The Journal of the Convergence on Culture Technology (JCCT)
Vol. 10, No. 4, pp.175-181, July 31, 2024. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2024.10.4.175

JCCT 2024-7-19

북한의 사이버 공격 변화 양상에 대한 연구

A Study on the Change of Cyber Attacks in North Korea

박찬영*, 김현식**

Chanyoung Park*, Hyeonsik Kim**

요 약 유엔 안전보장이사회 산하 대북제재위원회는 북한이 2017년부터 2023년까지 가상자산 관련 회사를 상대로 사이버 공격을 벌여 탈취한 금액이 약 4조원으로 추산하고 있다고 평가했다. 북한의 사이버 공격은 국제사회의 경제제재로 인한 외화확보가 제한되자 가상화폐 해킹으로 자금을 확보하고 있고, 방산업체에 대한 기술탈취의 형태도 보여주고 있으며 이렇게 확보하 자금은 김정은 정권유지와 핵·미사일 개발에 사용되고 있다. 2017년 9월 3일 북한이 제 6차 핵실험을 단행하고 같은 해 11월 29일 대륙간탄도미사일(ICBM) 발사를 계기로 국가 핵무력 완성을 선언하자 유엔은 대북제재를 가하였는데 이는 역사상 가장 강력한 경제제재로 평가된다. 이러한 경제적 어려운 상황에서 북한은 사이버 공격을 통해 위기를 극복하고자 하였는데 북한의 사이버 공격 사례를 통해 그 변화 양상을 분석한 결과 1기는 2009년~2016년까지로 전략적 목표로 국가 기간망 무력화와 정보 탈취를 통해 북한 스스로 사이버 능력을 검증 및 과시는 모습과 남한 내 사회혼란을 조성하려는 의도로 보여졌다. 2기는 2016년 대북제재로 외화벌이가 제한되자 가상화폐를 탈취하여 김정은 정권유지 및 핵·미사일 개발 고도화를 위한 자금확보의 모습을 보였다. 3기는 국내외 방산업체에 대한 기술해킹으로 2021년 8차 당대회에서 김정은 위원장이 제시한 전략무기 5대 과업 달성을 위한 핵심기술 탈취에 집중하는 모습을 보이고 있다. 북한의 사이버 공격에 대해 국가 차원에서 국가기관 뿐 아니라 민간업체에 대한 보안대책을 수립해야 될 것이고 이과 관련된 법령 제도, 기술적 문제, 예산 등에 대한 대책이 시급히다. 또한 화이트 해커와 같은 전문인력 양성 및 확보에 주력하여 날로 발전하고 있는 사이버 공격에 대응할 수 있도록 시스템 및 인력 구축이 필요하다.

주요어 : 사이버 공격, 해킹, 기술탈취, 북한

Abstract The U.N. Security Council's North Korea Sanctions Committee estimated that the amount of North Korea's cyberattacks on virtual asset-related companies from 2017 to 2023 was about 4 trillion won. North Korea's cyberattacks have secured funds through cryptocurrency hacking as it has been restricted from securing foreign currency due to economic sanctions by the international community, and it also shows the form of technology theft against defense companies, and illegal assets are being used to maintain the Kim Jong-un regime and develop nuclear and missile development. When North Korea conducted its sixth nuclear test on September 3, 2017, and declared the completion of its national nuclear armament following the launch of an intercontinental ballistic missile on November 29 of the same year, the U.N. imposed sanctions on North Korea, which are considered the strongest economic sanctions in history. In these difficult economic situations, North Korea tried to overcome the crisis through cyberattacks, but as a result of analyzing the changes through the North's cyber attack cases, the strategic goal from the first period from 2009 to 2016 was to verify and show off North Korea's cyber capabilities through the neutralization of the national network and the takeover of information, and was seen as an intention to create social chaos in South Korea. When foreign currency earnings were limited due to sanctions against North Korea in 2016, the second stage seized virtual currency and secured funds to maintain the Kim Jong-un regime and advance nuclear and missile development. The third stage is a technology hacking of domestic and foreign defense companies, focusing on taking over key technologies to achieve the five strategic weapons tasks proposed by Chairman Kim Jong-un at the 8th Party Congress in 2021. At the national level, security measures for private companies as well as state agencies should be established against North Korea's cyberattacks, and measures for legal systems, technical problems, and budgets related to science are urgently needed. It is also necessary to establish a system and manpower to respond to the ever-developing cyberattacks by focusing on cultivating and securing professional manpower such as white hackers.

