http://doi.org/10.33728/ups.2023.32.1.012

통일정책연구 제32권 1호 2023
pp. 323~353

북한 사이버 공격 전략의 진화: 대북제재 회피를 위한 외화벌이 수단으로서 사이버 전략*

이승열**

국문요약

북한의 사이버 공격이 국제사회의 안보 현안으로 떠오르고 있다. 2009년 국가 기간망 무력화와 정보 탈취를 목적으로 시작된 북한의 사이버 공격은 2016년을 기점으로 대북제재 회피를 위한 외화벌이 수단으로 진화하고 있다. 이에 미국을 비롯한 국제사회는 북한이 금융자산 및 가상화폐 공격을 통해 대북제재를 회피하고, 핵·미사일 관련 개발자금을 마련하고 있는 것으로 보고 이를 막기 위해 적극적으로 나서고 있다.

따라서 한미 당국과 국제사회는 북한의 사이버 공격 능력을 파악하고, 이에 대한 국제공조와 대응 시스템의 확립을 위한 구체적인 방안을 마련할 필요가 있다. 아울러 한국 정부는 민관의 통합된 사이버 안보 체계의 구축을 위해 현재 대통령 훈령인 「국가사이버안전관리규정」의 한계를 파악하고 이를 극복하기 위해 사이버 안보 관련 업무를 총괄할 수 있는 사이버 관련 기본법 제정에 적극적으로 나설 필요가 있다.

주제어: 사이버 공격, 디도스, 라자루스, 블루노로프, 안다리엘

* 본 논문은 저자가 국회입법조사처에서 발간한 보고서인 "북한 사이버테러 위협의 증가와 대응방안." 『이슈와논점』 제1127호와 "북한 사이버 공격의 현황과 쟁점." 『이슈와논점』. 제2034호에서 제기한 일부 내용을 더욱 깊이 확장하여 발전시킨 논문입니다.

** 국회입법조사처 입법조사관

Ⅰ. 들어가며

2022년 5월 21일 윤석열 대통령 취임 이후 첫 번째 한미정상회담이 열렸다. 한미 양 정상은 공동성명에서 "북한으로부터의 다양한 사이버 위협에 대응하기 위한 협력을 대폭 확대해 나갈 것"이라고 밝혔다.[1] 특히 양 정상은 '사이버'(Cyber)란 단어를 총 10번이나 언급하면서, 북한 사이버 공격의 주요 대상인 국가 핵심 인프라 시설의 사이버 보안과 사이버 범죄 및 이와 관련한 사이버 자금세탁에 대한 대응 더 나아가 글로벌 사이버 정책 집행에서 양국 간 협력을 지속적으로 심화시켜 나가기로 합의하였다.[2]

미국은 북한의 사이버 위협을 포함해 국제사회의 사이버 공격을 국가안보(national security)의 최우선 과제로 내세우며 강력히 대응하고 있다. 바이든(J. Biden) 대통령은 2021년 1월 백악관 내 '국가 사이버 국장직'을 신설하였고, 동년 8월에는 '국가사이버안보회의'를 개최하여 애플, 아마존, 마이크로소프트 등 미국의 대표적인 빅테크 기업들과 사이버 안보에 관한 민관협력을 강조하였다.[3] 그리고 동년 11월에는 '랜섬웨어 대응회의'를 개최하여 한국과 일본 등 35개국과의 국제적 협력 방안을 모색하였다.[4] 그리고 2022년 3월 15일 바이든 대통령은 미국의 사이버 대응 능력을 더욱 강화하기 위해 「2022년 미국 사이버 강화법」(Strengthening American Cybersecurity Act of 2022)에 서명하였다.[5]

북한의 사이버 공격에 대한 한미 당국의 대응이 빨라지고 있는 가운데 특히 미국의 대응이 눈에 띄게 강화되었다. 2022년 7월 25일 네드 프라이스(Edward Price) 미 국무부 대변인은 국무부가 "북한의 악의적 사이버 활동을 주시하고 있으며, 모든 가용한 수단을 동원해 북한 사이버 공격 세력을 추적하고 있다"고 밝혔

---

1 제20대 대통령실, "한미 정상 공동성명," 2022.5.21., 〈https://www.korea.kr/news/policyNewsView.do?newsId=148901846〉 (검색일: 2023.4.2.).

2 위의 글.

3 박형주, "미 국토안보장관, 북한, 암호화폐 등 10억달러 이상 탈취…WMD 자금 조달," 『VOA』, 2021.10.19., 〈https://www.voakorea.com/a/6795295.html〉 (검색일: 2023.2.23.).

4 위의 글.

5 Lewis. Brisbois, "Strengthening American Cybersecurity Act of 2022 Signed Into Law," DIGITAL INSIGHTS, March 28, 2022, 〈https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/update-strengthening-american-cybersecurity-act-of-2022-signed-into-law〉 (Accessed April 2, 2023).

다.[6] 그는 북한이 '랜섬웨어'(ransomware) 공격을 통해 '몸값'을 요구하는 악의적인 금융사기를 자행하고 '가상화폐'(cryptocurrency)를 탈취하여 사이버 공격을 대북제재의 회피 수단으로 악용하고 있다고 강조했다.[7]

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'(wanna cry) 랜섬웨어(ransomware) 공격을 주도하면서 미 법무부에 의해 기소된 전력이 있는 것으로 나타났다.[8]

북한의 대남 사이버 공격이 국내적으로 본격화된 것은 2009년 7월 7일부터 한국과 미국의 주요 기관 등 총 35개의 웹사이트에 대하여 북한이 '분산서비스거부공격'(디도스: DDoS)을 감행하면서 시작되었다.[9] 그리고 미국이 북한의 사이버 공격에 대해 직접적으로 행정명령을 발동한 사건은 2014년 12월 24일 김정은 위원장 암살 관련 영화('인터뷰')를 제작한 소니픽처스사에 대한 사이버 공격이었다. 이후 한국과 미국을 비롯한 국제사회는 북한의 사이버 공격을 국가안보에 대한 중대한 위협으로 인식하였다.[10]

북한의 사이버 공격이 본격적으로 국제사회의 안보 이슈로 떠오른 이유는 북한이 국제사회의 대북제재로 인한 경제적 피해를 만회하고 핵과 미사일 개발을 위한 자금을 확보하는 수단으로 사이버 공간을 이용하고 있기 때문이다.[11] 따라서 본

---

6 조은정, "미 국무부 "북한 사이버 공격 세력 추적에 가용한 모든 수단 동원"," 『VOA』, 2022.7.26., 〈https://www.voakorea.com/a/6673300.html〉 (검색일: 2023.4.11.).

7 위의 글.

8 박현주, "한, 악명높은 라자루스·박진혁 때렸다…북사이버 첫 독자재제," 『중앙일보』, 2023.2.10., 〈https://www.joongang.co.kr/article/25139694#home〉 (검색일: 2023.4.20.).

9 이승열, "북한 사이버테러 위협의 증가와 대응방안," (국회입법조사처 이슈와논점 제1127호, 2016.2.23.), p. 1, 〈https://www.nars.go.kr/report/view.do?page=7&cmsCode=CM0043&categoryId=&searchType=NM&searchKeyword=%EC%9D%B4%EC%8A%B9%EC%97%B4&brdSeq=18172〉 (검색일: 2023.4.20.).

10 정민경·임종인·권헌영, "북한의 사이버공격과 대응방안에 관한 연구," 『한국IT서비스 학회지』, 제15권 제1호 (2016), p. 72.

11 송태은, "북한의 사이버 공격과 우리의 대응," (외교안보연구소 IFANSFOCUS IF2022-28K, 2022.10.31.), p. 2, 〈https://www.ifans.go.kr/knda/ifans/kor/pblct/PblctList.do?menuCl=P07&pageIndex=1〉 (검색일: 2023.4.20.).

