김정은 정권의 사이버 공격과 주요국 대응

김보미 | 국가안보전략연구원 북한연구실장 | bomi@inss.re.kr

Ⅰ. 머리말

블록체인 분석기업인 체이널리시스(Chainalysis)는 「2025 가상자산 범죄 보고서(2025 Crypto Crime Report)」를 통해 2024년 북한에 의해 탈취된 암호화폐 금액이 사상 최대치를 기록했다고 발표했다. 북한에 의한 해킹 피해액은 약 13억 4천만달러(한화 약 2조원)로 집계되었는데, 이는 역대최고 액으로 전년 대비 102% 이상 증가한 수치였다(체이널리시스, 2025, p.77). 보고서에 따르면, 2024년 전체 암호화폐 탈취 금액의 61%가 북한 소행으로 지목되었으며, 전체 해킹 사건 수의 약 20%를 북한이 차지했다. 체이널리시스는 북한의 사이버 공격이 규모뿐만 아니라 정교함 측면에서도 급격히 고도화되고 있다고 지적했다.[1)]

국제사회는 북한의 암호화폐 해킹과 같은 악의적 사이버 활동을 글로벌 금융안보를 위협하는 심각한 위험 요인으로 지목하며, 공동 대응의 필요성을 지속적으로 강조하고 있다. 2025년 5월 캐나다 밴프에서 열린 G7 재무장관 회의에서 주요국들은 북한의 암호화폐 탈취가 전례 없이 심각한 수준에 이르렀다고 평가하며, 국제 공조를 통한 긴급 대응 체계 구축의 필요성을 확인하였다. 다만 북한의 암호화폐 공격 위협에 대한 국제사회의 경각심이 높아지고 있음에도, 이에 효과적으로 대응할 국제 공조 플랫폼이 아직 미흡하여 실질적인 협력에는 한계가 있다.

본고는 북한의 사이버 공격 양상과 이에 대한 주요국의 대응을 살펴본다. 이러한 사이버 공격은 북한의 불법 핵·미사일 개발 자금 조달의 핵심 수단이 되는 만큼, 국제 금융 시스템의 안정성을 해치는 중대한 위협으로 거론되고 있다. 이에 본 연구는 김정은 시대를 중심으로

1) 체이널리시스, 2025, p.77.

북한의 암호화폐 공격 양상을 살펴보고, 나아가 한국과 미국을 포함한 주요국의 대응 양상과 그 한계를 분석함으로써 국제 공조의 방향을 모색하고자 한다.

Ⅱ. 김정은 정권의 진화하는 사이버 공격 양상

1. 북한의 암호화폐 공격

북한이 감행하는 사이버 공격의 목적은 외화 벌이, 정보・기술 탈취, 핵・미사일 개발 자금 확보, 사회 혼란 조성 등 다양하지만, 최근에는 주로 외화 확보를 위한 사이버 공격에 집중하고 있다. 북한의 암호화폐 공격은 2016년 UN 안보리의 대북제재 강화로 외화 수입 경로가 차단되면서 본격적으로 활성화되기 시작했다. 2013~14년경에는 한국이나 일본 등 아시아 기반의 금융기관들을 상대로 제한적인 해킹 활동을 벌였다. 당시 암호화폐 시장 자체가 작았기 때문에 탈취 규모는 비교적 소규모였으며, 이러한 금융권에 대한 공격 중 일부는 정치적 동기에 따른 것이기도 했다.[2] 그러나 암호화폐 시장이 급격히 성장하고 2016년 UN 안보리 대북제재로 인해 외화 고갈이 맞물리면서 북한은 조직적으로 암호화폐 탈취를 시도하였다. 특히 2017년 워너크라이(WannaCry) 랜섬웨어 공격은 전 세계 150여 개국에 약 1억 달러 상당의 피해를 주며 국제사회에 북한 사이버 위협의 심각성을 각인시켰다.

김정은 정권은 라자루스 그룹(Lazarus Group), 안다리엘(Andariel), 블루노로프(BlueNorOff), 김수키(Kimsuky) 등 다양한 해커 조직들을 배후에서 조종하며 암호화폐 탈취 규모를 확대해 나갔다. 이들은 암호화폐 거래소들은 물론 개인지갑까지 공격하면서 수억 달러 규모의 피해를 발생시켰다. 최근에는 이러한 북한 해킹 조직들이 독립적으로 활동하기보다는 기술적 자산과 인프라를 공유하며 공동 작전을 수행하는 형태로 전환되고 있는 경향이 포착된다. 이는 암호화폐 거래를 통한 자금 탈취라는 공통의 목적에 따른 것으로 해석된다.[3] 북한 해커들은 탈취한 암호화폐를 쪼개 누가 전송했는지 출처를 불분명하게 만드는 믹싱 기술을 활용하여 암호화폐의 이동 추적을 어렵게 만들었다. 이러한 자금세탁 과정이 끝나면 암호화폐는 아시아 기반 거래소를 통해 중국 위안화 등 법정통화로 환전되어 현금으로 확보되었다.[4]