Keywords : Cyber attacks, hacking, technology steal, North Korea

*정회원, 육군대학 소령 (제1저자)
**정회원, 육군3사관학교 정치외교학과 조교수 (교신저자)
접수일: 2024년 4월 19일, 수정완료일: 2024년 5월 20일
게재확정일: 2024년 6월 7일

Rececеived: Apil 19, 2024 / Revised: May 20, 2024
Accepted: June 7, 2024
**Corresponding Author: itsme1025@naver.com
Dept. of Chemical and Environmental sciences
Korea Army Academy at Yeongcheon, Korea

Ⅰ. 서 론

북한은 2017년 9월 3일 6차 핵실험을 단행하고 같은 해 11월 29일 대륙간탄도미사일(ICBM) 발사를 계기로 국가 핵무력 완성을 선언하였다. 이에 유엔은 안전보장이사회를 개최하여 대북제재를 가하였는데, 이는 역사상 가장 강력한 경제제재로 평가된다.

2018년 역사상 최초로 美·北 정상회담이 개최되어 트럼프 대통령과 김정은 위원장이 싱가포르와 베트남 하노이에서 비핵화 협상을 진행하였다. 양측은 빅딜(Big Deal)을 기대했지만 비핵화와 관련된 실질적인 성과가 없어 노딜(No Deal)로 끝나게 되었다. 이에 북한은 '강대강', '정면돌파'를 선언하였고 핵·미사일 고도화뿐만 아니라 2021년 8차 당대회에서 선언한 5대 전략무기 확보에 집중하는 모습을 보이고 있다. 유엔 안전보장이사회 산하 대북제재위원회는 북한이 2017년부터 2023년까지 사이버 공격으로 약 4조원의 가상자산을 탈취한 것으로 추산하고 있다. 수출입을 통한 외화벌이 수단이 막힌 북한은 대북제재를 회피하는 수단으로 사이버 공격을 택하였고, 추적이 어렵고 현금화가 용이한 가상자산을 타겟으로 하였다. 북한은 탈취한 불법적 자산을 핵무기와 탄도미사일 등 첨단무기 개발에 이용하고 있다고 대북제재위원회는 평가하였다. 또한, 북한은 국내·외 방산업체 해킹으로 핵심기술을 탈취하여 자력갱생과 비대칭 전략무기 개발에 집중하고 있으며, 극초음속 미사일 등 개발완료를 발표하는 등 경제제재임에도 불구하고 군사적 진보를 보이고 있는 것이 사실이다.

본 논문에서는 북한의 사이버 공격 양상의 변화과정과 전략적 목표는 무엇인지에 대해 주목하고자 한다. 먼저 21세기 새로운 안보영역으로 부각되고 있는 사이버 안보와 주요 국가의 사이버 공격 사례, 북한의 대남 사이버 공격 사례 및 사이버전 수행능력을 문헌분석 기법으로 살펴보고, 북한의 사이버 공격을 시기 및 목표를 기준으로 3기로 구분하여 변화 양상을 분석하였다.

