,

⁹ U.S. Department of Justice 2024.

¹⁰ U.S. Department of Justice, Office of Public Affairs. 2025a. “Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers’ Illicit Revenue Generation Schemes.” June 30. <https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote>.

¹¹ Collier 2025.

¹² Collier 2025.

¹³ Collier 2025.

Payoneer 등의 서비스가 이용되었다.¹⁴ 이 과정에서 한 사람이 여러 국가에서 동시에 취업을 시도하거나, 뉴욕에 있는 것으로 알려진 기업용 노트북이 런던에서 접속되는 사례도 포착되었다.¹⁵ 이 문제의 핵심은 단순히 북한 노동자들이 미국에서 유럽으로 이동했다는 데 있지 않다. 북한 IT 노동자의 상당수는 특정 국가(미국·영국 등 서구권 국가)에 실제로 거주하며 이동해 일하는 것이 아니라, 중국이나 러시아처럼 북한에 우호적인 제3국에 머무르면서 서구권 국가에 있는 것처럼 신분을 위장한 채 원격취업 활동을 벌이기 때문이다. 바뀐 것은 이들의 물리적 위치가 아니다. 바뀐 것은 이들이 구직 활동을 벌이는 무대, 그리고 이들이 사용하는 국적·신분·접속경로·현지 조력자·플랫폼·결제수단의 조합이다. 다시 말해 미국이라는 단일 고용시장에서 위험 비용이 상승하자, 동일한 노동력이 복수의 가상 신분과 디지털 인프라를 통해 다른 관할권에 접속함으로써 유럽이라는 새로운 시장을 개척한 것이다.

이러한 고용시장 개척은 2026년에도 지속되고 있다. CrowdStrike는 북한과 연계된 위협행위자 FAMOUS CHOLLIMA가 북미·유럽·아시아의 테크 기업들을 상대로 위장취업을 시도했으며, 이는 2025년 4월 1일부터 2026년 3월 31일까지 기술 부문에서 관측된 국가 배후 '대화형 침투(interactive intrusions)'의 47%를 차지했다고 보고했다.¹⁶ 이는 북한의 위장취업 활동이 특정 국가에 국한된 한시적 문제가 아니라, 여러 지역의 테크 기업을 동시에 겨냥하는 운영모델로 진화하고 있음을 말해준다.

¹⁴ Collier 2025.

¹⁵ Collier 2025.

¹⁶ CrowdStrike. 2026. "CrowdStrike 2026 Technology Threat Landscape Report: China's Ambitions Fuel Attacks." June 9. <https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-technology-threat-landscape-report/>.

따라서 이번 북한 IT 노동자의 유럽 확산 사례에서 주목해야 할 것은 새로운 활동 지역의 출현 그 자체가 아니다. 오히려 주목할 점은, 미국 내 법 집행 강화가 위장취업에 압박을 가하자 북한 IT 기술자들이 원격근무의 속성을 활용하여 활동 공간을 재편했다는 사실이다. 이동한 것은 북한 기술자들의 '신체'라기보다 이들이 연결되는 '시장'과 '디지털 인프라'였다. 이는 인터넷 연결망이라는 '기술'과 원격근무라는 '제도'를 통해 영토주권과 개인의 물리적 한계를 뛰어넘었다는 점에서 기존 대북제재 감시체계의 허점을 드러낸다. 이처럼 어느 한 국가의 영토에 고정되지 않은 채 활동이 이루어지는 경우, 특정 영토와 관할권을 중심으로 설계된 기존 대북제재가 어떻게 실효성을 거둘 수 있을 것인가?

