INSS
전략보고
November 2021. No.147

www.inss.re.kr
INSTITUTE FOR NATIONAL SECURITY STRATEGY

김정은 시대 북한의 사이버 위협과 주요국 대응

김보미 부연구위원
bomi@inss.re.kr

오일석 연구위원
nusl2006@inss.re.kr

Ⅰ. 문제 제기

Ⅱ. 김정은 시대 북한의 사이버 위협 역량과 특징

Ⅲ. 북한 사이버 위협에 대한 주요국 대응

Ⅳ. 결론

국가안보전략연구원

국문 초록

김정은 시대 들어 북한의 사이버 공격 능력은 더욱 강화되고 있으며 북한의 소행으로 추정되는 국제 사이버 위협 역시 증가하고 있다. 김정은 정권은 사이버전 수행 능력을 주요 비대칭 전력의 하나로 인식하고 국가적 차원에서 해커를 육성하고 있으며 이들은 전 세계를 무대로 사이버 공격을 감행하고 있다. 북한은 사이버 공격을 통해 경제적·정치적 이익을 취하려는 의도를 지닌 것으로 보인다. 현재 북한의 사이버 능력은 주요 외화벌이 수단이 되어 대북제재를 무력화하고 있을 뿐만 아니라 핵·미사일 전력에 소요되는 비용을 충당해줌으로써 국제사회에 심각한 위협이 되고 있다. 이밖에도 북한은 군사·외교 기밀 유출과 같은 다양한 목적으로 외국 정부, 군사기관 및 방위산업체, 에너지연구소 등을 대상으로 사이버 공격을 광범위하게 가하고 있다. 이에 대해 미국을 비롯한 국제사회는 경제제재를 주요 수단으로 대북 사이버 위협에 대응하고 있으나 북한에 의한 해킹 피해가 증가하고 심각해지는 만큼 미국 일각에서는 보다 강력한 대응책의 필요성을 주장하고 있다. 그러나 사이버 공격은 익명성으로 인해 책임소재가 불분명하여 사이버 공격자에 대한 처벌에 타당성을 갖기 어렵다는 치명적 단점이 있다. 북한의 상시적인 사이버 위협에 놓인 한국 정부로서는 적극적 사이버안보 활동을 통해 북한의 사이버 위협을 사전탐지하고 모니터링하여 예방하는 현실적 대비책을 마련해야 할 것이다.

핵심어: 북한, 사이버 안보, 해킹, 대북제재, 라자루스

목차

Ⅰ. 문제 제기

Ⅱ. 김정은 시대 북한의 사이버 위협 역량과 특징

1. 북한의 사이버 위협 역량 및 주요조직

2. 김정은 시대 북한 사이버 공격의 특징

Ⅲ. 북한 사이버 위협에 대한 주요국 대응

1. 주요국의 대응

2. 한국의 대응 및 개선 방향

Ⅳ. 결론

Ⅰ. 문제 제기

• 2021년 2월 25일, 미 하원 외교위원회의 그레고리 믹스(Gregory Meeks) 위원장과 마이클 매카울(Michael McCaul) 공화당 간사 등 6명은 사이버 공간에서 미국의 정책확립을 위한 "사이버 외교법(The Cyber Diplomacy Act of 2021)"을 발의
  - 동 법안은 북한을 포함한 주요국의 사이버 위협에 미국의 대응을 요구하는 법안으로 미 하원의 북한 사이버 위협 관련 발의는 2017년과 2019년에 이어 세 번째
  - 해당 법안은 미국의 사이버안보를 해치는 북한 단체와 기관에 대한 제재를 권고하는 내용을 포함

• 북한의 사이버 공격 능력을 심각한 위협으로 간주하고 적극적 대응의 필요성을 강조해 온 미 정부는 바이든(Joe Biden) 대통령의 집권 이후 더욱 강력하고 현실적인 대응방안의 필요성을 주장하는 상황
  - 2월 17일 네드 프라이스(Ned Price) 국무부 대변인은 북한의 핵·탄도미사일 프로그램 못지 않게 사이버 활동을 주시하고 있으며 대북 정책 검토에도 총체적으로 고려할 것임을 언급
  - 미국 국가정보국장실은 4월 13일 발간한 『연례위협평가 2021(Annual Threat Assessment 2021)』에서 북한의 사이버 능력을 미국의 인프라와 기업 네트워크에 위협으로 평가
    ※ 미 공군장관 지명자 프랭크 켄달(Frank Kendall) 역시 5월 25일 열린 상원 인준청문회에 앞서 제출한 서면 답변에서 북한의 사이버 능력이 미국의 우주 안보에 위협이 될 수 있다고 분석

• 북한은 김정은 집권 이후 사이버 능력을 핵·미사일과 함께 비대칭 전력 중 하나로 적극 활용하고 있으며 현재 북한의 사이버 공격 능력은 세계 최고 수준인 것으로 평가받고 있음[1)]

1) 본 보고서에서 칭하는 사이버 능력은 구체적으로 사이버 공간안에서 혹은 사이버 공간을 통해 영향력을 행사하거나 목표를 달성하는 수단을 의미하는 것으로 광범위하게는 해킹, 데이터 유출, 범죄활동, 스파이 행위와 같은 일반적인 행동을 포함하며 좁게는 컴퓨터 네트워크 이용, 방어, 운영과 같은 활동들을 포함한다.

- 김정은 국무위원장은 사이버전(戰)을 “핵미사일과 함께 우리 인민군대의 무자비한 타격 능력을 담보하는 만능의 보검”으로 소개하고 3대 전쟁수단으로 간주
- 김정일 시대부터 체계적으로 육성해 온 사이버 인력은 현재 6,800여 명으로 2013년 3,000여 명에 비해 2배 이상 증가하였으며, 미 사이버 보안업체 크라우드스트라이크(Crowdstrike)는 2019년 북한의 사이버 공격 능력을 러시아에 이은 세계 2위 수준으로 평가[2)]

• 최근까지도 북한은 자산 탈취, 군사·외교 기밀 유출과 같은 다양한 목적하에 세계 각국의 금융기관, 외국 정부, 군사기관 및 방위산업체, 에너지연구소 등을 대상으로 사이버 공격을 광범위하게 진행 중
- 사이버 공격은 익명성으로 인해 책임소재가 불분명하여 사이버 공격자에 대한 처벌이 쉽지 않다는 특성이 있어 비교적 자유롭게 불법적 활동을 통해 이익을 취득 가능
- 특히 김정은 시대에는 북한의 사이버 능력이 외화벌이 수단이 되어 대북제재를 무력화하고 있을 뿐만 아니라, 핵·미사일 전력에 소요되는비용을 충당해줌으로써 국제사회에 심각한 위협이 되고 있다는 평가
  ※ 가상화폐 거래소 해킹 후 실제 화폐로 돈세탁을 하거나 합작회사의 해외 계정, 홍콩 소재 위장회사, 가짜 신분 및 가상사설망(VPN)을 활용해 국제 금융시스템에 접근하여 불법 수익을 취득
- 불법적 사이버 활동을 통한 수익은 핵·미사일 능력을 확장하기 위해 자금이 절실한 김정은 정권에 현금 공급망이 되어 줌으로써 비핵화를 위한 국제사회의 노력에 장애물로 작용

• 북한의 사이버 위협 능력 증강과 비례하여 국제적으로 피해 규모가 확대되고 심각성이 가중됨에도 이와 관련한 논의는 핵·ICBM 등 다른 비대칭 전력과 비교했을 때 충분한 관심을 받지 못하고 있는 상황
- 대부분의 기존연구들은 북한의 사이버 역량과 조직에 대한 일반적인 소개, 사이버 공격에 활용하는 기술, 일부 사례 분석, 국제법적 관점에서 한국의 대응방안 등에 주목[3)]

---

2) 국방부, 『국방백서 2020』 (서울: 국방부, 2020), p. 23; 국기연, “북한 사이버 공격 능력 러시아에 이어 세계 2위,” 『세계일보』, 2019년 2월 20일, https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=100&oid=022&aid=0003341501 (검색일: 2021.10.5.).

3) 대표적 기존연구로는 황지환, “북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산,” 『동서연구』, 제29권 1호(2017), pp.139-159; 김윤영·양철호, “북한의 사이버테러에 대비한 법·제도 개선방안 연구,” 『유럽헌법연구』, 제33호 (2020), pp. 355-384; 백상미, “북한의 대남 사이버 공격에 대한 국제법적 검토와 이에 대한 한국의 대응전략,” 『서울국제법연구』 제27권 2호(2020), pp. 39-66; 정영애, “북한의 사이버 공격 역량의 진화: 사이버 공격 사례 분석을 중심으로,” 『평화학연구』, 제20권 4호 (2019), pp. 125-143.