Ⅱ. 사이버 공격의 역사

1. 사이버 안보

국가는 정보, 경제, 국방, 안전 등 국가운영에 필요한 중요 요소를 정보통신기술에 의존하고 있다. 물리적 공간과 마찬가지로 국가·비국가 행위자에 의한 다양한 사이버 공격, 테러 등으로 사회·경제·국가적 피해가 발생하였다. 이에 사이버 안보(Cyber Security)의 중요성이 대두되었다. '24년 2월 정부는 '국가사이버안보전략'을 발표하여 국가 차원의 사이버 공격과 위협에 대한 대비·대응을 본격화하였다. 또한, 국가정보원의 사이버 안보업무 수행을 위한 법적 기반을 마련하고자 「사이버 안보 업무규정」(2024. 3. 25. 시행)을 제정하였다. 본 규정에서는 안보를 해치는 사이버 공격과 위협을 정의하고, 안보업무의 범위를 정하여 본격적인 사이버 안보 정보활동의 수행을 보장하였다. 최근 우리나라뿐만 아니라 미국, 영국, 일본 등 다수 국가가 사이버 공간에서의 안보유지를 위한 법적·제도적 기반을 마련하고 다자 협력체를 만드는 등 사이버 안보를 중요시하는 정책을 펼치고 있다.

2. 사이버 공격의 역사

사이버 공격은 인터넷의 등장 및 발달과 비례적으로 증가하였다. 사이버 공간이 등장한 초기에는 주로 컴퓨터에 관심이 많은 개인들이 단순 흥미나 과시 등 개인 만족을 위해 해킹이나 바이러스 유포, 컴퓨터 시스템 장애를 유발하는 행위를 하였다. 대부분 혼자서 활동하는 10-20대로서 공격 성공 자체로부터 오는 만족감과 같은 단편적이고 일회적인 목표 달성을 추구하였다. 공격 대상 역시 민간 시설이나 전자 상거래망, 개인용 컴퓨터 등에 한정되었다[1]. 따라서 국가안보에 미치는 영향이 거의 없었으며, 사회혼란, 경제질서 파괴 등 대규모 피해를 끼치는 경우는 드물었다. 하지만, 사이버 공간이 고도화되어 국가의 모든 영역을 연결하고 핵심시설에 대한 접근이 가능해지고, 사이버 공격자의 능력이 과거보다 상향되었다. 이에 사이버 공격도 개인적인 수준에서 경제적 이득, 정치적 목적 달성, 사회 혼란, 테러 등 목적 지향적 활동 양상으로 변모되었다. 공격 목적 달성을 위해 사이버 공격자의 성향 또한 비조직적에서 전문화, 조직적 특성을 보이기 시작했다. 국가·비국가 행위자는 이들을 고용·훈련시켜 다양한 사이버 공격을 감행하였다.

전쟁에서의 사이버 공격은 1990년대 미국 주도로 적(敵)국의 지휘통제망에 대해 주로 수행했다면, 2000년대 들어 고도의 사이버전 능력을 갖추게 된 러시아나 이란이 사이버 공격을 수행하기도 하였다. 표 1을 참고하면 사이버 공격이 다양한 양상으로 수행된 것을 볼

수 있다[2]. 이는 물리적 공격과는 다르게 주체가 바로 드러나지 않는 사이버 공격 특성을 이용해 물리적 공격을 감행한 수준의 효과를 얻는 전략을 수행했다고 볼 수 있다. 이는 사이버 공격이 전·평시를 막론하고 목적 달성을 위해 매우 유용한 수단이 될 수 있음을 의미한다. 미국은 2010년 이란 핵시설에 대한 사이버 공격을 감행하여 물리적 파괴라는 효과를 이끌어냈는데, 이 사례를 통해 항공 폭격이나 특수부대를 활용한 파괴공작을 수행하지 않아도 적의 핵심시설을 물리적으로 파괴할 수 있는 수단으로써 사이버 공격의 유용성이 입증되었다.

표 1. 주요국의 사이버 공격 주요 사례(재구성)
Table 1. Cases of Cyber Attacks in major countries

구분	주체	내 용
2022 ~ 2023	러시아	우크라이나 농업 시설 악성코드 공격
		NATO 국가 대상 사이버 공격
		우-러 전쟁 前 DDOS, 악성코드 공격
2016	러시아	美 DNC 정보 차단
2015	중국	美 연방공무원 2150만명 정보 유출
2014	러시아	美 백악관 전산망 침투
2012	이란	美 금융회사, 이스라엘 정부 공격
2010	미국	이란 핵시설 파괴(스턱스넷)
2008	러시아	그루지아 정부 홈페이지 공격(DDOS)
2007	이스라엘	시리아 공군망 무력화
	러시아	에스토니아 인터넷망 마비(DDOS)
2001	미국	이라크 정보시스템, C2 체계 무력화
1993	미국	세르비아 네트워크 기반시설 무력화
1991	미국	이라크 정보망, 공군망 방해공격