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. 사이버 공격에 대한 정의와 국제사회의 논의 현황

미국의 「국가안보대통령지시」(National Security Presidential Directive-54)는 사이버 공간을 "인터넷, 통신 네트워크, 컴퓨터 시스템, 내장형 프로세스와 기반산업시설의 제어시스템 등이 포함된 정보 기술의 상호 의존적 네트워크"라고 정의하고 있다.[12] 유럽의 「사이버범죄협약」(Convention on Cybercrime)은 사이버 공간을 컴퓨터 혹은 어떤 기계든지 상호 연결되어 프로그램을 수행하거나, 자료와 정보를 교환·처리·수집·저장하는 기계들을 네트워크로 연결하여 형성된 물리적 또는 가상의 공간을 의미한다고 정의하고 있다.[13]

사이버 공격은 사이버 공간 안에서 이루어지는 범죄행위이며 상대방의 사이버 공간에 접속하여 컴퓨터와 컴퓨터 네트워크에 있는 정보를 방해·거부·성능저하·조작·파괴하기 위해 컴퓨터 네트워크를 사용하는 행위를 의미한다.[14] 사이버 안보는 사이버 공격으로부터 컴퓨터와 전자통신시스템, 서비스, 연결망, 정보의 손상을 막고, 보호하고, 회복시키는 모든 활동이라고 정의할 수 있다.[15] 이처럼 미국을 비롯한 서방세계는 사이버 공간에서 일어나는 사이버 공격을 사이버 안보의 관점에서 보고 있으며 새로운 안보 영역으로 인식하고 있다.[16]

---

12 The White House, "National Security Presidential Directive/NSPD-54/HSPD23," January 8, 2008, p. 3, 〈https://irp.fas.org/offdocs/nspd/nspd-54.pdf〉 (Accessed June 1, 2023).

13 Council of Europe, "Convention on Cybercrime, European Treaty Series-No. 185, Budapest, 23. XI. 2001, pp. 4~5, 〈https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf〉 (Accessed June 1, 2023).

14 The White House, "National Security Presidential Directive/NSPD-54/HSPD23," p. 2.

15 Ibid., p. 3.

16 Joseph S. Nye Jr., "International Norms in Cyberspace," Project Sindicate, May 11, 2015, 〈https://www.project-syndicate.org/commentary/international-norms-cyberspace-by-joseph-s—nye-2015-05〉 (Accessed June 1, 2023).

한국의 「국가사이버안전관리규정」 제2조는 '사이버 공격'을 해킹 · 컴퓨터바이러스 · 논리폭탄 · 메일폭탄 · 서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입 · 교란 · 마비 · 파괴하거나 정보를 갈취 · 훼손하는 일체의 공격행위라고 정의하고 있다.[17] 또한 사이버 공격으로 인해 초래된 상황을 '사이버 위기'로 규정하면서, 정보통신망을 통해 유통 · 저장되는 정보를 유출 · 변경 · 파괴함으로써 국가안보에 영향을 미치거나 사회 · 경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손 · 정지되는 등 무력화되는 상황이라고 정의하고 있다.[18]

미국과 유럽 그리고 한국은 사이버 공간을 국가안보의 핵심 영역으로 규정하고 있으며, 사이버 공격으로 초래되는 사이버 전쟁을 대규모 피해나 사상자가 발생하는 실질적인 공격행위로 인식하고 있다. 마이클 슈미트(Michael N. Schmitt)가 주관하고 있는 『탈린매뉴얼』(Tallinn Manual)은 이러한 미국과 나토의 사이버 방어센터(NATO CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence)의 인식을 바탕으로 사이버 작전에 적용할 수 있는 국제사회의 규범을 마련하고자 하는 노력의 일환이었다.

조셉 나이(J. Nye)는 국제안보 환경에 나타난 새로운 변화를 설명하면서 정보혁명의 발전에 따라 사이버 공간이 만들어지면서 기존의 재래식 전쟁과 차별화된 사이버전을 수행하는 '사이버 파워'(cyber power)가 등장했다는 점을 강조하였다.[19] 그는 사이버 파워가 사이버 공간의 급속 팽창으로 국제정치의 새로운 개념으로서 매우 중요하며, 무엇보다 기존 강대국들뿐만 아니라 '작은 행위자'(smaller actor) 즉, 테러 집단과 실패국가 등도 사이버 공간의 낮은 진입장벽과 익명성, 취약성의 비대칭성으로 인해 사이버 공간에서 하드파워와 소프트파워를 발휘할 수 있는 능력을 더 많이 갖추게 되었다고 주장하였다.[20]

---

17 「국가사이버안전관리규정」 (시행 2013. 9. 2. 대통령훈령 제316호, 2013. 9. 2., 일부개정), 제2조 2항,,〈https://www.law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EC%A0%84%EA%B4%80%EB%A6%AC%EA%B7%9C%EC%A0%95#liBgcolor0〉 (검색일: 2023.5.31.).

18 위의 법령, 제2조 4항.

19 Joseph S. Nye Jr., "Nuclear Lesson for Cyber Security?" *Strategic Studies Quarterly*, vol. 5, no. 4 (2011), pp. 18~38.

20 Joseph S. Nye Jr. "Cyber Power," Belfer Center for Science and International Affairs, May 2010, p. 1, 〈https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf〉 (검색일: 2023.5.31.).

이처럼 기존의 강대국(미국, 러시아, 중국)뿐만 아니라 '불량국가'(rogue state)인 이란과 북한 등이 사이버 공격의 새로운 강국으로 등장한 현실에서 사이버 안보는 21세기 국제정치학의 핵심 주제로 주목받게 되었고 이에 대한 국제사회의 논의가 활발하게 진행되고 있다. 특히 국제사회는 4차 혁명시대의 과학기술의 발달과 초국가적 네트워크의 연결로 인해 사이버 안보가 일국 차원의 문제를 넘어 초국가적 차원의 문제로 확산되자 국제적 합의를 끌어내고 이를 기반으로 국제적 규범을 세우기 위한 다양한 노력을 시도하고 있다. 그러나 아직까지 사이버 안보에 대한 국제적 합의는 마련되지 않았고, 오히려 미국, 러시아, 중국 등 강대국 간의 이해관계로 인해 더 복잡해지는 양상을 띠고 있다.

그 결과 사이버 안보 위협에 대한 국제사회의 논의는 주로 UN의 '정부전문가그룹'(GGE, Group of Governmental Experts)과 '탈린매뉴얼' 활동, 그리고 「사이버범죄협약」 등을 통해 이뤄지고 있다. 먼저 UNGGE의 활동이 주목받기 시작하였는데, 2004년 UN은 사이버 관련 국제법을 제정하고자 각국으로부터 전문가들을 모아 제1차 UN 사이버안보 GGE를 개최하였다. 2004년 이후 그동안 여섯 개의 UNGGE가 설치되었고, 가장 최근 2021년 3월 12일 제6차 UNGGE와 제1차 개방형워킹그룹(OEWG, Open-ended working group)의 최종 보고서가 채택되었다.[21] 주요 내용은 ① 현존 및 잠재위협 ② 국제법의 적용 ③ 책임 있는 국가 행동의 자발적 비구속적 규범 ④ 신뢰구축 조치 ⑤ 역량구축 조치 등이 다뤄졌다. 이러한 논의를 통해 국가들은 사이버공간을 규율하는 국제법, 즉 「국제사이버법」을 발전시키고 있다.[22] 한국의 경우 제3차 UNGGE회의를 제외하고 모두 참여했다.

다음 탈린매뉴얼은 전통적인 국제법의 틀을 원용하여 사이버 공간에서 발생하는 공격에 대응하기 위한 것으로 2009년부터 20여 명의 국제법 전문가들이 나토 CCDCOE의 총괄하에 작성한 95개 항의 사이버전 지침서를 정리하여 2013년 발간하였다. 탈린매뉴얼에서 언급된 '사이버전'(Cyber Warfare)은 국가들이 사이버 공간에서 적대적인 군사행위를 하는 사이버 공격, 즉 상대국의 주요 인프라나 명령통제시스템의 파괴로 인한 인명살상, 목표물의 손상 등 물리적 타격을 의미한

[21] UN General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunication in the context of international security*, UN Doc. A/AC290/2021/CPR.2 March 10, 2021.

[22] 박노형 · 박주희, "제6차 UNGGE 보고서 채택과 국제사이법의 발전," 『국제법학회논총』, 제66권 제3호 (2021), pp. 173~174.