- 현 김정은 정권의 사이버 위협의 심각성이 더욱 강조되고 있는 만큼 김정은 시대의 북한 사이버 공격의 현황과 특징에 초점을 맞춘 연구의 필요성 증대

- 이에 따라 본 전략보고는 김정은 시대 북한의 사이버 위협 능력과 특징을 알아보고 주요국의 대응방안을 소개함으로써 북한 사이버 능력의 현 주소를 이해하는 한편, 향후 우리의 정책적 대안을 제시하는 것을 목적으로 함
  - 기술적 내용에 집중하기보다 공개된 자료에 근거하여 현재까지 드러난 북한의 사이버 공격의 형태와 유형 및 사이버 공격의 배후에 숨겨진 김정은 정권의 전략 등을 분석
  - 2장에서는 김정은 시대 북한의 사이버 능력 및 공격현황, 특징을 분석하고 3장에서는 미국·EU·UN의 대응전략을 소개하는 한편 북한의 사이버 위협에 대한 한국의 대응과 향후 개선점을 제안

Ⅱ. 김정은 시대 북한의 사이버 위협 역량과 특징

1. 북한의 사이버 위협 역량 및 주요조직

(1) 북한의 사이버 능력

- 김정은 정권은 △사이버전 대비 △국방기술 탈취 △대남공작 △외화벌이 △최고존엄 모욕에 대한 보복 등 다양한 이유와 목적으로 사이버 공격을 적극 활용
  - 높은 수준의 사이버 공격 역량은 재래식 전력의 취약점을 상쇄함으로써 북한의 주요 비대칭 전력 중 하나로 역할
  - 사이버 공격의 낮은 진입 비용, 높은 잠재적 수익률, 책임귀속 규명의 어려움, 효과적인 억제력 부족 등의 특성은 북한 당국이 사이버 능력에 대한 투자를 지속하도록 유도하고 있는 것으로 추정

- 북한의 사이버 전략이나 독트린, 지휘통제에 대해서는 아직까지 공식적으로 밝혀진 것이 거의 없으나 김정일-김정은 시대로 이어지면서 북한 내부에서 사이버 공격 능력 강화에 대한 중요성이 커지고 있는 상황
  - 2010년 김정일은 "현대전쟁은 기름전쟁, 알(탄약) 전쟁으로부터 정보전쟁으로 바뀌었다"며 "정보전부대는 핵무기와 함께 나의 배짱이고 예비대"라고 강조하는 등 사이버전력의 중요성을 역설[4)]
  - 김정은 또한 사이버전을 "핵·미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"으로 부를 정도로 현대 정치·군사 경쟁에 핵심으로 간주[5)]
    ※ 조선노동당과 최고지도자 김정은의 지시하에 무력단체와 정보기관이사이버 공격을 담당하고 있는 것으로 알려져 있음

- 북한 소행으로 의심되는 대부분의 사이버 작전은 정찰총국의 6개국 가운데 하나인 일명 '121국'(별칭 '사이버전지도국')에서 관할하는 것으로 추정[6)]
  - 121국은 허위정보, 사이버 범죄, 스파이 활동을 개시하는 6,000여 명의 상근 사이버 요원 및 지원 인력을 보유
  - 2020년 7월 발표된 미 육군 보고서에 따르면 121국 산하에는 라자루스(Lazarus), 블루노로프(BlueNorOff), 안다리엘(Andarial) 등의 해킹그룹이 있으며 소속 해커들은 대부분 벨라루스와 중국, 인도, 말레이시아, 러시아 등 해외에서 활동[7)]
  - 이밖에도 북한은 총참모부 산하 전자전 사령부를 비롯하여 여러 개의 하위 전자정보전 집단을 운용 중인 것으로 알려짐[8)]

---

4) 김귀근, "김정일 "정보전부대는 나의 배짱이고 예비대"," 연합뉴스, 2011년 6월 28일, https://www.yna.co.kr/view/AKR20110628128400043 (검색일: 2021.9.30.).

5) 이영종·윤호진, "김정은 "사이버전은 만능의 보검" 3대 전쟁수단 운용," 『중앙일보』 2013년 11월 5일, https://www.joongang.co.kr/article/13048072#home (검색일: 2021.9.30.).

6) 정찰총국은 2009년 노동당 작전부와 35호실, 인민무력성 정찰국을 통합하여 설립되었으며 현재 육·해상 정찰국(1국), 정찰국(2국), 기술정찰국(3국(기술국)), 해외정찰국(5국(구 35호실)) 등 총 6개국으로 구성. 이중에서 기술정찰국이 사이버지도국, 121국 등으로 통칭되고 있음. 문동희,"정찰총국 인사조치에 대남 사이버 공격 강화 우려…어떤 부서길래," 『데일리NK』, 2020년 9월 23일, https://www.dailynk.com/%ec%a0%95%ec%b0%b0%ec%b4%9d%ea%b5%ad-%ec%9d%b8%ec%82%ac%ec%a1%b0%ec%b9%98%ec%97%90-%e5%b0%8d%e5%8d%97-%ec%82%ac%ec%9d%b4%eb%b2%84%ea%b3%b5%ea%b2%a9-%ec%9a%b0%eb%a0%a4-%ec%96%b4%eb%96%a4-%eb%b6%80/ (검색일: 2021.9.31.).

7) U.S. Army Headquarters, "North Korean Tactics," July 2020, p.E-2, https://irp.fas.org/doddir/army/atp7-100-2.pdf (검색일: 2021.9.30.).

8) 미키 배(Mickey Bae), "미 국방보고서 북한 사이버·전자정보전 역량 일선 부대서도 운용," 『ENB』, 2020년 8월 18일, http://www.enbnews.org/news/articleView.html?idxno=21530 (검색일: 2021.9.30.).

- 북한의 사이버 능력에 대한 평가는 평가기관과 국가별로 다양하게 나타나고 있지만 대체적으로 높은 수준이라는 평가가 지배적
  - 2009년 이후로 북한의 해킹 능력이 크게 성장하였고 현재는 첨단의 사이버 공격 능력을 보유하고 있으며 어떤 나라의 시설도 공격할 수 있을 정도로 능력을 갖추었다는 평가[9)]
  - 반면 영국의 IISS(The International Institute for Strategic Studies)는 북한에 정교한 사이버 정보(intelligence) 능력이 전혀 없고 사이버보안 수준 또한 세계 최하위라며 전반적인 사이버 능력이 가장 낮은 3그룹(Third-tier)에 속한다고 주장
    ※ 구체적으로 북한 당국이 인터넷 접속을 엄격히 통제하고 세계 인터넷망에 연결하기 위한 게이트웨이(gateway)가 중국과 러시아 서비스 제공업체가 제공하는 극소수에 의존하여 공격에 취약한 것으로 분석[10)]
  - 그러나 이러한 구식 인프라로 인해 사이버 보복에 덜 취약하고 해커들의 활동 또한 해외에서 이루어져 북한에 가해지는 제재 역시 효과를 거두기 어렵다는 평가[11)]

- 김정은 시대 들어 북한 소행으로 추정되는 사이버 공격에 관한 발표가 급증하고 있는 상황
  - 2010년대 중반 이후로 특히 경화(hard currency) 확보를 위한 대규모 사이버 사기행위와 갈취 등이 발견되고 있음
  - 느슨하게 규제되는 가상자산(virtual asset) 서버의 네트워크를 악용하여 불법적으로 획득한 가상자산을 법정화폐로 변환함으로써 수입을 확충하고 제재를 회피하려는 의도를 갖고 있는 것으로 추정

9) 이태규, "북한 해킹 능력, 정교하지 않지만 위협적," 『한국일보』, 2021년 8월 2일, https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=104&oid=469&aid=0000621287 (검색일: 2021.9.30.).

10) The International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," IISS, February 2019, p. 125. IISS의 보고서 발표 이후 미 국무부는 북한의 악의적 사이버 활동이 미국과 전 세계 국가를 위협하고 있다며 금융기관에 대한 심각한 사이버 위협이자 사이버 간첩 위협으로서 파괴적인 사이버 활동을 수행할 능력을 보유하고 있다고 반박. 김정률, "미 국무부, 북한, 파괴적 사이버 활동 능력 보유," 『뉴스1』, 2021년 6월 30일, https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=104&oid=421&aid=0005446233 (검색일: 2021.9.30.).

11) David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (검색일: 2021.9.30.).

- 미국 및 EU, UN 등 국제사회는 북한의 주요 해킹조직과 사이버 요원들에게 제재를 부과하는 방식으로 대응하거나 사이버 위협에 대한 경각심을 높일 것을 호소하고 있으나 북한 당국은 관련 혐의를 부정
  - 북한이 2014년 소니픽처스 영화사 해킹 사건이 발생하였을 당시 배후로 지목되었을 당시 UN주재 북한대표부 관계자는 조작된 것이라고 반박[12)]
  - 최근 한국항공우주산업(KAI)과 한국원자력연구원 등의 해킹사태의 북한 배후설에 대해서도 "황당무계한 모략소동"이라며 "저열한 기술로 해킹을 당한 것"이라며 자신들의 소행임을 강하게 부정[13)]

(2) 북한의 대표적인 해킹조직

- 북한의 대표적인 해킹조직으로 라자루스, 블루노로프, 안다리엘, 김수키(Kimsuky, 탈륨(Thallium)) 등을 꼽을 수 있음([표 1] 참조)[14)]

- 라자루스 그룹은 정찰총국 산하 해킹조직으로 2007년초 설립된 것으로 추정되며 해외 정부와 금융기관, 방송매체들을 주요 타겟으로 설정
  - 2017년 워너크라이 랜섬웨어 사건에 관여하여 150여 개국에 악영향을 끼치고 30만대의 컴퓨터에 피해를 일으키고 2014년 소니픽처스 해킹 사건에도 직접 관여한 것으로 의심
    ※ 미 재무부에 따르면 북한 당국은 2007년 초에 정찰총국 제3국(제3 기술정찰국) 110연구소 소속으로 라자루스 그룹을 창설한 것으로 알려짐[15)]

12) 김성진, "북한, 소니 영화사 해킹 배후설은 조작," KBS, 2014년 12월 5일, https://news.kbs.co.kr/news/view.do?ncd=2978823 (검색일: 2021.9.30.).
13) "고질적 버릇, 상투적 수법," 『우리민족끼리』, 2021년 7월 12일.
14) 이밖에 화학, 전자, 제조, 항공우주, 자동차 및 의료기관을 포함하여 광범위한 산업분야를 타겟으로 삼는 해킹 조직인 스카크러프트(Scarcruft)도 존재.
15) 하윤해, "미, 6800억원 탈취한 북 해킹그룹 3곳 제재, 정찰총국이 배후," 2019년 9월 15일, 『국민일보』, http://news.kmib.co.kr/article/view.asp?arcid=0013711916&code=61131111&cp=nv (검색일: 2021.9.25.). 110연구소는 121국의 산하조직이거나 개편조직인 것으로 추정. The International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," IISS, February 2019, p. 127.

