제27권/제10호
Vol.27/No.10

KDI

북한경제리뷰

KDI Review of the North Korean Economy

2025. 10

October

KDI 북한경제리뷰

KDI Review of the North Korean Economy

2025. 10

KDI

KDI 북한경제리뷰 편집진

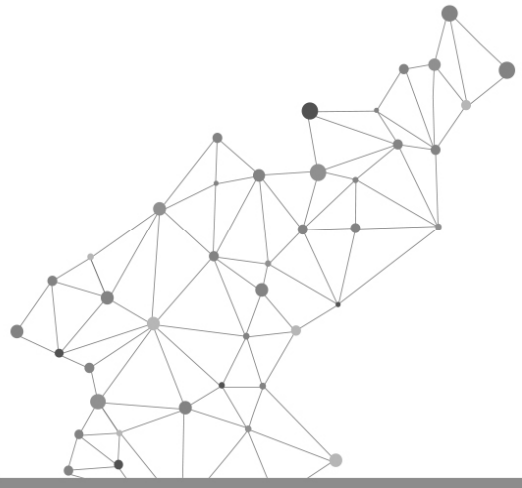
KDI 북한경제리뷰는
북한경제의 실태, 남북한 경제협력 및 경제통합과
관련한 주요 이슈를 분석 정리하여
정책당국자, 학계 및 업계 등의 이해를 높이고
정책방안을 도출하는 데 도움을 드리고자
월별로 발간되고 있습니다.
본 보고서의 내용은 출처 및 집필자를
명시하는 한 자유로이 인용할 수 있습니다.
전화번호 044-550-4114
팩스번호 044-550-4920

본 자료는
KDI 홈페이지(http://www.kdi.re.kr)로
접속하시면 보실 수 있습니다.

목차

동향과 분석

동향과 분석



북한 사이버 공격 전략의 진화: 대북제재 회피를 위한 외화 벌이 수단으로서 사이버 전략[1)]

이승열 | 국회입법조사처 입법조사관 | summer20@naver.com

Ⅰ. 들어가며

미국은 북한의 사이버 위협을 포함해 국제사회의 사이버 공격을 국가안보(national security)의 최우선 과제로 내세우며 강력히 대응하고 있다. 미국 바이든 행정부는 2021년 1월 백악관 내 '국가 사이버 국장직'을 신설한 직후, 국내적으로 '국가사이버안보회의'를 개최하여 미국의 대표적인 빅테크 기업들과 사이버 안보에 관한 민관협력을 강화하였고, 국제적으로 '랜섬웨어 대응회의사'를 개최하여 한국과 일본 등 35개국과의 국제적 협력 방안을 모색하였다.[2)] 그리고 2022년 3월 15일 미 백악관은 미국의 사이버 대응 능력을 더욱 강화하기 위해 「2022년 미국 이버 강화법」(Strengthening American Cybersecurity Act of 2022)에 서명하였다.

무엇보다 북한의 사이버 공격에 대한 한미 당국의 대응이 빨라지고 있다. 2022년 7월 25일 미 국무부는 북한이 '랜섬웨어'(ransomware) 공격을 통해 '몸값'을 요구하는 악의적인 금융사기를 자행하고 '가상화폐'(cryptocurrency)를 탈취하여 사이버 공격을 대북제재의 회피 수단으로 악용하고 있다고 판단하고, "북한의 악의적 사이버 활동에 대해 가용한 모든 수단을 동원해 북한 사이버 공격 세력을 추적하고 있다"고 밝혔다.[3)] 이러한 미 행정부의 노력은 트럼프 행정부 2기에서도 계속되고 있다. 2025년 6월 6일 트럼프 대통령은 행정명령 「국가 사이버 안보 강화를 위한 선택적 조치 지속」에 서명하면서 미국의 사이버 안보를

1) 본고는 이승열, 「북한 사이버 공격 전략의 진화: 대북제재 회피를 위한 외화 벌이 수단으로서 사이버 전략」, 『통일정책연구』, 제32권 1호(2023)에 게재된 논문을 발췌, 요약, 정리한 것임을 밝힌다.
2) 『VOA』, 2021. 10. 19.
3) 『VOA』, 2022. 7. 26.

위협하는 나라로 북한, 러시아, 이란 등을 새롭게 추가했다.[4]

우리 정부도 2023년 2월 북한의 '라자루스' 등 해킹 관련 기관 7곳과 해커 4명에 대해 처음으로 독자 제재를 결정하였다. 정부의 제재 대상에 오른 기관은 라자루스(Lazarus), 블루노로프(BlueNorOff), 안다리엘(Andarial), 조선엑스포합영회사, 기술정찰국, 110호 연구소, 지휘자동화대학 등이며, 개인의 경우는 박진혁, 조명래, 송림, 오충성 등이 리스트에 올랐고, 이중 박진혁은 이미 2014년 미국 소니픽쳐스(sonypictures) 엔터테인먼트사 해킹과 2017년 '워너크라이'(WannaCry) 랜섬웨어(ransomware) 공격을 주도하면서 미 법무부에 의해 기소된 전력이 있는 것으로 나타났다.[5]

북한의 사이버 공격이 이처럼 국제사회의 안보 이슈로 떠오른 이유는 북한이 국제사회의 대북제재로 인한 경제적 피해를 만회하고 핵과 미사일 개발을 위한 자금을 확보하는 수단으로 사이버 공간을 이용하고 있기 때문이다.[6] 따라서 본 글은 국제적 안보 이슈로 떠오른 북한의 사이버 공격 전략의 진화를 분석하고, 이를 토대로 북한의 사이버 공격에 대한 한미 당국과 국제사회의 대응 방안을 살펴보도록 하겠다.

Ⅱ. 북한의 사이버 공격 전략과 능력

1. 북한의 사이버 공격 전략

북한이 사이버 군사 전략을 수립한 계기는 1991년 미국의 걸프전 이후 현대전에서 전자전의 중요성을 인식하면서부터 시작되었다. 이후 북한은 조선인민군 총참모부 산하에 '지휘자동화국'을 설치하고, 각 군단에는 '전자전 연구소'를 설치한 후 사이버전 능력을 국가전략으로 채택하고 발전시켰다.[7] 이를 위해 북한은 '김일성정치군사대학'(일명 미림대학), 김책공대, 평양컴퓨터기술대학 등에서 사이버전을 수행할 수 있는 전문 인력을 양성하였으며 졸업 후 총참모부, 정찰총국, 통일전선부에서 활동할 수 있는 해킹 전문 인력을 연간 300여 명씩 양성・배치하고 있다.[8]

당시 김정일은 "지금까지 전쟁이 총알전쟁, 기름전쟁이었다면 21세기 전쟁은 정보전"이라

4) 『한계레』, 2025. 7. 4.
5) 『중앙일보』, 2023. 2. 10.
6) 송태은, 「북한의 사이버 공격과 우리의 대응」, 『IFANSFOCUS』. IF2022-28K, 2022. 10, p.2.
7) 위의 자료, p.149.
8) 신충근・이상진, 「북한의 대남 사이버테러 전략 분석 및 대응 방안에 관한 고찰」, 『경찰학연구』, 제13권 제4호, 2013, p.206.

고 언급하며, "적의 군사정보를 얼마나 강력하게 제어하고, 자신의 정보력을 충분히 구사할 수 있는지가 전쟁의 승패가 좌우한다"고 강조했다.[9] 이에 따라 북한은 1995년 100여 명 수준의 '중앙당 35호실 기초자료조사실'을 설치하여 중앙당 부서에 필요한 해외 국가기관, 단체, 개인에 관한 기밀자료를 수집하였다. 1998년에는 사이버 부대(121국)를 창설하였고, 1999년에는 200여 명 수준의 사이버 심리전 부대인 적공국 '204소'를 설립하여 사이버 심리전을 펼쳤다.[10]

북한의 사이버 공격 능력은 2009년 2월 해외·대남 정보기구인 '정찰총국'(Reconnaissance General Bureau: RGB)의 등장으로 크게 발전하였다. 정찰총국의 활동 부서는 총 6개국(작전국(1국), 정찰국(2국), 해외정보국(3국), 대남 조정국(5국), 기술국(6국), 후방지원국(7국))으로 구성돼 있으며, 이 중 해외정보국(3국)은 북한 해킹 조직의 배후로 지목된 '121국'(일명 '사이버전지도국')으로 불리며, 북한의 직접적인 사이버공격을 담당하는 것으로 알려졌다. 제121국은 첩보와 공격을 담당하며 평양 대동강 유역의 무신동 지역에 본부를 두고 있으며, 주로 해킹 공격을 수행하여 한국과 미국의 시스템을 무력화시키고 주요 기밀을 위조하고 있다.

특히 '121국' 내의 산하 조직인 '110호 연구소'(컴퓨터기술연구소)는 컴퓨터 네트워크에 침입하여 정보를 획득함은 물론 금융기관 등의 네트워크에 바이러스를 이식하는 기술을 가지고 있는 것으로 알려져 있다. 북한의 주요 해킹 조직인 '라자루스'(Lazarus, 일명 Hidden Cobra), '블루노로프'(BlueNorOff), '안다리엘'(Andarial), 김수키(Kimsuky, 일명 탈륨(Thallium)) 등이 활동하고 있다.

먼저 북한의 금융분야 공격을 주도하는 '라자루스'는 2007년 초 설립되었으며, 2014년 소니픽쳐스 엔터테인먼트사 해킹과 2017년 워너크라이 랜섬웨어 사건, 국제 금융기관에 대한 해킹의 배후로 지목된 기관이다.[11] 다음은 라자루스의 하위 그룹으로 알려진 '블루노로프'와 '안다리엘'도 국제 금융기관, 카지노, 금융거래 소프트웨어 개발, 그리고 암호화폐 등 불법적인 금전적 수입을 확충하는 데 특화된 조직으로 알려졌다. '블루노로프'는 2016년 방글라데시 중앙은행을 대상으로 벌어진 8,100만달러 규모의 해킹을 주도한 주범으로 지목받았다. '김수키'도 정찰총국 산하 조직으로 2010년부터 활동한 것으로 알려졌으며, 주로 정보 탈취 업무를 수행하며 이를 위해 피싱 이메일 등 악성코드를 유포하는 수법을 쓴다. 특히 한·미·일 정부와 싱크탱크를 중심으로 정보수집 임무를 담당하고 있으며 일명 '탈륨'과

---

9) 김흥광, 「북한의 정보전 전략과 사이버 전력: 돈 없는 북한의 최후의 선택 사이버 전쟁」, 『월간조선』, 2011. 6.
10) 김진광, 「북한의 사이버조직 관련 정보 연구:조직 현황 및 주요 공격사례 중심으로」, 『한국컴퓨터학정보학회』, 제28권 제2호, 2020, p.113.
11) 김보미·오일석, 「김정은 시대 북한의 사이버 위협과 주요국 대응」, 『INSS 전략보고』, 제147호, 2021, p.7.

동일조직으로 추정하고 있다.[12]

현재까지 알려진 바로는 '121국'에 소속된 상근 사이버 요원(해커) 및 지원 인력은 6,000여 명(직접적인 해킹을 기획하는 인력이 약 1,200명, 기술지원 인력이 약 1,800명이며, 유관조직 사이버 요원도 약 3,000명 정도로 추정)이며, 소속 해커들은 대부분 벨라루스와 중국, 인도, 말레이시아, 러시아 등 해외에서 활동하고 있다.[13] 이것은 과거 북한 해커들이 중국 선양(칠보산 호텔)을 중심으로 헤이룽장, 산둥, 푸젠, 랴오닝성과 베이징 인근 지역 등 중국을 중심으로 사이버전 수행 거점을 설치하고 활동했던 것에 비해 최근 활동 범위가 크게 넓어진 것이다.

2. 북한의 사이버 공격 능력

북한의 사이버 공격은 핵과 미사일 능력과 함께 대표적인 '비대칭전략'(asymmetric strategies)으로서 새로운 안보 위협으로 평가되고 있다.[14] 이에 주요국들이 북한의 사이버 능력을 어느 수준으로 평가하는지를 살펴보는 것은 중요한 일이다. 먼저 영국의 국제전략연구소(The International Institute for Strategic Studies: IISS)는 북한의 사이버 능력을 최하위인 3그룹(Thrid-tier)에 속한다고 평가절하했다.[15] 무엇보다 북한의 사이버 인프라와 보안 수준이 세계 최하위이며, 세계 인터넷망과 연결하는 '게이트웨이'가 중국과 러시아 서비스 제공업체에 전적으로 의존하여 외부 공격에 취약하다고 밝혔다.[16]

그러나 미국은 열악한 북한의 사이버 인프라와는 달리, 북한의 사이버 공격 능력을 미국과 러시아 그리고 중국보다는 떨어지지만 매우 높은 수준으로 평가하고 있다. 미국 최대 소프트웨어 업체인 '마이크로소프트'사는 2020년 10월 발표한 「마이크로소프트 디지털 방어 보고」(Microsoft Digital Defense Report)라는 보고서에서 북한을 러시아, 이란, 중국 다음으로 세계 4번째 사이버 공격 국가로 분류하였다.[17]

미국의 민간연구 단체인 '외교협회'(Council on Foreign Relations: CFR)도 2022년 7월 발간한 사이버 안보 관련 특별 보고서인 "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet"에서 '사이버 공격을 후원하는 미국의 적국'(U.S. adversaries are sponsoring cyberattacks)으로 중국, 러시아, 이란, 북한 4개국을 지목했다(Adam Sagal and Gordon M. Goldstein, 2022). 이 보고서는 2005년부터 2021년까지 미국을 상대로

---

12) 위의 자료, p.7.
13) 이승열, 「북한 사이버테러 위협의 증가와 대응방안」, 『이슈와논점』, 제1127호, 2016, p.2.
14) 이승열, 「북한 사이버 공격의 현황과 쟁점」, 『이슈와논점』 제2034호, 2022, p.1.
15) 김보미 · 오일석, 「김정은 시대 북한의 사이버 위협과 주요국 대응」, 『INSS 전략보고』, 제147호, p.5.
16) 위의 자료, p.5.
17) 『VOA』, 2021. 10. 6.