다.[23] 이 책의 책임자 겸 총편집자인 슈미트(M. Schmitt)는 탈린매뉴얼이 새로운 법체계를 구축하기보다는 기존의 국제법 테두리 내에서 사이버 공간에서의 무력 행위를 규정하는 방식으로 연구되었다고 밝혔다.[24] 탈린매뉴얼은 사이버 공간에서도 전통적인 교전수칙이 적용될 수 있다는 점을 강조하고 있다. 또한 지난 2017년에는 19명의 국제법 전문가들이 기존 탈린매뉴얼을 보완하여 사이버 작업을 규율하는 154개의 "블랙레터" 규칙들을 식별하고 각 규칙에 대한 방대한 해설을 제공한 『Tallinn Manual 2.0』을 발간하면서 국제적 논의를 이어가고 있다.

마지막으로 「사이버범죄협약」은 일명 '부다페스트조약'이라고도 하며, 사이버범죄에 대해 상세한 규정을 두고 이를 처벌하도록 한 최초의 국제조약이다. 「사이버범죄협약」은 2001년 11월 유럽평의회에서 채택되고, 헝가리 수도 부다페스트에서 30개국이 서명에 참가하여 2004년 7월 발효되었고, 2022년 10월까지 가입국은 미 · 일 · 호주 등 총 67개국이다. 한국은 그동안 「통신비밀보호법」 등 국내법과 상충 문제로 가입하지 않다가 2022년 10월 외교부는 「사이버범죄협약」 가입을 위한 첫 단계로 유럽평의회에 협약 가입의향서를 제출하였다.[25] 국제사회의 사이버 공격이 한 국가에서 이뤄지는 것이 아니라 여러 나라를 거쳐 국내망에 침투하기 때문에 국제적인 공조 없이는 정확한 공격의 진원지를 증명하기 어렵다. 따라서 「사이버범죄협약」은 이에 대한 국제사회의 공조가 가능한 첫 국가 간 조약이라는 점에서 의미가 있다.

---

23 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.), pp. 5~6.

24 Micheal N. Schmitt, "the Introduction of Tallinn Manual," in *Tallinn Manual on the International Law Applicable to Cyber Warfare*, ed. Michael N. Schmitt (Cambridge: Cambridge University Press, 2013).

25 외교부, "사이버범죄협약(일명 '부다페스트협약') 가입의향서 제출."(외교부 보도자료, 2022.10.11.), 〈https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=372854&page=1〉 (검색일: 2023.6.5.).

Ⅲ. 북한의 사이버 공격 전략과 능력

1. 북한의 사이버 공격 전략

2013년 북한의 사이버 전략에 대해 김정은은 "사이버전이 핵, 미사일과 함께 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"이라며 사이버 전의 중요성을 강조하였다.[26] 북한이 사이버를 군사 전략으로 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.[27] 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.[28]

당시 김정일은 "지금까지 전쟁이 총알전쟁, 기름전쟁이었다면 21세기 전쟁은 정보전"이라고 언급하며, "적의 군사정보를 얼마나 강력하게 제어하고, 자신의 정보력을 충분히 구사할 수 있는지가 전쟁의 승패가 좌우한다"고 강조했다.[29] 이를 통해 북한은 사이버 테러가 자본주의 나라에서 사람들에게 불안과 공포를 주는 파괴 무기가 되었다며, 사이버 공간에서의 위협과 공격에 관심을 갖기 시작하였다.[30]

1995년 당시 100여 명 수준의 '중앙당 35호실 기초자료조사실'을 설비하여 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.[31]

---

[26] 황지환, "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산," 『동서연구』, 제29권 제1호 (2017), p. 142.
[27] 위의 글, p. 149.
[28] 신충근 · 이상진, "북한의 대남 사이버테러 전략 분석 및 대응 방안에 관한 고찰," 『경찰학연구』, 제13권 제4호 (2013), p. 206.
[29] 김흥광, "북한의 정보전 전략과 사이버 전력: 돈 없는 북한의 최후의 선택 사이버 전쟁," 『월간조선』, 2011.6.
[30] 황지환, "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산," p. 142.

북한의 사이버 공격 능력은 2009년 2월 해외·대남 정보기구인 '정찰총국'(RGB: Reconnaissance General Bureau)의 등장으로 크게 발전하였다. 정찰총국은 대남 무력 도발과 간첩 남파 그리고 해외 공작 등을 총괄하기 위해 인민무력부 산하 '정찰국'과 대남간첩 침투 등을 관리하는 조선노동당 산하 '작전부' 그리고 해외정보 수집을 담당하는 '35호실' 등을 통합해 만들었다. 해킹, 사이버 공격, 사이버상의 간첩 활동 등 그동안 북한의 사이버 공격은 정찰총국이 담당하는 것으로 알려져 있다.[32]

정찰총국의 활동 부서는 총 6국(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.[33]

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 금융 분야 공격을 주도하는 '라자루스'는 2007년 초 설립되었으며, 2014년 소니픽쳐스 엔터테인먼트사 해킹과 2017년 워너크라이 랜섬웨어 사건, 국제 금융기관에 대한 해킹의 배후로 지목된 기관이다.[34] 다음은 라자루스의 하위 그룹으로 알려진 '블루노르프'와 '안다니엘'도 국제 금융기관, 카지노, 금융거래 소프트웨어 개발, 그리고 암호화폐 등 불법적인 금전적 수입을 확충하는 데 특화

---

31 김진광, "북한의 사이버조직 관련 정보 연구: 조직 현황 및 주요 공격사례 중심으로," 『한국컴퓨터학정보학회』, 제28권 제2호 (2020), p. 113.

32 조해수·유지만, "북한 해킹 그룹 김수키·라자루스·스카크러프트·안다리엘," 『시사저널』, 2021.6.18., 〈https://www.sisajournal.com/news/articleView.html?idxno=218951〉 (검색일: 2023.5.17.).

33 Steve Sin, "Cyber Threat Posed by North Korea and China To South Korea and US Forces Korea," SCRIBD, May 2009, 〈http://www.scribd.com/doc/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US- Forces-Korea〉 (Accessed March 6, 2023).

34 김보미·오일석, "김정은 시대 북한의 사이버 위협과 주요국 대응," p. 7.

된 조직으로 알려졌다.[35] '블루노르프'는 2016년 방글라데시 중앙은행을 대상으로 벌어진 8,100만 달러 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 동일조직으로 추정하고 있다.[36]

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.[37] 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.

정찰총국과 함께 북한의 사이버 활동의 또 다른 축은 조선인민군 총참모부로 알려졌다.[38] 총참모부는 정찰총국처럼 직접적인 사이버 공격을 수행하지는 않지만, 군사작전을 지원하기 위해 총참모부 산하 '지휘자동화국'은 해킹 및 통신 프로그램 개발을 담당하는 기구로서 31소는 '멀웨어'(malware) 개발을 맡고 있고, 32소는 군사용 소프트웨어 개발을 담당하고, 56소는 군사 지휘 통제 소프트웨어를 담당하고 있는 것으로 알려졌다.[39]

이외에도 조선노동당 통일전선부는 2012년 대남간첩공작을 담당하는 225국을 흡수하여 외곽기구인 조국평화통일위원회(조평통) 웹사이트인 '구국전선'과 '우리민족끼리'를 운영하면서 북한 체제를 홍보하고 대남 심리전을 담당하고 있는 것으로 알려졌다.[40] 이는 북한이 전통적인 대남 심리전을 사이버 영역에서 더욱 강화하려는 것으로 「로동신문」과 「조선중앙통신」을 온라인화하여 사이버 영역에서 선전전을 강화하는 것도 같은 맥락이라고 볼 수 있다.[41]

---

35 조해수·유지만, "북한 해킹 그룹 김수키·라자루스·스카크러프트·안다리엘."
36 위의 글.
37 이승열, "북한 사이버테러 위협의 증가와 대응방안," p. 2.
38 황지환, "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산," p. 147.
39 위의 글, p. 148.
40 엄응용·김효진, "북한의 대남 사이버공격에 대한 대비전력," 『한국경찰연구』, 제17권 제2호 (2018), p. 159.
41 황지환, "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산," p. 148.