최근 사이버 공격은 잠재 적국에 대한 정보탈취, 전산망 마비 등의 범위를 넘어 심리전, 기술탈취, 전쟁 여건 조성 등 다양한 양상으로 변모하고 있다. 美 최신 전력인 F-35와 글로벌호크 무인기 등 설계도를 중국이 해킹으로 탈취하는가 하면, 우크라이나-러시아 전쟁 직전 러시아가 비전투 분야인 우크라이나 농업시설을 공격하여 여건조성작전을 수행한 바 있다.

III. 북한의 사이버 공격 사례 및 능력

1. 북한 사이버 공격 사례

북한은 1990년대 이후부터 사이버 공간을 '남조선혁명의 해방구'로 간주하고 선전선동, 해킹, 테러, 간첩교신, 사이버 외화벌이 등을 다방면으로 전개해왔다[3]. 표 2는 북한의 주요 사이버 공격 사례를 연도별로 정리한 것이다. 대표적인 대남 사이버 공격은 2009년과 2013년 에 발생한 사례이다. 북한의 대남 사이버 공격이 본격화된 것은 2009년 7월 7일부터 한국과 미국의 주요 기관 등 총 35개의 웹사이트에 대하여 북한이 '분산서비스거부공격'(디도스: DDoS)을 감행하면서이다[4]. 당시 악성코드에 감염된 수만대의 좀비 PC가 청와대, 국방부 등 국가기관 사이트를 마비시킨바 있다.

2013년 3월 20일에는 KBS, MBC, YTN 등 주요 방송사와 농협, 신한은행 등 금융기관의 컴퓨터 대부분이 일시에 다운됐다. MBR(Master boot record) 및 VBR(Variable Bit Rate)이 파괴돼 복구 불가였다. 한국 주요 기관의 전산망이 대대적으로 마비된 것이다. 총 32,000여 대의 컴퓨터와 전산장비가 파괴돼 피해규모가

표 2. 북한의 대남 사이버 공격 주요 사례
Table 2. Cases of North Korea's cyber attacks on the South Korea

구분	내 용
2023	군사자료 탈취 목적 군 협력업체 노트북 악성코드 공격
2022	한미연합훈련 워게임 운용업체 직원 이메일 해킹
2021	한국원자력연구원, 한국항공우주산업 해킹 (원전기술, KF-X, 잠수함 기술 등 탈취)
2019	韓 암호화폐거래소 해킹(580억원 가상화폐 탈취)
2018	美, 인니 기업 해킹 3700만 달러 탈취
	韓 암호화폐거래소 해킹(350억원 가상화폐 탈취)
2017	슬로베니아 기업 해킹 7500만 달러 탈취
	워너크라이 랜섬웨어 공격
2016	방글라데시 은행 해킹 8100만 달러 탈취
	韓 국방부 통합데이터망 해킹(2급비밀 등 탈취)
2015	韓 서울메트로 해킹
2014	韓 한국수력원자력 해킹, 美 소니픽쳐스社 공격
2013	韓 언론사, 금융기관 대규모 공격, 마비
2011	韓 NH 전산망 마비
2009	韓, 美 정부기관 등 웹사이트 DDOS 공격(7·7 공격)
2001	韓 1 .25 인터넷 대란

8,600억 원 이상으로 추정됐으며, 우리 정부는 북한의 정찰총국 소행으로 추정된다고 발표했다[5].