한 사이버 공격은 중국이 156건으로 가장 많았고, 다음은 러시아가 110건, 그리고 이란이 55건, 북한은 54건이라고 주장했다.[18]

또한 미국 하버드대 케네디스쿨 '벨퍼센터'(Belfer Center)가 발간한 사이버 관련 2022년 보고서 「국가별 사이버 역량지표 2022(National Cyber Power Index 2022)」에서 북한의 사이버 능력이 전체 지표상으로는 세계 14위를 기록했지만 사이버 금융해킹 능력을 입증하는 금융부문에서는 전 세계 1위를 기록했다고 밝혔다.[19] 무엇보다 북한이 암호화폐 탈취나 금융기관에 대한 사이버 공격에 집중했기 때문이라고 분석된다. 그러나 이에 반해 '감시'(surveillance) 능력은 세계 17위, '정보'(intelligence) 능력은 세계 25위, '규범'(norms)과 '방어'(defence) 부문에서는 세계 30위로 조사국 중 최하위를 기록했으며, 단지 '파괴'(destructive) 부문에서 상위권인 세계 6위를 기록했다.[20]

결과적으로 이상의 논의를 통해 볼 때, 북한의 사이버 능력의 불균형이 매우 크다고 볼 수 있다. 즉, 사이버 공격 능력은 강하지만 이에 비해 국내 사이버 인프라의 취약성으로 인하여 사이버 보호 능력은 현저하게 낮다는 양면성을 잘 보여주고 있다. 하지만 북한의 사이버 공격 능력에 대한 국제사회의 관심은 북한 내의 사이버 인프라가 아니라 공격 능력이며, 북한의 사이버 공격 능력은 국제사회의 평가가 증명하듯 국제사회의 관심을 끌기에 충분하다고 볼 수 있다.

Ⅲ. 북한의 사이버 공격 전략의 변화와 원인

1. 북한의 사이버 공격 전략의 변화

북한의 사이버 공격은 2009년 7월 7일 한국과 미국의 주요 기관 35개의 웹사이트에 대하여 디도스 공격을 감행함으로써 시작되었다. 이후 네 차례에 걸친 대남 사이버 공격으로 정부 기관을 비롯한 68개 주요 포털사이트가 장애를 일으켰다.[21] 북한은 2011년 3월 4일 정부 기관과 금융기관 그리고 플랫폼 기업 등 총 40개의 인터넷 사이트를 대상으로 디도스 공격을 감행하였고, 동년 4월 12일에는 농협의 금융전산시스템에 대한 사이버 공격으로

18) Adam Sagal and Gordon M. Goldstein, "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet," *CFR Independent Task Force Report*, No. 80, 2022.
19) Julia Voo and Irfan Hemani and Daniel Cassidy, *National Cyber Power Index 2022*, September 2022, p.13.
20) 위의 자료, pp.10~12.
21) 이승열, 「북한 사이버테러 위협의 증가와 대응방안」, 『이슈와논점』, 제1127호, 2016, p.2.

273대가 전산 장애를 일으켰다. 그리고 2013년 3월 20일에 북한은 KBS, MBC, YTN과 신한은행, 농협, 제주은행 등에 대해 사이버 공격을 감행하였고, 6월 25일에는 정부 기관, 언론사 등 69개 기관에 대하여 사이버 공격을 감행하여 총 155대 서버를 파괴하였다.[22]

북한은 한국수력원자력(한수원) 직원의 컴퓨터에 자료 파괴형 악성코드를 유포하여 2014년 12월 9일부터 12일까지 한수원의 내부 자료를 유출했다. 2014년 12월 24일 미국의 소니픽처스 엔터테인먼트사는 북한의 사이버 공격으로 내부 전산망이 다운되었다. 북한은 2015년 10월 서울 지하철 1~4호선 서버를 해킹하였고, 2015년 10월 20일에는 청와대, 국회, 외교부, 국방부, 통일부 등 정부 기관에 대한 해킹을 또다시 시도하였다. 그리고 2016년 1월 6일 4차 핵실험 직후 북한은 청와대와 국회 등 정부 기관으로 사칭한 악성코드가 내장된 이메일을 대량으로 유포하였다.

이처럼 2009년부터 북한의 사이버 공격의 전략적 목표는 국가 기간망의 무력화와 국가 주요 정보 및 국방 관련 기술을 탈취하려는 목적으로 이뤄졌다. 그러나 2016년 4차 핵실험 이후부터는 북한의 사이버 공격의 전략적 목표가 국제사회의 대북제재로 인해 야기된 외화 부족 상황을 만회하고 동시에 핵과 미사일 시험 발사를 위한 자금 확보의 수단으로 전환된 것으로 나타났다.[23] 이를 위해 북한은 해외 금융기관에 대한 공격과 랜섬웨어 공격 그리고 가상화폐 거래소에 대한 해킹에 관련 인력과 장비를 집중하고 있다.

미국을 비롯한 국제사회가 북한의 사이버 위협을 심각한 국가안보 위기로 인식하게 된 중요한 계기는 2017년 5월 북한이 전 세계 150여 개국 국가에 대해 약 30만대 이상의 컴퓨터에 대한 '랜섬웨어' 공격이었다. 또한 북한이 가상화폐 해킹의 주범으로 주목받기 시작한 시기는 2017년 2월 국내 가상화폐 거래소인 '빗썸'에 대한 700만달러 해킹의 배후로 북한이 지목되면서부터다. 빗썸은 북한의 사이버 공격으로 네 번에 걸쳐 6,500만달러(약 792억원)를 피해를 봤다고 한다.[24] 북한은 빗썸 이외에도 2019년 11월에는 '업비트'를 공격해 이더리움 560억의 손실을 끼친 것으로 전해지고 있다.[25]

북한은 국내뿐만 아니라 2020년 9월 슬로바키아의 가상화폐 거래소에 침입하여 약 540만달러의 가상화폐를 해킹하였으며, 202년 3월에는 블록체인 기반 게임업체인 '액시 인피니티(Axie Infinity)'를 상대로 감행한 해킹으로 역대 최대 규모인 약 6억1,500만달러라는 손실을 기록한 것으로 확인되었다.[26]

---

22) 위의 자료, pp.2~3.
23) 송태은, 「북한의 사이버 공격과 우리의 대응」, 『IFANSFOCUS』, IF2022-28K, 2022. 10, p.2.
24) 『중앙일보』, 2019. 8. 13.
25) 『BBC NEWS KOREA』, 2021. 7. 5.
26) 김보미, 「북한의 암호화폐 공격과 미국의 대응」, 『INSS 전략보고』, 191호, 2022, p.5.

2022년 3월 1일 공개된 UN 안보리 산하 '대북제재위원회'의 전문가패널보고서(S/2022/132)에 따르면, 북한이 미사일 개발에 필요한 자금을 조달하기 위해 지난 2020년부터 2021년 중반까지 북아메리카, 유럽, 아시아 등 최소 3곳 이상의 가상화폐 거래소에서 약 5,000만달러 가치의 가상화폐를 훔쳤다고 밝혔다.[27]

또한 전문가패널보고서는 미국의 블록체인 분석기업인 '체이널리시스'(Chainalysis)의 평가를 인용하면서 북한이 2021년 한 해 동안 가상화폐 거래소뿐만 아니라 투자회사 등에 대한 총 7번의 사이버 공격으로 약 4억달러 가치의 가상화폐를 훔쳤다고 밝혔다.[28] 이와 함께 미국 연방수사국(FBI)도 2022년 3월 발생한 게임업체 '액시 인피니티'(Axie Infinity)의 가상화폐 해킹 배후에 북한의 '라자루스'가 탈취 사건에 책임이 있음을 확인했다고 밝혔다.[29] 2009년 이후 현재까지 북한의 사이버 공격 사례의 변화는 〈표 1〉과 같다.

〈표 1〉 북한의 사이버 공격 사례

날짜	내용	날짜	내용
2009. 7.	디도스(DDoS) 공격 (청와대 등 정부 기관)	2017. 5.	워너크라이 랜섬웨어 공격 (150여 개국에 피해)
2011. 3.	디도스(DDoS) 공격 (방송사, 금융기관, 인터넷기업)	2017. 7.	빗썸 가상화폐거래소 공격 700만달러 상당의 가상화폐 탈취
2011. 4.	농협전산망 해킹	2017. 12.	한국유빗해킹, 1차(4월)55억원, 2차(12월)170억원 가상화폐 탈취
2014. 12.	한수원 원전 해킹	2018. 1.	일본 가상화폐 코인체크 공격 550억엔 가상화폐 탈취
		2018. 6.	빗썸 가상화폐거래소 공격 가상화폐 3,100만달러 탈취
2014. 12.	소니픽쳐스사 해킹	2019. 11.	업비트 가상화폐거래소 공격 가상화폐 560억원 탈취
2015. 10.	서울지하철 1~4호선 서버 해킹	2020. 9.	슬로바키아의 가상화폐거래소 공격
2015. 10.	청와대, 국회, 통일부 대상 해킹	2020. 12.	신풍제약 등, 코로나 신기술 탈취 공격
2016. 1.	청와대 사칭 악성코드 유포	2021. 3~7.	한국항공우주산업, 한국원자력연구원 공격
2016. 8.	국방부 합참 전시작전계획 해킹 대우조선 이지스함 체계 해킹	2021. 4.	켄자스주와 플로리다주의 병원 등에 대한 랜섬웨어 공격, 50만달러 탈취
2016. 2.	방글라데시 중앙은행의 뉴욕연방준비 계좌에서 8,100만 달러 탈취	2022. 3.	게임업체 액시 인피니티에 대한 6억달러 가상화폐 탈취

자료: 이승열, 「북한 사이버 공격의 현황과 쟁점」, 『이슈와 논점』, 제2034호, 2022.

27) United Nations Security Council, S/2022/132, March 1, 2022.
28) 위의 자료.
29) 『BBC NEWS KOREA』, 2022. 7. 5.

2. 북한의 사이버 공격 전략 변화의 원인

한미 양국은 북한이 2022년 한 해 동안 탈취한 가상화폐를 금액이 약 1조 7천억원 이상이라고 밝혔다.[30] 무엇보다 북한이 국제사회의 대북제재와 코로나19로 인한 국경 봉쇄의 장기화로 경제적으로 매우 어려워진 상황에서 2022년 40여 회 이상의 미사일 도발을 할 수 있었던 이유가 가상화폐 탈취를 통한 외화 벌이에 성공했기 때문이라는 분석이다.

알레한드로 마요르카스(Alejandro Mayorkas) 미 국토안보부 장관은 2022년 10월 18일 싱가포르에서 열린 행사에서 "북한이 지난 2년 동안 10억달러가 넘는 암호화폐와 경화의 사이버 탈취를 통해 대량살상무기 프로그램을 지원했다"고 밝혔다.[31] 또한 앤 뉴버거(Anne Neuberger) 백악관 국가안보회의(NSC) 사이버・기술 담당 부보좌관은 7월 '신미국안보센터'(CNAS)에서 열린 대담회에서 "북한이 악의적 사이버 활동을 통해 미사일 개발에 필요한 자금의 최고 3분의 1까지 충당하는 것으로 추산된다"고 밝혔다.[32]

북한의 사이버 공격이 시스템 파괴 및 정보 탈취에서 가상화폐 등 금융자산에 대한 공격으로 전환된 가장 중요한 이유는 2016년 1월 4차 핵실험 이후 본격적으로 추진된 '핵무력 완성' 전략으로 인한 UN 안보리(UNSC)와 미국의 대북제재로 김정은과 핵심 엘리트 집단의 외화 부족 사태, 즉 통치자금 고갈이 가장 중요한 원인이었다.[33]

북한은 2016년 1월 6일 제4차 핵실험을 시작으로 2017년 11월 29일 화성-15형 대륙간탄도 미사일 발사 후 '국가핵무력완성'을 선언한 시점까지 모두 세 차례의 핵실험과 44차례의 각종 탄도 미사일 시험 발사를 감행하여 국제사회와 미국의 강력한 대북제재를 맞게 되었다. UN 안보리는 북한의 핵・탄도 미사일 개발 프로그램의 중단을 위해 총 10차례의 'UN 안보리 결의안'(UN Security Council Resolution: UNSCR)을 채택하였다.

UN 안보리는 2006년 10월 북한의 제1차 핵실험으로 채택된 결의안 1718호를 근거로 안보리 15개국으로 구성된 '대북제재위원회'를 구성하였다. 그 내용으로 보면 제1차 핵실험 이후 채택된 4번의 대북제재(1718호, 1874호, 2087호, 2094호)는 대량살상무기(WMD) 이전 통제에 초점을 맞춘 제재였지만, 2016년 4차 핵실험 이후 채택된 6번의 대북제재(2270호, 2321호, 2356호, 2371호, 2375호, 2397호)는 북한경제 일반에 대한 포괄적 제재로 북한의 수출입을 비롯한 경제분야의 전면적인 금수조치였다.

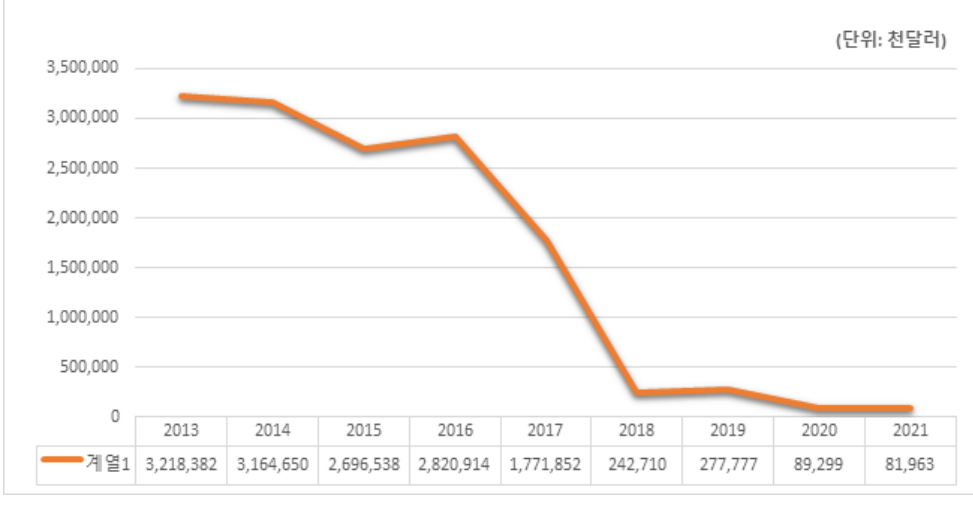
UN 안보리의 대북제재가 효과를 발휘한 것은 바로 미국의 독자 제재가 어느 때보다

30) 『조선일보』 2022. 11. 7.
31) 『VOA』, 2022. 10. 19.
32) 『RFA』, 2022. 7. 28.
33) 이승열, 「북한 사이버테러 위협의 증가와 대응방안」, 『이슈와논점』, 제1127호, 2016, p.3.