2. 북한의 사이버 공격 능력

북한의 사이버 공격은 핵과 미사일 능력과 함께 대표적인 '비대칭전략'(asymmetric strategies)으로서 새로운 안보 위협으로 평가되고 있다.[42] 이에 주요국들이 북한의 사이버 능력을 어느 수준으로 평가하는지를 살펴보는 것은 중요한 일이다. 먼저 영국의 국제전략연구소(IISS: The International Institute for Strategic Studies)는 북한의 사이버 능력을 최하위인 3그룹(Thrid-tier)에 속한다고 평가절하했다.[43] 무엇보다 북한의 사이버 인프라와 보안 수준이 세계 최하위이며, 세계 인터넷망과 연결하는 '게이트웨이'가 중국과 러시아 서비스 제공업체에 전적으로 의존하여 외부의 공격에 취약하다고 밝혔다.[44]

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.[45]

미국의 민간연구 단체인 '외교협회'(CFR: Council on Foreign Relations)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 · Gordon M. Goldstein 2022). 이 보고서에 따르면, 2005년부터 2021년까지 미국을 상대로

---

[42] 이승열, "북한 사이버 공격의 현황과 쟁점," (국회입법조사처 이슈와논점 제2034호, 2022.12.28.), p. 1, 〈https://www.nars.go.kr/report/view.do?page=1&cmsCode=CM0043&categoryId=&searchType=NM&searchKeyword=%EC%9D%B4%EC%8A%B9%EC%97%B4&brdSeq=41005〉 (검색일: 2023.4.20.).

[43] 김보미 · 오일석, "김정은 시대 북한의 사이버 위협과 주요국 대응," (국가안보전략연구원 INSS 전략보고 제147호, 2021.11.6.), p. 5, 〈https://inss.re.kr/publication/bbs/js_view.do?nttId=410208〉 (검색일: 2023.4.20.); The International Institute for Strategic Studies. "Cyber Capabilities and National Power: A Net Assessment," IISS, February, 2019), p. 125, 〈https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power〉 (검색일: 2023.4.20.).

[44] 김보미 · 오일석, 위의 글, p. 5.

[45] 오택성, "MS 북한 사이버 공격 세계 4번째…개인정보 탈취 집중," 『VOA』, 2021.10.6., 〈http://www.voakorea.com/korea/korea-politics/microsoft-report-analyzed-nsns〉 (검색일: 2021.7.1.).

한 사이버 공격은 중국이 156건으로 가장 많았고, 다음은 러시아가 110건, 그리고 이란이 55건, 북한은 54건이라고 주장했다.[46]

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 금융 부문에서는 전 세계 1위를 기록했다고 밝혔다.[47] 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.[48]

결과적으로 이상의 논의를 통해 볼 때, 북한의 사이버 능력의 불균형이 매우 크다고 볼 수 있다. 즉, 사이버 공격 능력은 강하지만 이에 대응해서 국내 사이버 인프라의 취약성으로 인해 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.

Ⅳ. 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

---

46 Adam Sagal · Gordon M. Goldstein, "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet," (CFR Independent Task Force Report No 80, July 2022), 〈https://www.cfr.org/report/confronting-reality-in-cyberspace〉 (Accessed April 21, 2023.).

47 Julia Voo · Irfan Hemani · Daniel Cassidy, "National Cyber Power Index 2022," September 2022., p. 13, 〈https://www.belfercenter.org/publication/national-cyber-power-index-2022〉 (Accessed December 11, 2022).

48 *Ibid.*, pp. 10~12.

사이버 공격으로 정부기관을 비롯한 68개 주요 포털사이트가 장애를 일으켰다.[49] 북한은 2011년 3월 4일 또다시 정부기관과 금융기관 그리고 플랫폼 기업 등 총 40개의 인터넷 사이트를 대상으로 디도스 공격을 감행하였다. 그리고 동년 4월 12일에는 농협의 금융전산시스템에 대한 사이버 공격으로 273대가 전산 장애를 일으켰다. 그리고 2013년 3월 20일에 북한은 KBS, MBC, YTN과 신한은행, 농협, 제주은행 등에 대해 사이버 공격을 감행하였고, 6월 25일에는 정부기관, 언론사 등 69개 기관에 대하여 사이버 공격을 감행하여 총 155대 서버를 파괴하였고, 해당 웹사이트에 대한 접속 장애를 일으켰다.[50]

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 다운되었고 김정은 국무위원장을 암살하는 내용을 담은 영화 '인터뷰'의 사전 유출로 1천억 원대의 손실이 발생했다. 북한은 2015년 10월 서울 지하철 1-4호선 서버를 해킹하였고, 2015년 10월 20일에는 청와대, 국회, 외교부, 국방부, 통일부 등 정부기관에 대한 해킹을 또다시 시도하였다. 그리고 2016년 1월 6일 4차 핵실험 직후 북한은 청와대와 국회 등 정부기관을 사칭한 악성코드가 내장된 이메일을 대량으로 유포하였다. 유포된 이메일이 2014년 말 한수원 해킹 사건과 동일한 중국 랴오닝성의 IP임이 밝혀져 북한의 소행으로 최종 확인되었다.

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.[51] 이를 위해 북한은 해외 금융기관에 대한 공격과 랜섬웨어 공격 그리고 가상화폐거래소에 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. 최초의 공격 대상이었던 영

---

49 이승열, "북한 사이버테러 위협의 증가와 대응방안," p. 2.
50 위의 글, pp. 2~3.
51 송태은, "북한의 사이버 공격과 우리의 대응," p. 2.

국의 국가보건의료서비스(NHS) 산하 병원에서는 환자의 수술 일정을 재조정하거나 응급실 혼란으로 퇴원 조치를 취하는 등 심각한 부작용이 있었다고 보고했다.[52] 무엇보다 북한의 공격은 아주 단기간에 피해가 광범위하게 발생하였고, 주요 강대국들이 예외 없이 공격을 받았다는 점에서 심각성을 일깨워주었다.[53]

또한 북한이 가상화폐 해킹의 주범으로 주목을 받기 시작한 시기는 2017년 2월 국내 가상화폐거래소인 '빗썸'에 대한 700만 달러 해킹의 배후로 북한이 지목되면서부터다. 빗썸은 북한의 사이버 공격으로 네 번에 걸쳐 6,500만 달러(약 792억 원)를 피해를 봤다고 한다.[54] 북한은 빗썸 이외에도 2019년 11월에는 '업비트'를 공격해 이더리움 560억의 손실을 끼친 것으로 전해지고 있다.[55]

북한은 국내뿐만 아니라 2020년 9월 슬로바키아의 가상화폐거래소에 침입하여 약 540만 달러의 가상화폐를 해킹하였으며, 202년 3월에는 블록체인 기반 게임업체인 '액시 인피니티(Axie Infinity)를 상대로 감행한 해킹으로 역대 최대 규모인 약 6억1,500만 달러라는 손실을 기록한 것으로 확인되었다.[56]

2022년 3월 1일 공개된 유엔안보리 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 가상화폐거래소에서 약 5,000만 달러 가치의 가상화폐를 훔쳤다고 밝혔다.[57]

또한 전문가패널보고서는 미국의 블록체인 분석기업인 '체이널리시스'(Chainalysis)의 평가를 인용하면서 북한이 2021년 한 해 동안 가상화폐거래소뿐만 아니라 투자회사 등에 대한 총 7번의 사이버 공격으로 약 4억 달러 가치의 가상화폐를 훔쳤다고 밝혔다.[58] 이와 함께 미국 연방수사국(FBI)도 2022년 3월

---

52 장노순, "랜섬웨어와 북한의 사이버위협," (제주평화연구원 JPI PeaceNet 2017-48호, 2017. 8.2.), 〈http://jpi.or.kr/wp-content/uploads/2021/07/pn201748.pdf〉 (검색일: 2023.4. 22.).

53 위의 글.

54 정효식, "한국만 北에 암호화폐 10번 털렸다…빗썸 6500만 달러 피해," 『중앙일보』, 2019.8.13., 〈https://www.joongang.co.kr/article/23551061〉 (검색일: 2023.4.8.).

55 "북한, 해킹으로 가상화폐 3500억 원 훔쳐," BBC NEWS KOREA, 2021.7.5., 〈https://www.bbc.com/korean/news-57663787〉 (검색일: 2023.4.6.).

56 김보미, "북한의 암호화폐 공격과 미국의 대응," (국가안보전략연구원 INSS 전략보고 191호, 2022.11.25.), p. 5, 〈http://www.inss.re.kr/publication/bbs/js_view.do?nttId=410585〉 (검색일: 2023.4.24.).