또한, 북한은 국적을 불문하고 은행, 가상화폐거래소 등을 상대로 해킹을 벌여 자금을 탈취하거나 군사정보 획득을 위해 악성코드를 유포하는 등 다방면의 사이버 공격을 수행하였다. 美 법무부는 '21년 2월 해킹을 통해 전세계의 은행·기업에서 13억달러(약 1조4000억원) 이상의 현금 및 가상화폐를 탈취, 요구한 협의로 북한 해커 박진혁, 전창혁, 김일을 기소했는데, 모두 정찰총국 소속으로 알려졌다.[6] '22~'23년에는 韓·美연합훈련을 위해 파견된 워게임(War-Game) 프로그램 운용업체 직원의 이메일로 악성코드를 발송하여 개인 컴퓨터를 감염시킨 뒤 韓·美의 군사전용망에 접속을 시도한 적이 있다.

2. 북한 사이버 공격 능력

북한은 국가 주도하 1980년대부터 사이버전 능력을 길러왔다. 소련의 컴퓨터 전문가 약 40여 명을 초빙해 사이버전 학습을 시작, 사이버 전사 양성을 위한 대학을 설립하는 등 사이버전 능력 배양을 위해 노력해왔다. 표 3은 북한 수뇌부의 사이버전에 대한 인식을 나타낸 발언을 종합한 것이다[3]. 걸프전에서 연합군의 사이버·전자전 능력과 전쟁에 미치는 영향을 체감한 북한은 사이버전에 대한 본격적인 투자를 시작하였다. 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, 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 배치하는 등 전략차원에서 사이버전을 접근하였다[8].

북한은 1995년부터 100여 명 수준의 '중앙당 35호실 기초자료조사실'을 설비하여 중앙당 부서에 필요한 다른 나라 국가기관, 단체, 개인에 관한 기밀자료를 사이버 공간을 통해 수집하였다. 1998년에는 사이버부대(121소)를 창설하였고, 1999년 200여명 수준의 사이버심리전 부대인 적공국 204소를 설립하여 대남, 해외 사이버 심리전을 펼쳤다. 이후 북한은 인민무력부 정찰국, 노동당 작전부, 중앙당 35호실 등 분산되어있던 공작부서를

표 3. 사이버전 관련 북한 수뇌부 방침(재구성)
Table 3. North Korea's leadership policy on cyber warfare

구분	내 용
김정일 (1991)	20세기 전쟁이 기름전쟁이고, 알탄(탄환) 전쟁이라면, 21세기 전쟁은 정보전쟁이다. - 코소보 전쟁 이후 김정일 발언
김정은 (2013.8)	사이버전은 핵·미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 만능의 보검이다 - 국정원장 국회 정보위 북한 사이버전 실태 보고
김정은 (2014.6)	적들의 사이버 거점을 일순에 장악하고 무력화할 수 있는 만반의 준비를 갖추라 김정은 정찰총국 기술정찰국 방문 시

'정찰총국(2009)'을 창설하면서 사이버전 조직을 확대개편하였다. 121소 인원을 500명에서 3,000명으로 증강하였고, 사이버지도국(121국)으로 개편하였다[9]. 특히 '121국' 내 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 조직으로는 '라자루스'(Lazarus, 일명 Hidden Cobra), '블루노로프'(BlueNorOff), '안다리엘'(Andarial), 김수키(Kimsuky, 일명 탈륨(Thallium) 등이 알려져 있다.[4] '2022 국방백서'에 따르면 북한은 현재 6,800여 명의 사이버전 인력을 운영하여 최신 기술에 대한 연구 개발을 지속하는 등 사이버 전력 증강을 위해 노력하고 있다[10].

현재 북한의 사이버 인프라는 전반적으로 열악하지만, 사이버 공격 역량만은 미국, 중국, 러시아, 이란 등에 이어 세계 5위로 평가되고 있다. 최근 미국 사이버 보안업체 'Fire eye'는 북한이 인터넷으로 연결돼 있지 않은 대상까지 해킹할 수 있을 정도로 세계 최고 수준의 사이버 공격역량을 보유하고 있다고 평가했다. 북한이 보유하고 있는 비대칭 전력 중 가장 '저비용-고효율'이 바로 사이버 전력이다[3].