강력했기 때문이다. 미국은 2016년 북한의 4차 핵실험 이후 UN 안보리의 대북제재 외에도 2건의 행정명령(13722호, 13810호)과 2건의 제재법(「대북제재 강화법」, 「러시아・이란・북한 제재법」, 「오토웜비어북핵제재이행법」 등 별도의 제재를 부과하였다. 특히 트럼프(D. Trump) 대통령은 2016년 2월 발효된 「대북제재강화법」을 기반으로 2017년 9월 북한과 거래하는 외국 금융기관에 대한 제재(세컨더리 보이콧)을 내용으로 하는 「행정명령 13810」에 서명함으로써 대북제재의 실효성을 높였다.[34)]

그 결과 북한 김정은 통치자금의 주 수입원인 수출이 급락하였다. 대북제재가 본격화되기 전인 2016년 북한의 대외 수출은 28억 2천만달러였지만 2021년에는 8천 1백만달러로 2016년 대비 약 97%까지 추락하면서 사실상 수출로 인한 외화 벌이 사업이 파산했다고 볼 수 있다. 여기에 더해 2020년 초부터 시작된 코로나19로 인해 북한의 수출입의 물량의 90% 이상을 차지하고 있는 북중 간 국경이 장기간 폐쇄됨에 따라서 수출뿐만 아니라 수입까지 타격을 받게 됨으로써 향후 상당 기간 북한의 대외교역이 회복될 가능성이 현저히 낮아졌다. 북한의 수출량 감소 현황은 [그림 1]과 같다.

[그림 1] 북한의 수출량 감소 현황



자료: 통계청.

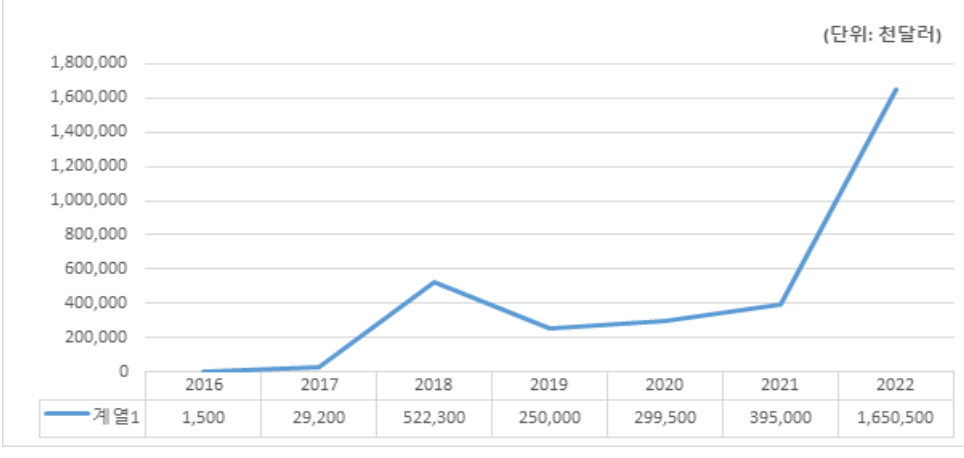
34) 이승열, 「김정은 집권 10년, '우리식경제관리방법'의 성과와 정치경제적 함의」, 『JNKS』, vol.7, no.2, 2021, p.79.

대북제재의 효과는 북한 최고 지도부에 외화 부족 사태를 일으켰으며, 이로 인해 북한은 부족한 외화 벌이 수단으로 전 세계 금융기관과 암호화폐 거래소에 대한 사이버 공격을 활용하기 시작했다. 특히 2016년 2월 방글라데시 중앙은행 뉴욕연준 계좌에서 총 9억 5,100만 달러 금액을 인출하려다 8,100만달러에 그친 이 사건은 북한이 국제결제시스템인 SWIFT를 해킹하여 디지털 자금을 탈취한 사례로써 북한 사이버 해킹의 위험성을 알리는 중요한 계기였다.

이때부터 북한은 암호화폐를 디지털 자금 탈취의 중요한 대상으로 삼았다. 미국 '체이널리시스'는 북한 연계 해커 조직들이 사이버 공격을 통해 2016년 150만달러에서 출발하여 2018년에는 5억 2,230만달러, 2022년에는 16억 5,050만달러(약 2조 300억원)의 가상화폐를 훔쳤다고 밝혔다. 이는 지난해 전 세계에서 도난당한 가상화폐 38억달러의 약 43%에 해당하는 금액이다.[35] 북한의 사이버 공격을 통한 외화 벌이 총액은 수출 감소 현황과 반대로 2021~22년 급격히 높아졌음을 알 수 있다. 2016년 이후 북한의 사이버 공격을 통한 외화 벌이 현황은 [그림 2]와 같다.

북한은 이렇게 획득한 외화 자금을 바탕으로 2022년에만 최소 33회에 걸쳐 73발의 탄도 미사일을 발사하였다. 2019년 하노이 회담 결렬 이후 25발, 2020년에는 8발, 2021년에는 6발에 그쳤던 탄도 미사일 시험 발사가 2022년에는 73발로 미사일 시험 발사에 든 비용만

[그림 2] 북한의 사이버 공격을 통한 외화 벌이 현황



자료: 체이널리시스.

35) 『동아일보』, 2023. 2. 4.

약 5억 6,000만달러(7,200억원)을 쏟아부은 것이다.[36] 수년째 대북제재로 외화난에 시달리는 북한의 입장에서 미사일 발사에 수반되는 비용은 부담일 수밖에 없지만, 북한이 작년부터 이렇게 많은 횟수의 미사일 시험 발사를 했다는 것은 그 비용을 충당할 수 있는 소득원이 작동하고 있다는 것이다. 대북제재로 대외무역이 막힌 현시점에서 북한의 유일한 소득원은 사이버 공격을 통한 금융자산 탈취 외에는 방법이 없기에 국제사회의 우려가 현실로 나타나고 있다고 볼 수 있다.

Ⅳ. 북한의 사이버 공격에 대한 국제사회의 대응

UN 안보리의 '대북제재위원회'가 북한의 핵과 미사일 위협에 대한 '플랫폼'(platform) 역할을 하는 것과는 달리 북한의 사이버 공격에 대해 국제사회의 '국제 공조 체제'는 아직 확고하게 구축되어 있지 않은 상태다. 다만 사이버 작업에 적용할 수 있는 국제법에 관한 『탈린매뉴얼 2.0』 등이 논의되고 있다.[37] 그러나 2017년 5월 150여 개국의 컴퓨터를 감염시킨 북한의 '워너크라이 랜섬웨어' 공격은 북한의 사이버 공격을 국제사회의 안보 이슈로 부각시킨 대표적인 사건으로서, 이후 관련국 간의 다자간 협력 체제가 마련되는 계기가 되었다.

미국 국가정보국장실은 2021년 4월 발간한 「연례위협평가 2021」(Annual Threat Assessment 2021)에서 북한의 사이버 능력을 미국의 인프라와 기업 네트워크에 대한 위협으로 평가하였다.[38] 2021년 6월 13일 G7 정상회의에서 각국 정상들은 공동선언문을 통해 랜섬웨어에 대한 공동 대처를 명시하였으며, 동년 11월 바이든 대통령은 '랜섬웨어 대응회의'를 개최하여 랜섬웨어가 세계적인 규모로 경제와 안보를 위협하고 있다는 데 인식을 같이하고 유럽, 중동, 아프리카, 아시아 등 35개국과의 국제적 협력 방안을 담은 공동성명을 발표하였다.[39] 유럽연합(EU)도 '2019년 법규'(Council Decision 2019/797 and Council Regulation No.2019/796)에 따라 '워너크라이' 랜섬웨어 공격을 주도한 '조선엑스포합영회사'을 제재 리스트에 올렸다.[40]

북한의 핵과 미사일 자금 마련을 차단하기 위해 미국은 북한의 가상화폐 해킹을 대북제재의

---

36) 『중앙일보』, 2023. 2. 21.
37) Michael N. Schmitt, 국가보안기술연구소 옮김, 『탈린매뉴얼 2.0』, 박영사, 2018, pp.1~7.
38) Office of the Director of National Intelligence, "2021 Annual Threat Assessment of the U.S. Intelligence Community," April 13, 2021.
39) 『VOA』, 2021. 12. 29.
40) 김보미・오일석, 「김정은 시대 북한의 사이버 위협과 주요국 대응」, p.24.

영역으로 확대하고 있다. 미국은 북한의 사이버 공격이 핵과 미사일 개발 및 실험 자금으로 활용되고 있다고 보고 있으며, 중국과 러시아의 협력이 필요한 UN 안보리를 통한 방식이 아닌 독자 제재를 통한 신속한 제재를 추진하고 있다. 2019년 9월 미국은 북한의 대표적인 3대 사이버 해킹 조직인 라자루스 그룹과 블루노로프, 안다리엘을 대북제재 리스트에 포함시켰다. 또한 2020년 12월 미 법무부는 미국을 비롯해 멕시코, 폴란드, 파키스탄, 베트남, 몰타 등의 주요 은행과 가상화폐 거래소에 대해 13억달러(약 1조4,000억원) 규모의 현금과 가상화폐 절취를 목적으로 사이버 공격을 시도한 혐의로 북한 정찰총국 소속 해커 전창혁・김일・박진혁 등을 기소하였다.[41]

미 재무부는 2022년 8월 북한이 사이버 해킹으로 탈취한 4억 5,500만달러의 가상화폐에 대한 세탁에 가담한 믹서(mixer)기업(가상화폐를 쪼개 누가 전송했는지 알 수 없도록 만드는 기술을 보유한 돈세탁 기업)인 '토네이도 캐시'(Tornade Cash)를 제재 대상에 올렸다.[42] 이외에도 미국은 북한의 암호화폐 공격에 대응하여 법무부와 국무부 내에 사이버 범죄 전담 부서를 신설하였고, 연방수사국(FBI)과 재무부는 북한 해킹그룹인 '라자루스'의 위협을 경고하는 부처 합동주의보를 발령하여 경각심을 높이고 있다.[43]

더 나아가 미국은 북한의 가상화폐 탈취 자금에 대한 환수도 적극적으로 추진하고 있다. 북한의 가상화폐 해킹 수법은 투자자들이 가상화폐를 임시 저장하는 '크로스체인 브리지'(crosschain bridge)를 주요 해킹 대상으로 삼아 해킹을 시도한 후, 탈취한 가상화폐를 믹서기업을 통해 돈세탁을 시도하고, 이후 세탁된 가상화폐를 중국 등 아시아의 비상장 거래소를 통해 현금화하는 방식이다. 이에 대해 미국은 북한 해커 그룹과 연계된 가상화폐 거래소 지갑을 추적해 '블랙리스트'를 만든 후에 주요 거래소에 이들 계좌에 대한 자금 거래 동결을 요청하고, 북한의 자금 세탁에 가담한 믹서 기업을 제재하여 가상화폐의 이동을 차단하고, 최종 단계에서는 북한 해커의 가상화폐 자금을 역(逆) 해킹하여 자금을 환수하고 있다.[44]

바이든 대통령은 2022년 3월 15일 새롭게 주요 인프라 기업이 사이버 공격을 받으면 신고해야 할 법적 의무를 부과하는 「2022년 미국 사이버보안 강화법」(Strengthening American Cybersecurity Act of 2022)에 서명하였다.[45] 주로 랜섬웨어 공격에 따라 주요 인프라 기업이 사이버 공격을 받았다고 인식한 시점부터 72시간 이내에 미 국토안보부의

41) 『중앙일보』, 2021. 2. 19.
42) 『조선일보』, 2022. 11. 7.
43) 『VOA』, 2022. 10. 19.
44) 『동아일보』, 2023. 2. 4.
45) 정민정, 「바이든 대통령 사이버보안 강화법 서명의 의미와 시사점」, 『이슈와논점』, 제1937호, 2022. 4. 13, p.1,

사이버 보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency: CISA)에 보고해야 한다는 내용이다.[46] 이를 통해 미국은 국내 주요 기관(국가 기관, 기업, 대학, 연구소 등)에 대해 적극적인 사이버 보안 의무를 부과함으로써 공격적인 사이버 대응이 가능한 법적 토대를 마련하였다.

그러나 북한의 사이버 공격에 대한 국제사회, 특히 UN 안보리(UNSC) 차원의 직접적인 제재는 아직 제대로 갖추지 못했다고 볼 수 있다. 다만, 대북제재위에서 북한의 사이버 공격이 핵과 미사일 개발자금으로 전용되는 상황에서 매년 북한의 사이버 위협 능력과 피해 사례를 조사하여 이에 대한 국제사회의 경각심을 일깨우는 수준이다. 따라서 북한 사이버 공격에 대한 국제사회의 대응이 보다 효과를 발휘하기 위해서는 UN 안보리 차원의 대북제재와 같은 강력한 조치가 이뤄질 필요가 있으며, 이에 북한 사이버 공격에 대한 국제사회의 협력이 어느 때보다 중요하다.

Ⅴ. 나가며

북한의 사이버 공격이 국제 금융 질서를 위협하는 수준으로 발전하자 미국의 국가 사이버 전략은 또한 점차 강경해지고 있다. 무엇보다 미국은 북한의 사이버 공격이 대북제재의 우회 수단으로 활용되는 상황을 우려하고 있다. 전술했듯이 블록체인 기업 체이널리시스는 북한의 2022년 가상화폐 해킹 규모가 16억 5,000만달러로 동년 전 세계에서 일어난 가상화폐 해킹 규모인 38억달러의 절반에 이른다고 분석했다. 국제사회의 대북제재로 인해 북한의 주요 외화 소득원인 수출이 97% 이상 줄어든 상황에서 가상화폐 해킹을 통한 외화 벌이는 대북제재를 통해 북한의 핵 야망을 무력화시키려는 미국의 계획을 위협하고 있다고 볼 수 있다.

한국정부도 북한의 사이버 공격을 심각한 안보위협으로 인식하고, 북한의 핵고도화 능력이 진전되는 배경에는 사이버 공격을 통한 외화 벌이가 매우 중요한 역할을 하고 있다고 인식하고 있다. 한국은 사이버 보안 능력과 관련하여 법, 기술, 조직, 역량개발, 협력의 5개 영역을 평가하는 국제전기통신연합(International Telecommunication Union: ITU)의 '글로벌사이버보안지수'(Global Cybersecurity Index: GCI)에서 4위를 기록할 만큼 높은 수준의 사이버 보안체계를 갖추고 있다. 하지만 문제는 사이버 위기 대응 체계가 국방, 공공, 민간 등 각

46) 위의 자료, p.3.

영역으로 나뉘어 분절적인 체계를 갖추고 있다는 점이다.[47]

국가 주요 정보통신기반시설인 한전, 농협, KT 등의 경우는 「정보통신기반보호법」이 우선으로 적용되도록 입법화되어 있으며, 이외 사이버 공격 대상이 되는 공공분야의 경우는 대통령 훈령인 「국가사이버안전관리규정」이 적용되며, 대기업 등 민간분야의 경우 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 적용하고 있다.[48] 이와 같은 입법체계의 분절성과 상이성으로 인해 북한의 사이버 공격에 실질적이고 효율적인 대응이 어려운 한계가 있다.