• 블루노로프와 안다리엘은 외국 금융기관에 대한 사이버 공격을 통해 불법적으로 수입을 확충하는 것으로 알려져 있으며 수입의 일부는 북한의 핵무기와 탄도미사일 개발에 흘러 들어가는 것으로 의심받고 있음
  - 블루노로프는 총 1,700명 규모로 알려졌으며 외국 금융기관에서 11억 달러의 탈취를 시도하였고, 인도, 멕시코, 파키스탄, 필리핀, 대만, 한국 등 11개국 16개 기관에서 자금 탈취에 성공한 것으로 알려짐
  - 안다리엘은 적의 전산망에 대한 감시와 취약점을 분석하는 1,600명의 해커로 이루어진 조직으로, 2016년 9월 한민구 전 국방장관의 컴퓨터와 국방부 인트라넷에 침임하여 군사 작전('작계 5015') 정보 탈취를 시도

• 김수키는 정찰총국 산하조직으로 2010년부터 활동한 것으로 알려졌으며 국제적인 정보수집 임무를 담당
  - 지능형 지속 공격(Advanced Persistent Threat, APT) 해킹조직으로 알려졌으며 2013년 러시아 정보보안업체가 해커의 이메일 계정인 '김숙향(kimsukyang)'이라는 이름으로 보고서를 발표하면서 존재 확인
  - 한·미·일 정부 및 싱크탱크 등 여러 분야 전문가들을 상대로 한반도 관련 안보문제와 관련하여 집합적인 정보활동을 벌이고 있으며 탈륨이 동일 조직인 것으로 추정

[표 1] 북한의 주요 해킹조직

해킹조직	조직의 특징 및 활동
김수키	• 정찰총국 산하조직으로 2010년 이래 활동한 것으로 추정 • 북한 정권의 글로벌 정보수집 임무를 담당 • 주요 해킹기술: 일반적인 사회공학 전술, 스피어피싱[16], 워터링 홀 공격 등을 사용하여 피해자로부터 원하는 정보 색출 • 주요 타겟: 한국, 미국, 일본의 개인 및 싱크탱크, 정부조직의 전문가(한반도 및 핵정책, 제재 관련 외교 정책 및 국가안보 문제 관련), 탈북자 • 대표적 해킹 사례: 2020년 폴란드 정부 해킹, 2021년 6월 서울대병원 해킹, 2021년 한국원자력연구원 해킹. • 기타: 탈륨은 김수키와 동일조직으로 추정되며, 2019년 MS가 인터넷 계정 도용 혐의로 미연방법원에 고소

16) 악성 첨부파일을 이메일에 포함시키는 형태로 김수키의 공격에서 가장 많이 발견되는 방법.

라자루스	• 정찰총국 산하조직으로 2007년초 조직된 것으로 추정 • 2009-2014년까지는 한국과 미국을 집중적으로 공격하였으나 2015년 이후에는 금전적 수익을 목적으로 공격범위를 확장 • 주요 타겟: 가상화폐 거래소, 은행, 언론사, 엔터테인먼트 기업 등 다양한 산업분야와 방산분야에 대한 사이버 공격 • 대표적 해킹 사례: 2014년 소니픽처스 엔터테인먼트, 2017년 워너크라이 랜섬웨어 공격 배후 의심 • 기타: 히든 코브라(Hidden Cobra)로 불리기도 함
블루노로프	• 정찰총국 121국 산하조직으로 약 1,700명 안팎의 규모로 알려져 있으며 2014년초 최초 활동 포착 • 금전적 수익을 얻을 수 있는 곳만을 공격 • 주요 타겟: 남한을 포함한 글로벌 금융회사, 카지노, 가상화폐거래소, 금융 거래 소프트웨어 개발사 등 • 대표적 해킹 사례: 2016년 방글라데시 중앙은행 폴란드 금융감독원 해킹, 2018년 칠레 은행 해킹.
안다리엘	• 정찰총국 121국 산하조직으로 약 1,600명 안팎의 규모로 2016년 최초 활동 포착 • 무기개발 관련 정보 획득 및 경제적 이익 창출을 위한 해킹 활동 • 주요 타겟: 국내 방위산업체, 보안업체, 에너지연구소, 국방관련 기구를 비롯 도박게임, 여행사, 암호화폐거래소, ATM 기기 등 • 대표적 해킹 사례: 2016년 국방통합데이터센터 해킹, 2021년 KAI 해킹.

* 출처: 필자 작성.

- 이외 북한의 악명높은 해커로는 박진혁, 전창혁, 김일 등이 존재
  - 박진혁, 전창혁, 김일은 2021년 2월, 미 법무부에 전세계 은행과 기업을 상대로 13억 달러를 훔치려 한 혐의로 기소되었으며 이들의 자금세탁을 도운 갈렙 알라우마리에게 징역 11년 8개월이 선고된 상황
  - 박진혁은 앞서 2014년 소니픽처스 사이버 공격에 연루되어 2018년 미 정부에 기소당한 바 있으며 이는 미국이 사이버 범죄와 관련해 북한 공작원을 상대로 처음 기소한 사례

    ※ 박진혁은 미 재무부의 북한 제재대상에 올라 있는 북한 해커들의 위장회사인 '조선엑스포 합영회사'에서 10년 이상 근무

2. 김정은 시대 북한 사이버 공격의 특징

- 김정은 시대 사이버 공격의 특징은 '경제핵무력병진노선', '사회주의경제건설총력집중노선' 등 북한의 새로운 국가전략과 연계되어 시기별로 차별성을 가진다는 것
  - 이외에도 핵실험, 경제제재, 남북 및 북미 정상회담, 코로나19, 바이든 정부 출범 등 대내외 환경 변화와 연동되어 북한 소행으로 추정되는 사이버 공격이 노출되는 경우도 심심찮게 발견
    ※ 비록 김정은 시대 북한의 모든 사이버 공격이 반드시 특정시기와 정책적 노선을 중심으로 명확히 구분되고 분류될 수 있는 것은 아니지만 일부 경향성이 나타나고 있는 것은 분명해 보임

(1) 경제핵무력병진노선(2013.3.31~2018.4.20) 시기

가. 핵능력 강화와 관련된 사이버 공격

- (핵실험 연계 사이버 공격) 이 시기 북한은 경제핵무력병진노선을 새로운 전략노선으로 설정하고 핵능력을 꾸준히 증강하여 핵무력 완성을 선언(2017.11.)함에 따라 핵실험과 연계된 사이버 공격 감행
  - 2013년 2월 제3차 핵실험에 맞추어 방송사와 금융권에 대한 사이버 공격(2013.3.20.)과 청와대와 주요 정부기관에 대한 사이버 공격(2013.6.25.) 감행
  - 북한은 2016년 1월, 제4차 핵실험 감행에 맞추어 청와대 사칭 이메일 공격을 감행하였고, 2016년 9월 제5차 핵실험과 연계하여 사이버사령부 및 국방통합데이터센터 서버에 해킹 공격 시도
  - 2017년 9월, 제6차 핵실험과 연계하여 다음(daum) 이메일의 취약점을 이용한 공격과 가상화폐거래소 공격

- (투발수단 관련 신기술 탈취) 핵무력 완성을 위해 국내 방산업체 전산망과 해킹(2016.6.)은 물론 대우조선해양 해킹을 통해 잠수함, 무인기, 비행기 등 핵 투발수단 관련 국방신기술 탈취(2016.4.) 시도

- (미국과 국제사회에 대한 시위) 미국 영화사 소니픽처스 해킹(2014.11.)을 통해 기밀정보를 무차별적으로 유출하는 한편, '워너크라이 2.0' 랜섬웨어 공격을 통해 150여 개 국가에서 30만 대 이상의 컴퓨터를 감염시킴으로써 미국과 국제사회에 사이버 공격 능력을 과시(2017.5.)