노동의 탈영토화와 대북제재 집행의 관할권 문제

북한 IT 노동자들의 원격취업은 단순히 기존의 해외노동자 제재를 회피하는 새로운 수법에 그치지 않는다. 보다 근본적인 문제는 제재가 전제하는 노동의 공간과 실제 노동이 이루어지는 공간이 분리되기 시작했다는 데 있다. 유엔 안전보장이사회 결의안 2375호는 회원국이 자국 관할권 내 북한 국적자에게 신규 노동허가를 발급하는 것을 원칙적으로 금지하며, 결의안 2397호는 2019년 12월까지 회원국이 자국 관할권 내에서 소득활동을 하는 북한 국적자를 송환하도록 의무화했다.¹⁷ '노동허가', '자국 영토 내 입국', '송환'이라는 표현에서 드러나듯, 대북제재 결의안 2375호와 2397호의 노동 관련 조치들은 북한 노동자가 다른 국가에 물리적으로 현지에 파견되어 현지에서 일하고 외화를 벌어들이는 전통적인 해외파견노동 모델을 전제로 하고 있다.

¹⁷ United Nations Security Council. 2017a. "Resolution 2375 (2017)." S/RES/2375. September 11.

———. 2017b. "Resolution 2397 (2017)." S/RES/2397. December 22.

그러나 원격근무는 이러한 기존 대북제재가 전제해온 공간적 전제를 흔든다. 2025년 다국적제재모니터링팀(MSMT)은 북한이 해외파견 IT 노동자 운용을 지속하는 동시에 북한 내부에서는 해외 기업을 위해 일할 수 있게 하는 IT 노동 인프라와 역량 또한 확대하고 있다고 보고했다. 또한 북한 IT 노동자들은 위조 및 도용된 신분으로 온라인 노동 플랫폼에서 일감을 얻고, 해외 조력자와 노트북 팜, 원격접속 프로그램, 제3자 명의의 금융계좌 및 가상자산을 결합하여 실제 소재지를 숨긴다.¹⁸ 이 경우 한 사람의 노동을 구성하는 여러 요소가 서로 다른 국가에 분산될 수 있다. 노동자는 북한·중국·러시아에 있고, 고용기업은 독일이나 영국에 있을 수 있으며, 허위 신분은 제3국 국적자의 것이고, 플랫폼과 서버는 또 다른 국가에 소재하며, 급여는 해외 조력자의 계좌나 가상자산을 거쳐 이동하는 방식이다.

이러한 구조 아래에서는 어느 한 국가도 북한의 해외노동자 파견 시스템 전체를 조망하기 어렵다. 고용기업이 위치한 국가는 해당 북한 국적자의 실제 입국이나 노동허가 신청을 전혀 접하지 못할 수 있으며, 노동자가 실제로 거주하는 국가는 그가 어느 해외기업으로부터 얼마의 소득을 얻고 있는지 파악하기 어려울 수 있다. 플랫폼 운영자는 계정과 거래 기록을 보유하고 있지만, 실제 이용자의 국적과 소재지를 확인하지 못할 수 있으며, 금융기관은 결제 흐름의 일부만을 포착한다. 한편 노트북을 대신 보관하거나 노동자를 대신해 면접과 신원확인을 처리하는 조력자는 노동자와 고용기업 어느 쪽과도 다른 관할권에 존재할 수 있다. 고용관계는 하나이지만, 이를 입증하는 신원·접속·고용·지급의 증거는 여러 관할권에 흩어져 있는 것이다.

그렇다고 해서 북한 IT 노동자가 기존 대북제재의 적용 범위 밖에 있다는 뜻은 아니다. 소득활동에 종사하는 북한 국적자를 송환해야 한다는 결의 2397호상의 의무 외에도, 유엔 제재대상 단체로 자금이 이전되는 경우 자산동결 및 금융제재에 관한 다른 안보리 결의들이 적용될 수 있으며,

¹⁸ MSMT 2025, 53, 68, 80-81, 89-90.

각국의 국내 제재법과 형사법 역시 작동한다. 실제로 2026년 7월 31일 11개국이 발표한 공동주의보는 북한 IT 노동자와 계약을 체결하거나 이들에게 대가를 지불하는 행위가 한국·미국·일본 등 다수 국가에서 법적·금융적 제재로 이어질 수 있다고 경고한 바 있다.¹⁹ 따라서 문제의 핵심은 제재 규범의 공백이라기보다는 '집행의 분절'에 더 가깝다. 북한의 수익창출 네트워크는 하나의 초국적 과정으로 작동하지만, 이를 적발·규제·처벌할 권한은 여전히 개별 국가의 관할권 안에 나뉘어 있는 것이다.