북한의 사이버 공격이 공공과 민간의 영역을 가리지 않는 상황에서, 북한의 사이버 공격으로부터 국가 기반 시설을 보호하기 위해서는 보다 포괄적인 법적 기반과 함께 국가 사이버 안보 정책을 총괄하는 컨트롤 타워를 조속히 마련해야 할 필요성이 제기되고 있다. 이를 위해 크게 세 가지 방안이 제기되고 있다. 첫째, 국가사이버안전에 대한 총괄 입법체계가 필요하다. 현재 대통령 훈령인 「국가사이버안전관리규정」만으로는 고도화되는 북한의 사이버 공격에 대응하는 데는 한계가 있다. 따라서 정부는 이러한 한계를 고려하여 국가 사이버 안보에 대한 기본법 제정을 비롯해, 민・관・군의 사이버 안보체계를 통괄할 수 있는 컨트롤 타워 구축에 적극적으로 나설 필요가 있다.

둘째, 사이버 안보 관련 국제 규범 제정에 더욱 적극적으로 참여할 필요가 있다. 한국은 UNGGE 회의에서 기본적으로 사이버 공간은 피해국에 일방적으로 불리한 구조이기 때문에, 피해국에 유리한 방향으로 국제법의 해석과 규범의 창출이 필요하다는 입장이다. 이러한 입장 이면에는 한국의 주 관심사가 북한의 사이버 공격을 막고, 북한 공격의 주된 경유국인 중국의 협조를 확보하는 데 있기 때문이다. 이를 위해서는 국제법의 적용에 있어서 피해국의 권리를 보장하기 위해 국제법의 상세화가 필요하다.[49] 따라서 한국의 접근은 국제법의 제정을 넘어 국제법의 세세한 규정까지 피해국의 입장을 보호할 수 있는 방향으로 전개될 수 있도록 노력할 필요가 있다. 이에 최근 외교부가 「사이버범죄협약」 가입을 위한 첫 단계로 유럽평의회에 가입의향서를 제출한 것으로 매우 중요한 진전이라고 볼 수 있다.

마지막으로 북한에 의한 사이버 공격을 피할 수 없다면 복원력 중심의 연구개발과 국내 사이버 위협 정보에 대한 공유 등 피해 최소화 방안을 모색할 필요가 있다.[50] 사이버 공간의 특성상 사이버 공격의 발원지를 찾아 특정 국가나 단체에 귀속시키기에 어려움이 따르기 때문에 사이버 공격의 주체와 상관없이 피해를 최소화하기 위해 회복력 중심의 연구개발이

---

47) 송태은, 「북한의 사이버 공격과 우리의 대응」, pp.2~3.
48) 김윤영・양철호, 「북한의 사이버테러에 대비한 법・제도 개선 방안」, 『유럽헌법연구』, 제33호, 2020, p.375.
49) 김상배, 「사이버 안보의 국제규범과 한국외교: 주요국 이해갈등의 프레임 경쟁 사이에서」, 『사이버 안보의 국가전략 2.0』, 서울대학교 국제문제연구소・국회입법조사처 주최 사이버안보 세미나 발표집, 2018, p.18.
50) 정민경・임종인・권헌영, 「북한의 사이버공격과 대응방안에 대한 연구」, 『한국IT서비스 학회지』, 제15권 제1호, 2016, p.75.

수행되어야 한다. 또한 국내에서 국가기관과 민간기관의 사이버 공격에 대한 위협 정보공유를 의무화하여 사이버 위협을 조기에 탐지하는 방안을 마련할 필요가 있다.

참고문헌

「7400억원 규모 암호화폐 게임 해킹 배후에 북한 해커」, 『BBC NEWS KOREA』, 2022. 7. 5.

「북한, 해킹으로 가상화폐 3500억원 훔쳐」, 『BBC NEWS KOREA』, 2021. 7. 5.

김보미, 「북한의 암호화폐 공격과 미국의 대응」, 『INSS 전략보고』, 제191호, 2022.

김보미・오일석, 「김정은 시대 북한의 사이버 위협과 주요국 대응」, 『INSS전략보고』, 제147호, 2021.

김상배, 「사이버 안보의 국제규범과 한국외교: 주요국 이해갈등의 프레임 경쟁 사이에서」, 『사이버 안보의 국가전략 2.0』, 서울대학교 국제문제연구소・국회입법조사처 주최 사이버안보 세미나 발표집, 2018. 9. 20.

김윤영・양철호, 「북한의 사이버테러에 대비한 법・제도 개선 방안」, 『유럽헌법연구』, 제33호, 2020.

김진광, 「북한의 사이버조직 관련 정보 연구: 조직 현황 및 주요 공격사례 중심으로」, 『한국컴퓨터학정보학회』, 제28권 제2호, 2020.

김흥광, 「북한의 정보전 전략과 사이버 전력: 돈 없는 북한의 최후의 선택 사이버 전쟁」, 『월간조선』, 2011. 6.

송태은, 「북한의 사이버 공격과 우리의 대응」, 『IFANSFOCUS』, IF2022-28K, 2022. 10.

신충근・이상진, 「북한의 대남 사이버테러 전략 분석 및 대응 방안에 관한 고찰」, 『경찰학연구』, 제13권 제4호, 2013.

이승열, 「북한 사이버테러 위협의 증가와 대응방안」, 『이슈와논점』, 제1127호, 2016.

_____, 「김정은 집권 10년, '우리식경제관리방법'의 성과와 정치경제적 함의」, 『JNKS』, vol.7 no.2, 2021.

_____, 「북한 사이버 공격의 현황과 쟁점」, 『이슈와논점』, 제2034호, 2022.

_____, 「북한 사이버 공격 전략의 진화: 대북제재 회피를 위한 외화벌이 수단으로서 사이버 전략」, 『통일정책연구』, 제32권 1호, 2023.

정민경・임종인・권헌영, 「북한의 사이버공격과 대응방안에 관한 연구」, 『한국IT서비스학회지』, 제15권 제1호, 2016.

정민정, 「바이든 대통령 사이버보안 강화법 서명의 의미와 시사점」, 『이슈와논점』, 제1937호, 2022.

『RFA』, 2022. 7. 28.
『VOA』, 2021. 10. 6.
『VOA』, 2021. 10. 19.
『VOA』, 2021. 12. 29.
『VOA』, 2022. 10. 19.
『VOA』, 2022. 10. 19.
『VOA』, 2022. 7. 26.
『동아일보』, 2023. 2. 4.
『조선일보』 2022. 11. 7.
『조선일보』, 2022. 11. 7.
『중앙일보』, 2021. 2. 19.
『중앙일보』, 2023. 2. 10.
『한계레』, 2025. 7. 4.

Michael N. Schmitt, 국가보안기술연구소 옮김, 『탈린매뉴얼 2.0』, 박영사, 2018, pp.1~7.

Office of the Director of National Intelligence, "2021 Annual Threat Assessment of the U.S. Intelligence Community," April 13, 2021.

Sagal, Adam and Gordon M. Goldstein, "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet," CFR Independent Task Force Report, No. 80, 2022.

Schmitt, Micheal N, 국가보안기술연구소 옮김, 『탈린매뉴얼 2.0』, 박영사, 2018.

Voo, Julia, Irfan Hemani, and Daniel Cassidy, National Cyber Power Index 2022, September 2022.

북한 사이버 공격 변화에 따른 향후 전망과 대응[1)]

김성진 | 한국수출입은행 차장 | sungjin.kim@koreaexim.go.kr

Ⅰ. 머리말

비대칭 전력은 상대적으로 군사력이나 자원이 열악한 국가나 특정 세력이 자신들보다 우세한 상대를 대상으로 사용하는 비정규적이고 비균형적인 공격 수단으로 대량 살상 및 기습 공격, 게릴라전이 가능한 무기체계를 의미한다. 비대칭 전력 활용한 공격은 예상하지 못한 의외성을 바탕으로 공격을 시도하기 때문에 공격받는 입장에서는 신속하게 대처하기 어려운 상황에 직면한다.[2)] 대표적인 비대칭 전력으로는 핵・미사일(ICBM, SLBM 등), 생화학 무기 등을 언급할 수 있으며, 최근에는 IT 기술이 발전하면서 새로운 비대칭 전력으로 사이버 공격(해킹, SNS 등을 통한 심리전 등), 드론 및 무인기를 활용한 공격이 주목받고 있다. 특히, 사이버 공격은 일상생활에 필요한 서비스들이 인터넷을 기반으로 작동하고 있는 현대 사회에서 가장 큰 피해를 유발할 수 있는 비대칭 전력이다. 또한 사이버 공격은 핵무기, 생화학 무기와 비교했을 때 상대적으로 적은 비용으로 운용이 가능할 뿐 아니라 실제 공격 주체의 신원이 명확하게 드러나지 않는다는 점에서 공격 시도에 대한 보복 공격이 발생할 가능성이 낮은 장점으로 가장 많이 사용되고 있는 비대칭 전력이다.

북한은 사이버 공격을 위해 국가 차원에서 해킹 그룹을 육성하고 관리하고 있다. 북한의 해커들이 본격적으로 사이버 공격을 전개하던 초기(2000년대)에는 주로 남한, 미국 등을 대상으로 사회적 혼란 유발과 정보 탈취를 목적으로 공격을 시도했다. 그러나 대북제재가

1) 본고는 다음 논문을 요약하였다. 김성진, 「북한의 가상자산 탈취 및 자금세탁 방법 변화 양상에 대한 연구"를 요약 및 보완」, 『평화학연구』, 제26권 제2호, 2025, pp.31~52.
2) Montgomery Meigs, ed. US Army War College Editorial Board, "Unorthodox Thoughts about Asymmetric Warfare," *Parameters: Journal of the US Army War College*, Carlisle, PA: US Army War College, 2003, p.4.

강화되면서 대외무역, 해외 노동자 파견 등 주요 외화 벌이 사업에 제약이 생기면서 사이버 공격의 성격도 변화하고 있다. 최근 북한은 국가 차원에서 해킹 그룹을 구성하고, 수익을 목적으로 하는 다양한 사이버 공격을 전 세계 불특정 다수를 향해 시도하고 있다. 특히, 전통적인 금융시스템과 비교할 때 상대적으로 보안이 취약하고, 자금세탁이 용이한 가상자산을 목적으로 하는 사이버 공격이 증가하고 있는 모습을 보이고 있다.

다만, 미국을 중심으로 가상자산 및 관련 산업들이 제도권으로 편입되고, 이를 관리할 수 있는 다양한 법・제도가 구축되고 있다는 점에서 북한의 사이버 공격 방식의 변화가 예상된다. 따라서, 본고에서는 북한의 사이버 공격 진행 현황과 공격 방식의 주요 특징을 살펴보고 이를 바탕으로 향후 북한의 사이버 공격이 변화할 방향을 예측하고 이에 대한 대응 방안을 모색해 보고자 한다.

Ⅱ. 북한 사이버 공격 변화 과정

북한의 사이버 공격 준비는 1986년 김일성의 지시로 미림대학을 설립하고 100여 명의 컴퓨터 전문 요원을 양성하면서 시작했다. 이후, 1991년 발생한 걸프전에서 미국이 다양한 전자 장비를 활용한 사이버 공격을 통해 이라크군의 방공망을 무력화시키는 모습이 전 세계에 중계되면서 본격적으로 사이버 공격을 위한 준비를 시작한다. 걸프전 이후 김정일은 인민군 총참모부 산하에 '지휘자동화국'을 창설하고, 심리전을 포함한 다양한 사이버 공격을 수행할 수 있는 인력과 관련 프로그램을 개발하는 전문 인력 양성에 집중하기 시작했다.[3)]

북한의 해커들은 2000년대에 들어서면서 본격적으로 사이버 공격을 활용한 광범위한 대남 도발을 실시한다. 당시 북한 사이버 공격의 주목적은 인터넷 기반에서 제공되는 서비스를 불능 상태로 만들어 남한 사회 전반에 혼란을 유도하고, 이를 바탕으로 광범위한 대남 심리전을 실시하는 것이었다.[4)] 북한은 남한 사회에서 사용 빈도가 높은 정부의 홈페이지 및 민간 포털 사이트 등을 주요 공격 대상으로 정하고, 디도스(Distributed Denial of Service Attack: DDoS)[5)] 공격을 통해 서비스 이용에 장애를 발생시킴으로써 사회적 혼란을 유도했다.

2009년 북한이 남한과 미국을 대상으로 실시한 대규모 디도스 공격인 '7.7 디도스 대란'은

3) 고명현, 「북한의 사이버 전력(戰力)과 금융범죄」, 『KDI 북한경제리뷰』, 10월호, 2021, p.56.
4) 상대적으로 인터넷 보급률이 저조하던 과거에는 주요 정부 기관의 웹사이트가 공격 대상이었으나 IT기술의 발달로 일상의 많은 영역이 온라인상에서 진행됨에 따라 금융기관 및 민간 포털 사이트 등 광범위한 사이버 공격이 진행되었다.
5) 분산 서비스 거부 공격(Distributed Denial of Service Attack: DDoS)은 공격자가 최대한 많은 PC를 악성코드에 감염시킨 뒤 특정 서버, 사이트 등에 동시접속을 함으로써 과도한 트래픽을 발생시켜 정상적인 서비스 제공이 불가능하도록 하는 공격방법이다.

국내 주요 22개 사이트와 미국의 14개 사이트를 마비 시켰다. 당시 공격을 받은 국내 사이트들은 최대 72시간까지 접속 장애를 겪었으며, 공격에 사용된 악성코드는 감염된 PC의 하드디스크를 자동으로 파괴하도록 설정된 프로그램이 포함되어 있어서 많은 피해를 발생시켰다. 2009년 대규모 디도스 공격을 시작으로 북한은 지속적으로 사이버 공격 방법을 고도화 시키면서 국내 주요 기관들을 대상으로 사이버 공격을 통한 교란 및 정보 탈취를 시도했다.

2016년을 전후하여 북한의 사이버 공격은 기존과 다른 양상으로 전개된다. 이러한 변화는 주요 물품에 대한 수・출입 제한 및 SWIFT 시스템에서 퇴출 등 대북제재가 강화되면서 기존 외화 벌이 사업에 많은 제약이 발생한 것이 원인으로 추정된다. 이 시기 북한의 사이버 공격의 성격은 불특정 다수를 대상으로 수익 추구를 강화하는 모습으로 변하기 시작한다.

북한의 사이버 공격이 수익성 추구로 변화한 초기에는 주로 금융기관들을 대상으로 외화 탈취를 시도했다. 북한이 2015~19년 동안 17개국을 대상으로 은행의 SWIFT 시스템과 ATM 단말기 네트워크 해킹 공격을 통해 약 20억달러를 탈취한 것으로 추정하고 있다.[6)]

다만, 최근 북한의 사이버 공격 대상을 살펴보면 전통적인 금융기관 보다는 가상자산 거래소 및 관련 기업, 가상자산 투자자 등에 집중되는 모습을 보여주고 있다. 대표적인 블록체인 데이터 분석 기업인 체이널리시스의 보고서에 따르면, 전 세계적으로 발생하는 가상자산 관련 범죄에 가장 적극적인 단체는 북한의 해킹 그룹으로 파악되고 있으며, 이들이 탈취한 가상자산은 핵・미사일 개발의 재원으로 사용되는 것으로 추정되고 있다.