57 United Nations Security Council, S/2022/132, March 1, 2022, 〈http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf〉 (Accessed April 29, 2023).

발생한 게임업체 '액시 인피니티'(Axie Infinity)의 가상화폐 해킹 배후에 북한의 '라자루스'가 탈취 사건에 책임이 있음을 확인했다고 밝혔다.[59] 2009년 이후 현재까지 북한의 사이버 공격 사례의 변화는 아래 [표 1]과 같다.

〈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 가상화폐거래소 공격 700만 달러 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 3,100만 달러 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 6억 달러 가상화폐 탈취

자료: 이승열, "북한 사이버 공격의 현황과 쟁점," (국회입법조사처 이슈와 논점 제2034호, 2022.12.28.).

58 *Ibid.*

59 J. Tidy, "7400억원 규모 암호화폐 게임 해킹 배후에 북한 해커," BBC NEWS KOREA, 2022.7.5., 〈https://www.bbc.com/korean/international-61118634〉 (검색일: 2023.4.23.).

2. 북한의 사이버 공격 전략 변화의 원인

한미 양국은 북한이 2022년 한 해 동안 탈취한 가상화폐를 금액이 약 1조7천억 원 이상이라고 밝혔다.[60] 무엇보다 북한이 국제사회의 대북제재와 코로나19로 인한 국경봉쇄의 장기화로 경제적으로 매우 어려워진 상황에서 2022년 40여 회 이상의 미사일 도발을 할 수 있었던 이유가 가상화폐 탈취를 통한 외화벌이에 성공했기 때문이라는 분석이다.

알레한드르 마요르카스(Alejandro Mayorkas) 미 국토안보부 장관은 2022년 10월 18일 싱가포르에서 열린 행상에서 "북한이 지난 2년 동안 10억 달러가 넘는 암호화폐와 경화의 사이버 탈취를 통해 대량살상무기 프로그램을 지원했다고 밝혔다.[61] 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.[62]

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' 전략에 따른 유엔안보리(UNSC)와 미국의 대북제재로 김정은과 핵심 엘리트 집단의 외화 부족 사태, 즉 통치자금 고갈이 가장 중요한 원인이었다.[63]

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

---

60 김은중, "北, 코인 해킹한 돈으로 미사일 쐈다…올해만 1조7000억원 탈취," 『조선일보』 2022.11.7., 〈https://www.chosun.com/politics/diplomacy-defense/2022/11/07/XBBCXVHCJ5BJPOQ4KLV3LKQCHQ/〉 (검색일: 2023.2.22.).

61 박형주, "미 국토안보장관, 북한, 암호화폐 등 10억달러 이상 탈취…WMD 자금 조달," 『VOA』, 2022.10.19. 〈https://www.voakorea.com/a/6795295.html〉 (검색일: 2023.2.23.).

62 J. Anderson, "뉴버거 백악관 부보좌관, "북, 사이버 활동으로 미사일 개발자금 3분의 1 충당"," 『rfa』, 2022.7.28., 〈https://www.rfa.org/korean/in_focus/nkhacker-07282022165047.html〉 (검색일: 2023.2.23.).

63 이승열, "북한 사이버테러 위협의 증가와 대응방안," p. 3.

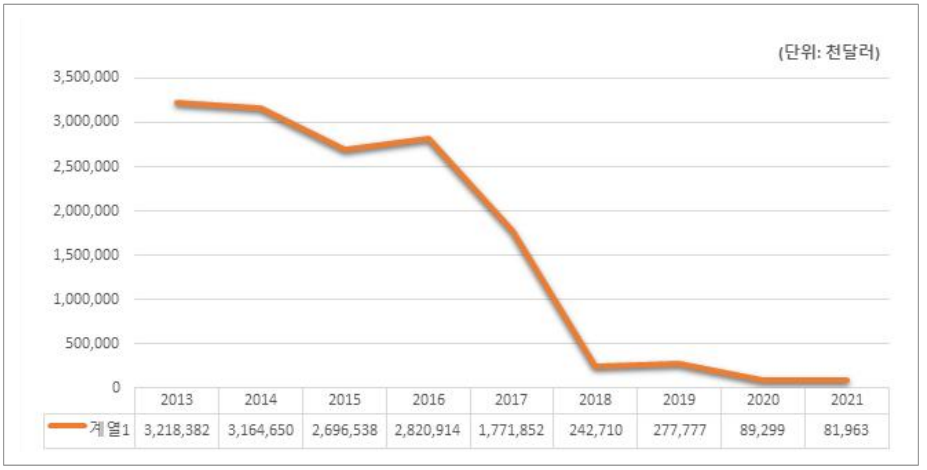
유엔안보리는 2006년 10월 북한의 제1차 핵실험으로 채택된 결의안 1718호를 근거로 안보리 15개국으로 구성된 '대북제재위원회'를 구성하였다. 그 내용으로 보면 제1차 핵실험 이후 채택된 4번의 대북제재(1718호, 1874호, 2087호, 2094호)는 대량살상무기(WMD) 이전 통제에 초점을 맞춘 제재였지만, 2016년 4차 핵실험 이후 채택된 6번의 대북제재(2270호, 2321호, 2356호, 2371호, 2375호, 2397호)는 북한 경제 일반에 대한 포괄적 제재로 북한의 수출입을 비롯한 경제 분야의 전면적인 금수조치였다.

유엔안보리의 대북제재가 효과를 발휘한 것은 바로 미국의 독자제재가 어느 때보다 강력했기 때문이다. 미국은 2016년 북한의 4차 핵실험 이후 유엔안보리의 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.[64]

그 결과 북한 김정은 통치자금의 주 수입원인 수출이 급락하였다. 대북제재가 본격화되기 전인 2016년 북한의 대외 수출은 28억2천만 달러였지만 2021년에는 8천1백만 달러로 2016년 대비 약 97%까지 추락하면서 사실상 수출로 인한 외화벌이 사업이 파산했다고 볼 수 있다. 여기에 더해 2020년 초부터 시작된 코로나19(COVID-19)로 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 아래 〈그림 1〉과 같다.

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

〈그림 1〉 북한의 수출량 감소 현황



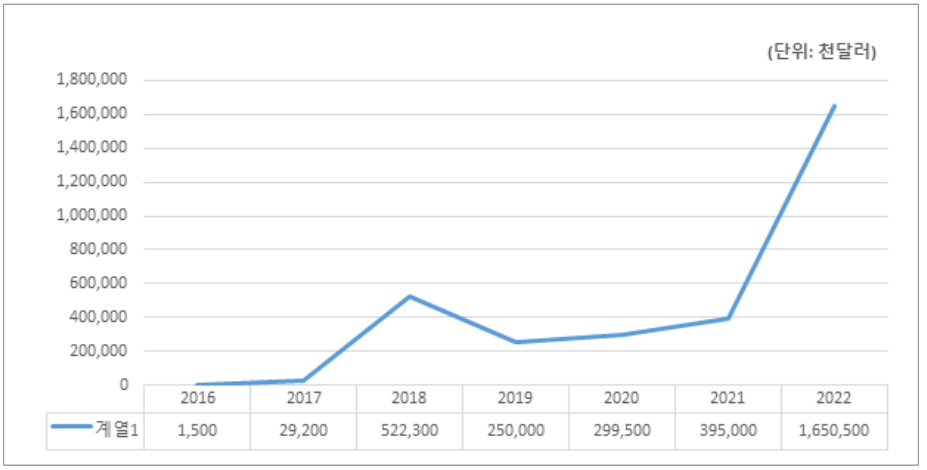
자료: 통계청 〈https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_1ZGA92&conn_path=I2〉

대북제재의 효과는 북한 최고 지도부에 외화부족 사태를 일으켰으며 이로 인해 북한은 전세계 금융기관과 암호화폐거래소에 대한 사이버 공격을 부족한 외화벌이 수단으로 활용하기 시작했다. 특히 2016년 2월 방글라데시 중앙은행 뉴욕연준 계좌에서 총 9억5,100만 달러 금액을 인출하려다 8,100만 달러에 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 150만 달러에서 출발하여 2018년에는 5억2,230만 달러, 2022년에는 16억5,050만 달러(약 2조300억원)의 가상화폐를 훔쳤다고 밝혔다. 이는 지난해 전세계에서 도난당한 가상화폐 38억 달러의 약 43%에 해당하는 금액이다.[65] 북한의 사이버 공격을 통한 외화벌이 총액은 수출감소 현황과 반대로 2021-2022년 급격히 높아졌음을 알 수 있다. 2016년 이후 북한의 사이버 공격을 통한 외화벌이 현황은 아래 〈그림 2〉와 같다.