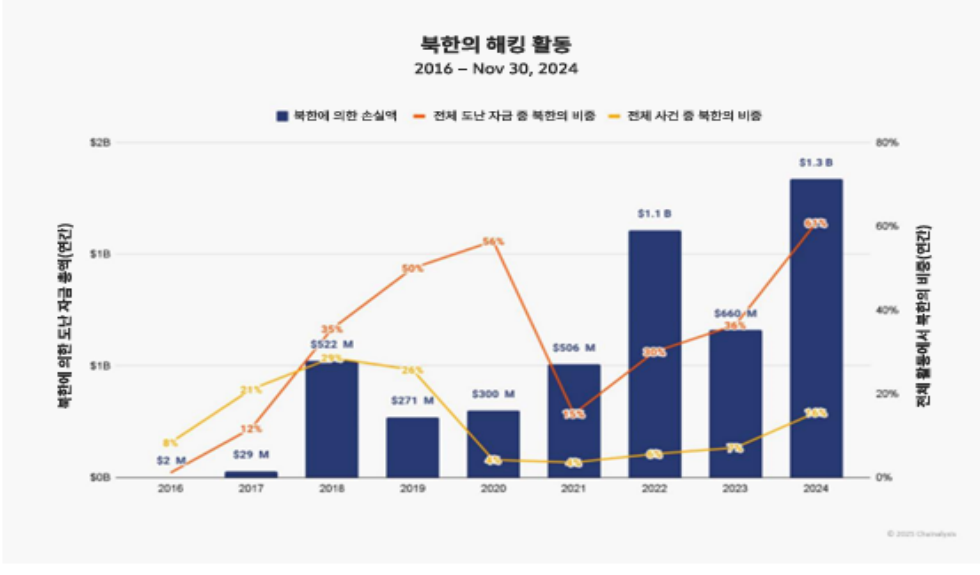
---

2) 김보미, 2022, p.6.
3) 김보미, 2025, p.174.
4) Chainalysis Team, 2022. 1. 13.

결과적으로 북한의 암호화폐 공격에 따른 피해 규모는 비교적 꾸준하게 증가하였다(그림 1 참조). 피해 국가도 아시아 국가들만이 아닌 미국, 유럽 등 글로벌 지역으로 확대되었다. 2024년 북한의 암호화폐 공격은 역대 최고치를 기록하였으며, 특히 북한의 암호화폐 해킹 공격 빈도는 압도적인 수준이다. 뿐만 아니라 2025년 2월, 북한은 세계 2위의 암호화폐 거래소 '바이비트(Bybit)'를 공격하여 역대 최대금액인 미화 14억 6천만달러 어치(한화 약 2조 1천억원)의 암호화폐를 탈취한 배후로 지목되었다. 앞서 역대 최대 단일 사건은 2022년 3월 블록체인 기반 게임 플랫폼 '액시 인피니티(Axie Infinity)'에 대한 공격이었다. 게임 내 네트워크 시스템인 '로닌(Ronin)'의 보안 취약점을 이용하여 대규모 암호화폐를 탈취한 후, 약 1만 2천개 이상의 가상 계좌를 통해 은닉을 시도한 것으로 알려졌는데, 피해액이 약 6억 2,500만달러에 달할 것으로 추정되었다.

이러한 일련의 사건들은 북한의 암호화폐 공격이 단순한 범죄를 넘어, 국가전략 차원의 외화 조달 및 금융시스템 교란 수단으로 자리 잡고 있음을 보여준다.

[그림 1] 지난해 북한의 암호화폐 탈취 규모



자료: 체이널리시스, 「2025 가상자산 범죄 보고서」, 2025. 2. 27(chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.chainalysis.com/wp-content/uploads/2025/04/the-2025-crypto-crime-report-korea-release.pdf), p.78.

2. 신기술을 활용한 사이버 공격의 진화

최근에는 북한의 해킹 기술이 진화하여 점차 고도화 및 교묘해지는 추세에 있다. 북한 해커들은 초기의 단순한 피싱 이메일이나 가짜 웹사이트를 이용한 침투 방식에서 벗어나, 링크드인(LinkedIn)・깃허브(GitHub) 등 취업・개발자 플랫폼을 악용한 가짜 채용공고, 이메일 내 QR 코드를 활용한 악성 앱 설치를 유도하는 큐싱(Qshing), 생성형 인공지능(Generative AI) 기반의 맞춤형 피싱 공격 등 보다 정교한 기법을 구사하고 있다.[5] 침투 경로 또한 사용자 단말기 수준을 넘어, 블록체인 네트워크 자체의 취약점이나 거래소 서버를 직접 겨냥하는 방향으로 확대되고 있다.[6] 자금세탁 방식 역시 단순 믹서(mixer) 활용이 아닌, 탈취 자산을 NFT (대체불가능토큰) 형태로 전환하거나 온라인 게임 아이템・자산으로 위장하는 등 추적 회피 전략이 지능화되고 있다(김보미, 2025, p.178).