- (원자력발전소 해킹으로 불안감 조성) 한국수력원자력의 직원 이메일을 통한 사이버 공격으로 원자력발전소 도면 등 기관 내부 자료와 청와대·국방부·국정원 작성문서로 추정되는 자료를 공개하여 국민 불안감 조성(2014.12.~2015.4.)[17]

- (핵개발 재원 마련) 방글라데시 중앙은행(2016.2.), 2017년 '워너크라이 2.0' 랜섬웨어 공격(2017.5.) 등을 통해 핵개발 자금을 마련한 것으로 추정[18]

- 경제핵무력병진노선 시기 북한의 사이버 공격은 방송 통신은 물론 원자력 발전소 등 기반시설에 대한 공격과 청와대 등 정부기관에 대한 공격, 핵 투발수단과 기타 국방기술 관련 사이버 무력시위를 감행하고 핵개발 자금을 확보하는데 주력했던 것으로 분석

나. 포괄적 경제제재에 대응한 사이버 공격

- 2016년 3월, 북한은 UN 역사상 가장 강력한 것으로 알려진 대북제재 결의안 2270호의 통과로 무기수출과 경제교역을 통한 외화수급에 심대한 차질이 생기자 사이버 공격을 적극 활용
  - 방글라데시 중앙은행을 공격(2016.2.)하여 8,100만 달러를 탈취한 사건을 비롯하여 '워너크라이 2.0' 랜섬웨어 공격(2017.5.), 가상화폐거래소 공격 등 경제제재 회피를 위한 사이버 공격을 지속 감행
  - 북한이 사이버 공격을 통해 매년 벌어들이는 수입은 최소 10억 달러로 추정되고 있으며 이는 북한의 연간 총 수출액의 1/3 수준[19]

17) 조원일, "'한수원 해킹' 결정적 단서는 없지만… "北 소행"," 『한국일보』, 2015년 3월 17일, https://www.hankookilbo.com/News/Read/201503171885878015 (검색일: 2021.9.30.).
18) 김상욱, "북한 사이버 공격으로 핵개발 자금 마련, 연간 약 10억 달러," 『뉴스타운』, 2017년 10월 21일, https://www.newstown.co.kr/news/articleView.html?idxno=301943 (검색일: 2021.10.3.).
19) Ibid.

(2) '사회주의경제건설총력집중' 노선(2018.4.20.~2021.1.) 시기

- 북한 당국은 남북 및 북미대화에 앞서 대북전략을 탐색하고, 경제발전에 필요한 외화확보와 민생경제 활성화에 필요한 기술탈취를 목적으로 사이버 공격 감행
  - 기존의 전략노선인 경제핵무력병진노선의 승리를 선언하고 새로운 전략노선으로 사회주의 경제건설총력집중노선을 제시하면서 경제제재 완화와 민생경제 활성화를 위해 사이버 공격을 적극 활용

가. 대북전략 공략을 위한 사이버 공격

- 2018년과 2019년 문재인 정부의 대북전략을 탐색하기 위해 통일부를 대상으로 수차례 해킹을 시도한 것으로 추정(2018, 630건: 2019, 767건)[20]

- 하노이 북미정상회담이 사실상 실패로 끝나면서 남북대화 역시 소강상태에 접어들자 북한은 국회 외통위, 정보위, 국방위 소속 국회의원들에 대한 사이버 공격(2019.9.)과 대북 전문가 집단에 대한 사이버 공격(2019.4.)으로 한국정부의 대북전략 탐색을 시도

- 2020년 6월, 북한의 남북연락사무소 폭파로 남북관계가 더욱 얼어붙으면서 북한의 해커조직인 탈륨은 한국정부의 대응전략을 파악하기 위한 차원에서 남한 외교안보라인에 대한 사이버 공격 감행(2020.7.)

나. 경제개발 관련 사이버 공격

- 관광산업 활성화를 위한 원산갈마관광지구 건설과 주민보건을 위한 평양종합병원 건설 등 김정은의 민생경제 행보가 잇따르면서 건설사업에 필요한 외화를 획득하기 위해 빗썸 가상화폐거래소 공격(2018.6.) 및 일본 가상화폐 코인체크 자산 탈취(2018.1.) 시도

20) 배영경, "통일부 대상 사이버 공격 2018년부터 급증…"피해는 없어"," 연합뉴스, 2021년 7월 7일, https://www.yna.co.kr/view/AKR20210707168700504 (검색일: 2021.10.1.).

다. 코로나19 대응 관련 사이버 공격

- 북한은 코로나19가 전(全) 세계적으로 확산됨에 따라 낙후된 의료체계를 고려하여 국경봉쇄와 주민들의 이동통제로 대응

- 공식적으로 김정은 정권은 북한내 코로나19 감염자가 없다고 발표하였으나 코로나19 백신 및 치료제 기술에 접근하기 위해 존슨앤 존슨, 노바백스, 신풍제약 등 한국·미국·영국의 6개 제약사에 해킹 시도

- 또한 코로나19로 인한 국경봉쇄와 제재의 장기화로 외화수급과 자원조달에 차질이 생기면서 비글보이스를 비롯한 해킹 조직들의 금융기관(2020.2.)과 가상화폐거래소(2020.11.)에 대한 사이버 공격 지속

(3) 제8차 당대회 이후(2021.1.~현재)

- 2021년 1월 개최된 제8차 조선노동당대회에서 김정은이 국방력 강화와 국가경제발전 5개년 계획의 실행을 천명하면서 핵무기 고도화를 위한 신기술 탈취, 민생경제 지원을 위한 의료정보 수집 및 남북대화 탐색을 위한 전방위적 사이버 공격 등이 발생

가. 핵무기 고도화를 위한 신기술 탈취

- 3000t급 신형 잠수함 등 각종 함정을 건조하는 대우조선해양(2021.6.)과 원자력 추진 잠수함에 필요한 소형 원자로 개발에 관여해온 것으로 알려진 한국원자력연구원에 대한 해킹(2021.7.) 시도

- 김수키의 소행으로 알려진 한국항공우주산업(KAI)에 대한 해킹으로 인해 KF-21 보라매 전투기와 한국형 다목적 기동헬기인 수리온 헬기 관련 기술이 유출된 것으로 추정(2021.3., 2021.5.)

나. 코로나19 관련 의료정보 수집

- 북한 해킹 조직인 김수키가 서울대병원 서버 1대와 업무용 PC 62대를 해킹하여 환자 정보 6,969건 유출된 것으로 분석(2021.6)

- 서울대병원뿐만 아니라 다른 국가기관 및 병원에 대한 대규모 침해 시도가 있었던 것으로 미루어 볼 때, 코로나19 관련 의료정보 탈취를 위한 공격으로 추정

다. 남북대화 탐색

- 북한은 2021년 5월 21일 열린 한·미정상회담을 전후로 '스피어 피싱(spear phishing)'을 대대적으로 감행(2021.5)하였으며 탈륨은 통일부 이메일을 사칭하여 '월간북한동향'과 통일연구원의 '조선노동당 제8차 대회' 분석 자료처럼 보이는 URL을 링크하여 공격

- 이들은 남북미 대화의 재개 가능성 등을 고려하여 한국정부의 전략을 탐색하고자 사이버 공격을 감행한 것으로 추정

- 이상의 내용을 간략히 정리하면 다음 [표 2]와 같음

[표 2] 김정은 시대 시기별 북한의 사이버 공격 특징

시기	주요 사건	주요 사이버 공격 사례	특징
경제 핵무력 병진 노선 (2013. 3.31 ~ 2018. 4.20)	핵실험 (2013.2.-2017.9) 및 핵무력 완성 선언 (2017.11.29)	• 3.20, 6.25 DDos(2013) • 청와대 사칭 스마트폰 공격(2016.1) • 사이버사령부, 국방통합데이터센터 공격(2016.9) • 다음 이메일 해킹공격(2017.9) • 잠수함 기술 해킹(2016.4) • 소니픽처스(2014.11) • 한수원 해킹(2014.11~2015.4) • 워너크라이 랜섬웨어 2.0(2017.5) • 한국은행 서버 해킹 시도(2017.9)	□ 사이버 무력행사 시기 • 핵실험과 연계된 사이버 공격 • 기반시설 마비를 통한 남한 사회 교란 • 국방 신기술 탈취 • 미국에 대한 시위 • 핵실험 재원 마련

〃	포괄적 경제 제재[21] (2016. 3) 및 7차 당대회 (2016.5)	• 방글라데시 중앙은행 해킹(2016.2) • 국제금융기관 해킹 (라자루스, 2016.10 ~2017.3) • 워너크라이 랜섬웨어 2.0(2017.5)	□ 경제제재 회피 시기 • 외화 획득(경제적 이득) • 핵실험 재원 마련
사회주의 경제건설 총력집중 (2018. 4.20 ~ 2021.1)	대화기 (평창-하노이-판문점, 2018.2 ~2019.6)	• 통일부 대상 해킹 시도 (2018, 630건: 2019, 767건) • 국회 외통위, 정보위, 국방위 소속 의원 공격(2019.9) • 한글 취약점 이용 대북 전문가 공격 (2019.4)	□ 대화탐색기 • 남북대화 전략 파악
	냉각기 (연락사무소 폭파, 2020.6~)	• 탈륨, 외교안보 공격(2020.7)	• 남한과 미국의 대북전략 파악
	경제 개발 (2018 ~2020)	• 빗썸 가상화폐거래소 공격(2018.6) • 일본 가상화폐 코인체크 자산 탈취 공격(2018.1)	□ 민생경제지원 공격기 • 원산갈마(2018.3~2019.10), 평양종합병원(2020.3~) 등 경제개발 외화벌이 공격
	코로나19 이후 (2019.12 ~ 현재)	• 금융기관 공격 (비글보이스 등, 2020. 2) • 가상화폐 거래소(2020.11), • 코로나 신기술 탈취 공격 (신풍제약 등, 2020.12)	□ 민생경제지원 공격 확산기 • 외화획득으로 민생경제 지원 • 코로나19 백신 및 치료제 기술 탈취 시도
8차 당대회 이후 (2021.1. ~현재)	8차 당대회 (2021.1)	• 한국원자력연구원(2021.7) • 한국항공우주산업(2021.3 및 5) • 대우조선해양(2021.6) • 서울대병원(2021.6) • 한미정상회담 사이버 공격 (2021.5. 전후) • 탈륨, 조선노동당 8차 대회 분석 위장 이메일 해킹 공격(2021.2)	□ 전방위 공격기 • 신기술 탈취 공격 • 민생경제지원 공격 • 남북대화 탐색

* 출처: 필자 작성.