65 신진우 · 고도예, "美, 北이 탈취한 가상화폐 역해킹, 작년 절반이상 회수… 1조원 달해," 『동아일보』, 2023.2.4., 〈https://www.donga.com/news/Politics/article/all/20230204/117729669/1〉 (검색일: 2023.4.24.).

〈그림 2〉 북한의 사이버 공격을 통한 외화벌이 현황



자료: 체이널리시스 〈https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/〉

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 약 5억6,000만 달러(7,200억원)을 쏟아부은 것이다.[66] 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 대외 무역이 막힌 현시점에서 북한의 유일한 소득원은 사이버 공격을 통한 금융자산 탈취 외에는 방법이 없기에 국제사회의 우려가 현실로 나타나고 있다고 볼 수 있다.

66 정진우, "7200억 '미사일 폭주' 약발 다했다…10살 김주애 내민 北딜레마," 『중앙일보』, 2023. 2.21., 〈https://www.joongang.co.kr/article/25141995#home〉 (검색일: 2023.4.24.).

V. 북한의 사이버 공격에 대한 국제사회와 한국의 대응 방안

1. 국제사회의 대응 방안

북한의 핵과 미사일 위협에 대한 유엔안보리의 '대북제재위원회'가 '플랫폼'(platform) 역할을 하는 것과는 달리 북한의 사이버 공격에 대해 국제사회의 '국제공조체제'는 아직 확고하게 구축되어 있지 않은 상태다. 다만 사이버 작업에 적용할 수 있는 국제법에 관한 『탈린매뉴얼 2.0』 등이 논의되고 있다.[67] 그러나 2017년 5월 150여 개국의 컴퓨터를 감염시킨 북한의 '워너크라이 랜섬웨어' 공격은 북한의 사이버 공격을 국제사회의 안보 이슈로 부각시킨 대표적인 사건으로서, 이후 관련국 간의 다자간 협력체제가 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.[68] 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 있다는데 인식을 같이하고 유럽, 중동, 아프리카, 아시아 등 35개국과의 국제적 협력 방안을 담은 공동성명을 발표하였다.[69] 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.[70]

미국은 북한의 가상화폐 해킹을 핵과 미사일 자금 마련을 차단하기 위한 대북제재의 영역으로 확대하고 있다. 미국은 북한의 사이버 공격이 핵과 미사일 개발 및

---

67 Michael N. Schmitt, 국가보안기술연구소 옮김, 『탈린매뉴얼 2.0』 (서울: 박영사, 2018), pp. 1~7.

68 Office of the Director of National Intelligence, "2021 Annual Threat Assessment of the U.S. Intelligence Community," April 13, 2021, 〈 https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2204-2021-annual-threat-assessment-of-the-u-s-intelligence-community〉 (Accessed July 1, 2022).

69 박형주, "바이든 '사이버 안보' 강조…북한, 올해 '전방위 사이버 활동' 전개," 『VOA』, 2021.12.29., 〈https://www.voakorea.com/a/6373229.html〉 (검색일: 2023.6.2.).

70 김보미 · 오일석, "김정은 시대 북한의 사이버 위협과 주요국 대응," p. 24.

실험 자금으로 활용되고 있다고 보고 있으며, 중국과 러시아의 협력이 필요한 유엔안보리를 통한 방식이 아닌 독자제재를 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 가상화폐거래소에 대해 13억 달러(약 1조4,000억원) 규모의 현금과 가상화폐 절취를 목적으로 사이버 공격을 시도한 혐의로 북한 정찰총국 소속 해커 전창혁·김일·박진혁 등을 기소하였다(박현영 2021).[71]

미 재무부는 2022년 8월 북한이 사이버 해킹으로 탈취한 4억5,500만 달러의 가상화폐에 대한 세탁에 가담한 믹서(mixer)기업(가상화폐를 쪼개 누가 전송했는지 알 수 없도록 만드는 기술을 보유한 돈세탁 기업)인 '토네이도캐시'(Tornade Cash)를 제재 대상에 올렸다.[72] 이외에도 미국은 북한의 암호화폐 공격에 대응하여 법무부와 국무부 내에 사이버 범죄 전담부서를 신설하였고, 연방수사국(FBI)과 재무부는 북한 해킹그룹인 '라자루스'의 위협을 경고하는 부처 합동 주의보를 발령하여 경각심을 높이고 있다.[73]

더 나아가 미국은 북한의 가상화폐 탈취 자금에 대한 환수도 적극적으로 추진하고 있다. 북한의 가상화폐 해킹 수법은 투자자들이 가상화폐를 임시 저장하는 '크로스체인 브리지'(crosschain bridge)을 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.[74]

---

71 박현영, "미국 북한 해커, 총 대신 키보드로 가상지갑 턴 세계의 강도," 『중앙일보』, 2021.2.19., 〈http://news.joins.com/article/23995352〉 (검색일: 2022.2.28.).

72 김은중, "北, 코인 해킹한 돈으로 미사일 쐈다…올해만 1조7000억원 탈취," 『조선일보』, 2022.11.7.

73 박형주, "미 국토안보장관, 북한, 암호화폐 등 10억달러 이상 탈취…WMD 자금 조달," 『VOA』, 2022.10.19.

74 신진우·고도예, "美, 北이 탈취한 가상화폐 역해킹, 작년 절반 이상 회수… 1조 원 달해," 『동아일보』, 2023.2.4.

마지막으로 미국은 사이버 보안과 관련한 법적 토대를 강화하였다. 미국은 지난 1984년 「컴퓨터사기 남용법」(Computer Fraud and Abuse Act) 제정을 시작으로 사이버안보에 관한 강력한 법적 토대를 갖추고 있다. 주요 법률은 「1985년 통일영업비밀법」 (Uniform Trade Secrets Act of 1985), 「1996년 경제스파이법」 (Economic Espionage Act of 1996), 「2012년 영업비밀침해 석명법」 (Theft of Trade Secrets Clarification Act of 2012), 「2013년 경제스파이처벌 강화법」 (Penalty Enhancement Act of 2013), 「2016년 사이버정보공유 및 보호법」 (Cyber Intelligence Sharing and Protection Act of 2016) 등이 있다.[75]

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)을 서명하였다.[76] 주로 랜섬웨어 공격에 따라 주요 인프라 기업이 사이버 공격을 받았다고 인식한 시점부터 72시간 이내에 미 국토안보부의 사이버 보안 및 인프라 보안국 (Cybersecurity and Infrastructure Security Agency: CISA)에 보고해야 한다는 내용이다.[77] 이를 통해 미국은 국내 주요 기관(국가기관, 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 유엔안보리(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 유엔안보리 차원의 대북제재와 같은 강력한 조치가 이뤄질 필요가 있으며, 이에 북한 사이버 공격에 대한 국제사회의 협력이 어느 때보다 중요하

---

75 한희원, "미국 경제간첩법에 대한 소고: 법리적 이해와 운용을 중심으로," 『형사법의 신동향』, 제34호 (2012), pp. 162~192.

76 정민정, "바이든 대통령 사이버보안 강화법 서명의 의미와 시사점," (국회입법조사처 이슈와논점 제1937호, 2022.4.13.), p. 1, 〈https://www.nars.go.kr/report/view.do?categoryId=&cmsCode=CM0043&searchType=NM&searchKeyword=%EC%A0%95%EB%AF%BC%EC%A0%95&brdSeq=38714〉. (검색일: 2023.4.24.).

77 위의 글, p. 3.

다. 다만 북한 외에 세계 최고의 사이버 공격 능력을 보유한 러시아와 중국을 설득하는 것이 필요하다.