체이널리시스의 「2025 가상자산 범죄 보고서」는 북한의 암호화폐 해킹 공격 횟수와 탈취 금액이 증가한 배경에 대한 흥미로운 분석을 내놓았다. 보고서는 북한의 공격이 단순한 외부 침투에 그치지 않고 내부 접근권 확보를 통한 장기적 침투 전략을 병행하고 있다고 분석했다. 특히 북한의 IT 인력이 암호화폐 관련 기업에 침투하여 그들의 네트워크, 운영 시스템의 무결성을 훼손할 가능성을 제기했다. 체이널리시스는 이들이 내부 접근 권한을 확보하기 위해 가짜 신분, 제3자 채용 중개업체 이용, 원격 근무 기회 조작과 같은 고도로 정교한 전술과 기법을 활용하고 있음을 지적했다.[7] 이는 북한이 일회성 해킹을 넘어, 공격 대상 시스템 내부에 영구적인 거점 및 접근 권한을 구축하려는 진화된 전략을 구사하고 있음을 시사한다.

더 나아가, 김정은 국무위원장은 최근 AI 활용에 깊은 관심을 표하고 있는데, 특히 AI 기술이 적용된 드론과 같은 무기체계의 개발과 함께 AI 기술의 급속한 발전을 주문한 바 있다(『조선중앙통신』, 2025. 9. 19). 이러한 관심은 단순한 기술적 호기심을 넘어, 사이버 활동에도 AI를 적용하려는 시도와 관련이 있다는 추측을 가능케 한다. 실제로 구글은 북한 해커들이 암호화폐와 금융 관련 정보 수집, IT 인력 위장 취업 등 다양한 활동에 자사의 AI 프로그램인 제미나이(Gemini)를 활용했다고 주장했다.[8] 구글은 또한 제미나이가 군사체계와 암호화폐 시장 동향 등 북한정부의 전략적 관심사를 연구하고 조사하는 데 활용되었다고

---

5) 김보미, 2025, p.178.
6) 홍지인・조다운, 「국정원 "러 파병 북한군, 사망자 600명 포함 4천 700여명 사상"」, 『연합뉴스』, 2025. 4. 30(https://www.yna.co.kr/view/AKR20250430096351001?input =1195m).
7) 체이널리시스, 2025, p.80.
8) 구글 위협 인텔리지전스 그룹, 2025. 1. 30.

발표했다.[9] 이는 북한의 해커들이 반드시 불법적인 방법이 아니더라도 자신들의 위협성을 고도화하고 진화시킬 수 있는 방법이 늘어나고 있다는 것을 의미한다.

종합적으로 볼 때, 북한의 사이버 위협은 단순한 공격 기술의 변화를 넘어 전략적이고 조직적인 시스템 침투 단계로 진화하고 있는 것으로 보인다. 북한은 정교한 내부 침투 전략을 통해 장기적 이득을 추구하는 한편, 생성형 AI와 같은 최신 기술을 활용하여 공격의 효율성과 정밀도를 극대화하고 있다. 진화하는 북한의 사이버 공격은 국제사회의 경각심 제고와 이를 공동으로 방어할 실질적인 공조체계 구축의 필요성을 제기한다.

Ⅲ. 김정은 정권의 사이버 공격에 대한 주요국 대응

1. 한국

한국 국가정보원(이하 국정원)은 『2025 국가정보보호백서』를 발간하고 한국에 대한 사이버 공격의 80%를 북한 소행으로 추정하였다. 백서에 따르면 한국을 겨냥한 사이버 공격은 하루 수십만 건에 이르며 첨단 산업기술 탈취와 사회 혼란 조장 등 다양한 목적으로 발생된다.[10] 그러나 사이버 공격의 피해 규모가 큼에도 불구하고 적극적인 대응을 하고 있다고 평가하기 어렵다.