이러한 불일치는 북한에게 일종의 '관할권 차이(jurisdictional arbitrage)'를 제공한다. 특정 국가가 신원 확인이나 금융감시, 형사 집행을 강화하더라도, 북한 네트워크는 노동자의 물리적 위치를 옮기지 않은 채 다른 국적의 신분, 다른 구인 플랫폼, 다른 결제수단이나 조력자로 점점을 변경할 수 있다. 앞서 살펴본 미국의 단속 강화에 따른 유럽으로의 활동 확대 역시 이러한 맥락에서 이해할 필요가 있다. 이는 단순히 유럽의 규제가 미국보다 느슨하다는 의미가 아니라, 원격노동의 기술적 구조가 국가 간 규제·집행 수준의 격차를 메우는 일을 훨씬 쉽게 만들었다는 의미다. 자금세탁방지국제기구(FATF) 역시 2025년 확산금융 및 제재회피에 관한 보고서에서 북한을 대표적인 확산금융 위협으로 지목하며, 제재회피 행위자들이 국가별·부문별 취약점은 물론 관할권 간 차이를 악용하고 있다고 평가했다.²⁰ 이러한 이유로 FATF는 대응 방향으로 국내 기관 간 조율, 국제협력, 민관 정보공유를 동시에 강조한 바 있다.²¹

¹⁹ Department of Foreign Affairs and Trade (Australia). 2026. "Joint Statement on North Korean IT Workers." July 31.

²⁰ Financial Action Task Force (FATF). 2025. "Complex Proliferation Financing and Sanctions Evasion Schemes." June. <https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html>.

²¹ FATF 2025.

이러한 맥락에서 7월 31일 공동주의보는 국제사회의 문제의식이 변화하고 있음을 보여준다. 이 문건에서 11개국은 위장취업에 관여한 북한 노동자를 단속하고 송환할 것을 각국 정부에 촉구하는 데 그치지 않고, 온라인 플랫폼과 고용기업이 신원확인, 대면 또는 화상 면접, 의심계정 탐지, IP 접속패턴 검증, 결제계좌 명의 대조 등 강화된 조치를 도입할 필요성 또한 강조하고 있다. 제재 집행의 접점은 국경·출입국 통제에서 디지털 신원, 온라인 고용, 기업 네트워크, 결제 인프라로 확장되고 있는 것이다. 다만 이번 공동주의보가 이러한 새로운 접점들을 하나의 다자적 대응 틀 안에 처음으로 제시했다는 점에서 의의를 지니지만, 참여국들 사이에 동일한 법적 의무나 증거 기준, 수사·기소 절차를 만들어낸 것은 아니다.

결국 북한 IT 노동자 문제가 드러내는 역설은 명확하다. 노동은 '탈영토화'되었지만, 제재 집행은 여전히 개별 국가들의 '관할권별로 분절'되어 있다는 것이다. 북한은 바로 이 현행 제재체제의 허점을 파고들었다. 북한은 국경을 넘지 않고도 여러 국가의 노동시장과 금융시스템에 동시에 접근할 수 있는 반면, 국제사회는 각국이 확보한 부분적 정보와 법적 권한을 결합해야만 비로소 하나의 제재위반 사건을 완결할 수 있다. 따라서 다음으로 던져야 할 질문은 유럽이 몇 명의 북한 IT 노동자를 적발했는가가 아니다. 국경을 넘나들며 흩어진 행위들을 실제로 수사·기소 가능한 사건으로 전환하고 있는 곳이 어느 관할권이며, 왜 그 역할이 지금까지 미국에 집중되어 왔는가이다.