2. 한국의 대응 방안

한국은 북한의 사이버 공격에 주 대상이다. 그러나 북한의 증가하는 사이버 위협에 대한 우리 정부의 대응 능력에 대한 문제점이 지속적으로 지적되었으며, 관련법 제정을 비롯해 제재 능력, 정보공유, 국제공조 등에 대해 보완이 필요하다는 주장도 함께 제기되어 왔다. 지난 2022년 5월 21일 한미정상회담에서 양국 정상은 사이버 안보와 관련한 협력을 강화하기로 합의하였다. 이에 대한 후속 조치로서 랜섬웨어 공격을 대처하기 위해 법 집행 및 기관 간의 협력을 강화하는 데 중점을 둔 사이버 '워킹그룹'(working group)을 설립하기로 합의하였다. 그리고 2022년 11월 한미 양국은 북한 가상화폐 탈취 대응을 위한 공동 심포지엄을 개최하여 북한 가상화폐 탈취 문제의 심각성을 재조명하였다. 이 자리에서는 북한에 의해 탈취된 가상화폐가 핵·미사일 개발자금으로 전용되고 있는 현실에서 이를 방지하기 위한 민관의 협력과 국제공조의 필요성을 논의하였다(외교부 2022).[78]

한국 정부는 지난 2023년 2월 10일 불법 사이버 활동을 통해 북한의 핵과 미사일 개발자금을 조달하는 개인 4명과 기관 7개를 처음으로 독자제재 대상으로 지정했다. 이것은 한국 정부의 첫 사이버 분야 대북제재 조치라는 점에서 의미가 있다고 볼 수 있다. 이날 제재 대상에 오른 해킹 관련 기관은 라자루스 그룹, 블루노로프, 안다니엘, 조선엑스포합영회사, 기술정찰국, 110호연구소, 지휘자동화대학(미림대학)이다. 앞의 6개 그룹은 모두 정찰총국 산하 조직으로 기관해킹 및 가상자산 탈취와 같은 사이버 공격을 주도한 그룹이며, 미림대학은 사이버 전문 인력을 양성하는 기관이다.[79]

또한 정부는 4명의 해커를 제재 리스트에 올렸는데, 이중 가장 악명 높은 인물은 박진혁이다. 2014년 '소니 픽쳐스사' 해킹과 2017년 '워너크라이 랜섬웨어' 공격을 시도했던 인물로 알려졌다. 이미 미 법무부는 2018년 박진혁을 북한 해커로서

---

78 외교부, "북한 암호화폐 탈취 대응 한미 공동 민관 심포지엄 개최 보도자료," (외교부 보도자료, 2022.11.17.), 〈https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=373025〉 (검색일: 2023.5.24.).

79 박현주, "한, 악명높은 라자루스·박진혁 때렸다…북사이버 첫 독자제재," 『중앙일보』, 2023.2.10., 〈https://www.joongang.co.kr/article/25139694#home〉 (검색일: 2023.5.20.).

신병을 확보하지 않은 상태에서 기소하였다. 이외에도 조명래, 송림, 오충성 등이 함께 제재 리스트에 올랐다.

한국은 사이버 보안 능력과 관련하여 법, 기술, 조직, 역량개발, 협력의 5개 영역을 평가하는 국제전기통신연합(ITU: International Telecommunication Union)의 '글로벌사이버보안지수'(GCI: Global Cybersecurity Index)에서 4위를 기록할 만큼 높은 수준의 사이버 보안 체계를 갖추고 있다. 하지만 문제는 사이버 위기대응 체계가 국방, 공공, 민간 등 각 영역으로 나뉘어 분절적인 체계를 갖추고 있다는 점이다.[80]

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.[81] 이와 같은 입법체계의 분절성과 상이성으로 인해 북한의 사이버 공격에 실질적이고 효율적인 대응이 어려운 한계가 있다.

지난 2020년 9월 국가정보원이 국회 정보위원회에 보고한 내용에 따르면, 지난 5년간(2015.1-2020.6) 공공기관에서 발생한 사이버 공격 피해는 11,727건으로 약 70-80%가 북한의 사이버 공격이라고 밝혔다(김당 2022).[82] 하지만 공공분야에 대한 사이버 공격은 2015년을 정점으로 줄어들고 있지만, 금융기관 및 가상화폐 거래소 등 민간분야에 대한 북한의 사이버 공격은 오히려 증가하고 있다고 밝혔다.[83]

가장 큰 이유는 공공분야의 경우 「국가사이버안전관리규정」에 따라 '국가사이버안전센터'가 '컨트롤타워'(control tower)의 역할을 하고 있지만, 민간에 대한 사이버보안 의무를 강제하는 법적 기반은 아직 제대로 체계를 갖추지 못했기 때문이다.[84] 국정원은 이러한 법적 미비를 개선하기 위해 2022년 11월부터 민관 합동 '국가사이버안보협력센터'를 개소하였다.

---

80 송태은, "북한의 사이버 공격과 우리의 대응," pp. 2~3.

81 김윤영·양철호, "북한의 사이버테러에 대비한 법·제도 개선 방안," 『유럽헌법연구』, 제33호 (2020), p. 375.

82 김당, "공공분야 사이버공격 1만1727건…북한발 70-80%," 『UPI뉴스』, 2022.10.16., 〈https://www.upinews.kr/newsView/upi202010160030〉 (검색일: 2023.5.1.)

83 위의 글.

84 최경호, "국경없는 사이버테러, 대한민국이 위험하다," 『월간중앙』, 2022.1.23., 〈https://www.joongang.co.kr/article/25042729〉 (검색일: 2023.5.5.).

그러나 북한의 사이버 공격이 공공과 민간의 영역을 가리지 않는 상황에서, 북한의 사이버 공격으로부터 국가기반시설을 보호하기 위해서는 보다 포괄적인 법적 기반과 함께 국가 사이버 안보 정책을 총괄하는 컨트롤타워를 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 안보 체계를 통괄할 수 있는 컨트롤타워 구축에 적극적으로 나설 필요가 있다.

둘째, 사이버 안보 관련 국제규범의 제정에 더욱 적극적으로 참여할 필요가 있다. 한국은 UNGGE 회의에서 기본적으로 사이버 공간은 피해국에게 일방적으로 불리한 구조이기 때문에 피해국에 유리한 방향으로 국제법의 해석과 규범의 창출이 필요하다는 입장이다. 이러한 입장의 이면에는 한국의 주 관심사가 북한의 사이버 공격을 막고 북한의 공격의 주된 경유국인 중국의 협조를 확보하는 데 있기 때문이다. 이를 위해서는 국제법의 적용에 있어서 피해국의 권리를 보장하기 위해 국제법의 상세화가 필요하다.[85] 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.[86] 사이버 공간의 특성상 사이버 공격의 발원지를 찾아 특정 국가나 단체에 귀속시키기에 어려움이 따르기 때문에 사이버 공격의 주체와 상관없이 피해를 최소화하기 위해 회복력 중심의 연구개발이 수행되어야 한다. 또한 국내에서 국가기관과 민간기관의 사이버 공격에 대한 위협 정보공유를 의무화하여 사이버 위협을 조기에 탐지하는 방안을 마련할 필요가 있다.

---

85 김상배, "사이버 안보의 국제규범과 한국외교: 주요국 이해갈등의 프레임 경쟁 사이에서," p. 18.
86 정민경·임종인·권헌영, "북한의 사이버공격과 대응방안에 대한 연구," p. 75.

Ⅵ. 나가며

백악관의 사이버 부국장 켐바 월든(Kemba Walden)과 NSC 사이버 담당 부국장인 앤 뉴버거(Anne Neuberger)는 2023년 3월 2일 바이든 행정부의 국가 사이버 전략(National Cyber Strategy)을 발표하면서, 북한과 함께 중국, 러시아 그리고 이란을 사이버 적성국으로 규정하고 모든 역량을 동원해 관련 단체들을 파괴하고 분쇄하겠다고 밝혔다.[87] 특히 북한이 핵무력 완성을 위해 가상화폐 탈취와 랜섬웨어 공격을 통해 수익을 창출하면서 불법적인 사이버 활동을 벌이고 있다며 강력한 대응을 밝혔다.

북한의 사이버 공격이 국제 금융질서를 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 16억5,000만 달러로 동년 전 세계에서 일어난 가상화폐 해킹 규모인 38억 달러의 절반에 이른다고 분석했다. 국제사회의 대북제재로 인해 북한의 주요 외화 소득원인 수출이 97% 이상 줄어든 상황에서 가상화폐 해킹을 통한 외화벌이는 대북제재를 통해 북한의 핵 야망을 무력화시키려는 미국의 계획을 위협하고 있다고 볼 수 있다.