현재 우리 정부는 기업의 보안 위반 시 제재, 사이버 위협 관련 정보 공유, 독자 제재, 사이버 공격에 대비한 실전 중심 훈련 등을 강화해 나가고 있다. 방송통신위원회는 2017년 12월, 개인정보 파일을 암호화하지 않고 백신 소프트웨어 업데이트를 하지 않는 등 보안 조치 소홀을 이유로 빗썸에 과징금과 과태료를 부과하였으며 이는 암호화폐 거래소에 대한 첫 제재 조치 사례로 기록되었다. 또한 국정원은 국내 대형 암호화폐 거래소인 업비트, 빗썸, 코빗(Korbit), 코인원(Coinone) 등 4곳에 국내・외 주요 사이버 위협 정보를 제공하는 등 정보 공유 서비스를 확대하고 있다.[11] 나아가 정부는 2025년 8월, 국가비상사태에 대비해 행정체계를 점검하고, 전시 대비 국민생활의 안정을 유지하기 위한 범정부 차원의 종합훈련인 을지훈련(Ulchi Freedom Shield)을 실시하면서 북한의 군사위협뿐만 아니라 사이버 공격, 드론, GPS 교란 등과 같은 첨단 기술을 이용한 복합 위협에 대비하는 실전 중심 훈련을

9) 구글 위협 인텔리지전스 그룹, 2025. 1. 30.
10) 국가정보원, 2025. 6.
11) 김보미, 2022, p.15.

포함하였다.

또한 우리 정부는 사이버 위협에 대응하기 위한 국제 공조에도 적극적으로 참여하기 시작했다. 한국정부의 국제 공조는 주로 한미 양자 협력, 한미일 3국 협력 또는 다자 외교적 노력 중심으로 이루어지며 북한의 악의적 사이버 활동으로 인한 수입 창출을 차단하는 데 초점을 맞추고 있다. 우리 정부는 2022년 5월 한미정상회담을 개최하여 사이버 안보 전반에 걸쳐 미국과의 공동 대응에 합의하였고, 2023년 8월 캠프 데이비드 한미일 정상회담 합의에 따라 북한 사이버 위협 대응을 위한 한미일 외교당국 실무그룹을 창설하고 정기적으로 협의하고 있다. 실무그룹에서는 북한의 암호화폐 탈취 수법이나 해킹조직의 활동 동향, 그리고 IT 인력의 위장 취업 등 악성 사이버 활동 정보를 긴밀히 공유하고 있다. 이와 함께 한미 양국은 북한이 탈취한 가상자산을 동결 및 압류하는 노력을 공동으로 추진하며 자금줄 차단에 주력하고 있다.[12] 이밖에 우리 정부는 2022년 5월 NATO의 사이버 방위센터 회원 가입을 통해 양자 및 다자 협력 강화에 나서는 등 북한의 사이버 위협에 대한 글로벌 방어 시스템 구축에 집중하고 있다.

우리 정부는 북한의 불법 사이버 활동 이후 2023년 2월 사이버 분야 첫 독자 제재를 발표하였다. 북한 정찰총국, 라자루스, 김수키, 안다리엘 등이 독자 제재 대상으로 공식 지정되었다.[13] 제재 지정 대상에 대해서는 자산동결, 거래 금지, 입국 금지 등 조치가 적용된다. 그러나 사실상 해당 인물들이 한국을 방문할 가능성이 낮고 한국 금융시스템을 직접 이용하지 않는 경우가 대부분이라 제재를 통해 동결할 수 있는 실질적 자산이나 거래가 매우 제한적이다. 탈취 자금 또한 익명화되었거나 분산되어 있을 가능성이 커 한국의 독자 제재만으로는 세탁 경로를 추적하고 차단하기가 어렵다. 결국 북한에 대한 사이버 독자 제재는 북한의 불법 행위를 비난한다는 상징적 효과는 크지만, 북한의 핵・미사일 개발 속도를 늦추거나 외화벌이 자체를 멈추게 하는 결정적인 수단이 되기는 어렵다고 볼 수 있다.

위와 같은 사이버 안보 위협에 대응하기 위한 다각적인 노력에도 불구하고 가장 아쉬운 부분은 사이버 위협 대응체계 수립을 위한 법률안 제정이 미비된 상태라는 점이다. 국가사이버 안보법은 10년째 계류 중이다. 해당 법안은 국방, 공공, 민간으로 분산된 현재의 사이버 위기 대응체계를 국가 차원에서 일원화하고, 사이버 안보 정책의 컨트롤 타워 역할을 할 기구를 설치하는 것을 목표로 하고 있다. 북한의 암호화폐 탈취에 선제적인 대응을 위한

---

12) 미국 CNN은 2023년 1월, 국가정보원이 미국 민간 조사단과 합동작전을 벌여 암호화폐 100만달러(한화 약 13억원)어치를 회수하는 데 성공했다고 보도하였다. 김종훈, 「국정원-美 판교 모여 협동 작전, 北 훔친 암호화폐 회수했다」, 『머니투데이』, 2023. 4. 10(https://www.mt.co.kr/world/2023/04/10/2023041014085027920).

13) 정부의 독자 제재 목록에 오른 기관은 조선엑스포합영회사, 라자루스 그룹, 블루노로프, 안다리엘, 기술정찰국, 110호 연구소, 지휘자동화대학(미림대학) 등 7곳이며 개인은 박진혁, 조명래, 송림, 오충성 등 총 4명이다. 오수진, 「정부, 사이버분야 첫 대북 독자제재…개인 4명・기관 7곳 지정(종합)」, 『연합뉴스』, 2023. 2. 10(https://www.yna.co.kr/view/AKR20230210036651504).