21) UN의 대북 경제제재는 2016년 3월 2일 채택된 유엔 안보리 결의안 제2270호 이후 북한 경제 일반을 겨냥한 포괄적 제제로 변하였고 북한 경제에 심각한 타격을 가하고 있는 것으로 보임.

Ⅲ. 북한 사이버 위협에 대한 주요국 대응

1. 주요국의 대응

(1) 미국

- 미국의 사이버안보 관련 기관들은 북한의 사이버 공격에 특화된 대응 대책 마련을 위해 경보 발령과 사이버 공격의 특징을 정리한 보고서들을 발표함으로써 경각심 제고를 위해 노력
  - 연방수사국(FBI)과 CISA는 2020년 8월 26일 북한 해커들이 전 세계 은행들에 불법 접속해 불법 송금과 현금자동입출금기(ATM)를 통한 불법 인출을 시도하고 있다는 경보를 발령[22)]
  - 2020년 5월 12일, CISA와 사이버사령부, FBI는 북한 해커들이 사용하는 악성코드 3개에 대한 분석 보고서를 공동 작성·발간하여 악성코드의 개요와 대응 권장사항, 피해 경감대책 등을 정리하여 발표[23)]
  - 2020년 4월 15일, 미국 국무부, CISA, 재무부, 연방수사국(FBI) 등은 북한의 사이버 위협에 대한 인식제고를 위해 과거 북한의 사이버 공격 활동, 대책을 위한 권장 사항 등이 정리된 새로운 지침서를 발표[24)]

- 미 정부는 북한을 중국·러시아·이란과 더불어 사이버 보안상 '관심국'으로 지정하고 전담 모니터링 요원을 충원한 것으로 확인
  - 주로 북한 해킹 위협 등에만 포커스를 맞추어 추적·분석하는 컴퓨터 네트워크 보안 전문가를 배치

22) 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 (검색일: 2021.9.20.).
23) 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 (검색일: 2021.10.3.).; Cyber Security and Infrastructure Security Agency, "North Korea Cyber Threat Overview and Advisories," https://www.us-cert.gov/northkorea (검색일: 2021.10.3.).
24) 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 (검색일: 2021.9.20.).

- 북한이 사이버 공격시 미 국무부 등에 소속된 북한 전문가들이 필요한 자문에 신속하게 나설 수 있도록 시스템 정비[25]

• 또한 미국은 민간 기업과의 정보교류 범위를 확대하는 등 보다 공격적으로 대북(對北) 사이버전(戰)을 전개

• 미국은 북한의 사이버 공격에 주로 경제제재로 대응하고 있으며 대북 사이버 경제제재는 개인과 단체를 가리지 않고 적용되고 있는 상황
- 미국은 세계 금융기관 등에 대한 북한 사이버 공격의 심각성을 인식하고 2019년 9월 13일 라자루스 그룹, 블루노로프, 안다리엘 등 북한 3개 해킹조직을 제재 리스트에 포함[26]
- 2020년 12월에는 북한 정찰총국 소속 해커 전창혁·김일·박진혁 등을 미국 및 멕시코·폴란드·파키스탄·베트남·몰타 등 전 세계 은행과 기업, 암호화폐거래소 등에 대한 사이버 공격으로 13억 달러(약 1조 4,000억 원) 규모의 현금과 암호화폐를 절취 시도한 혐의로 기소[27]

• 미국의 제재로 북한의 해킹기관들과 해커들의 미국 내 자산은 동결되고 미 국민들과의 거래 역시 금지
- 향후 바이든 정부는 미국과 전략적 경쟁을 펼치고 있는 중국, 미국내 선거개입 의혹을 사고 있는 러시아뿐만 아니라 북한의 사이버 공격에 대한 경제제재를 더욱 확대해 나갈 것으로 전망[28]

• 그러나 바이든 정부는 경제제재만으로는 날로 심각해지는 러시아와 중국 및 북한의 사이버 공격에 제대로 대응할 수 없다고 판단하고 보다 공세적인 정책 집행을 예고한 상황[29]

---

25) 신진우·최지선, "미 '북 사이버 공격' 맞대응 나섰다...전담 모니터링 요원 배치," 『동아일보』, 2021년 7월 16일, https://www.donga.com/news/Politics/article/all/20210716/107979812/1 (검색일: 2021.9.30.).

26) 신헌철, "美, 北 해킹그룹 3곳 제재-강온 투트랙 전략," 『MK뉴스』, 2019년 9월 15일, https://news.mk.co.kr/v2/economy/view.php?year=2019&no=729729 (검색일: 2021.10.3.).

27) 이들은 '크립토뉴로 트레이더' 앱을 사용해 2020년 8월 뉴욕 금융기관에 침투해 디지털 지갑에서 1,180만 달러 규모의 암호화폐를 절취하였으며 슬로베니아 기업에서 7,500만 달러, 인도네시아 기업에서 2,490만 달러 등 총 1억 1,200만 달러의 암호화폐를 탈취한 혐의를 받고 있음. 박현영·이철재·고석현, "미국, "북한 해커, 총 대신 키보드로 가상지갑 턴 세계의 강도"," 『중앙일보』, 2021년 2월 19일, https://www.joongang.co.kr/article/23995352#home (검색일: 2021.10.5.).

28) 이미 미 재무부는 전문지식을 통해 사이버 공격 도구 및 인프라 개발, 악성 사이버 활동 지원 등 러시아 정보국의 사이버 프로그램을 지원한 혐의로 6개 기술기업에 대해 경제제재 조치를 단행.

29) David E. Sanger, Julian E. Barnes and Nicole Perlroth, "Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China", *The New York Times*, March 7, 2021, https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html (검색일: 2021.9.30.).

- 2021년 7월 27일, 바이든 대통령은 미국 정보공동체에 대한 연설을 통해 사이버 위협이 가상세계를 넘어 현실 세계에서도 점점 더 큰 장애와 피해를 야기하고 있다고 주의를 환기
- 특히 "세계 주요 경쟁국(major power) 사이에서 실제 교전(real shooting war)이 발생한다면 이는 사이버 공격으로 인한 심각한 결과의 산물"일 것이라고 하면서 사이버 안보의 중요성을 강조

• 최근 미국 국토안보부는 위험에 기반한 보안접근법을 개발하였고[30] 이를 사이버 안보에도 적용[31]
- 이 접근법에 따르면 위험(risk)은 위협(threat)과 취약성(vulnerability) 및 결과발생(consequence)의 곱으로 평가
  ※ 위협, 취약성, 결과발생을 감소시키면 위험은 감소하며, 이중 하나라도 완전히 제거하면 위험은 발생하지 않음
- 위협 제거를 위해서는 공격원점에 대한 타격이 가장 확실한 대응일 수 있으나, 공격원점에 대한 명백하고 확실한 증거, 타격의 동가치성 등에 따른 문제들로 인해 현실적 대응방안으로 활용 난망[32]

(2) 유럽연합(European Union, EU)

• 2019년 5월 22일, EU는 사이버 공격자에 대해 제재를 부과하는 법규(Council Decision 2019/797 and Council Regulation No.2019/796)를 통과
- EU는 사이버 공격을 감행한 개인과 기업 또는 국가기관을 상대로 자산동결과 여행금지 등 제재를 취할 수 있게 됨[33]

30) Department of Homeland Security, 2013 National Infrastructure Protection Plan: Partnering to Enhance Protection and Resilience, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf (검색일: 2021.10.1.).

31) Michael Chertoff, "Foreword," Cybersecurity Symposium: National Leadership, Individual Responsibility, 4 *Journal of National Security Law and Policy* (2010), p, 3.

32) 그러나 결과발생이나 위협의 감소를 위하여 대응타격의 개발(developing counter-strike capabilities)과 적극적 방어(active defense)를 강조하는 견해도 있다. Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *25 Harvard Journal of Law and Technology 429* (2012), pp. 474-485.

33) 최선영, "'영국, 북한 러시아 등의 사이버 공격에 제재할 것," 『연합뉴스』, 2019년 5월 24일, https://www.yna.co.kr/view/AKR20190524034600504 (검색일: 2021.10.1.).

