국회입법조사처 | 2022. 12. 28. | 제2034호
이슈와 논점
Issues and Perspectives

북한 사이버 공격의 현황과 쟁점

이 승 열

북한의 사이버 공격이 국제사회의 안보 현안으로 떠오르고 있다. 2009년 시작된 북한의 사이버 공격은 2016년을 기점으로 정보 탈취에서 외화벌이로 진화하고 있다. 이에 국제사회는 북한이 금융 자산 및 암호화폐 공격을 통해 핵·미사일 관련 개발자금을 마련하고 있는 것으로 보고 이를 막기 위해 적극적으로 나서고 있다. 북한의 사이버 능력을 파악하고, 이에 대한 국제공조와 대응 시스템의 확립을 위한 구체적인 방안 마련이 필요하다. 아울러 민관의 통합된 사이버 안보 체계의 구축을 위한 기본법 제정에 나설 필요가 있다.

1 들어가며

북한의 사이버 공격에 대한 한·미 당국의 대응이 강화되고 있다. 지난 2022년 5월 개최된 한미정상회담에서 양 정상은 '사이버'를 10번이나 언급하면서, 북한의 사이버 공격의 주요 대상인 국가 핵심 기반시설의 보안과 사이버 범죄와 관련한 자금세탁 대응 및 사이버 정책에 대한 국가간 공조를 지속·심화시켜 나가기로 합의하였다.[1)]

2022년 11월 17일 서울에서는 한미 공동으로 '북한 암호화폐 탈취 대응 한미 공동 민관 심포지엄'이 개최되었다. 외교부는 이번 회의가 지난 8월 9일 제1차 북한 사이버 위협 대응 한미 실무그룹(working group) 회의의 후속 조치로 열린 것이며, 16개국의 정부 인사 및 암호화폐 거래소 ·블록체인 기업·싱크탱크 등이 참여했다고 밝혔다.[2)]

이번 한미 공동 심포지엄에서는 북한 암호화폐 탈취 문제의 심각성이 주로 강조되었는데, 특히 북한에 의해 탈취된 암호화폐가 핵·미사일 개발자금으로 전용되고 있는 현실과 이를 방지하기 위한 민관협력과 국제공조의 필요성이 논의되었다.[3)]

북한의 사이버 공격은 지난 2009년 7월 디도스(DDoS) 공격으로 주목을 받기 시작했으며, 최근에는 랜섬웨어 공격과 국제금융기관 및 암호화폐 거래소에 대한 해킹으로 진화하면서 국제적인 안보 현안으로 떠오르고 있다.

따라서 본 글에서는 국제적 안보 이슈로 떠오른 북한의 사이버 공격 현황을 분석하고, 이를 토대로 북한 사이버 공격으로 제기된 쟁점을 살펴보도록 하겠다.

2 북한의 사이버 공격 현황

(1) 북한의 사이버 공격 조직

1) 제20대 대통령실, 「한미 정상 공동성명」, 2022.5.21., (최종 검색일: 2022.8.2.), 〈https://www.korea.kr/news/policyNewsView.do?newsId=148901846〉.

2) 외교부, "북한 암호화폐 탈취 대응 한미 공동 민관 심포지엄 개최 보도자료," 2022.11.17.(최종 검색일: 2022.11.24.) 〈https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=373025〉.

3) 위의 글.

NARS www.nars.go.kr
발행처 국회입법조사처
발행인 이신우 국회입법조사처장 직무대리
저 자 이승열 정치행정조사실 외교안보팀 조사관/ 북한학박사
02-6788-4557 summer20@assembly.go.kr
국회입법조사처 NATIONAL ASSEMBLY RESEARCH SERVICE

북한은 1990년대 초 미국의 걸프전쟁 이후 조선인민군 총참모부 산하에 '지휘자동화국'과 '전자전 연구소'를 설치하고, 사이버전 능력을 국가전략으로 채택하여 발전시켰다.[4] 북한의 사이버 공격 능력은 2009년 북한의 해외·대남 정보기구인 '정찰총국'(RGB: Reconnaissance General Bureau)의 등장으로 비약적으로 발전하였다. 특히 사이버 공격의 핵심 부서는 정찰총국 산하 '121국'(사이버전 지도국: Cyber Warfare Guidance Unit)에 의해 이뤄지고 있다.[5]

'121국'의 산하조직인 '110호 연구소'(컴퓨터기술연구소)에는 북한의 금융 관련 해킹 조직인 '라자루스'(Lazarus), '블루노로프'(Bluenoroff), '안다리엘'(Andarial) 등이 있으며, 정보수집 임무를 담당하는 해킹조직인 '김수키'(Kimsuky) 등이 활동하고 있는 것으로 알려져 있다.[6]