법적 근거 마련이 시급하고, 미국, 일본 등 주요국과의 사이버 안보 공조를 위해서도 해당 법안의 필요성이 제기된다. 그러나 국가정보원 및 정보기관의 권한 과잉 우려, 민간인 사찰 악용, 기업 부담 증가 가능성 등 여러 문제점으로 인해 아직 국회를 통과하지 못하고 있다.

2. 미국

미국은 그 어느 나라보다 국가 배후 해킹에 선제적으로 대응하며, 국제 공조를 중시해 왔다. 특히 2014년 소니 픽처스 해킹 사건 이후 사이버 위협이 실질적인 안보 이슈로 부각되면서, 미국정부는 2015년 '행정명령 13687호(Executive Order 13687)'를 제정하여 북한의 악의적 사이버 활동에 연루된 기관 및 개인을 독자적으로 제재할 수 있는 권한을 마련하였다.[14] 미국의 주요 사이버 안보 기관들은 북한에 특화된 대응책을 마련하고, 주기적인 경보 발령과 기술 분석 보고서를 통해 경각심을 제고해 왔다. 국무부(State Department), 재무부(Treasury Department), 연방수사국(FBI)은 공동으로 「북한 IT 노동자 관련 주의 권고문(IT Workers Advisory)」을 발간하여, 북한 인력이 제3국 신분을 도용해 미국 기업의 원격 근무자로 위장 취업하는 사례를 경고하고 기업이 유의해야 할 '레드 플래그(red flags)'를 제시하였다. 또한 사이버보안 및 기반시설안보청(Cyber Security and Infrastructure Security Agency: CISA)은 북한의 악성 사이버 활동을 분석하고 공공·민간 부문이 취해야 할 방어 조치를 안내하는 기술적 지침을 지속적으로 제공해 왔다.[15]

바이든 행정부는 이러한 흐름을 이어받아 제도적으로 강화하였다. 2021년 10월에는 법무부 산하에 국가 암호화폐단속국(National Cryptocurrency Enforcement Team: NCET)을 신설해 암호화폐 관련 불법 활동 수사를 전담하게 하고, 2022년 4월에는 국무부가 사이버공간 및 디지털 정책국(Bureau of Cyberspace and Digital Policy: CDP)을 출범시켜 랜섬웨어와 인터넷 거버넌스 등 국제 사이버 규범 논의에 대응하였다. 2023년 이후 이들 기관은 북한의 해외 IT 인력 위장 취업, 암호화폐 탈취, 인공지능(AI) 악용 등 새로운 위협 양상에 대응하기 위한 분석 및 정책 개발을 강화하였다.

이러한 조직 신설과 더불어, 법 집행 및 제재 조치 역시 한층 강화되었다. 법무부는 북한

14) 이 행정명령은 이후 북한의 해커 조직 라자루스, 킴수키, 안다리엘 등에 대한 표적 제재의 법적 기반이 되었다.
15) 실제로 FBI와 CISA는 2020년 북한 해커들의 불법 송금과 ATM 인출 시도에 대한 경보를 발령했으며, CISA·재무부·국토안보부·FBI는 암호화폐 공격을 포함한 북한의 악의적 사이버 활동 관련 공동 보고서를 발표한 바 있다. Cyber Security and Infrastructure Security Agency, "Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a; "Alert (AA20-106A): Gudiance on DPRK Cyber Threat Advisory," April 15, 2020, https://www.cisa.gov/uscert/ncas/alerts/aa20-106a; Cyber Security and Infrastructure Security Agency, "North Korean Malicious Cyber Activity," May 12, 2020, https:// www.us-cert.gov/ncas/current-activity/2020/05/12/ north-korean-malicious-cyber-activity.

IT 인력이 위장 신분으로 해외 암호화폐 기업에 침투하거나 원격 근무를 통해 외화를 탈취한 사건들에 대해 관련 피의자 기소, 관련 웹사이트 폐쇄, 자산 압류 등의 실질적 조치를 취하였다. 2025년 6월에는 다수의 주(州)가 협력하여 북한의 원격 IT 노동자 네트워크를 해체하고, 200여 대의 컴퓨터와 수십 개의 은행 계좌를 동결하였다. 재무부 역시 북한의 사이버 조직과 그 지원 네트워크에 대한 제재를 지속하고 있다. 2022년 5월에는 액시 인피니티 해킹 자금 세탁에 연루된 믹서 기업 블렌더(Blender)를 제재했으며, 2023년 5월에는 불법 사이버 활동으로 외화를 벌어들이는 북한 단체 및 개인을, 2025년에는 북한 IT 노동자의 해외 원격 근무 활동에 관여한 기업과 인물을 추가로 제재 대상에 올렸다.[16)]