유럽에서 드러난 집행의 한계: 왜 미국 법정인가?

최근 사례들은 유럽이 북한의 위장취업 네트워크를 적발하는 중요한 공간으로 부상하고 있음을 보여주지만, 실질적인 법적 처리는 여전히 미국을 중심으로 이루어지고 있다. 우크라이나 국적의 올렉산드르 디텐코(Oleksandr Didenko) 사건은 이러한 구조를 가장 명확하게 보여준다. 디텐코는

해외 IT 노동자에게 도용된 신분과 미국 온라인 구직·금융계좌를 제공하고, 미국 내 최소 3곳의 '노트북 팜' 운영을 지원한 혐의로 2024년 5월 미국의 요청에 따라 폴란드에서 체포되었다.²² 폴란드 당국은 같은 해 12월 디텐코를 미국으로 인도했고, 그는 2026년 2월 미국 연방법원에서 징역 60개월을 선고받았다.²³ 그가 관리한 가상신분은 최대 871개에 달했으며, 북한 IT 노동자는 이를 이용해 미국 기업 약 40곳에 취업하고 미국의 송금 서비스를 통해 급여를 해외로 송금했다.²⁴ 이 사건에서 폴란드는 체포와 인도라는 핵심 집행 역할을 수행했지만, 범죄 행위를 하나의 사건으로 구성하여 최종적으로 유죄판결을 이끌어낸 것은 미국이었다. 이와 유사하게 멕시코 국적자 페드로 에르네스토 알론소 데 로스 레예스(Pedro Ernesto Alonso de los Reyes)는 북한 국적자 2명 및 미국인 조력자들과 함께 북한 IT 인력이 미국 기업 60여 곳에 위장 취업하도록 지원한 혐의로 미국에서 기소되었다.²⁵ 그는 2025년 1월 미국의 체포영장에 따라 네덜란드에서 체포되었으며, 2026년 5월 기준 미국으로의 인도를 기다리고 있다.²⁶ 이 두 사례는 유럽 국가들이 체포·인도

²² U.S. Attorney's Office, District of Columbia. 2026. "Ukrainian National Sentenced in 'Laptop Farm' Scheme That Helped North Korean Information Technology Workers Obtain Remote Jobs at 40 U.S. Companies." U.S. Department of Justice. February 19. <https://www.justice.gov/usao-dc/pr/ukrainian-national-sentenced-laptop-farm-scheme-generated-income-north-korean-it-workers>.

²³ U.S. Attorney's Office, District of Columbia 2026.

²⁴ U.S. Attorney's Office, District of Columbia 2026.

²⁵ U.S. Department of Justice, Office of Public Affairs. 2025b. "Two North Korean Nationals and Three Facilitators Indicted for Multi-Year Fraudulent Remote Information Technology Worker Scheme That Generated Revenue for the Democratic People's Republic of Korea." January 23. <https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote>.

²⁶ U.S. Attorney's Office, Southern District of Florida. 2026. "Two U.S. Nationals Sentenced for Facilitating Fraudulent Remote Information Technology Worker Schemes to Generate Revenue for the Democratic People's Republic of Korea." U.S. Department of Justice. May 6.

과정에 참여한 반면 기소관할권은 미국이 행사했다는 공통점을 지닌다. 또한 두 사건 모두 미국인 피해기업, 미국인의 신원, 미국 내 노트북 팔, 미국 내 금융거래 등 미국 관할권과의 두터운 연결고리를 공유한다. 특히 알론소 데 로스 레예스 사건은 최소 64개 미국 기업을 겨냥한 것이었다.