〈표 1〉 북한 사이버 공격의 시기별 주요 목적 및 특징

단계별 구분	주요 목적	대표사례	특징
초기 (2000~10)	- 시스템 교란 - 정보 수집	- 7・7 디도스 대란(2009)	- DDoS 공격 방법을 활용한 단순 공격
고도화・다양화 (2010~15)	- 인프라 파괴 - 정보 수집	- 농협 전산망 마비(2011) - 3・4 디도스 대란(2011) - 한수원, 소니픽쳐스 해킹(2014)	- APT, 스피어피싱 등 공격 방법의 고도화
수익 중심, 글로벌 확장 (2016~20)	- 외화 확보 - 금융시스템 교란 - 첨단 기술 탈취	- 방글라데시 중앙은행 해킹(2016) - 워너크라이 랜섬웨어 공격(2017) - 업비트 해킹(2018)	- 암호화폐 주요 표적 - 랜섬웨어 공격을 통한 공격 대상 확대
다차원적 공격 (2021~25)		- 로닌 브리지 해킹(2022) - 바이비트 해킹(2025) - 위장취업을 통한 정보 및 금전 탈취	- 보안시스템 강화 및 국제사회의 규제에 대응한 사회 공격 수법의 고도화

자료: 김성진, 「북한의 가상자산 탈취 및 자금세탁 방법 변화 양상에 대한 연구」, 『평화학연구』, 제26권 제2호, 2025, p.36.

6) Panel of Experts on the DPRK, "Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee," UN Doc., S/2019/691, New York: United Nations, 2019, p.26.

Ⅲ. 최근 북한 사이버 공격의 주요 특징

1. 랜섬웨어 공격을 통한 갈취

사이버 공격을 통한 수익을 추구하는 방법은 협박에 의한 갈취와 해킹을 통한 직접적 탈취로 구분할 수 있다. 북한 해킹 그룹이 사이버 공격을 시작한 초기에는 랜섬웨어 공격을 통한 갈취의 방법을 활용했다. 랜섬웨어(Ransomware)는 몸값(Ransome)과 소프트웨어(Software)의 합성어로 공격 대상자의 컴퓨터 및 네트워크에 악성코드를 설치하여 공격받은 컴퓨터를 장악한 뒤 일종의 몸값을 요구하는 방식으로 공격이 진행된다. 랜섬웨어는 공격 방식에 따라 여러 유형으로 존재하고 있으며, 대표적인 공격 유형은 스크린 로커(Screen Locker), 암호화 랜섬웨어(Encrypting Ransomeware), 독스웨어(Doxware), 서비스형 랜섬웨어(Rass) 등이 있다.

대중적으로 알려진 랜섬웨어 공격 방식은 스크린 로커와 암호화 랜섬웨어 방식으로 공격 대상에 침투한 악성코드는 피해자의 컴퓨터(혹은 네트워크) 접속 자체를 제한하거나 보유하고 있는 데이터를 암호화 시킨뒤 이를 복구해 주는 대가로 금전을 요구하는 방식이다. 대표적인 사례로 2017년 북한의 해킹 그룹 라자루스가 주도한 '워너크라이(WannaCry)' 랜섬웨어 공격이 있다. 해당 공격은 라자루스가 수익을 목적으로 불특정 다수를 대상으로 시행된 대규모 사이버 공격이었으며, 약 150개국 23만대의 PC 및 서버가 직접적 피해를 본 것으로 알려졌다.[7] 라자루스는 피해자들에게 공격당한 시스템을 정상화시켜주는 조건으로 가상자산을 요구했으나 대부분의 피해자가 몸값을 지불하지 않고 데이터 복구를 포기하는 선택을 했다. 그 결과, 라자루스가 몸값으로 획득한 수익은 원화 기준 1억원에 미치지 못하는 것으로 확인되고 있다.[8] 당시 북한뿐 아니라 많은 해커 집단들이 불특정 다수를 대상으로 랜섬웨어 공격을 시도하고 몸값을 요구했으나, 몸값을 지불하는 경우에도 암호화된 파일을 복구해 주지 않았기 때문에 몸값을 지불하는 대신 암호화된 자료를 포기하는 경우가 일반적이었다. 그 결과, 북한의 해킹 그룹들은 암호화 랜섬웨어 공격 대상을 선정할 때 다수의 일반인보다는 몸값 지불 가능성이 높은 중요한 정보를 취급하는 기업 및 관공서를 대상으로 공격을 시도하는 경향을 보이고 있다. 대표적으로 2022년 미국의 의료기관들을 대상을 실시한 암호화 랜섬웨어

---

7) 『중앙일보』, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 4. 2(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

8) 『지디넷코리아』, 「랜섬웨어 워너크라이 피해 현황은」, 2017. 5. 16(https://zdnet.co.kr/view/?no=20170516162743, 접속일: 2025. 4. 25). 일반적으로 랜섬웨어 공격을 받은 피해자들이 해커의 요구대로 금전을 지불하는 경우에도 암호화된 파일을 복구해 주지 않는 경우가 빈번하기 때문에 대부분의 피해자들은 해커의 요구에 불응하는 경향이 높다.

공격 사례가 있다. 당시 북한의 해커들은 미국의 병원과 의료기관의 서버를 대상으로 랜섬웨어 공격을 시도했으며, 환자들의 진료기록을 암호화하고 이를 복구해 주는 조건으로 가상자산을 요구했다. 당시 병원 운영진들은 응급환자의 진료를 위해 해커에게 가상자산을 입금하고 자료를 복구할 수밖에 없었다.[9)]

랜섬웨어 공격이 세계적으로 증가하면서 랜섬웨어 공격을 대비하여 자료를 별도로 백업하여 이중으로 보관하는 기관들이 증가했으며, 개인의 경우 암호화된 파일을 포기하고 시스템을 포맷하는 방법을 선택하는 경우가 증가했다. 그 결과, 금전적 이익을 목표로 랜섬웨어 공격을 시도하는 해커들은 새로운 랜섬웨어 공격인 독스웨어 공격을 선호하게 된다. 독스웨어는 개인정보를 온라인에 공개하는 것을 뜻하는 신조어 '독싱(Doxing)'의 개념을 활용하는 진화된 랜섬웨어 공격 방식으로 컴퓨터에서 민감한 개인정보 등을 획득한 후 이를 유포하겠다는 협박을 통해 몸값을 갈취한다. 민감한 개인정보, 기업의 영업 비밀 등 외부로 유출될 경우 피해자들에게 지속적인 피해가 발생할 수 있으며, 자료 백업 및 시스템 포맷으로 대응할 수 없다는 특징을 가지고 있다.

마지막으로 최근 가장 문제가 되고 있는 서비스형 랜섬웨어는, 랜섬웨어 개발자들이 자신들이 개발한 랜섬웨어 코드 및 멀웨어(Malware)[10)]를 다른 해커들에게 판매하고 해당 공격을 통해 발생 수익을 공유하는 개념이다. 이는 악성코드를 개발할 능력이 없는 해커들도 손쉽게 랜섬웨어 공격을 시도할 수 있기 때문에 랜섬웨어 범죄가 증가하는 데 결정적 요인을 한 것으로 분석된다. 초기 자체적으로 제작한 악성코드를 중심으로 랜섬웨어 공격을 진행하던 북한의 해킹 그룹은 최근 Rass 서비스 활용 및 다른 랜섬웨어 조직들이 사용한 수법을 분석하여 새로운 유형의 랜섬웨어 악성코드 및 공격 방법을 개발하면서 가상자산 탈취 및 사이버 스파이 활동을 하고 있는 것으로 파악된다. 2022년 미국의 마이크로소프트의 분석에 따르면 북한의 해킹 그룹인 '문스톤 슬릿(Moonstone Sleet)'이 러시아 기반 랜섬웨어 조직이 제공하는 서비스형 랜섬웨어인 '킬린(Killeen)'을 사용한 정황을 포착한 바 있다.[11)]

랜섬웨어 공격은 금전적 피해를 유발할 뿐 아니라 사회 기반 시설이 공격받을 경우 대규모 혼란을 초래할 수 있어 많은 국가가 정부 차원에서 랜섬웨어 공격을 대비할 수 있는 계획을 수립하고 있다. 미국정부는 해당 사건 외에도 대표적인 랜섬웨어 범죄 집단인 '하이브'의 시스템 해킹에 성공하여 탈취한 자금을 몰수하는 등 랜섬웨어 공격에 전면적으로 대응하고

9) 『VOA』, 「북한, 미 의료기관 겨냥 변종 랜섬웨어 공격… 법무부 50만달러 회수」, 2022. 7. 20(https://www.voakorea.com/a/6665412.html, 접속일: 2025. 4. 29).
10) 컴퓨터의 정상적인 기능을 방해하거나 데이터 탈취, 시스템 파괴, 시스템에 무단 접근 등을 목적으로 설계된 소프트웨어이며, 대표적으로 트로이 목마, 스파이웨어, 랜섬웨어 등이 있다.
11) 『VOA』, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 3. 12(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

있다.[12]

2. 해킹을 통한 탈취: 지능형 지속 위협(APT)를 중심으로

북한이 랜섬웨어 공격과 함께 가장 많이 활용하는 사이버 공격 방법은 해킹을 통해 현금, 가상자산 등을 직접 탈취하는 방법이다. 초기에는 은행 전산망, ATM 시스템을 해킹하여 달러 인출을 시도하는 일반 해킹 방법을 사용했으나, 최근에는 탐지 및 대응이 어려운 APT(Advanced Persistent Threat) 공격 방식을 적극적으로 활용하고 있다. APT 공격은 오랜 기간 동안 공격 대상을 관찰하면서 정밀하게 수립된 맞춤형 전략으로 진행되는 사이버 공격 방법을 총칭하는 표현이다. 해커들은 APT 공격 과정에서 스피어 피싱[13]을 통한 악성코드 유포 및 다양한 사회공학적 기법[14] 을 사용하고 있다.

2016년 발생한 방글라데시 중앙은행 해킹 사건은 북한이 1년 이상 준비한 전형적인 스피어 피싱을 활용한 APT 공격에 해당한다. 북한의 대표적인 해킹 그룹 '라자루스'는 방글라데시 중앙은행 직원들을 대상으로 스피어 피싱에 성공한 이후 약 1년 동안 은행 업무 과정을 관찰하면서 SWIFT 시스템을 이용한 달러 이체 업무 절차를 파악하고 이를 바탕으로 범행 계획을 수립했다. 또한, 탈취한 달러를 이체하고 인출하는 과정에서 정부나 금융기관들이 절차를 강제 중단 시킬 수 없도록 범행 일자와 인출 과정까지 계획 단계부터 치밀하게 준비된 공격이었다. 라자루스는 방글라데시 공휴일 전날인 2월 4일(목요일) 탈취한 은행 직원 계정을 통해 SWIFT 시스템에 접속한 후 뉴욕 연방준비은행에 총 35건(약 10억 달러 규모)의 달러 이체 요청과 함께 방글라데시 중앙은행이 보유한 프린터기 시스템의 작동을 강제 중단 시켰다. 해당 프린터 시스템은 SWIFT 시스템을 통한 자금 이체가 완료되면 송금 내역을 자동으로 출력하도록 설정되어 있었으나, 사건 당일 해커들이 작동을 강제 중단 시킴으로써 직원들이 송금 요청 사실을 즉시 인지하지 못했다. 또한, 2월 6일(토요일) 근무를 개시하고 프린터가 복원될 시점에는 FED(미국 연방준비제도)가 위치한 미국 현지 시각이 금요일 저녁으로 FED의 담당자들이 퇴근하여 신속한 대응이 불가능하다는 점도 계획에 반영했다. 북한은 탈취한 자금을 필리핀 은행을 통해 필리핀에 위치한 카지노의 계좌로 분산 입금을 시도했다.[15] 다만, 라자루스의 방글라데시 은행 해킹 사건은 현금화 단계에서 예상치 못한 변수와 해커들의

---

12) 『지디넷코리아』, 「미 FBI, 랜섬웨어 갱단 '하이브' 해킹해 사이트 압수」, 2023. 1. 29(https://zdnet.co.kr/view/?no=20230129120014, 접속일: 2025. 2. 17).
13) 공격 대상자에 대한 사전 조사를 바탕으로 설계된 맞춤형 피싱 공격을 의미한다.
14) 사이버 공격을 시도할 때 물리적, 기술적 보안 취약점을 이용하는 것이 아니라 사람 간 상호 관계를 바탕으로 공격 대상자의 신뢰 형성을 바탕으로 상대를 속여 정상적인 보안 절차를 무력화시키는 방법으로 인간관계의 취약성을 이용하는 공격 방법이다.
15) 김홍선, 『보이지 않는 위험』, 한빛미디어, 2023, pp.37~42.

단순 실수로 6,500만달러 정도만 탈취된 것으로 파악된다.[16]

북한의 APT 공격은 가상자산 분야에 대한 공격에도 적극적으로 활용되고 있다. 대표적인 사례로 2023년 에스토니아 가상자산 기업 '코인스페이드'의 가상자산을 탈취 사건이 있다. 북한의 해커들은 유령회사를 설립하고 온라인 구직 서비스인 '링크드인'에 코인스페이드 직원들의 관심을 유발할 수 있는 맞춤형 채용 조건 및 고액 연봉을 제시하는 공고를 통해 범행 대상을 물색하고 있었다. 이후, 채용 과정에 지원한 코인스페이드 직원들에게 화상 면접을 제안하면서 해당 직원들의 컴퓨터에 악성코드를 설치해 내부망 접근 권한을 획득했다. 내부망 침투에 성공한 북한의 해커들은 약 3,730만달러 규모의 가상자산을 탈취하는 데 성공했다. 이와 함께, 2025년 발생한 가상자산 거래소 '바이비트' 해킹 사건 역시 북한의 해킹 그룹이 범인으로 지목되고 있다. 해당 사건의 정확한 해킹 방법을 확인하지는 못했으나, 거래소 직원을 대상으로 스피어 피싱에 성공한 후 바이비트 거래소의 콜드월렛의 가상자산 이체 과정을 모니터링하면서 멀티시그 월렛의 취약점을 공략한 것으로 추정하고 있다.

3. 기타

현대 사회는 코로나19 팬데믹을 경험하면서 일상에서 많은 부분에 변화가 발생했다. 대표적으로 비대면 서비스가 증가했으며, IT 기업을 중심으로 채용 과정에서 온라인 화상 면접 증가 및 근로자들에게 출근할 필요 없이 원격 재택근무로 업무를 수행하는 것을 허용하고 있다.