이와 함께 미국은 도난당한 자금을 해킹으로 다시 회수하는 카운터해킹(counter-hacking)을 통해 북한의 불법 자금 회수를 적극 추진하고 있다. 2022년 9월, FBI는 라자루스 그룹이 '액시 인피니티'에서 탈취한 암호화폐를 현금화하려 한 시도를 차단해 약 3천만달러를 회수했으며, 같은 해 7월에는 캔자스주의 한 병원이 랜섬웨어 공격으로 지불한 암호화폐 50만달러를 회수하였다. 이러한 대응은 북한의 해킹 역량이 정교해질수록 미국의 사이버 전략 또한 보다 공세적이고 전방위적으로 진화하고 있음을 보여준다.[17)]

그러나 2024년 대선 이후 트럼프 행정부가 출범하면서 미국의 사이버 및 암호화폐 정책은 새로운 전환점을 맞고 있다. 트럼프 대통령은 암호화폐 산업을 전략산업으로 격상하고 규제 완화를 추진하고 있으며, 이에 따라 2025년 4월 법무부는 NCET를 해체하고 그 기능을 기존 컴퓨터범죄·지식재산국(Computer Crime and Intellectual Property Section: CCIPS)으로 통합하였다.[18)] 이는 암호화폐에 대한 형사 규제를 축소할 뿐만 아니라 오히려 산업 진흥 중심으로 전환하겠다는 신호로 평가된다. 상품선물거래위원회(Commodity Futures Trading Commission: CFTC) 역시 대통령 행정명령에 따라 암호화폐 단속팀을 축소하며, 디지털 자산 단속 부서는 두 곳만 남게 되었다[19)].

이러한 변화는 트럼프 행정부가 사이버 보안 강화나 범죄자 처벌보다는 디지털 자산 산업 활성화에 정책적 무게중심을 두고 있음을 의미한다. 그러나 규제 완화는 소비자 보호 약화와 금융시스템 불안정성을 초래할 수 있으며, 사이버 보안 공백은 북한의 국가 주도 해킹 조직이 악용할 위험이 높다. 따라서 향후 미국의 사이버 안보정책은 산업 진흥과 보안 강화라는

---

16) 조준형, 「美, 北 IT노동자 해외 파견 관여한 기업·개인 제재」, 『연합뉴스』, 2025. 7. 25(https://www.yna.co.kr/view/AKR20250725007900071?input=1195m).
17) 김보미, 2022, p.12.
18) 트럼프 본인과 가족이 암호화폐 산업에 직접 관여함으로써 공적 정책과 사적 이해 사이의 경계가 모호해지고 있다는 평가이다(Lang, Hannah, "Trump Signs Bill to Nullify Expanded IRS Crypto Broker Rule," *Reuters*, April 11, 2025(https://www.reuters.com/world/us/trump-signs-bill-nullify-expanded-irs-crypto-broker-rule-2025-04-11/?utm_source=chatgpt.com, accessed: April 27, 2025).
19) 손정환, 「미 법무부, 암호화폐 집행팀 전격해체…트럼프식 규제 완화 본격화」, 『토큰포스트』, 2025. 4. 10(https://www.tokenpost.kr/news/cryptocurrency/236568).

두 가지 목표 사이에서 새로운 균형점을 모색해야 할 것으로 보인다.

3. 유럽 및 국제기구

유럽연합(EU)과 국제기구들은 북한의 악의적 사이버 활동에 대해 신속하고 지속적인 대응을 이어가고 있다. EU는 독자적인 사이버 제재 체제를 운영하며 북한 관련 기관과 개인에 대한 제재를 강화하고 있다. 2020년 7월 EU는 북한, 중국, 러시아의 사이버 공격 연루 기관을 대상으로 첫 제재를 단행했으며, 이때 북한의 조선엑스포합영회사도 제재 대상에 포함되었다. 제재 대상 기관은 EU 내 자산 동결, 입국 금지, EU 내 자금 지원 금지 등의 조치를 받는다. 조선엑스포합영회사는 2017년 워너크라이 랜섬웨어 공격과 관련이 있다고 평가되었으며, 제재 조치는 정기적으로 연장되고 있다. 2025년 초에는 북한 해커 조직과 연계된 개인들이 제재 대상으로 추가 지정되었으며, 5월에는 유럽 내외에서 수행되는 악의적 사이버 활동에 참여한 개인과 기관에 대해 자산 동결과 여행 금지 제재를 유지・강화하는 규정을 마련하였다.[20] 이러한 조치는 EU가 북한의 사이버 위협을 국제 금융 안전과 사이버 안보 차원에서 심각한 위협으로 인식하고 있음을 보여준다.