유럽 기업 자신이 직접적인 피해자가 된 사건에서조차 형사기소가 미국에서 이루어진 사례가 확인된다. 2025년 6월, 미국 조지아 북부지검은 원격 IT 노동자로 위장 취업해 전신송금사기와 자금세탁 혐의로 북한 국적자 4명을 기소했다.²⁷ 피고인들은 북한 여권으로 아랍에미리트에 입국해 팀을 이루어 미국 애틀랜타의 블록체인 회사와 세르비아의 가상 토큰 회사에 각각 허위신분으로 취업했다. 이후 세르비아 회사는 먼저 채용된 북한 노동자의 추천으로 또 다른 북한 국적자를 추가로 채용했다. 두 회사에서 탈취된 가상자산은 당시 기준 90만 달러를 넘었으며, 기소장에 따르면 이 자금은 이후 믹서와 허위 명의로 등록된 가상자산 계정을 통해 세탁되었다.²⁸ 2026년 8월 기준 피고인들은 체포되지 않은 상태로 기소 유지 중이다. 이 사건은 유럽 내 북한 IT 노동자의 활동이 단순한 구직 시도에 그치지 않고 유럽 기업에 대한 직접적인 피해로 이어질 수 있음을 보여주는 동시에, 이러한 초국경적 행위가 미국 기업과 결합된 하나의 범죄 네트워크로 구성될 경우 미국 법원에서 사건화 될 수 있음을 보여준다.

<https://www.justice.gov/usao-sdfl/pr/two-us-nationals-sentenced-facilitating-fraudulent-remote-information-technology>.

²⁷ U.S. Attorney's Office, Northern District of Georgia. 2025. "Four North Koreans Charged in Nearly \$1 Million Cryptocurrency Theft Scheme." U.S. Department of Justice. June 30.

<https://www.justice.gov/usao-ndga/pr/four-north-koreans-charged-nearly-1-million-cryptocurrency-theft-scheme>.

²⁸ U.S. Attorney's Office, Northern District of Georgia 2025.

그렇다면 왜 미국인가? 분산된 불법행위를 하나의 국가안보·제재회피 사건으로 묶어 수사·형사절차로 전환할 수 있는 제도를 갖추고 있기 때문이다. 앞선 사례에서 보듯, 현재 미국 법원에 기소된 주요 사건들은 미국 기업의 피해, 미국인 신원 도용, 미국 내 노트북 팜과 조력자, 미국 내 구인·금융 서비스, 미국 기업의 임금 지급 등 미국이 관할권을 행사할 수 있는 다수의 연결고리를 포함하고 있다. 이에 따라 미국 법무부는 2024년 "DPRK RevGen: Domestic Enabler Initiative"를 출범시키며 북한 IT 인력을 개별 취업사기 사건이 아닌 북한 정권의 불법 수익창출 네트워크의 일부로 규정하고, 형사기소와 더불어 계좌·도메인·불법수익의 압수, 노트북 팜 폐쇄, 민간기업과의 협력, 해외 사법공조를 하나의 집행전략으로 결합해왔다.²⁹

바로 이 점에서 미국의 사례는 유럽 논의에서 벗어난 우회로가 아닌 핵심적인 비교 기준이 된다. 현재 공개된 자료만으로 유럽 국가들이 미국과 동일한 방식으로 북한 IT 인력 관련 사건을 독자적으로 기소·재판할 수 없다고 단정하기는 어렵다. 폴란드와 네덜란드는 미국 수사에 협력하여 용의자를 체포·인도했고, 영국과 독일 역시 기업을 대상으로 한 경보와 제재 준수 지침을 운영하고 있다. 차이는 대응의 유무에 있다기보다, 여러 국가에 흩어진 정보와 증거를 하나의 형사사건으로 결합하는 방식과 정도에 있다.

더욱이 유럽에 이러한 초국적 사건을 공동으로 다룰 제도적 기반을 갖추지 못한 것도 아니다. Europol이 범죄 적발과 수사를 지원하는 한편, Eurojust는 회원국 수사·기소 기관 간 사법공조를 연결하고 이후의 기소·사법 조치를 조율하는 역할을 수행한다.³⁰ 특히 2026년 6월

²⁹ U.S. Department of Justice 2024; 2025a.