• EU는 위 결정에 따라 2020년 7월 30일 처음으로 사이버 공격을 이유로 경제제재를 단행하고 조선엑스포합영회사를 제재 목록에 포함[34)]
  - 동 제재는 사이버 공격(Wanna Cry, Not Petya, Cloud Hopper 작전, 화학무기 금지기관에 대한 부정접속)을 시도한 북한, 러시아와 중국 등 해커 6명과 해커 그룹 3개에 대해 EU 역내 계좌 동결과 도항을 금지[35)]
  - 조선엑스포합영회사는 2017년 '워너크라이 2.0' 랜섬웨어 공격, 2017년 폴란드 금융 감독청 해킹, 2014년 소니픽처스 영화사 해킹, 2016년 방글라데시 중앙은행 사이버 공격 등을 감행
  - EU는 조선엑스포합영회사의 사이버 공격으로 EU와 회원국이 지대한 피해를 입었으며 특히 2017년 워너크라이 랜섬웨어는 EU내 기업을 포함한 세계 정보시스템에 상당한 지장을 발생시켜 경제활동과 필수 서비스 유지에 악영향을 초래하였다고 지적

• 2021년 5월, EU는 중국·러시아·북한 등에 부과한 사이버 제재 조치를 1년 더 연장하기로 결정
  - 2022년 5월 18일까지 EU나 회원국들을 위협하는 사이버 공격에 대한 제재 조치를 연장
  - 제재대상인 북한과 러시아, 중국의 개인 8명과 4개 기관의 자산이 동결되고 입국이 금지되는 한편, EU 회원국에 속한 개인이나 기관은 제제대상에 자금제공이 금지됨

• 앞서 EU는 2020년 12월 16일, 새로운 <EU 사이버안보 전략(EU Cybersecurity Strategy)>을 발표하고 사이버 위협 대응방향을 정립하였으며 이에 따라 대북 사이버 제재 역시 강화될 것으로 예상
  - EU는 보고서를 통해 사이버 위협으로부터 유럽의 회복력을 강화하고 시민들과 기업들이 사이버 공간에서의 신뢰성 확보로 혜택받도록 할 것임을 선언
    ※ 사이버 공간에서의 국제기준이나 표준에 관한 유럽연합의 리더십을 확대하고 안전한 사이버 공간을 촉진하기 위한 세계 각지의 파트너와의 협력 강화를 주장

34) 오다인, "EU, 첫 사이버 제재 이행...북한 조선 엑스포 등 개인 6·기관 3곳," 『전자신문』, 2020년 7월 31일, https://m.etnews.com/20200731000135 (검색일: 2021.10.1.).

35) Council of the European Union, "EU Imposes the First Ever Sanctions against Cyber-Attacks," July 30, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ (검색일: 2021.9.30.).; Laurens Cerulus and Elisa Braun, "In a First, EU Slaps Sanctions on Hackers in Russia, North Korea, China," July 30, 2020, https://www.politico.eu/article/eu-slaps-sanctions-on-hackers-in-russia-north-korea-china/ (검색일: 2021.9.30.).

- 한편 사이버 위협에 대한 대응으로 사이버 공간에서의 회복력뿐만 아니라 물리적인 회복력도 강화하여, 사이버 공격으로부터 범죄는 물론 자연재해나 인터넷 관련 모든 위협에 대응할 것임을 예고[36]

• 현재까지 EU의 대북 사이버 제재는 미국에 비해 정교하다고 평가할 수는 없으나 일부 유사성이 확인되고 있음
- 사이버 공격 의심 대상에 대한 제재를 정당화하는 것뿐만 아니라 여행금지와 자산동결과 같이 제재대상이 되는 주체와 제재 유형에도 유사성이 발견됨
- 예를 들어, EU가 제재하고 있는 조선엑스포합영회사의 경우 이미 미 재무부의 제재대상인바, 향후 EU는 미 정부와 북한·중국·러시아 등 공동의 사이버 위협 대상에 대해 제재협력을 기대할 수 있을 것으로 예상[37]

(3) 국제연합(United Nations, UN)

• UN은 아직까지 북한의 사이버 위협과 관련하여 직접적으로 제재를 가하고 있진 않지만 대북제재위 보고서 등을 통해 북한의 사이버 위협 능력과 피해 사례 증가에 대해 경각심을 제고하고 있음

• 2019년 UN안보리는 17개국에서 발생한 35건의 사이버 사건의 배후로 북한을 지목하고 UN 제재 위반임을 발표
- UN안보리는 북한이 불법송금 및 이체, 암호화폐거래소 해킹 등을 통해 군대운영을 위한 자금으로 사용하고 있다고 주장하는 한편, 북한의 사이버 공격을 대북제재 위반시도로 규정

36) European Commission, "New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient," December 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (검색일: 2021.9.30.).
37) Ramon Pacheco Pardo, "From Engagement to Pressure: The EU Gets Tougher on North Korean Sanctions," 38 North, September 10, 2020, https://www.38north.org/2020/09/rpachecopardo091020/ (검색일: 2021.9.30.).

• 한편 UN안보리 산하 대북제재위원회는 전문가 패널 조사보고서를 통해 북한의 핵·미사일 프로그램 동향과 함께 사이버 위협 능력 강화를 예의 주시
  - 대북제재위는 약 2천 명에 달하는 북한 국적의 사람들이 중국에 단순 방문비자로 입국하여 IT분야에 진출해 있으며 암호화폐 해킹 등을 통해 수입을 올리고 있다고 주장
  - 또한 북한이 사이버 공격을 통해 창출한 금전적 이익을 핵·미사일 프로그램에 투자함으로써 국제적 비확산 노력이 물거품이 될 가능성이 있다고 지적

• 2021년 3월 발표된 UN안보리 대북제재위 보고서는 북한이 2019·2020년 해킹으로 3억 1,640만 달러(약 3,610억 원)를 탈취했다고 발표
  - 보고서는 북한 관련 해킹기관들이 대량살상무기 및 탄도미사일 프로그램 지원 자금 조달을 목적으로 2020년에 금융기관과 가상화폐 거래소를 대상으로 작전을 지속했다고 지적
  - 나아가 대북제재위는 사이버 공간에서 대부분의 불법행위를 지휘한 주체로 정찰총국을 지목[38)]

• 이밖에도 UN안보리는 북한이 개최하는 암호화폐 컨퍼런스에 참석하지 말 것을 경고하는 한편, 미국과 공동으로 무기와 자동차 시스템을 겨냥한 북한의 해킹 가능성에 대해 경고
  - 대북제재 전문가들은 암호화폐 컨퍼런스 참석이 김정은 정권의 제재 회피와 자금세탁을 돕는 행위로 간주될 수 있어 제재 위반에 따른 기소 가능성을 경고
  - 또한 사실상 북한의 사이버 위협을 억지하는 것은 불가능하지만, 운영비용을 늘려 북한 인프라를 교란 및 노출시키고 공격하는 것이 필요하다고 조언[39)]

38) 신진우·최지선, "미, '북 사이버 공격' 맞대응 나섰다…전담 모니터링 요원 배치," 『동아일보』, 2021년 7월 16일, https://www.donga.com/news/Politics/article/all/20210716/107979812/1 (검색일: 2021.10.1.).

39) Eun Dubois, "Building Resilience to the North Korean Cyber Threat: Experts Discuss," Brookings Institution, December 23, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/12/23/building-resilience-to-the-north-korean-cyber-threat-experts-discuss/ (검색일: 2021.10.4.).

2. 한국의 대응 및 개선 방향

(1) 대응 상황

- 한국은 북한의 사이버 위협에 대해 △구조화된 지휘통제시스템 △인터넷으로부터 인트라넷을 분리하는 강력한 네트워크 분리정책 △정부가 조직한 사이버 위협 정보 공유 시스템 △공공 및 민간부문에서 사이버 전문가 양성을 위한 교육 및 Peer-to-Peer 멘토링 프로그램 등으로 대응[40)]
  - 한국의 인터넷-인트라넷 완전 분리 방침은 중요도에 따라 정보를 분리하는 다른 나라보다 엄격한 조치로 볼 수 있음

- 위와 같은 대응책에도 불구하고 한국의 북한 사이버 위협 대응은 몇 가지 도전과제를 안고 있는 상황
  - 현 대응책은 클라우드 서비스와 개인 데이터 전송을 포함하는 한국의 4차산업 정책과 배치되며 사이버 안보 분야 전문가 육성에 난항

- 문재인 정부는 2019년 4월 3일 역대 최초로 〈국가사이버안보전략〉을 발표하여 사이버 공간에서 우리 국민의 안전을 보장하기 위한 사이버안보분야 정책 방향을 정립
  - 동 전략은 △국가 핵심 인프라 안전성 제고 △사이버 공격 대응 역량 고도화 △신뢰와 협력 기반 거버넌스 정립 △사이버보안 산업 성장기반 구축 △사이버보안 문화 정착 △사이버안보 국제협력 선도 등 6대 전략과제을 제시
  - 정부는 국가사이버안보전략을 차질 없이 추진하기 위하여 6대 전략과제별로 2019년부터 2022년까지를 대상으로 하는 범부처 차원 국가사이버안보 기본계획을 수립·시행

- 이와 함께 국가정보원은 「국가정보원법」의 전면 개정으로 국제 및 국가배후 해킹조직 등 사이버안보"에 관한 정보의 수집·작성·배포의 직무를 수행하는 법적 근거를 확립[41)]

40) Ibid.
41) 「국가정보원법」 제4조 제1항 제1호 마목.