북한의 금융 분야 공격을 주도하는 '라자루스' 그룹은 2007년 초 설립되었으며, 2014년 소니픽쳐스사 해킹과 2017년 워너크라이(WannaCry) 랜섬웨어 사건, 해외 금융기관에 대한 해킹의 배후로 지목된 기관이다.[7] 또한 라자루스의 하위 그룹으로 알려진 '블루노르프'와 '안다니엘'도 금융기관, 카지노, 금융거래 소프트웨어 개발, 그리고 암호화폐 등 불법적인 금전적 수입을 확충하는 데 특화된 조직으로 알려져 있다.[8] '김수키'는 정찰총국 산하 조직으로 2010년부터 활동한 것으로 알려져 있으며, 한·미·일 정부를 포함하여 세계적인 정보수집 임무를 담당하고 있다. 특히 한반도 관련 안보 전문가들을 대상으로 한 정보활동을 벌이고 있는 것으로 알려졌다.[9]

(2) 북한의 암호화폐 공격 현황

북한의 사이버 공격은 2009년 7월 국가 기간망의 무력화를 노린 디도스(DDoS) 공격을 시작으로 초기에는 국가 기관의 주요 정보 및 기술 탈취를 목적으로 이뤄졌지만, 2016년 이후부터는 국제사회의 대북제재로 인해 야기된 외화 부족 상황을 해결하기 위한 외화벌이 수단으로 활용되었다. 이를 위해 북한의 사이버 공격은 해외 금융기관 공격, 랜섬웨어 공격, 암호화폐 거래소에 대한 해킹 등에 집중되었다.

2022년 3월 1일 공개된 UN안보리 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 암호화폐 거래소에서 약 5,000만 달러 가치의 암호화폐를 훔쳤다고 밝혔다.[10]

또한 보고서는 블록체인 분석기업 'Chain Anaysis'의 평가를 인용하면서, 북한이 2021년 한 해 동안 암호화폐 거래소뿐만 아니라 투자회사 등에 대한 총 7번의 사이버 공격으로 약 4억 달러 가치의 암호화폐를 훔쳤다고 밝혔다.[11] 이와 함께 미국 연방수사국(FBI)도 2022년 3월 발생한 게임업체 '액시 인피니티'(Axie Infinity)의 암호화폐 해킹 배후에 북한의 '라자루스'가 탈취 사건에 책임이 있음을 확인했다고 밝혔다.[12]

2009년 이후 북한의 사이버 공격 사례는 아래 [표 1]과 같다.

4) 황지환, "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산," 『동서연구』, 제29권 제1호, 2017, p147.

5) E. Avery·J. Rollins·L. Rosen·C. Theohary, North Korea Cyber Capabilities: In Brief, CRS REPORT, p.2, August 3, 2017,(최종 검색일: 2022.12.20.), 〈 https://crsreports.congress.gov/product/pdf/R/R44912〉

6) 조해수·유지만, "북한 해킹 그룹 김수키·라자루스·스카크러프트·안다리엘, 「시사저널」, 1713호, 2022, 8.13., (최종 검색일: 2022.8.17.), 〈 https://www.sisajournal.com/news/articleView.html?idxno=218951〉. 탈륨(Thallium)과 동일조직으로 추정.

7) 김보미·오일석, "김정은 시대 북한의 사이버 위협과 주요국 대응," 『INSS 전략보고』, 147호, 2022.9, p. 7.

8) 위의 글, pp.7-8

9) 위의 글, pp.7-8.

10) United Nations Security Council, *S/2022/132*, p. 80, March 1, 2022 (최종 검색일: 2022.11.29.), 〈http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf〉.

11) 위의 글, p. 80.

12) J. Tidy, "7400억원 규모 암호화폐 게임 해킹 배후에 북한 해커," 「BBC NEWS KOREA」, 20227.5.,(최종 검색일: 2022.12.2.).