³⁰ European Commission. 2026. "Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust) and Repealing Regulation (EU) 2018/1727." COM(2026) 570 final. Supporting documents for the 2026 revision of Eurojust. June 24. https://commission.europa.eu/publications/supporting-documents-2026-revision-eurojust_en.

유럽연합집행위원회가 제안한 Eurojust 규정 개정안은 사이버범죄와 EU 제한조치 위반을 Eurojust의 강화된 대응 영역으로 명시하고, 회원국 간 합동수사팀(JIT) 등 운영 차원의 협력과 Europol 및 제3국과의 사법공조 확대를 제안하고 있다.³¹ 이는 유럽의 과제가 새로운 초국가적 기소기구를 만드는 데 있다기보다, 기존의 수사·사법공조 체계를 복한 IT 인력의 초국가적 제재회피 사건과 연결하여 유럽 내부에서도 이러한 사건들을 구성할 수 있는 역량을 강화하는 데 있음을 시사한다.

이러한 관점에서 보면 7월 31일 공동주의보의 의의와 한계도 명확해진다. 북한 IT 노동자가 제기하는 위협에 대한 인식과 정보 발령은 이미 다자화 되었으며, 수사와 체포 단계에서도 국제공조라 이뤄지고 있다. 그러나 정보를 공동으로 발령하는 것과 여러 국가에 흩어진 신원·고용·접속·결제 정보를 결합하여 실제 제재위반 또는 형사사건으로 구성하는 것은 별개의 문제다. 다수 국가가 확보한 부분적 증거와 법적 권한을 서로 연결하여 집행 가능한 하나의 사건으로 전환할 수 있을 때 비로소 경보의 다자화가 집행의 다자화로 이어질 수 있다. 한국을 포함한 11개국에 남겨진 과제는 이러한 전환을 어떤 제도적 수준에서 설계할 것인가이다.

향후 대응 방향: 주의보에서 집행으로

2026년 7월 31일의 공동주의보는 11개국이 북한 IT 인력 문제를 더 이상 개별 기업의 채용사거나 특정 국가만의 사이버보안 문제가 아니라는 사실상 공동의 문제의식을 형성했음을 보여준다. 한국 정부 역시 외교부와 경찰청 명의로 이번 공동주의보에 참여하면서 향후 국제사회 및 민관 협력을 강화하겠다고 밝혔다.³² 그러나 앞서 살펴보았듯이 위협 인식의 다자화가 곧 집행의 다자화를

³¹ European Commission 2026.

³² 외교부 2026.

의미하지는 않는다. 노동과 수익 창출 네트워크가 탈영토화된 상황에서 필요한 것은 단순히 더 많은 개별 사건을 적발하는 것보다 여러 국가와 민간부문에 흩어진 정보와 권한을 연결하는 국가 차원의 전략이 필요하다.

첫째, 한국은 북한의 IT 노동자, 사이버 탈취, 가상자산 세탁, 해외노동 및 조력자 네트워크를 개별 현안으로 다루기보다 북한의 '불법수익' 차단이라는 하나의 국가안보 의제로 통합할 필요가 있다. MSMT 제2차 보고서가 북한의 사이버 활동과 IT 노동을 대량살상무기 및 탄도미사일 프로그램을 위한 수익창출 체계의 일부로 함께 다룬 것도 이러한 상호연관성을 반영한다.³³ 따라서 외교·비확산, 사이버보안, 금융 및 가상자산 규제, 정보·법집행을 하나의 목표 아래 조정하는 범정부 전략이 필요하다. 핵심은 새로운 조직을 만드는 데 있지 않다. 북한의 수익창출망을 하나의 시스템으로 보고 국가 차원에서 위협을 식별하고 차단 우선순위를 설정하는 데 있다.