- 나아가 △중앙행정기관 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회 △지방자치단체와 그 소속기관 △그밖에 대통령령으로 정하는 공공기관 등을 대상으로 하는 사이버 공격 및 위협에 대한 예방 및 대응 업무를 수행하기로 결정[42]
- 국가정보원은 사이버 공격에 대해 단순한 기술적 대응을 넘어 국외로부터 발생하는 공격에 대한 탐지와 예방을 기초로 정보의 분석과 판단을 통해 복구 및 회복력을 담보할 것을 확인

• 그럼에도 불구하고 북한은 핵무기 고도화를 위한 신기술 탈취, 민생경제 지원, 한국정부의 대남전략 탐색 등을 위해 전방위적 사이버 공격을 감행하고 있으며 우리의 대응에도 일부 한계가 노정되고 있는 상황
  - 사이버 공격에 대해 북한의 소행이라는 명백하고 확실한 직접적인 증거(clear and convincing evidence)의 제시가 어려운 데다 가해 당사자로 의심되는 북한이 이를 부인하면서 사이버 공격의 책임을 부담하기 곤란하다는 현실적 어려움 존재

• 그러므로 사이버 위협을 사전 탐지하고 모니터링하여 예방함으로써 취약성을 감소시키는 것이 가장 현실적 대안
  - 사이버 공격에 대한 △모니터링과 조기경보체계 △취약성 평가 △신속한 위기대응 체계 가동 및 복구 등을 통해 위협, 취약성 및 결과 발생을 감소시킴으로써 사이버 공격에 효과적으로 대응할 필요

(2) 정책적 개선 방안

• 만약 미국이나 국제사회가 북한의 사이버 공격에 대해 물리적 타격을 고려한다면 한국정부는 이를 저지하는 한편, 기술적 지원을 통한 갈등 관리에 주력하는 것이 바람직

42) 「국가정보원법」 제4조 제1항 제4호.

- 미국의 경우, 디지털 정밀 전쟁 시대에 사이버 공격은 자위권 발동을 가능하게 하는 무력행사이므로[43] 물리적 공격이 가능하다는 이론적 기반하에 공세적 사이버 안보 정책을 추진할 가능성도 농후[44]
- 바이든 정부가 사이버 공격에 대해 사이버적 수단과 비사이버적 수단을 사용하여 실질적인 비용을 부과시키는 방식으로 비례적으로 대응할 것이라고 밝힌 것을 볼 때 보다 강력한 비사이버적 수단을 적극 활용할 것으로 전망[45]
- 아시아유럽정상회의(ASEM), 아세안안보포럼(ARF), G20 등을 통해 북한의 사이버 공격이 관리되도록 회원국들과 협력하고 이들에 대한 기술적 지원 확대
- 물리적 수단을 사용하는 경우 명백성, 인도성, 비례성 및 필요성 등 국제법 원칙을 준수하여야 함을 강조하고 사용 자제를 유도
- 아울러 북한의 금융기관과 가상화폐거래소 등에 대한 해킹 공격은 더욱 거세질 것으로 보이는바, 이를 지속적으로 모니터링하고 피해를 차단하기 위한 기술적 지원을 강화

• 북한의 랜섬웨어 공격에 대한 국제사회의 대응에는 한국정부 역시 사이버 범죄 대응차원에서 참여할 필요
  - 2021년 5월 21일, 한미정상회담에서 문재인 대통령과 바이든 대통령은 랜섬웨어 공격에 대처하기 위해 법집행 및 국토안보 기관 간의 협력을 강화하는데 중점을 둔 사이버워킹그룹을 신설하기로 합의
    ※ 바이든 정부는 랜섬웨어 공격이 대가 지급을 노린 사이버범죄 행위라는 판단하에, 러시아 등 권위주의 국가와 협력하여 대응하는 것까지 고려
  - 한국정부는 랜섬웨어 공격자들의 가상화폐를 통한 대가 수취를 차단하기 위해 가상화폐로 대가 지급시 정부에 보고하도록 하고, 가상화폐거래소와 금융기관으로 하여금 거래보고나 등록 조치를 시행하도록 함으로써 가상화폐의 익명성을 제한할 필요

43) Yevgeny Vindman, "Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is.", *LAWFARE* (January 26, 2021).
44) James Andrew Lewis, "Toward a More Coercive Cyber Strategy", CSIS Report, March 10, 2021, https://www.csis.org/analysis/toward-more-coercive-cyber-strategy (accessed: March 29, 2021).
45) The White House, *Interim National Security Strategic Guidance*, March 2021. p.18. respond swiftly and proportionately to cyberattacks by imposing substantial costs through cyber and noncyber means.

Ⅳ. 결론

- 김정은 시대 들어 북한은 사이버 능력 개발에 더욱 심혈을 기울이고 있으며 현재 상당한 사이버 공격 능력을 갖춘 것으로 평가
  - 사이버 공격은 초기 비용이 적게 들고 익명성과 비밀이 보장되어 북한이 비교적 자유롭게 불법적 활동을 통한 이익을 취할 수 있다는 장점을 지님
  - 현재 북한의 사이버 공격 능력은 어떤 나라의 시설도 공격할 수 있을 정도로 위협적인 능력을 갖추었다는 평가

- 김정은 정권은 사이버 공격을 외화벌이 수단으로 활용하여 대북제재를 무력화하고 있을 뿐만 아니라 핵·미사일 전력에 소요되는 비용을 충당하고 있는 것으로 알려져 국제사회에 심각한 위협이 되고 있음
  - 북한은 경제적 이유뿐만 아니라 군사·외교 기밀 유출과 같은 다양한 목적으로 외국 정부, 군사기관 및 방위산업체, 에너지연구소 등을 대상으로 광범위하게 사이버 공격을 가하고 있는 상황

- 미국 및 EU, UN 등 국제사회는 북한의 주요 해킹조직과 사이버 요원들에게 제재를 부과하거나 사이버 위협에 대한 경각심을 높이는 방식으로 대응
  - 미 정부는 북한 3개 해킹조직을 제재 리스트에 포함하는 한편, 일부 북한 해커들을 해킹을 통한 현금 및 암호화폐 절취 시도 혐의로 기소
  - 이 같은 미국의 제재로 북한의 해킹기관들과 해커들의 미국 내 자산은 동결되고 미 국민들과의 거래 또한 금지되고 있으며 EU 역시 조선엑스포합영회사를 제재 대상에 포함

- 그러나 날로 심각해지는 북한의 사이버 위협에 대해 미 정부는 제재 이상의 강력한 대응의 필요성을 주장하고 있으며 심지어 일각에서는 물리적 타격의 가능성까지 언급하고 있는 상황

- 이에 따라 우리 정부는 미국을 설득하여 물리적 타격과 같은 극단적 대응을 저지하는 한편, 위협을 사전 탐지하고 모니터링함으로써 예방할 수 있도록 지원할 필요

- 특히 사이버 위협에 대한 취약성을 감소시키기 위하여 컴퓨터 네트워크 시스템에 대한 취약성 분석 평가 및 관리 체계를 구축하고 일정 시점마다 평가하는 것이 필요
  - 결과 발생의 방지나 예방과 관련하여 신속한 복구 및 회복력의 담보가 실행되도록 하여야 하며 특히 주요 정보통신기반에 대한 사이버 공격 결과가 심각하기 때문에 기반보호에 관심 요구
  - 아울러 신속한 복구와 회복력을 위해 시스템의 백업, 운영인력 현황 등에 대하여도 주기적으로 점검할 필요

- 결국 △사이버 공격에 대한 모니터링과 조기경보체계 △취약성 평가 △신속한 위기대응 체계 가동 및 복구 등을 통해 위협, 취약성 및 결과 발생을 감소시키도록 유도함으로써 사이버 공격에 효과적으로 대응하는 자세가 필요

참고문헌

국문

「국가정보원법」 제4조 제1항 제1호 마목.

「국가정보원법」 제4조 제1항 제4호.

국기연. "북한 사이버 공격 능력 러시아에 이어 세계 2위." 『세계일보』. 2019년 2월 20일, https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=100&oid=022&aid=0003341501 (검색일: 2021.10.5.).

국방부. 『국방백서 2020』 (서울: 국방부, 2020).

김귀근. "김정일 "정보전부대는 나의 배짱이고 예비대"." 연합뉴스. 2011년 6월 28일. https://www.yna.co.kr/view/AKR20110628128400043 (검색일: 2021.9.30.).

김문경. "과거와 다른 핵-경제 병진...한미에 공 넘긴 북," YTN, 2021년 1월 14일. https://www.ytn.co.kr/_ln/0101_202101140025017924 (검색일: 2021.10.4.).

김상욱. "북한 사이버 공격으로 핵개발 자금 마련, 연간 약 10억 달러." 『뉴스타운』. 2017년 10월 21일. https://www.newstown.co.kr/news/articleView.html?idxno=301943 (검색일: 2021.10.3.).

김성진. "북한, 소니 영화사 해킹 배후설은 조작." KBS. 2014년 12월 5일. https://news.kbs.co.kr/news/view.do?ncd=2978823 (검색일: 2021.9.30.).

김윤영·양철호 "북한의 사이버테러에 대비한 법·제도 개선방안 연구." 『유럽헌법연구』. 제33호 (2020), pp. 355-384.

김정률. "미 국무부, 북한, 파괴적 사이버 활동 능력 보유." 『뉴스1』. 2021년 6월 30일. https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=104&oid=421&aid=0005446233 (검색일: 2021.9.30.).

김지원. IAEA "북한, 핵 프로그램에 전력 중. 매우 유감"…북핵 감시 강화, 『경향신문』. 2021년 9월 20일. https://m.khan.co.kr/world/world-general/article/202109201957001#c2b (검색일: 2021.10.5.).