북한의 해커들은 비대면 서비스가 일상화된 사회 변화를 활용해 제3국에 거주하면서 미국, 유럽에 위치한 IT 기업에 취업하거나, 직접 유령 회사를 설립하고 구직자들을 대상으로 화상 면접을 진행하는 과정에서 악성코드를 이용한 가상자산 탈취를 시도하고 있다. 2024년 미국 국무부의 발표에 따르면 북한의 해커들은 위장 취업을 통해 기업의 기밀 정보 및 약 8,800만달러에 달하는 자금을 탈취한 것으로 추정된다고 발표했다.[17]

같은 해 미국 법무부도 북한의 해커들이 IT기업에 위장 취업하여 기업의 기밀 정보를 탈취하거나 악성코드를 활용해 회사와 직원들이 보유하고 있는 가상자산을 탈취하는 행위를 적발했다고 발표했다. 법무부에 적발된 북한의 해커들은 미국에 거주하는 아이작 크누트가

16) 당시, 탈취한 자금을 이체하기 위해 개설한 필리핀 RCBC 은행 마닐라 지점의 주소 일부가 이란의 제재 대상 선박 이름과 일치하면서 일부만 이체가 완료됐으며, 이체에 성공한 자금 중 일부를 자금세탁을 위해 이체하던 중 수신자 영문명에 오타가 발생하여 수신인 불일치로 입금 절차가 중단됐다.

17) 『VOA』, 「FBI, 위장 취업 북한IT 노동자들 기업 데이터 훔친 뒤 금전 요구」, 2025. 1. 25(https://www.voakorea.com/a/7949475.html, 접속일: 2025. 2. 19).

제공하는 위장 신분증을 활용해 취업에 성공하면 기업들로부터 수령한 업무용 노트북을 동남아, 중국 등 제3국에 있는 자신의 거처에 설치했다. 이후, 해당 노트북에 원격제어 프로그램을 설치하여 미국에서 근무를 하는 것처럼 위장하는 방법을 사용했다.[18]

위장 취업과 함께 북한의 해커들은 직접 유령회사를 설립하여 구직자들을 대상으로 가상자산 탈취를 시도하고 있다. 북한의 해커들은 미국, 멕시코 등에 유령회사를 설립한 후 암호화폐 개발자들을 대상으로 가상자산 탈취를 시도했다. 구직자들에게 화상 면접을 제안하고, 면접을 구실로 악성코드가 포함된 화상회의 프로그램을 구직자들에게 배포한 뒤 구직자들의 컴퓨터에서 개인지갑 접속 권한 및 암호 문구를 탈취한 후 보유한 가상자산을 탈취하고 있다.

Ⅳ. 향후 전망 및 대응 방안

본고에서는 북한의 사이버 공격의 변화 과정과 함께 최근 북한 해킹 그룹들이 사용하는 공격 방법에 대해 살펴봤다. 북한 사이버 공격의 주요 특징을 살펴보면, 첫째, 포괄적 대북제재 시행을 기점으로 사이버 공격의 주목적은 수익성 추구로 변화하고 있다. 특히, 가상자산의 가치가 상승함에 따라 전통적인 금융기관들 보다 상대적으로 보안이 취약하고, 자금세탁이 수월한 가상자산에 집중하는 경향을 보이고 있다. 둘째, 사이버 공격의 주요 목적이 수익성 추구로 변화하면서 공격 대상이 불특정 다수로 변화하고 있다. 마지막으로, 북한의 사이버 공격 방식이 지속적으로 고도화되면서 각국 정부가 신속한 대응을 하기 어려워지고 있으며, 국가 간 협력을 통한 공동 대등이 필요한 상황으로 변하고 있다.

다만, 북한의 사이버 공격이 수익성 추구 경향이 높아지고 있지만, 동시에 수익 추구 목적과 무관한 정보 탈취를 위한 공격도 병행하고 있다. 올해 8월 미국의 비영리 단체 '디도시크릿츠(The DDosecrets)'는 해킹 관련 전문 매체인 '프랙(Phrack) 매거진'을 통해 'KIM'으로 통칭되는 해커의 서버를 해킹해 해당 해커가 보유한 자료를 검토하던 중 남한의 행안부, 외교부, 군, 검찰 등 주요 정부 부처 및 KT, LG 유플러스, 네이버, 카카오 등 국내 대기업들을 해킹한 자료를 확보한 사실을 공개했다. 'KIM'으로 통칭되는 해커의 서버에서 발견된 자료들을 분석한 결과 해커의 정체는 북한의 대표적인 해킹 그룹인 '김수키'가 유력한 것으로 추정하고 있다. 해당 발표 이후 정부는 자체 내부 점검을 통해 지난 3년간 해당 해커에게 정보를

18) 『TECHWORLD』, 「미국 기업에 위장 취업한 북한 IT 인력, 연간 3억 이상 수익 올려」, 2024. 8. 14(https://www.epnc.co.kr/news/articleView.html?idxno=305271, 접속일: 2025. 2. 19).

탈취 당한 사실은 인정했으나, 해커의 정체가 김수키라는 명확한 근거가 부족하기 때문에 확정 지을 수 없다는 입장을 보이고 있다.[19]

북한의 사이버 공격은 대북제재가 지속되는 환경에서 현재와 같이 외화 벌이를 목적으로 전 세계를 대상으로 지속될 뿐 아니라, 국제사회의 대응에 맞춰 새로운 방식으로 공격을 시도할 것으로 예상된다. 따라서, 북한 사이버 공격을 예방할 수 있도록 다차원적인 분석과 함께 현재 시점에서 공격에 취약한 지점에 대한 점검과 국제사회의 협력을 강화해야 한다. 특히, 북한이 집중적으로 공격하고 있는 가상자산 관련 산업(거래소, 가상자산 사업자, 개인 거래자 등)은 상시 감시체계 강화 및 정보보호 관련 교육 확대 등 내부 통제 시스템을 강화하고, 국제협력을 통한 글로벌 정보 공유 체계를 구축할 필요성이 있다. 가상자산 거래소의 경우 이상거래 패턴 감시 시스템 구축과 국제사회의 제재 대상 등 블랙리스트에 연관된 것으로 추정되는 가상자산 지갑에 대한 정보를 공유해야 한다. 이미 규모가 큰 가상자산 거래소는 자금세탁방지 준수를 위한 내부통제 시스템을 마련하고 있지만, 중소형 거래소 및 DEX, De-Fi 시스템 등 상대적으로 규모가 작은 기업들은 여전히 보안이 취약한 상태로 운영되고 있기 때문에 국제사회 차원에서 대비책 마련이 필요하다. 실시간 감시체계 및 국제협력의 중요성은 2025년 2월 발생한 바이비트 거래소 해킹 사건에서 확인할 수 있다. 바이비트 거래소의 경우 비정상 거래 발생 즉시 해킹 범죄를 인지하고 공유함으로써 도난당한 가상자산의 일정 부분에 대해서 현금화를 방지할 수 있었다. 당시, 바이비트의 신속한 정보 공유로 주요 가상자산 거래소들은 탈취된 이더리움이 입금된 지갑 주소에 '바이비트 해킹'이라는 태그를 달고 블랙리스트로 관리함으로써 해당 지갑을 동결할 수 있었다.

향후 북한 해킹 그룹의 가상자산 탈취 시도가 지속될 경우 다양한 블록체인 프로젝트에서 운영하고 있는 DAO[20] 생태계를 주의해야 할 것으로 보인다. 블록체인 프로젝트에서 많이 활용되는 DAO는 특정 가상자산의 메인넷에서 다양한 벤처 사업자들이 DApp을 등록하고 활동할 수 있는 플랫폼 성격을 가지고 있는 생태계이다. 이는 최근 IT 업계에서 주목하고 있는 차세대 인터넷 환경인 WEB3.0이 블록체인 기술을 통해 실현되고 있으며, WEB3.0을 가시화시키고 있는 결과물 중 하나가 DAO라는 점에서 활성화될 가능성이 높다. 대표적으로 솔라나(Solana), 비체인(Vechain)과 같은 주요 가상자산들은 자신들의 메인넷에 DAO 생태계를 구하여 DApp 사업자들의 참여를 유도하고 인센티브로 자신들의 가상자산을 부여하고 있다. 따라서, 북한의 해커들이 위장 회사를 창업하여 DAO 생태계에 참여한 뒤 사용자들에게

19) 『연합뉴스』, 「공무원 업무시스템 '온나라'·GPKI 인증 해킹 흔적」, 2025. 10. 17(https://www.yna.co.kr/view/AKR20251017062151530?input=1195m, 접속일: 2025. 10. 18).
20) Decentralized Autonomous Organization의 약자로, 탈중앙화 자율조직을 의미하며, 블록체인을 기반으로 한 공동 투자 조합의 성격이다.

높은 보상을 미끼로 고가의 NFT를 판매한 후 약속된 보상을 지급하지 않고 잠적하는 '러그풀(Rug pull)'[21]방식의 가상자산 탈취를 시도할 가능성이 높다.

또한 우리 정부의 경우 수익을 목적으로 하는 북한의 사이버 공격에 대한 대비와 함께 국가 주요 정보 탈취 및 주요 기반 시설 공격을 통한 사회 혼란 유발을 목적으로 하는 사이버 공격에 대한 철저한 사전 대비가 필요하다. 최근 북한은 남북 관계를 '적대적 두 국가' 관계로 규정하면서 통일을 부정하는 등 남한의 대화 요구에도 일절 호응하지 않으면서 한반도 긴장감을 지속적으로 높이고 있다. 특히, 북한은 자유민주주의 진영 국가들과 전체주의 진영 국가 간의 갈등이 심화되고 있는 국제 정세 속에서 중국, 러시아와 협력을 강화하고 있기 때문에 남북 간 대화가 단시간에 재개되기는 어려울 것으로 전망된다. 따라서, 현재와 같이 남북 관계 긴장이 지속될 경우 북한은 대내 체제 결속을 위해 남한 사회의 혼란을 유발하기 위한 대남 사이버 공격에 대한 대비도 필요할 것으로 보인다. 2022년 SK C&C 데이터센터[22] 및 2025년 국가정보자원관리원의 데이터센터 화재 사건은 북한의 사이버 공격과 무관한 사건이지만 남한 주민들의 일상의 많은 부분이 인터넷 환경에 기반하고 있으며, 주요 인터넷 인프라가 마비가 될 경우 사회적으로 큰 혼란과 경제적 손실이 발생할 수 있음을 보여준 사례다. 따라서, 남북 관계 갈등이 지속되고, 북한이 핵・미사일 발사가 아닌 사이버 공격을 통한 대남 도발을 감행할 경우 국민들에게 직접적인 피해가 발생하기 때문에 철저한 대비가 필요할 것으로 판단된다.

---

21) 러그풀은 가상자산과 De-Fi 분야에서 사용하는 용어로, 블록체인 프로젝트 개발자나 내부자가 가상자산의 사전 발행이나 NFT판매에 참여하는 사람들에게 막대한 보상을 지급할 것처럼 과대 광고를 한 후 획득한 가상자산을 가지고 잠적하는 사기행각을 의미한다.

22) 해당 화재로 인해 카카오톡 및 네비게이션, 모바일 결제 등 관련 주요 서비스가 약 10시간 동안 작동 불능 상태가 지속되면서 경제적 손실도 발생했다.

참고문헌

고명현, 「북한의 사이버 전력(戰力)과 금융범죄」, 『KDI 북한경제리뷰』, 10월호, 2021.

김성진, 「북한의 가상자산 탈취 및 자금세탁 방법 변화 양상에 대한 연구」,『평화학연구』, 제26권 제2호, 2025.

김홍선, 『보이지 않는 위험』, 한빛미디어, 2023.

『연합뉴스』, 「공무원 업무시스템 '온나라'·GPKI 인증 해킹 흔적」, 2025. 10. 17(https://www.yna.co.kr/view/AKR20251017062151530?input=1195m, 접속일: 2025. 10. 18).

『중앙일보』, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 4. 2(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

『지디넷코리아』, 「미 FBI, 랜섬웨어 갱단 '하이브' 해킹해 사이트 압수」, 2023. 1. 29(https://zdnet.co.kr/view/?no=20230129120014, 접속일: 2025. 2. 17).

_____, 「랜섬웨어 워너크라이 피해 현황은」, 2017. 5. 16(https://zdnet.co.kr/view/?no=20170516162743, 접속일: 2025. 4. 25).

『VOA』, 「FBI, 위장 취업 북한IT 노동자들 기업 데이터 훔친 뒤 금전 요구」, 2025. 1. 25(https://www.voakorea.com/a/7949475.html, 접속일: 2025. 2. 19).

_____, 「MS 북한 해커조직, 서비스형 램섬웨어 '킬린' 사용」, 2025. 3. 12(https://www.voakorea.com/a/8007269.html, 접속일: 2025. 4. 25).

_____, 「북한, 미 의료기관 겨냥 변종 랜섬웨어 공격... 법무부 50만 달러 회수」, 2022. 7. 20(https://www.voakorea.com/a/6665412.html, 접속일: 2025. 4. 29).

Montgomery Meigs, ed. US Army War College Editorial Board, "Unorthodox Thoughts about Asymmetric Warfare," *Parameters: Journal of the US Army War College,* 4-18. Carlisle, PA: US Army War College, 2003.

Panel of Experts on the DPRK, "Midterm Report of the Panel of Experts of the 1718 DPRK Sanctions Committee." UN Doc, S/2019/691, New York: United Nations, 2019.

『TECHWORLD』, 「미국 기업에 위장 취업한 북한 IT 인력, 연간 3억 이상 수익 올려」, 2024. 8. 14(https://www.epnc.co.kr/news/articleView.html?idxno=305271, 접속일: 2025. 2. 19).

최근 북한의 사이버 전력과 사이버 위협 추세: 실태와 함의

송태은 | 국립외교원 국제안보통일연구부 조교수 | tesong22@mofa.go.kr

Ⅰ. 들어가며

오늘날 북한은 공격의 기술과 규모 양 차원에서 전 세계를 상대로 고도의 사이버 위협을 구사하고 있다. 북한의 사이버 공격은 각국 정부 기관, 국가 인프라, IT 기업, 국방, 항공우주 산업, 공급망(supply chain), 가상자산(cryptocurrency)과 같은 디지털 금융시스템과 미디어를 포함하고 있고, 대상 국가도 한국, 미국, 일본, 중국, 러시아, 베트남, 중동, 남미, 아프리카에 이르기까지 전방위적이고 광범위하다.

북한은 디도스(Distributed Denial-of-Service: D-DoS) 공격, 멀웨어(malware) 공격, 가상자산 탈취(cryptocurrency heist), 공급망 공격, 사회공학 기법(social engineering)을 포함한 사이버 첩보 활동(cyber espionage) 등 다양한 사이버 공격 수단을 사용하고 있다. 특히 최근 한국의 통신사나 핵심 기반 시설 및 공급망에 북한의 공격이 증대하고 있는 것은, 북한이 한국에 위기 수준의 중대한 혼란을 유발하면서 한국정부의 대응 태세를 시험하며 취약점을 탐색하기 위한 목적을 갖는다.