[표 1] 북한의 사이버 공격 사례

날짜	내용	날짜	내용
2009.7	디도스(DDoS) 공격 (청와대 등 정부기관)	2017. 5	워너크라이 랜섬웨어 공격 (150여 개국에 피해)
2011.3	디도스(DDoS) 공격 (방송사, 금융기관, 인터넷기업)	2017. 7	빗썸 암호화폐거래소 공격
2011.4	농협전산망 해킹	2018.1	일본 가상화폐 코인체크 공격
2014.12	한수원 원전 해킹	2018.6	빗썸 가상화폐거래소 공격
2014.12	소니픽쳐스사 해킹	2019.9	업비트 가상화폐거래소 공격
2015.10	서울지하철 1-4호선 서버 해킹	2020.9	슬로바키아의 암호화폐거래소 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	남아공 화물 및 물류 회사에 대한 랜섬웨어 공격
2016.10	미국 뉴욕연방준비 은행 방글라데시 계좌에서 8,100만달러 탈취	2022.3	게임업체 액시 인피니티(Axie Infinity)에 대한 암호화폐 탈취

※ 자료: 국가 관계기관 보고서와 학술논문 그리고 언론 보도 자료를 참고하여 저자가 작성

3 북한의 사이버 공격 관련 쟁점

북한의 사이버 공격은 핵과 미사일 능력과 함께 대표적인 '비대칭전략'(Asymmetric Strategies)으로 새로운 안보위협으로 평가되고 있다. 북한의 사이버 공격에 대한 쟁점을 크게 세 가지 차원에서 분석할 수 있다.

첫째, 북한의 사이버 역량에 대한 국제사회의 시각이다. 영국의 IISS(The International Institute for Strategic Studies)는 북한의 사이버 능력을 최하위인 3그룹(Thrid-tier)에 속한다고 평가절하했다. 구체적으로 북한의 사이버 인프라와 보안 수준이 세계 최하위이며, 세계 인터넷망과 연결하는 '게이트웨이'가 중국과 러시아 서비스 제공업체에 전적으로 의존하여 외부의 공격에 취약하다고 밝혔다.[13] 그러나 미국은 열악한 북한의 사이버 인프라와는 달리, 사이버 공격 능력은 세계적인 수준이라고 평가하고 있다. 미국 마이크로소프트사(MS)는 2020년 10월 발표한 「2020 MS 디지털 방어 보고서」에서 북한을 러시아, 이란, 중국 다음으로 세계 4번째 사이버 해킹 국가로 분류하고 있다.[14] 또한 미국 하버드대 케네디스쿨 '벨퍼센터'(Belfer Center)는 '국가별 사이버 역량지표(NCPI) 2022'에서 북한의 사이버 금융해킹 능력이 전 세계 1위를 기록했다고 밝혔다. 무엇보다 북한이 암호화폐 탈취나 금융기관에 대한 사이버 공격에 집중했기 때문이라고 분석된다.[15]

둘째, 북한의 사이버 공격에 대한 국제공조와 관련된 문제이다. 북한의 사이버 공격에 대해 국제사회가 공동대응할 수 있는 '국제공조체제'는 아직 확고하게 구축되어 있지 않은 상태다. 북한의 핵과 미사일 위협에 대한 유엔안보리의 '대북제재위원회'가 '플랫폼'(platform) 역할을 하는 것과는 대조적이다.

그러나 사이버 공격에 대한 관련국 간의 다자간 협력체제는 마련되고 있다. 지난 2021년 11월 바이든 대통령은 '랜섬웨어 대응회의'를 개최하여 유럽, 중동, 아프리카, 아시아 등 35개국과의 국제적 협력

13) 김보미·오일석, "김정은 시대 북한의 사이버 위협과 주요국 대응," p.5. The International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," IISS, February 2019, p.125. 참조.

14) 오택성, "MS 북한 사이버 공격 세계 4번째…개인정보 탈취 집중," 「VOA」, 2020.10.6. (최종 검색일: 2021.7.1.), 〈http://www.voakorea.com/korea/korea-politics/microsoft-report-analyzed-nsns〉.

15) Julia Voo·Irfan Hemani·Daniel Cassidy, *National Cyber Power Index 2022*, p. 13, September 2022, (최종 검색일: 2022.12.1.) 〈https://www.belfercenter.org/publication/national-cyber-power-index-2022〉

방안을 담은 공동성명을 발표하였다.[16)]

또한 북한의 사이버 공격에 대한 양자간 협력도 추진되고 있다. 올해 5월 한미정상회담에서 양국은 사이버안보와 관련한 협력을 강화하기로 합의하였다. 이에 대한 후속 조치로서 11월 한미는 북한 암호화폐 탈취 대응을 위한 공동 심포지엄을 개최하였고, 12월에는 핵·미사일 개발과 관련된 금융거래 혐의를 받는 북한 금융기관 소속의 개인 8명과 기관 7곳을 독자제재 대상으로 지정하였다.[17)]