Ⅳ. 북한의 사이버 공격 변화 양상

북한의 사이버 공격은 시기별, 목적별로 변화하는 모습을 보였다. 제1기는 2009년부터 2016년까지로 대남도발 형태를 보였는데 2009년 한국과 미국의 주요 기관 웹사이트에 디도스 공격을 감행하면서 북한의 사이버 공격이 시작되었다. 2011년에는 농협의 금융전산시스템

에 대한 사이버 공격으로 컴퓨터 273대가 전산 장애를 일으켰고 2015년에는 서울 지하철 1-4호선 서버 해킹과 청와대, 국회, 외교부, 국방부, 통일부 등 주요 정부기관에 대한 해킹을 시도하였다. 북한의 사이버 공격 제1기의 전략적 목표는 국가 기간망 무력화와 정보 탈취를 통해 북한 스스로 사이버 능력을 검증하고 과시는 모습을 보이는 것이었다[4].

북한의 사이버 공격 제2기는 외화벌이가 주목적이었으며, 2016년부터 시작되었다. 북한은 2016년 수소탄 실험이라고 주장하는 4차 핵실험을 단행했고 유엔 안전보장이사회는 대북제재 결의 2270호를 통해 민생 목적을 제외한 북한의 주요 대외교역을 금지하는 조치를 명시하여 비군사적 조치로는 가장 강력하고 실효적인 제재를 추진하였다. 이 제재로 우리나라는 개성공단 가동을 전면 중단하는 조치를 취했고, 현재까지 가동이 중단된 상황이다. 그럼에도 북한은 2016년 5차 핵실험, 2017년 6차 핵실험을 감행하였고, 유엔 안보리는 이에 대응해 6차례의 대북제재를 가하였다. 6차례의 대북제재는 북한 경제 일반에 대한 포괄적 제재로 북한의 수·출입을 비롯한 경제 분야의 전면적인 금수조치였다[4].

그 결과 표-4와 같이 북한의 수출액이 줄어들기 시작해 무기개발 등을 위한 돈줄이 막혔다[11]. 대북제재가 본격화되기 전 2016년에는 수출총액이 28억 2천만 달러였지만, 2021년에는 8천만 달러로 2016년 대비 3% 수준으로 곤두박질치며 외화벌이에 큰 어려움을 겪게 되었다.

표 4. 북한의 수출량
Table 4. North Korea's export volume

구분	수출금액 (천달러)	증감률(%)
2013	3,218,382	11.7
2014	3,164,650	-1.7
2015	2,696,538	-14.8
2016	2,820,914	4.6
2017	1,771,852	-37.2
2018	242,710	-86.3
2019	277,777	14.4
2020	89,299	-67.9
2021	81,963	-8.2
2022	159,001	94

북한은 이를 극복하기 위해 암호화폐를 해킹하여 탈취하기 시작했고 유엔 안전보장이사회 산하 대북제재 위원회는 전문가 패널 보고서는 북한이 악의적 사이버 활동으로 전체 외화 수입의 50%를 창출했다고 밝혔고 2017년~2023년까지 가상화폐를 탈취한 금액이 약 30억 달러(약 4조원)로 추산하고 있으며 이 자금으로 핵무기 등 대량살상무기 개발 자금의 40%를 충당했다고 평가했다[12].

북한은 2022년 한 해에만 73발의 탄도미사일을 발사하였는데 그 비용만 약 5억 6,000천만 달러 수준이다.[13] 대북제재로 대외 무역이 막혀 외화가 부족한 상황이기에 가상화폐 탈취가 북한의 주요 소득원으로 작동하고 있는 것으로 평가된다. 북한은 2023년 가상화폐의 가치가 떨어지자 다시 금융권에 대해 랜섬웨어 공격을 가하기 시작했다[14].

북한의 사이버 공격 제3기는 방산업체 기술탈취에 주력하고 있다. 북한은 2021년 8차 당대회에서 '전략무기 5대 과업'을 교시했다. 대한민국을 순식간에 굴복시키고 미군의 증원을 무력화하기 위한 전략무기를 개발하는 것으로 극초음속미사일, 고체연료 대륙간탄도미사일(ICBM), 다탄두 개별유도탄, 군사정찰위성, 핵추진 잠수함 및 잠수함탄도미사일(SLBM)이다.