북한은 1990년대부터 사이버 능력 증진을 위한 준비를 시작했고, 특히 김정은 위원장 시기 사이버 역량이 크게 증강되었으나 사이버 기술을 통해 국가의 경제 발전을 도모하기보다 정권의 생존을 위한 사이버 공격에 사용하고 있다. 최근 美 연방수사국(FBI), 국토안보부 산하 '사이버보안 및 인프라 보안국(Cybersecurity & Infrastructure Security Agency: CISA), 법무부, 재무부, CIA 등 미 행정부의 여러 부처가 북한의 사이버 위협에 대해 강경하게 대응하며 동맹과 국제사회와의 공조를 추구하는 것도 북한이 구사하는 위협의 규모가 개별국

차원에서 대응할 수 있는 수준이 아니기 때문이다.

북한은 전 세계의 다양한 IT 업체, 범죄조직, 브로커, 자선단체, 카지노 등과 공조하거나 은행의 허위계정, 온라인 게임 및 도박 프로그램, 해외에서의 노트북 공장 운영을 비롯하여 해킹으로 탈취한 외국인들의 개인정보를 이용하여 신분을 위장하는 등 다양한 사회공학 기법을 통해 매우 정교한 사이버 위협을 구사하고 있다. 특히 최근 북한 해커들은 생성형 인공지능을 사용하면서 해킹 대상을 물색하고 대상에 걸맞은 해킹 방식을 탐색하며 신분 위장에 활용하는 등 한층 고도화된 사이버 공격을 수행하고 있다.

이러한 맥락에서 이 글은 북한이 어떤 대상에 대해 사이버 위협을 가하는지, 왜 그러한 위협을 구사하는지, 그리고 북한의 사이버 전력 수준은 어떠한지 살펴보며, 또한 최근 북한의 사이버 공격 대상과 위협 구사 방식에는 어떤 변화가 있는지 논의한다. 마지막으로 이 글은 이러한 북한의 사이버 공격을 포함한 다양한 외부로부터의 사이버 위협에 대한 우리의 대응책을 논하는 것으로 결론을 대신한다.

Ⅱ. 북한의 사이버 위협 실태

1. 북한의 사이버 공격 목적

북한의 사이버 공격은 2000년 초부터 시작되어 주로 한국과 미국의 정부 기관, 국방시스템, 금융시스템을 집중적으로 공략했으나, 김정은 위원장 집권 즈음부터 향상된 사이버 능력을 통해 세계 각국의 IT 기업, 방산업체, 금융기관 및 미디어 등 다양한 대상을 공격해 왔다.[1] 사이버 공격이 자금 창출의 유용한 수단으로 각인되기 시작한 2015년 말부터 북한의 사이버 역량은 본격적으로 자금 창출에 동원되기 시작했고, 2016년 말부터 북한은 가상자산 탈취와 불법적 자금세탁 활동을 본격화했다. 2017년 유엔의 대북제재 이후 북한은 정찰총국 산하 사이버 전담 부서 '기술정찰국'의 해킹 역량을 증진시켰고, 그 결과 북한 해커조직은 국제적으로 '고도의 지속적 위협(Advanced Persistent Threat: APT)'으로 분류되기 시작했다.

북한이 핵·생화학 무기와 함께 사이버 무기를 북한의 3대 비대칭 전력으로 간주하는 것은 국제사회로부터 고립되어 있고 소수의 국가와 외교 관계를 유지하고 있어 정상적인 외교 수단을 통해 국가 목표를 추구하기 어려운 북한이 자국의 정치·군사 안보 및 경제적

1) UNSC, 2019, p.27.

목적을 달성하기 위한 효과적인 전력으로서 사이버 위협을 인식하고 있기 때문이다. 따라서 표면적으로는 사이버 범죄의 성격을 갖는 북한의 사이버 공격이 금전적 이익 달성에 그치지 않고 전략적 목표를 다각적으로 노리는 경우가 대부분이다. 즉, 북한의 사이버 위협은 일회적인 성격의 공격이 아닌, 정찰총국의 주도하에 다양한 정치, 군사, 경제적 목적을 달성하려는, 조직적으로 수행되는 공세적인 사이버 작전이다. 북한이 네트워크 공격이나 탈취 등의 사이버 작전을 통해 얻고자 하는 군사전략적 목적은 ▲한국을 포함한 적성국의 국가 기능 마비, ▲적과 잠재적 적에 대한 정보의 우위 선점, ▲유사시와 전시 적성국에 대한 공격 지점과 군사작전 방해 전술 탐색 등이다.

2. 북한의 사이버 공격 대상

지난 10년간(2009~23년) 북한은 최소 29개국을 공격했는데, 공격 지역의 순위는 아시아가 77%, 북아메리카가 10%, 유럽이 10%이고, 국가별로는 한국이 65.7%, 미국이 8.5%이고 일본, 중국, 러시아, 베트남, 중동, 남미, 아프리카 순으로 이어졌다. 그런데 최근 마이크로소프트(Microsoft)가 분석한 바에 따르면, 북한의 최대 사이버 공격 대상은 한국이 아닌 미국으로 바뀌었다. 2023년의 경우 미국에 대한 북한의 공격이 전체 북한의 사이버 공격에서 42%를 차지했고 한국에 대한 공격은 15%를 차지하여 미국과 한국 두 국가에 대한 북한 사이버 공격의 50%를 차지하고 있다. 2024년에 이르면 북한은 한국보다 일본을 더 빈번하게 공격했다. 이러한 변화는 금전적 목적과 정보 탈취 공격 대상을 확대하는 과정에서 북한이 이미 오랫동안 공격해 온 한국보다 더 많은 새로운 공격 포인트가 미국에 존재하기 때문인 것으로 보인다.[2] 하지만 이러한 변화는 한국에 대한 북한의 공격이 줄어든 것을 의미하지 않고 북한의 전체 사이버 공격 규모와 범위가 더 증대한 것을 말해준다.

아주 최근인 2025년 7월, 미 법무부는 신분을 위조한 북한 IT 노동자들이 미국 16개 주(states)에서 29개의 노트북 농장(Laptop Farm)을 운영하는 현장을 적발했고 200여 개의 노트북을 압수했으며, 관련된 29개 계좌를 동결했고 가짜 웹사이트를 폐쇄했다. 미국은 2023년부터 기업이 직원을 원격으로 고용할 경우 전자고용인증인 'E-Verify'를 사용하도록 했는데, 애리조나, 테네시, 매사추세츠, 워싱턴 등에 위치한 미국 기업이 가짜 미국인 신분을 도용한 북한 IT 노동자들에게 속거나 혹은 공조하여 북한 해커들의 취업을 알선한 결과 이러한 미국인들이 FBI에 체포되기도 했다.

---

2) 송태은, 2024, pp.5~6.

미 정부의 조사에 따르면, 2020년부터 적발된 미국 Tech 회사, 미디어, 금융기업, AI 방산 기업 등 100개가 넘는 기업이 북한 IT 노동자들의 정체를 모르고 채용한 것으로 나타났다. 중국, 북한, 세르비아, 아랍에미리트 등에 거주하는 북한 해커들은 미국 현지에서 로그인하여 업무를 시작하는 것처럼 장소를 속이는 수법을 사용했는데, 이렇게 북한 해커들에게 속아 넘어간 미 회사들은 회사 내 민감 정보와 주요 기술을 북한에 탈취당한 것으로 드러났다.

최근 북한 해커들이 사용한 더욱 심각한 고도의 사이버 공격은 공격 대상 컴퓨터나 네트워크에 대해 별도의 악성 소프트웨어를 설치하지 않고, 운영체제(OS)나 원래 설치되어 있는 유틸리티, 스크립팅 언어, 관리 도구 등을 이용하여 빠르게 해킹하는 '리빙 오프더 랜드(Living off the Land: LoTL)' 공격이다. 전통적인 악성코드 기반의 사이버 공격에 대한 탐지를 회피할 수 있는 이러한 LoTL 공격은 해킹 과정에서 흔적을 남기지 않으므로 해커들에게 매력적이고, 보통 공격 대상에 대한 장기적으로 침입하여 오랫동안 들키지 않으면서 민감 데이터를 탈취하며 사이버 첩보활동을 수행하거나 중요한 시스템에 대한 사보타주 공격을 취할 수 있다. LoTL 공격은 해커 입장에서는 해킹한 네트워크 내부에 오래 머무르며 권한 상승, 데이터 수집과 유출 등 악의적 활동을 할 수 있어서 유리하다.[3)]

한편 북한은 사용자에게 전달되는 소프트웨어를 변조하여 공급망에 침투하는 형태의 '공급망 공격'도 본격적으로 전개하고 있다. '공급망 공격'은 소프트웨어 제조업체나 서비스 공급업체 등 신뢰받는 업체에 침투하여 악성코드를 심어놓고 고객사나 정부 기관에 배포되는 소프트웨어를 변조하여 공급망을 공격하는 해킹 수법이다. 2023년 1월 국정원, 경찰청, 한국인터넷진흥원(KISA)는 북한 해커들이 국내외 공공기관, 방산・바이오 업체 60여 곳의 인터넷뱅킹의 로그인이나 전자서명에 사용되는 금융보안 소프트웨어(SW) '이니세이프 크로스웹 EX(INISAFE CrossWeb EX)'을 대상으로 해킹하거나 악성코드를 유포한 활동을 적발한 바 있다.[4)] 2025년 6월에도 북한 해커그룹은 자바스크립트 패키지 레지스트리에 악성 패키지를 업로드하는 방식으로 공급망 공격을 수행했는데, 이러한 공격은 개발자들이 신뢰하는 오픈소스 패키지 생태계를 노렸다는 점에서 공격의 범위가 상당히 넓다는 것을 보여주었다. 즉 개발자 한 사람의 실수도 전체 애플리케이션/서비스를 위험에 빠뜨릴수 있는 것이다.[5)]

마이크로소프트의 분석에 의하면, 방산분야에 있어서 북한은 다양한 국가를 골고루 공격하고 있고, 가장 많이 해킹하는 국가는 러시아가 1위(14%)로서 러시아와의 군사적 협력이 오히려 북한의 러시아 방산에 대한 공격 유인이 증대하는 상황이고, 미국과 이스라엘이

3) 송태은, 2025, pp.9~10.
4) 이종현, 2023.
5) Jones, 2025.

공동 2위(10%, 10%)이며, 한국 방산에 대한 공격은 6%로 북한의 7위 공격 대상이다.

2024년 10월 유엔안전보장이사회(UNSC)는 북한에 대한 제재의 근거를 마련하기 위해 미국, 한국, 일본을 포함한 11개국의 다국적 연합 다자 제재 모니터링 팀(MSMT)을 설립했다. 이 MSMT의 최근 보고서에 의하면 북한의 해커 조직들이 2024년부터 2025년 9월까지 28억 3천만달러의 가상화폐를 탈취한 것으로 드러났다. 또한 북한이 탈취한 가상화폐를 현금화하는 과정에서 중국, 러시아, 캄보디아 등 제 3국의 장외거래(OTC) 브로커들과 금융회사를 이용하고 있으며, 캄보디아의 후이원 그룹 산하 금융 서비스 제공업체인 후이원 페이가 세탁에 이용되고 있는 사실도 이 보고서에서 밝히고 있다.[6)]

3. 북한의 사이버 전력

북한의 사이버 전력은 러시아, 중국, 이란과 같은 다른 권위주의 국가들과 비슷한 특징을 갖는다. 대개의 선진 민주주의 국가는 국가의 사이버 전력이 방어(defense) 역량에 집중되어 있는 반면, 이들 권위주의 국가의 사이버 전력은 방어력보다 공격력(offensive capabilities)이 더 우월하다. 아직도 지속되고 있는 러시아-우크라이나 전쟁에서 우크라이나에 대해 파괴적인 사이버 공격을 구사하고 있는 러시아의 경우 전 세계에서 발생하는 사이버 공격의 최대 진앙지이고, 우크라이나가 2위를 차지한다.[7)] 이 사실은 양국이 전면전에서 전개하고 있는 사이버전의 강도가 일반적인 사이버 공격과 달리 공격의 규모와 기간에 있어서 대단히 광범위하고 지속적으로 이루어지고 있음을 말해준다. 북한의 경우 전 세계 사이버 공격 진원지 순위에서 7위를 차지하는데, 이러한 측정치는 북한의 사이버 위협 대부분이 사이버 첩보 활동과 가상화폐에 대한 해킹임을 감안하면 북한이 얼마나 정보활동과 경제적 이익 창출에 사이버 전력을 집중하고 있는지를 짐작게 한다.

한편 한 국가의 사이버 전력은 공격력만으로 측정되지 않고 해당 국가가 사이버 공간을 사용하는 다양한 측면을 종합적으로 파악하여 평가된다.하버드 케네디 대학(Harvard Kennedy School)의 벨퍼센터(Belfer Center for Science and International Affairs)는 개별 국가의 사이버 역량(capability)을 다양한 영역에서 측정하고 그러한 역량을 사용하고자 하는 의도(intent)를 측정하여 종합적 사이버 역량(Comprehensive Cyber Power)을 국가별로 평가하여 '사이버국력지수(National Cyber Power Index: NCPI)'를 결정한다. NCPI는 세부 평가 항목은 대상 국가의 ▲사이버 전략 ▲ 외부 공격에 대한 방어 및 공격 작전 역량 ▲

6) U.S. Department of State(2025).
7) Miranda Bruce, *et al.*, 2024.

사이버 자원 제공 역량 ▲민간의 사이버 역량이고 이러한 사이버 역량은 ▲금융 ▲감시기술 ▲정보·첩보 ▲상업 ▲방어력 ▲정보통제 ▲공격력 ▲규범의 영역에서 평가된다.[8]

벨퍼센터의 NCPI를 통해 파악된 북한의 종합적인 사이버 역량은 2022년 세계 14위를 차지하고 있으며, 이 지표에서도 북한의 사이버 전력은 압도적으로 사이버 공격 활동과 불법적인 금융 활동에 집중되어 있다. 북한은 금융분야에서 가상화폐 탈취 기술이 매우 높아 최고치 100점에서 100점으로 평가받고 있는 반면 디지털 금융 활동과 관련된 사이버 역량과 그러한 역량의 사용 의도는 상대적으로 매우 낮다. 북한의 사이버 방어력이 사이버 공격력에 비해 낮은 것은 북한이 사이버 전력을 방어에 사용할 의지와 능력이 없기 때문이다. 즉 북한은 사이버 공격력을 사용하여 금전적 이익을 얻고자 하는 유인이 훨씬 큰 데다가 전체 주민의 오직 1%만이 외부 인터넷망에 접속할 수 있기 때문에 그 1%를 보호하기 위해 국가 자원을 사용할 경제적 여유가 없다. 하지만 외부로부터 사이버 공격을 받을 경우 북한이 경험할 피해의 범위나 수준은 북한 내부 정보에 대한 접근성이 극도로 제한되어 있기 때문에 측정하기 어렵다.