한국 정부도 북한의 사이버 공격을 심각한 안보위협으로 인식하고, 북한의 핵고도화 능력이 진전되는 배경에는 사이버 공격을 통한 외화벌이가 매우 중요한 역할을 하고 있다고 인식하고 있다. 이에 한국 정부는 북한의 사이버 공격에 대한 첫 대북제재를 발표하는 등 이전과 달리 매우 적극적인 대응 방안을 모색하고 있다. 하지만 우리 정부의 노력과 관계없이 국제사회의 공통된 협력체계가 부재한 상황에서 개별 국가의 노력은 한계가 있을 수밖에 없다.

현재 강력한 효과를 발휘하고 있는 대북제재는 2006년 유엔안보리 산하 대북제재위원회의 플랫폼을 통해 총 10번의 유엔안보리 대북제재가 발효 중이며, 국제

87 White House, "Background Press Call by Senior Administration Officials Previewing the Biden-Harris Administration's National Cyber Strategy," March 2, 2023, 〈 https://www.whitehouse.gov/briefing-room/press-briefings/2023/03/02/background-press-call-by-senior-administration-officials-previewing-the-biden-harris-administrations-national-cyber-strategy/〉 (Accessed April 6, 2023).

사회의 강력한 규범력을 발휘하여 그동안 번번이 대북제재를 무력화시켰던 중국과 러시아도 현재의 대북제재 거버넌스의 영향력 아래에 있다고 볼 수 있다. 특히 2017년 미국의 '세컨더리 보이콧' 제재의 효과는 대북제재의 실효성을 높이는 중요한 역할을 하고 있다.

무엇보다 우리 정부는 미국과 함께 북한의 사이버 공격에 대한 대응 차원에서 국제적 제재 플랫폼을 구축하는 데 적극적으로 나설 필요가 있다. 최근 미국은 사이버 공격에 대해 단순히 방어하는 수준을 넘어 적극 선제적 공격을 주도하는 '컨트롤타워'를 마련하고, 사이버 적성국들의 네트워크에 침입해 서버를 마비시키는 등 공격적인 사이버 전략을 구사할 것을 예고하고 있다. 사실상 사이버 전쟁을 준비하고 있다.

국제적으로 사이버 전쟁에 적용하는 비공식 매뉴얼로써 2009년 에스토니아의 수도 탈린(Tallinn)에서 북대서양조약기구 사이버방어센터(NATO Cooperative Cyber Defence Center of Excellence)가 만든 '탈린 매뉴얼(Tallinn Manual)'이 있다. 지난 2014년 오바마 대통령이 소니픽쳐스사에 대한 사이버 공격의 주범으로 북한을 지목하고 "비례적으로(proportionally)" 대응할 뜻을 밝힌 것도 탈린 매뉴얼의 원칙에 따른 것이라고 볼 수도 있다. 따라서 세계 최고 수준의 정보통신 기술을 보유하고 있으면서 북한의 사이버 공격에 취약한 우리 정부도 사이버 안보에 대한 국제규범의 확립에 더 적극적으로 참여할 필요가 있다.

■ 제출: 4월 27일 ■ 심사: 5월 26일 ■ 채택: 6월 14일

참고문헌

1. 단행본

대한민국정부. 『국가사이버안보계획』. 관계부처 합동, 2019.
청와대 국가안보실. 『국가사이버안보전략』. 2019.
Schmitt, Micheal N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.
_____. 국가보안기술연구소 옮김. 『탈린매뉴얼 2.0』. 서울: 박영사, 2018.

2. 논문

김상배. "사이버 안보의 국제규범과 한국외교: 주요국 이해갈등의 프레임 경쟁 사이에서." 『사이버 안본의 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.
박노형·박주희. "제6차 UNGGE 보고서 채택과 국제사이법의 발전." 『국제법학회논총』. 제66권 제3호, 2021.
신충근·이상진. "북한의 대남 사이버테러 전략 분석 및 대응 방안에 관한 고찰." 『경찰학연구』. 제13권 제4호, 2013.
엄응용. "김정은 집권 10년, '우리식경제관리방법'의 성과와 정치경제적 함의." 『JNKS』. vol.7, no.2, 2021.
엄응용·김효진. "북한의 대남 사이버공격에 대한 대비전력." 『한국경찰연구』. 제17권 제2호, 2018.
정민경·임종인·권헌영. "북한의 사이버공격과 대응방안에 관한 연구." 『한국IT서비스학회지』. 제15권 제1호, 2016.
한희원. "미국 경제간첩법에 대한 소고: 법리적 이해와 운용을 중심으로." 『형사법의 신동향』. 제34호, 2012.
황지환. "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산." 『동서연구』. 제29권 제1호, 2017.

Nye Jr. Joseph S. "Nuclear Lesson for Cyber Security?" *Strategic Studies Quarterly*, vol. 5, no. 4, 2011.
_____. "Cyber Power," *Belfer Center for Science and International Affairs*, May 2010.
_____. "International Norms in Cyberspace," *Project Sindicate*, May 11, 2015.

3. 기타 자료

『동아일보』.
『시사저널』.
『조선일보』.
『중앙일보』.
『BBC NEWS KOREA』.
『rfa』.
『월간중앙』.
『월간조선』.
『UPI뉴스』.
『VOA』.
『YTN』.
DIGITAL INSIGHTS.
SCRIBD.

외교부 〈https://www.mofa.go.kr〉.
제20대 대통령실 〈https://www.korea.kr〉.
통계청 〈https://kosis.kr〉.
BELFER CENTER 〈https://www.belfercenter.org〉.
Chainalysis 〈https://blog.chainalysis.com〉.
Council of Europe 〈https://www.europarl.europa.eu〉.
Office of the Director of National Intelligence 〈https://www.dni.gov〉.
The International Institute for Strategic Studies. 〈https://www.iiss.org〉.
The White House 〈https://www.whitehouse.gov〉.
United Nations General Assembly 〈http://www.un.org〉.
United Nations Security Council 〈http://www.securitycouncilreport.org〉.

「국가사이버안전관리규정」 제2조 2항, 4항.

김보미. “북한의 암호화폐 공격과 미국의 대응,” 국가안보전략연구원 INSS 전략보고 191호, 2022.
김보미 · 오일석. “김정은 시대 북한의 사이버 위협과 주요국 대응.” 국가안보전략연구원 INSS전략보고 147호, 2021.
송태은. “북한의 사이버 공격과 우리의 대응,” 외교안보연구소 IFANSFOCUS IF2022-28K, 2022.
이승열. “북한 사이버테러 위협의 증가와 대응방안.” 국회입법조사처 이슈와논점 제1127호, 2016.
_____. “북한 사이버 공격의 현황과 쟁점.” 국회입법조사처 이슈와논점 제2034호, 2022.
장노순. “랜섬웨어와 북한의 사이버위협.” 제주평화연구원 JPI PeaceNet 2017-48호, 2017.
정민정. “바이든 대통령 사이버보안 강화법 서명의 의미와 시사점.” 국회입법조사처 이슈와논점 제1937, 2022.

Abstract

Evolution of North Korea's Cyberattack Strategy:
Cyber strategy as a means of earning foreign currency to evade sanctions against North Korea

Lee, Seungyeol

North Korea's cyber attack is emerging as a security issue in the international community. Starting in 2009, North Korea's cyber attacks have evolved from neutralizing the national backbone network and stealing information to earning foreign currency to evade sanctions against North Korea since 2016. Accordingly, the international community, including the United States, believes that North Korea is evading sanctions through attacks on financial assets and cryptocurrency, and is preparing funds for nuclear and missile-related developments, and is actively working to prevent this. Therefore, it is necessary for South Korea and the US authorities and the international community to identify North Korea's cyber capabilities and prepare concrete measures to establish international cooperation and response systems. In addition, the Korean government needs to enact a cyber-related basic law that can oversee cyber security-related tasks because the current presidential order, 「National Cyber Security Management Regulations」, for the establishment of an integrated public-private cyber security system has limitations.

Key Words: cyber atrack, DDoS, Lazarus, BlueNorOff, Andarial