셋째, 북한의 사이버 공격에 대한 국가적 대응 시스템을 확립하는 문제이다. 2020년 12월 미 법무부는 미국을 비롯해 여러 나라의 주요 은행과 암호화폐거래소에 대해 13억 달러(약 1조4000억원) 규모의 현금과 암호화폐 절취를 목적으로 사이버 공격을 시도한 혐의로 북한 정찰총국 소속 해커 전창혁·김일·박진혁 등을 신병확보 없이 기소하였다.[18)]

이외에도 미국은 북한의 암호화폐 공격에 대응하여 법무부와 국무부 내에 사이버 범죄 전담부서를 신설하였고, 연방수사국(FBI)과 재무부는 북한 행킹그룹인 '라자루스'의 위협을 경고하는 부처 합동주의보를 발령하여 경각심을 높이고 있다.[19)]유럽연합(EU)도 2019년에 제정된 법규(Council Decision 2019/797 and Council Regulation No.2019/796)에 따라 '워너크라이' 랜섬웨어 공격을 감행한 '조선엑스포합영회사'를 제재 대상에 포함시키는 등 대북 사이버 제재를 강화하고 있다.[20)] 이와 관련 북한의 증가하는 사이버 위협에 대한 우리정부의 대응 능력에 대한 문제점이 지속적으로 지적되어 왔으며, 관련법 제정을 비롯해 제재 능력, 정보공유, 국제공조 등에 대해 보완이 필요하다는 주장이 제기되어 왔다.[21)]

4 나가며

2020년 9월 국정원이 국회 정보위원회에 보고한 내용에 따르면, 5년간(2015.1-2020.6) 공공기관에서 발생한 사이버 공격 피해는 11,727건이며, 이 중 70-80%가 북한의 사이버 공격이라고 밝혔다.[22)] 공공분야에 대한 사이버 공격은 2015년을 정점으로 줄어들고 있지만, 금융기관 및 가상화폐 거래소 등 민간분야의 사이버 공격은 오히려 증가하고 있다.

무엇보다 공공분야는 「국가사이버안전관리규정」에 따라 '국가사이버안전센터'가 컨트롤타워의 역할을 하며 운영되고 있지만, 민간에 대한 사이버보안 의무를 강제하는 법적 기반은 아직 제대로 체계를 갖추지 못했기 때문이다.[23)] 국정원은 이를 보완하기 위해 올해 11월 민관 합동 '국가사이버안보협력센터'를 개소한 바 있다.

하지만 북한의 사이버 공격이 공공과 민간의 영역을 가리지 않는 상황에서 현재 대통령 훈령인 「국가사이버안전관리규정」만으로는 고도화되는 북한의 사이버 공격을 대응하는 데 한계가 있다. 따라서 정부는 이러한 한계를 고려하여 국가 사이버 안보에 대한 기본법 제정 등 민관이 통합된 사이버 안보 체계 구축에 나설 필요가 있다.

※ 2022년 국회입법조사처 장/단기과제 관련 보고서입니다

16) 박형주, "바이든 '사이버 안보' 강조…북한, 올해 '전방위 사이버 활동' 전개," 「VOA」, 2021.12.29., (최종 검색일: 2022. 12. 2.), 〈https://www.voakorea.com/a/6373229.html〉.

17) 최서진, "정부, 대북 추가 독자제재..개인 8명, 기관 7개 지정," 「뉴시스」, 2022.12.2.,(최종 검색일: 2022.12.2.).

18) 박현영, "미국 북한 해커, 총 대신 키보드로 가상지갑 턴 세계의 강도", 「중앙일보」, 2021. 2. 19. (최종 검색일: 2022.12.1.), 〈http://news.joins.com/article/23995352〉.

19) 벅형주, "바이든, 사이버안보 강조…북한, 올해 전방위 사이버활동 전개," 「VOA」, 2021.12.29.,(최종 검색일: 2022.12.2.).

20) 김보미, "북한의 암호화폐 공격과 미국의 대응," 『INSS 전략보고』, 191호, 2022.11, p. 18.

21) 위의 글, p. 15.

22) 김당, "공공분야 사이버공격 1만1727건…북한발 70-80%," 「UPI뉴스」,2020.10.16.(최종 검색일: 2022.12.1.). 〈https://www.upinews.kr/newsView/upi202010160030〉.

23) 최경호, "국경없는 사이버테러,대한민국이 위험하다," 『월간중앙』, 2022.1.23.,(최종 검색일: 2022.12.5.).

07233 서울시 영등포구 의사당대로 1 국회입법조사처
Tel. 02-6788-4510
발간등록번호 31-9735008-000621-14
ISSN 2005-744X