북한은 사이버 공격 역량을 더 적극적으로 사용하고, 방어보다 공격에 초점을 둔 사이버 전력을 보유하고 있기 때문에 국제사회로부터 고립되어 있는 북한도 외부로부터 사이버 공격에 대해 대단히 취약하다. 북한은 2010년부터 중국 통신회사 차이나유니콤(China Unicom)의 인터넷 서비스를 사용하기 시작했고, 한동안 북한은 중국의 인터넷 서비스만을 사용해 온 것으로 알려져 있다. 그런데 2017년 북한이 러시아 통신회사 트랜스텔레콤(TransTeleCom: TTK)의 인터넷 서비스를 추가하며 중국의 인터넷 서비스 중 한 개를 대체한 것은 미국으로부터의 사이버 공격 때문으로 알려져 있다. 즉 북한이 복원력 차원에서 다수의 인터넷 서비스 제공 업체를 이용하는 것이 안전한 것으로 판단한 데 따른 결정으로 보인다.[9]

북한의 사이버 방어력이 얼마나 취약한지는 비교적 최근 사례에서도 목격되고 있다. 2022년 1월 14일 외부 사이버 공격으로 북한 전역의 인터넷 접속이 중단되어 15일 오전까지 조선중앙통신, 고려항공 등 북한의 웹 사이트, 이메일, DNS 서버가 간헐적 또는 전면적으로 접속되지 않았고, 1월 26~27일, 31일에도 북한에서 광범위한 인터넷 접속 중단 사태가 발생한 바 있다. DDoS 공격에 의한 현상으로 분석되고 있는 이러한 공격이 일어난 시점은 북한이 2022년 1월 5일부터 27일까지 두 차례의 '극초음속 미사일'시험 발사를 포함하여 총 6회에 걸친 미사일 도발 시점과 일치하고 있다.[10] 포브스(Forbes)는 북한에 대한 이러한 사이버

8) Voo, *et al.*, 2022.
9) DeYoung *et al.*, 2017; Williams 2017.

공격이 개인 해커가 자신의 행위라고 주장하고 있지만 미국 사이버사령부(U.S. Cyber Command)에 의한 것으로 추측하고 있고, 북한의 미사일 도발에 대한 미국의 경고 차원에서 이루어진 작전으로 추정했다.[11]

북한의 미사일 도발에 대해 앞으로도 이와 같은 패턴의 외부 사이버 공격이 빈번하게 수행될 것으로 예상해 볼 수 있는 것은 2022년 말에도 유사한 상황이 전개되었기 때문이다. 2022년 10월 31일부터 11월 5일까지 진행된 대규모의 한미공중훈련인 '비질런트 스톰(Vigilant Storm)' 기간 동안 이 훈련에 대한 반발의 차원에서 북한은 11월 2일 하루 동안 25발에서 30발이 넘는 미사일을 발사했고, 그중 1발은 사상 최초로 동해 북방한계선(NLL) 이남의 한국 영해 인근에 떨어져 경상북도 울릉군에 공습경보가 발령되었다.[12] 그런데 북한의 이러한 도발 직후 시점인 11월 17일 북한은 외부로부터의 두 차례에 걸친 DDoS 공격으로 북한 전역의 인터넷망이 마비되었다. 이 공격으로 북한의 외무성 홈페이지와 북한정부의 공식 포털 '내나라(Naenara)' 및 고려항공 홈페이지도 마비되었다. 북한에 대한 이러한 공격은 북한의 미사일 도발에 대한 한미의 경고 차원에서 이루어진 미국 사이버 사령부의 사이버 작전이다.[13]

Ⅲ. 정책적 함의

북한의 사이버 위협을 포함하여 고도의 첨단기술을 통해 파괴력이 증대하고 있는 초국가적 사이버 위협에 대응하는 일은 개별국 차원이 아닌 국가 간 신속하고 긴밀한 광범위한 공조를 통해서만 가능하다. 양자 간 혹은 다자 간 다양한 사이버 안보 협력과 공조는 위협에 대한 공동의 억지와 공격을 위한 실제 행동이 취해질 수 있다는 경고 메시지를 사이버 위협 주체에 대해 발신하는 일이다. 현재도 계속되고 있는 러시아-우크라이나 전쟁의 사이버전이 여실히 보여주고 있듯이 전시 국가 간 연합 전투력은 기술적 협력 외에도 정보공유, 동일한 플랫폼을 사용한 지휘통제 및 공동작전의 수행 등 긴밀하게 결합되고 통합된 능력을 요구한다. 한국은 동맹인 미국과 북한이 사이버 위협에 대해 공조하며 대응하는 한편 국가적으로도 다양한 공세적 사이버 작전 즉 '적극 방어(active defense)' 혹은 '공세적 방어(offensive defense)'의

10) Weisensee, 2022.
11) Winder, 2022.
12) 박형주, 2022.
13) Smith, 2022.

차원에서 발전되고 있다.

더군다나 최근 국가의 통신시스템과 핵심 인프라에 대해 급증하고 있는 사이버 공격은 공격 대상 국가에 대한 극심한 사회혼란을 유발할 수 있을 뿐 아니라 전시나 유사시에는 해당 국가의 국가 기능과 군사작전을 마비시킬 수 있기 때문에 최근 주요국의 사이버 안보 정책이 공세적으로 변화하는 데에 결정적인 영향을 끼치고 있다. 특히 통신망 침투는 정보 탈취뿐 아니라, 전시 공격 대상 국가의 지휘·통제를 마비시킬 수단이 될 수 있고 탈취한 개인정보를 통해 신원을 위장하여 디지털 신원 기반의 거의 모든 경제적·정치적 활동이 가능하므로 국가안보에 대단히 위협적이다. 통신망이 해킹되면 국가의 금융, 보안, 교통, 전자정부 시스템 등 디지털 사회 전체의 시스템이 위협받을 수 있으므로 통신사에 대한 해킹은 국가안보 문제가 된다. 해커가 통신사의 인프라를 장악할 경우 통신사가 보유한 정부와 군 기관과의 네트워크를 통해 주요 기관에 대한 사이버 공격이 가능해진다. 따라서 한국을 포함하여 많은 국가가 방어 중심의 접근으로는 국가의 핵심 인프라와 통신 시스템에 대한 지속적·지능적 침해를 억지하기 어렵다고 판단하게 되면서 자국의 사이버 안보 정책뿐 아니라 동맹 및 우호국과의 협력도 공세성을 띠어가고 있다.

최근 한국에 대한 북한과 중국 등의 사이버 공격은 한국의 통신사, 데이터가 저장되거나 관리되는 시스템, 법원을 포함한 국가의 공공기관 및 에너지, 교통, 항공, 의료 등 핵심 인프라 및 언론사들을 직접 겨냥하고 있고 단순히 정보 탈취뿐 아니라 전시나 위기 시 국가 기능을 마비시키기 위한 지점을 탐색하고 시험해 보는 목적을 가진 것으로 읽히고 있어 우리의 공세적 방어 정책의 실천과 공세적 사이버 역량 구비가 시급한 실정이다. 2024년 우리 정부는 '국가사이버안보전략'에서 '공세적 방어'를 주요 정책으로 내세웠으나 공세적 방어가 실제로 가능하기 위해서는 위협의 근원을 기술적으로 차단하고 고려할 수 있는 법제도적 절차와 외교적 절차가 모두 마련되어야 한다.

또한 한국의 북한에 대한 공세적 사이버 안보 정책이 가능하기 위해서는 동맹인 미국과의 사이버 안보 협력에 있어서 다양한 법, 제도적 정비가 필요하다. 미국의 경우 사이버 작전 권한, 민간기업과의 협력, 공격 대응 기준 등 사이버 작전 관련 법제 정비가 매우 발달해 있으나 우리의 경우 국가 사이버안보법도 부재한 데다가 공세적 방어, 선제 탐지 등에 대한 실제적 법제화가 미흡하다. 한국은 아직까지 사이버 안보 기본법이 없는 상태에서 대통령 훈령인 '국가사이버안전관리규정'에 근거하여 세계적 수준의 사이버 공격 능력을 구사하는 북한에 대응하고 있다. 따라서 북한의 사이버 공격에 대한 한미 연합작전 또는 공동 대응에서 법적 충돌 가능성이 존재하게 된다. 향후 한미 간의 공동작전이 가능해지려면 국내 법적·제도

적 정비가 신속하게 이루어져야 하고, 이러한 필요에 대하여 국내적으로도 주의를 환기할 필요가 크다.

무엇보다도, 민간 및 시민사회가 사이버 안보 위협에 대해 국가 및 국제사회와 동일한 민감성과 상황 인식 및 분별력을 갖기 위해서는 동 이슈에 대한 교육, 훈련 및 자문 등을 통한 정보와 대응 지침 제공이 상시로 이루어질 수 있어야 한다. 우리 정부가 동맹인 미국 및 우호국들과 함께 발표해 온 북한 IT 인력, 북한의 사이버 첩보 활동이나 공급망 공격 등에 대한 합동주의보와 같이 북한의 사이버 위협 구사 방식 등에 대한 정보를 민간과 시민사회가 분별하고 사이버 보안에 주의할 수 있도록 앞으로도 북한의 사이버 위협 관련 주요 정보를 선제적으로, 접근 가능한 방식으로 신속하게 제공하여 국가적 사이버 방첩 의식을 제고해야 한다. 즉 북한의 사이버 위협에 효과적으로 대처하기 위해서는 국가와 민간 및 시민사회가 동일한 사이버 안보 인식을 갖는 것이 조건이다. 사이버 공간을 이용한 해킹, 포르노・도박・마약밀매・사기 등 각종 범죄, 국가 기밀 유출, 스파이 활동 및 영향 공작, 테러리즘 모의 등은 대중이 일상적으로 사용하는 소셜미디어, 메타버스(metaverse) 혹은 챗GPT(ChatGPT) 등을 통해서도 이루어질 수 있기 때문에 민간의 안보의식이나 사이버 공간 사용 방식은 국가 안보와 직결된다.

참고문헌

박형주, 「[2022 연말기획] 1. 북한, 전례 없는 미사일 발사…'선제공격' 명문화로 긴장 고조」, Voice of America, 2022. 12. 26(https://www.voakorea.com/a/6889960.html).

송태은, 「통신 및 핵심 인프라에 대한 사이버 공격 실태와 주요국의 공세적 사이버 안보 정책: 현황과 과제」, 『주요국제문제분석』, 2025-33, 국립외교원 외교안보연구소, 2025.

송태은, 「최근 사이버 위협 실태와 한국의 인태 사이버안보 외교전략」, 『주요국제문제분석』, 2024-29, 국립외교원 외교안보연구소, 2024.

이종현, 「北 해커, KT 금융보안기업 이니텍 해킹 … 국정원·KISA가 적발」, 『디지털 데일리』, 2023. 3. 30(http://m.ddaily.co.kr/page/view/2023033011065890673).

DeYoung, Karen, Ellen Nakashima, and Emily Rauhala, "Trump signed presidential directive ordering actions to pressure North Korea," The Washington Post, September 30, 2017(https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html).

Miranda Bruce et al. "Mapping the global geography of cybercrime with the World Cybercrime Index," *PLoS ONE,* 19(4), 10 April, 2024(https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312, 접속일: 2025. 10. 2).

Smith, Josh, "North Korea's internet temporarily knocked offline, researcher says," *Reuters,* November 17, 2022(https://www.reuters.com/world/asia-pacific/north-koreas-internet-temporarily-knocked-offline-researcher-says-2022-11-17).

United Nations Security Council, S/2019/691, August 30, 2019. p.27(https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf).

U.S. Department of State, "Joint Statement of the Multilateral Sanctions Monitoring Team (MSMT) on the Report Covering DPRK Cyber and IT Worker Activities" (October 22, 2025). https://www.state.gov/releases/2025/10/joint-statement-of-the-multilateral-sanctions-monitoring-team-msmt-on-the-report-covering-dprk-cyber-and-it-worker-activities.

Voo, Julia, Irfan Hemani, and Daniel Cassidy, *National Cyber Power Index 2022*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2022.

Weisensee, Nils, "DDOS attack cuts off North Korea's internet after fifth missile test," *NK Pro,* January 26, 2022(https://www.nknews.org/pro/ddos-attack-cuts-off-north-koreas-internet-after-fifth-missile-test).

Williams, Martyn, "Russia Provides New Internet Connection to North Korea" *38 North*, October 1, 2017(https://www.38north.org/2017/10/mwilliams100117).

Winder, Davey., "One American Hacker Suddenly Took Down North Korea's Internet—All Of It," *Forbes,* February 5, 2022(https://www.forbes.com/sites/daveywinder/2022/02/05/one-american-hacker-suddenly-takes-down-north-koreas-internet-all-of-it/?sh=1651434c6698).

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]

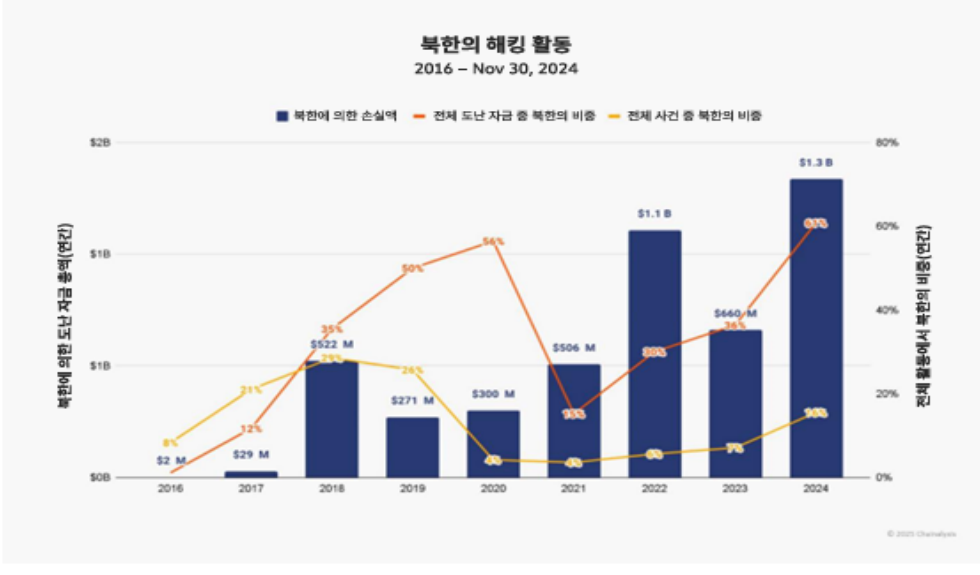
---

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).

본지에 수록된 내용은
집필자의 개인적인 견해이며, 당 연구원의 공식적인 의견이
아님을 밝혀 둡니다.