주요 7개국(G7) 역시 북한의 사이버 활동을 대량살상무기(WMD) 개발 자금 조달의 핵심 수단이자 국제 금융 안보를 위협하는 요소로 규정하며, 이에 대한 공동 대응의 중요성을 강조하고 있다. 2025년 5월, G7 재무장관 회의에서는 북한이 WMD 프로그램에 우선순위를 두고 디지털 자산 탈취 및 세탁을 시도하는 행위를 강력히 규탄하는 공동성명을 발표했다. G7 회원국들은 UN 안보리 결의에 따른 제재의 효과적 이행과 제재 회피 방지를 위해 상호 협력을 강화하겠다는 입장도 함께 천명하였다.[21]

한편, UN 안전보장이사회 차원의 대응은 기존 대북제재의 이행과 감시에 주로 초점을 두고 있다. 과거 UN 안보리 대북제재위원회 전문가 패널은 북한의 사이버 활동이 WMD 자금 조달에 미치는 영향을 분석하고 보고하는 역할을 수행했으나, 2024년 3월 러시아의 거부권 행사로 4월 30일부로 해당 패널의 활동이 중단되었다. 그럼에도 불구하고 안보리는 여전히 사이버 안보를 정기적인 의제로 다루고 있으며, 미국과 한국을 비롯한 주요 국가들은 북한의 불법적 사이버 활동에 대한 대응을 지속적으로 촉구하고 있다.[22] 이는 북한의 해킹

---

20) 제재 대상에 오른 인물은 리창호 정찰총국장과 신금철 조선인민군 총참모부 작전국 처장이다. EU 리창호가 러-우전쟁에 북한 군인을 파병하고, 라자루스 등 해킹조직을 동원해 사이버전 수행에 결정적인 역할을 했다고 보고 지적했다. 문가용, 「EU, 北 해커 수장 리창호 제재」, 『보안뉴스』, 2025. 2. 27(https://www.boan news.com/media/view.asp?idx=136281).
21) 『토큰포스트』, 2025. 5. 23.
22) UN안보리 대북제재위원회 전문가 패널이 종료됨에 따라, 2024년 10월 한미일이 주도하여 다국적제재모니터링팀(Multilateral Sanctions Monitoring Team: MSMT)을 출범시키고 북한의 사이버 관련 활동이 감시하고 있다.

행위가 국제사회가 합의한 '사이버 공간에서의 책임 있는 국가 행동' 원칙에 정면으로 위배됨을 국제사회에 공표하는 의미를 가진다.

종합하면, EU와 G7, UN 등 국제사회는 북한의 사이버 공격을 단순한 기술적 사건이 아닌 국제 금융 안보와 WMD 확산 문제와 직결된 중대 위협으로 인식하고 있으며, 제재, 모니터링, 정보 공유를 통한 다층적 대응 체계를 강화하고 있다. 그러나 북한의 사이버 역량이 점점 고도화됨에 따라, 국제 공조와 제재 집행의 실효성을 높이는 지속적 노력과 법·정책적 보강이 앞으로도 필수적이라고 평가된다.

Ⅳ. 평가 및 전망

북한의 사이버 공격은 단순한 해킹을 넘어 외화 조달, 핵·미사일 개발 자금 확보, 정보 탈취 등 국가 전략적 목적과 밀접하게 연계된 복합적 위협으로 진화하고 있다. 특히 암호화폐 탈취와 자금세탁 수법은 점차 고도화·지능화되고 있으며, 국제 금융안보에 심각한 영향을 미치고 있다. 이에 대응하여 미국, 일본, EU 등 주요국은 독자적인 사이버 제재와 법적 조치, 카운터 해킹, 정보 공유 및 국제 공조를 통해 북한의 공격을 억제하고 있다. 유엔 안전보장이사회(UNSC) 차원의 대응은 기존 제재 이행과 감시를 중심으로 하고 있으나, 일부 국가의 거부권 행사 등으로 인해 감시 기능이 약화되는 한계가 존재한다.

북한은 모든 사이버 범죄 행위에서 자국의 배후 연루를 부정하며, 북한 정권에 대한 실체 없는 것으로 일축하고 있다. 9월 1일, 김천일 북한 외무성 보도국장은 한미일 실무그룹회의를 언급하며, 주권 국가인 북한을 대상으로 한 집단적 압박과 공조가 지정학적 긴장을 심화시키는 도발적 움직임이며, 이를 사이버 안보 분야로까지 확대하고 있다고 비판하였다. 그러나 북한은 대북제재를 회피하고 외화를 확보하기 위한 수단으로 사이버 공격을 지속할 가능성이 높다. 북중, 북러 관계가 개선되더라도 북한은 여전히 제재의 적용을 벗어나지 못하며, 주변국이 모든 제재를 무력화할 가능성도 제한적이다. 미국과 유엔 안보리의 대북제재가 지속되는 한, 북한에 사이버 공격은 제한된 경제활동 환경에서 중요한 외화 획득 수단으로 남게 된다.