둘째, 한국은 MSMT가 축적한 위협정보를 참여국의 기존 법집행체계와 연결하는 다자적 '집행 인터페이스'를 의제화 할 필요가 있다. MSMT의 공식 목적이 대북 유엔제재 위반과 회피 행위를 조사·보고하는 데 있는 만큼, 이를 곧바로 수사·집행기관으로 전환하는 것은 적절하지 않다. 대신 미국의 법무부·연방수사국, 유럽의 Europol·Eurojust와 회원국 사법기관 등 참여국이 이미 보유한 기존 집행체계를 서로 연결함으로써, 한 국가에서 발견된 단서가 다른 국가의 수사·제재·자산동결로 이어질 수 있도록 해야 한다. 특히 유럽에서는 Europol과 Eurojust를 중심으로 한 기존의 수사·사법공조 체계와 사이버범죄 및 EU 제한조치 위반 대응 강화를 추진 중인 2026년 Eurojust 개정 방향을 활용할 수 있다.³⁴ 이를 토대로 한국은 MSMT 참여국 간 '공통의

³³ MSMT 2025.

³⁴ European Commission 2026.

증거분류 체계 및 사건정보 공유(common case-building)'을 의제화함으로써, 11개국의 분절된 집행체계를 연결하는 역할을 모색할 수 있다.

셋째, 제재 집행은 '디지털 관문(digital gateway)'뿐 아니라 탈영토화된 원격노동이 여전히 의존하고 있는 '물리적 병목(physical chokepoint)'까지 함께 겨냥해야 한다. 북한 IT 인력은 허위신분, 구인 플랫폼, 원격접속, 급여계좌와 가상자산을 활용해 노동을 탈영토화하지만, 그 과정에서도 기업이 지급한 업무장비, 이를 노동자 대신 관리하는 '노트북 팜', 그리고 현지 조력자와 결제계좌 같은 물리적 접점은 남는다. 미국이 노트북 팜과 국내 조력자에 대한 집중적인 수사·압수를 통해 북한 IT 노동자의 원격취업 인프라를 차단한 것은 이러한 병목의 중요성을 보여준다.³⁵ 따라서 한국을 포함한 참여국들은 고위험 원격고용 분야에서 신원뿐 아니라 업무장비의 실제 소재지, 비인가 원격접속 여부, 실제 이용자의 신원과 급여수령계좌 명의의 일치 여부 등을 공동으로 모니터링하고, 플랫폼·조력자·금융기관에서 포착된 위험신호가 정부의 제재집행으로 연결되도록 민관협력체계를 구축할 필요가 있다. 7월 31일 공동주의보가 기업과 플랫폼에 구체적인 검증조치를 요구한 것은 이러한 전환의 출발점으로 볼 수 있다.³⁶

북한 IT 노동자의 유럽 확산이 보여주는 것은 단순한 위협의 지리적 이동이 아니다. 노동과 자금은 이미 하나의 네트워크로서 국경을 넘어 움직이는 반면, 국제사회의 집행은 여전히 국가별 제도와 관할권으로 분절되어 있다는 사실이다. 노동과 자본이 '탈영토화'되었다면, 제재 집행 역시 개별 국가의 분절된 법체계를 넘어 '초국가적 집행협력망'으로 진화해야 한다. 한국의 과제는 더 많은 북한 IT 노동자를 적발하는 데 그쳐서는 안 된다. 북한의 불법수익을 비확산·사이버·금융·고용을 연결하는 국가안보 사안으로 재정의하고, 11개국이 제기한 경고를 실제

³⁵ U.S. Department of Justice 2025a.

³⁶ Global Affairs Canada 2026.

비용을 부과할 수 있는 집행 협력으로 발전시켜야 한다. 북한의 불법수익망은 이미 국경을 넘어 움직이고 있다. 이제는 국제사회의 대응 역시 더 이상 국경 안에 머물러서는 안 된다.■

■ **저자:** **조은정**_국가안보전략연구원 연구위원.

■ **담당 및 편집:** **임재현**_EAI 연구원

문의: 02-2277-1683 (ext. 209) | jhim@eai.or.kr

본 논평을 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 10월 23일 979-11-7584-163-5 95340
“영토적 제재 VS 디지털 침투: 북한 IT 노동자의 유럽 확산이 던지는 경고”

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