북한은 2021년 한국원자력연구원에서 소형 원자로 관련 자료 탈취, 한국항공우주산업(KAI)에서 한국형초음속전투기 'KF-21' 기술을 탈취했으며 2023년에는 조선업체 4곳에서 함정 도면 및 설계자료를, 무인기 업체에서는 무인기 엔진자료 등을 해킹하였다[15]. 방산업체에 대한 해킹은 전통적인 해킹기술을 통한 기술 탈취와 홈페이지 유지보수 업체를 통한 방산기관 우회침투, 방산업체 기술자에 기술유출에 대한 금전적 보상 등 다양한 방법으로 시도되고 있다. 북한이 전략무기 5대 과업을 달성하게 되면 미국의 선제공격에도 제2격(2nd strike)을 통한 치명적인 보복공격이 가능해질 것으로 판단되며 이는 미국에 대한 억지력이 강화되고 향후 비핵화 협상에서 북한이 유리한 협상전략을 펼칠 수 있게 될 것이다.

Ⅴ. 결 론

북한은 대북제재가 지속되는 상황 속에서 외화획득에 어려움을 겪으며 이를 타개하기 위해 매우 다양한

사이버 공격을 통한 가상자산을 탈취하였다. 탈취한 자금은 김정은의 통치 체제 유지와 핵·미사일 개발에 사용되고 있고, 북한의 불법적 행위를 저지하지 못해 제재의 실효성에 의문이 드는 실정이다. 또한 최근 사이버 공격은 방산업체를 해킹하여 핵심기술 탈취 집중하는 유형을 보이는데, 이는 북한이 2021년 8차 당대회에서 선언한 5대 핵심전력 달성을 위한 전략적 행위로 보여진다. 북한의 자칭 5대 핵심전력을 확보하게 되면, 북한은 핵무기 투발수단의 고도화를 이루어내는 것이기에 미 본토 공격능력이 획기적으로 상승하게 되는 것이다. 이는 미국에 대한 강력한 억지력을 확보하게 되는 것이고, 추후 비핵화 협상에서 유리한 카드를 가질 수 있게 되는 것이다. 이후의 비핵화 협상은 '先 비핵화 後 제재 완화'의 형태가 아니라 북한의 핵무기 동결 또는 일부 제거를 통한 대북제재 부분 완화의 모습을 보일 가능성이 높아질 것이고 이는 대한민국에 큰 위협이 될 것이다.

본 연구에서 북한의 사이버 공격 양상을 1기~3기까지 구분한 것은 북한이 수행하는 사이버전의 국면이 전면적으로 변화되는 시점이라고 보기는 어렵다. 3기에서 제시한 방산업체에 대한 기술탈취의 모습은 1기와 2기에서도 나타났으며 2기의 외화벌이 유형의 행태는 3기에서도 지속되고 있다. 즉 북한의 전략목표가 무엇이냐에 따라 사이버 공격의 중점이 달라진다는 것이다.

현재 북한 사이버 공격의 전략적 목표는 2021년 8차 당대회에서 김정은 위원장이 제시한 전략무기 5대 과업 달성에 기여하는 것이고, 이를 위해 기술력 확보를 우선시한다. 북한의 9차 당대회는 5년 뒤인 2026년에 개최할 가능성이 높다. 북한은 8차 당대회에서 제시한 목표의 달성 성과를 과시해야하기 때문에 향후 국내·외 주요 방산업체를 대상으로 5대 전략무기와 관련된 핵심기술을 탈취하려는 노력을 지속할 것이다.