문동희. "정찰총국 인사조치에 대남 사이버 공격 강화 우려…어떤 부서길래." 『데일리 NK』. 2020년 9월 23일. https://www.dailynk.com/%ec%a0%95%ec%b0%b0%ec%b4%9d%ea%b5%ad-%ec%9d%b8%ec%82%ac%ec%a1%b0%ec%b9%98%ec%97%90-%e5%b0%8d%e5%8d%97-%ec%82%ac%ec%9d%b4%eb%b2%84%ea%b3%b5%ea%b2%a9-%ec%9a%b0%eb%a0%a4-%ec%96%b4%eb%96%a4-%eb%b6%80/ (검색일: 2021.9.31.).

미키 배(Mickey Bae). “미 국방보고서 북한 사이버·전자정보전 역량 일선 부대서도 운용.” 『ENB』. 2020년 8월 18일. http://www.enbnews.org/news/articleView.html?idxno=21530 (검색일: 2021.9.30.).

박병수. “김정은 “핵무력 완성” 선언…북 ‘대화 국면’ 전환 가능성.” 『한겨레』. 2017년 11월 29일. https://www.hani.co.kr/arti/politics/defense/821244.html#csidx969ac0dc4dbbf8a9f9e4b4f849c8b1b (검색일: 2021.9.30.).

박현영·이철재·고석현. “미국, “북한 해커, 총 대신 키보드로 가상지갑 턴 세계의 강도”.” 『중앙일보』. 2021년 2월 19일, https://www.joongang.co.kr/article/23995352#home (검색일: 2021.10.5.).

박형주. “북한 ‘핵’ 언급 현저히 줄어…“김정은 내부 문제 집중, 핵 정책 변화 아냐”.” 『VOA』. 2021년 8월 28일. https://www.voakorea.com/a/korea_korea-politics_north-korea-nuclear-policy/6061281.html (검색일: 2021.10.4.).

배영경. “통일부 대상 사이버 공격 2018년부터 급증…“피해는 없어”.” 연합뉴스, 2021년 7월 7일. https://www.yna.co.kr/view/AKR20210707168700504 (검색일: 2021.10.1.).

백상미. “북한의 대남 사이버 공격에 대한 국제법적 검토와 이에 대한 한국의 대응전략.” 『서울국제법연구』. 제27권 2호(2020), pp. 39-66.

신진우·최지선. “미, ‘북 사이버 공격’ 맞대응 나섰다…전담 모니터링 요원 배치.” 『동아일보』. 2021년 7월 16일. https://www.donga.com/news/Politics/article/all/20210716/107979812/1 (검색일: 2021.10.1.).

신헌철. “美, 北 해킹그룹 3곳 제재-강온 투트랙 전략.” 『MK뉴스』. 2019년 9월 15일. https://news.mk.co.kr/v2/economy/view.php?year=2019&no=729729 (검색일: 2021.10.3.).

양문수. “핵-경제 병진노선 소멸된 북한, 지난 4월 ‘경제건설 집중’ 선언.” 『나라경제』, 2018년 8월호, https://eiec.kdi.re.kr/publish/naraView.do?cidx=11656 (검색일: 2021.9.27.).

오다인. “EU, 첫 사이버 제재 이행... 북한 조선 엑스포 등 개인 6·기관 3곳.” 『전자신문』. 2020년 7월 31일. https://m.etnews.com/20200731000135 (검색일: 2021.10.1.).

이영종·윤호진. “김정은 “사이버전은 만능의 보검” 3대 전쟁수단 운용.” 『중앙일보』 2013년 11월 5일. https://www.joongang.co.kr/article/13048072#home (검색일: 2021.9.30.).

이태규. “북한 해킹 능력, 정교하지 않지만 위협적.” 『한국일보』. 2021년 8월 2일. https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=104&oid=469&aid=0000621287 (검색일: 2021.9.30.).

정영애. “북한의 사이버 공격 역량의 진화: 사이버 공격 사례 분석을 중심으로.” 『평화학연구』. 제20권 4호 (2019), pp. 125-143.

조원일, “‘한수원 해킹’ 결정적 단서는 없지만… “北 소행”,” 『한국일보』, 2015년 3월 17일, https://www.hankookilbo.com/News/Read/201503171885878015 (검색일: 2021.9.30.).

최선영. “영국, 북한·러시아 등의 사이버 공격에 제재할 것.”『연합뉴스』. 2019년 5월 24일. https://www.yna.co.kr/view/AKR20190524034600504 (검색일: 2021.10.1.).

하윤해, “미, 6800억원 탈취한 북 해킹그룹 3곳 제재, 정찰총국이 배후,” 2019년 9월 15일,『국민일보』, http://news.kmib.co.kr/article/view.asp?arcid=0013711916&code=61131111&cp=nv (검색일: 2021.9.25.).

황지환. “북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산.”『동서연구』. 제29권 1호(2017), pp.139-159.

“고질적 버릇, 상투적 수법,”『우리민족끼리』, 2021년 7월 12일.

영문

Cerulus, Laurens and Elisa Braun. “In a First, EU Slaps Sanctions on Hackers in Russia, North Korea, China.” The Politico. July 30, 2020, https://www.politico.eu/article/eu-slaps-sanctions-on-hackers-in-russia-north-korea-china/ (검색일: 2021.9.30.).

Chertoff, Michael. “Foreword.” Cybersecurity Symposium: National Leadership, Individual Responsibility, 4 *Journal of National Security Law and Policy* (2010), pp. 1-6.

Council of the European Union. “EU Imposes the First Ever Sanctions against Cyber-Attacks.” July 30, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ (검색일: 2021.9.30.).

Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § § 1501 - 1510).

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 (검색일: 2021.9.20.).

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 (검색일: 2021.10.3.).

Cyber Security and Infrastructure Security Agency. “North Korea Cyber Threat Overview and Advisories.” https://www.us-cert.gov/northkorea (검색일: 2021.10.3.).

Department of Homeland Security, 2013 National Infrastructure Protection Plan: Partnering to Enhance Protection and Resilience, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf (검색일: 2021.10.1.).

Dubois, Eun. "Building Resilience to the North Korean Cyber Threat: Experts Discuss." Brookings Institution. December 23, 2020. https://www.brookings.edu/blog/order-from-chaos/2020/12/23/building-resilience-to-the-north-korean-cyber-threat-experts-discuss/ (검색일: 2021.10.4.).

European Commission. "New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient." December 16, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (검색일: 2021.9.30.).

Kesan, Jay P. and Carol M. Hayes. "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace." *25 Harvard Journal of Law and Technology 429* (2012), pp. 474-485.

Lewis, James Andrew. "Toward a More Coercive Cyber Strategy." CSIS Report. March 10, 2021, https://www.csis.org/analysis/toward-more-coercive-cyber-strategy (검색일: 2021.3.29.).

Pardo, Ramon Pacheco. "From Engagement to Pressure: The EU Gets Tougher on North Korean Sanctions." 38 North. September 10, 2020, https://www.38north.org/2020/09/rpachecopardo091020/ (검색일: 2021.9.30.).

Sanger, David E., David D. Kirkpatrick and Nicole Perlroth. "The World Once Laughed at North Korean Cyberpower. No More," The New York Times. October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (검색일: 2021.9.30.).

Pardo, Ramon Pacheco. "From Engagement to Pressure: The EU Gets Tougher on North Korean Sanctions." 38 North, September 10, 2020, https://www.38north.org/2020/09/rpachecopardo091020/ (검색일: 2021.9.30.).

The International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," IISS, February 2019.

The Treasury, and Homeland Security, and the Federal Bureau of Investigation, "Guidance on the North Korean Cyber Threat," U.S. Department of State, https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf (검색일: 2021.9.30.).

The White House. *Interim National Security Strategic Guidance*, March 2021.

U.S. Army Headquarters. "North Korean Tactics," July 2020, p.E-2, https://irp.fas.org/doddir/army/atp7-100-2.pdf (검색일: 2021.9.30.).

Vindman, Yevgeny "Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is." *LAWFARE* (January 26, 2021).

Abstract

The Rise of North Korean Cyber Threats in the Kim Jong Un Era: How Can We Respond?

Bomi Kim
IL SEOK OH
(Institute for National Security Strategy)

Over the past few years, the cyberattacks believed to have been committed by North Korea have soared. Pyongyang recognizes a cyber warfare capability as one of the major asymmetric power and trains hackers at the national level, and they are currently conducting cyberattacks around the world. Pyongyang is suspected of directing cyber heists to its units in order to fund its economy and nuclear and ballistic missile programs. North Korea is also known to be committing malicious cyberattacks extensively on foreign governments, military agencies, defense industry companies, and energy research institutes for various purposes, such as leaking military and diplomatic secrets. The international community is mainly responding to cyber threats by North Korea through economic sanctions, but as the hacking damage increases and becomes more serious, some in the U.S. are insisting on the need for strong countermeasures, including physical strikes. However, it is difficult to justify punishment for cyberattackers because responsibility is unclear due to anonymity. The South

Abstract

Korean government, facing the constant cyber threats from North Korea, should prepare realistic countermeasures to proactively detect, monitor, and prevent North Korean cyber threats through active cyber security activities.

Keywords: North Korea, Cyber Security, Hacking, sanctions on North Korea, Lazarus

INSS 전략보고

November 2021. No.147

※ 본지에 실린 내용은 집필자 개인의 견해이며, 국가안보전략연구원의 공식입장이 아닙니다.

국가안보전략연구원

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr