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).