북한의 사이버 공격에 대해 국가 차원에서 대책을 서둘러 강구해야한다. 일본은 첨단 반도체 공장 유치를 위해 막대한 보조금을 지원하는데, 그 조건 중 하나가 사이버 공격 대책을 갖추었냐가 포함된다. 우리 국가정보원은 국가핵심기술을 보유한 기업 등을 대상으로 기술탈취 방지를 위한 자문을 하거나 보안측정을 제공하는 것으로 알려져있다. 국가정보원 산하 '국가사이버안보센터'에서는 국가 중요정보의 유출 및 국가 주요 정보통신 서비스·기반시설 대상 사이버공격을 감시하고 방어하고 있다. 또한, '22년 개소한 센터 산하의 '국가사이버안보협력센터'에서 점차 고도화되는 사이버 공격에 효과적으로 대응하기 위해 민·관이 함께 임무를 수행하고 있다. 이처럼 북한의 사이버 공격을 사전에 막기 위한 제도적, 기술적 한계를 허물기 위한 노력을 우리 정부도 꾸준히 하고 있지다. 하지만, 사이버 공격을 우리 국가안보를 직접적으로 위협하는 행위로 규정하는 법안 제정과 보복능력 확보 등 보다 높은 수준의 정책적 접근이 필요하다.

국가안보를 위해 국군이 물리적 영역에서 압도적 전력을 유지하는 것과 같이 사이버 영역 또한 국가안보와 직결된다는 인식이 필요한 시점이다.

References

[1] Yun. M. W. "The issue and strategic meaning of cyber security threats and policy measures: South Korea and its neighboring states". National Security and Strategy, 14(4), 111-14, 2024. DOI : 10.23111/nsas.2014.14.4.004

[2] Ham. S. H. "Journal of the Korea Institute of Information & Communication Engineering". Vol. 21 Issue 9, 1669, 2017.

[3] Yoo. D. R. "North Korea's Cyber Threats and Countermeasures". The Journal of Strategic Studies, 28(3), 7-36, 2021.

[4] Lee. S. Y. "Evolution of North Korea's Cyberattack Strategy: Cyber strategy as a means of earning foreign currency to evade sanctions against North Korea". International Journal of Korean Unification Studies, 32(1), 323-353, 2023. DOI : 10.33728/ups.2023.32.1.012

[5] Park. E. J. "Increasing North Korean Cyber Security Threats and South Korea's Response". Joural of Patriots and Veterans Affairs in the Republic Korea, 19(4), 9-30, 2020. DOI : 10.24004/tkafp.2020.19.4.001

[6] Jung. J. Y. "U.S. Department of Justice, accused three hackers of the North Korean Reconnaissance General Bureau for hacking 1.4 trillion won", Daily Segye, 2021.2.18., https://m.segye.com/ampView/20210218502228

[7] Hwang. J. H. "North Korea's Cyber Security Strategy and the Korean Peninsula". The Journal of East and West Studies, 29(1), 139-159, 2017. UCI : G704-SER000014470.2017.29.1.001

[8] Shin C. G. “A Study of countermeasure and strategy analysis on North korean cyber terror”. The Journal of Police Science, 13(4), 201-226, 2013. DOI : 10.22816/polsci.2013.13.4.008
[9] Kim J. G. “North Korea’s cyber organization-related information research (Based on organization status and major attack cases)”. Proceedings of the Korean Society of Computer Information Conference, 2020.
[10]Defense White Paper, Republic of Korea, 2022.
[11]North Korea's export volume, https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_1ZGA92&conn_path
[12]Ko. D. Y, “North Korea's Sanctions Committee, Making Foreign Currency from Cyber Extortion 40% of funds such as nuclear development", Daily Donga, 2024.3.21. https://www.donga.com/news/Politics/article/all/20240321/124094548/1
[13]Jeong. J. W. “We've made 720 billion 'missile explosions'...The dilemma of 10 year old Kim Joo-ae”, The JoongAng, 2023.2.21. https://www.joongang.co.kr/article/25141995#home
[14]Kim. B. M. “North Korea's evolving cyberattacks and Response”. INSS. ISSUE BRIEF 472, 2023.
[15]Shin. J. W.. "North Korea Shortens SLBM Development by Stealing 'Coldronch' Technology in Korea" Daily Donga, 2024.2.27. https://www.donga.com/news/Politics/article/all/20240227/123708087/1

※ 이 논문은 2024년도 육군3사관학교 충성대 연구소의 연구 지원에 의하여 연구되었음