따라서 북한의 사이버 공격은 단순한 기술적 위협을 넘어 국제 정치·경제 체계와 밀접히 연계된 복합적 도전으로 볼 수 있으며, 효과적 대응을 위해서는 개별 국가의 조치뿐 아니라 국제사회 차원의 협력과 새로운 감시·대응 메커니즘 구축이 필수적이다. 특히, 북한의 공격 수법이 점점 지능화되고 AI 등 신기술 활용 가능성까지 커지는 상황에서, 국제사회는 기존

제재와 정보 공유 체계만으로는 한계가 있음을 인식하고, 사이버 위협 대응을 위한 법적·정책적 틀의 지속적 강화와 민관 협력을 확대해야 한다.

이와 같은 맥락에서, 북한의 사이버 공격은 단순한 안보 문제가 아니라 국제 금융 안정, 기술 경쟁력, 국가 주권과 직결된 문제임을 보여준다. 향후 대응전략은 기술적 방어와 법적 제재를 병행하면서, 국제 공조를 통한 선제적 예방과 피해 최소화에 초점을 맞추는 것이 핵심적 과제로 자리할 것이다.

참고문헌

김보미, 「북한의 암호화폐 공격과 미국의 대응」, 『INSS 전략보고』, No. 191, 2022(https://www.inss.re.kr/common/viewer.do?atchFileId=F20221125092229956&fileSn=0).

_____, 「북한의 암호화폐 공격 양상과 트럼프 2.0 시대 전망」, 『통일과 담론』, 제4집 1호, 2025, pp.167~193.

체이널리시스, 「2025 가상자산 범죄 보고서」, 2025. 2. 27(chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.chainalysis.com/wp-content/uploads/2025/04/the-2025-crypto-crime-report-korea-release.pdf).

『조선중앙통신』, 2025. 9. 19.

〈웹사이트〉

『토큰포스트』, "G7, 북한 암호화폐 해킹에 '전례 없는 위협' 경고…글로벌 공조 강화 나서", 2025. 5. 23(https://www.tokenpost.kr/news/cryptocurrency/250712).

구글 위협 인텔리전스 그룹(Google Threat Intelligence Group), "생성형 AI의 두 얼굴: 악용사례와 대응전략(Adversarial Misuse of Generative AI)," 2025. 1. 30(https://cloud.google.com/blog/ko/topics/threat-intelligence/adversarial-misuse-generative-ai).

국가정보원, 『2025 국가정보보호백서』, 2025. 6(https://www.kisa.or.kr/skin/doc.html?fn=20250617_180527_194.pdf&rs=/result/2025-06/).

김종훈, 「국정원-美 판교 모여 협동 작전, 北 훔친 암호화폐 회수했다」, 『머니투데이』, 2023. 4. 10(https://www.mt.co.kr/world/2023/04/10/2023041014085027920).

문가용, 「EU, 北 해커 수장 리창호 제재」, 『보안뉴스』, 2025. 2. 27(https://www.boannews.com/media/view.asp?idx=136281)

손정환, 「미 법무부, 암호화폐 집행팀 전격해체…트럼프식 규제 완화 본격화」, 『토큰포스트』, 2025. 4. 10(https://www.tokenpost.kr/news/cryptocurrency/236568).

오수진, 「정부, 사이버분야 첫 대북 독자제재…개인 4명·기관 7곳 지정(종합)」, 『연합뉴스』, 2023. 2. 10(https://www.yna.co.kr/view/AKR20230210036651504).

조준형, 「美, 北 IT노동자 해외 파견 관여한 기업·개인 제재」, 『연합뉴스』, 2025. 7. 25

(https://www.yna.co.kr/view/AKR20250725007900071?input=1195m)

홍지인・조다운,「국정원 "러 파병 북한군, 사망자 600명 포함 4천 700여명 사상"」, 『연합뉴스』, 2025. 4. 30(https://www.yna.co.kr/view/AKR20250430096351001?input=1195m).

Chainalysis Team, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," January 13, 2022 (https://blog.chainalysis.com/reports/north-korean-hackershave-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/).

Cyber Security and Infrastructure Security Agency, "Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," August 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a

_____, "Alert (AA20-106A): Gudiance on DPRK Cyber Threat Advisory," April 15, 2020(https://www.cisa.gov/uscert/ncas/alerts/aa20-106a).

_____, "North Korean Malicious Cyber Activity," May 12, 2020(https:// www.us-cert.gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity

Lang, Hannah, "Trump Signs Bill to Nullify Expanded IRS Crypto Broker Rule," *Reuters*, April 11, 2025(https://www.reuters.com/world/us/trump-signs-bill-nullify-expanded-irs-crypto-broker-rule-2025-04-11/?utm_source=chatgpt.com, 접속일: April 27, 2025).