INSS 연구보고서 2022-03

북한 사이버위협의 특징과 대응방안

: 김정은 시대를 중심으로

김보미 · 오일석

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

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

비매품/무료
94340
9 791189 781828
ISBN 979-11-89781-82-8
ISBN 979-11-89781-79-8 (세트)

INSS 연구보고서 2022-03 북한 사이버위협의 특징과 대응방안 : 김정은 시대를 중심으로 | 김보미 · 오일석

2022
INSS
RESEARCH
REPORT

INSS 연구보고서 2022-03

북한 사이버위협의 특징과 대응방안

: 김정은 시대를 중심으로

김보미 bomi@inss.re.kr
오일석 nusl2006@inss.re.kr

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY 국가안보전략연구원

2022
INSS
RESEARCH
REPORT

INSS 연구보고서 2022-03

북한 사이버위협의 특징과 대응방안

: 김정은 시대를 중심으로

김보미
오일석

INSS INSTITUTE FOR NATIONAL SECURITY STRATEGY
국가안보전략연구원

김보미 (金甫美)

| 국가안보전략연구원 부연구위원

미국 University of Michigan, Ann Arbor를 졸업한 후 New York University에서 정치학 석사, 북한대학원대학교에서 북한학 박사학위를 받았다. 비대칭 전력과 군사전략, 당군관계 등 북한 군사 분야를 중점적으로 연구 중이다. 저서로는 『김일성과 중소분쟁』(단독), 『민군관계와 대한민국 육군』(공저), 『북한학의 새로운 시각』(공저) 등이 있으며, 학술논문으로는 "북한 핵프로그램의 시작과 성장," "김정은 정권의 핵무력 고도화의 원인과 한계," "North Korea's Siege Mentality: A Sociopolitical Analysis of the Kim Jong-un Regime" 등이 있다.

오일석 (吳一錫)

| 국가안보전략연구원 연구위원

고려대학교 법학 박사학위를 받았으며, 주요 연구분야는 사이버안보, 신기술과 법제, 에너지 및 보건안보, 신흥안보 분야 남북협력, 계약법과 불법행위법, 국가정보 등이다. 주요 저서 및 논문으로는 『입법과정의 이론과 실제(2016)』, "메타버스 공간에서의 남북교류 가능성에 대한 고찰(공저, 2022)", "코로나19 디지털 접촉 추적과 개인정보 보호(2021)", "코로나19 이후 신안보 위협과 대응전략(공저, 2020)", "미국 정보기관 제로데이 취약성 대응 활동의 법정책적 시사점(2019)", "가짜뉴스에 대한 법적 고찰(공저, 2018)" 등이 있다.

INSS 연구보고서 2022-03

북한 사이버위협의 특징과 대응방안

: 김정은 시대를 중심으로

김보미
오일석

목차

국문초록

김정은 시대 북한의 사이버능력의 발전과 함께 정권 차원에서 이를 불법적으로 활용하는 사례가 늘어나고 있다. 김정은 집권 이후 북한은 사이버능력을 핵 · 미사일과 함께 비대칭 전력 중 하나로 적극 활용하고 있으며 북한은 자산 탈취, 군사 · 외교 기밀 유출과 같은 다양한 목적하에 세계 각국의 금융기관, 외국 정부, 군사기관 및 방위산업체, 에너지연구소 등을 대상으로 사이버공격을 광범위하게 감행하고 있다. 특히 북한이 불법적 사이버 활동을 통해 확보한 수익은 핵 · 미사일 능력을 지탱하기 위해 자금이 절실한 김정은 정권에 현금 공급망이 되어 비핵화를 위한 국제사회의 노력에 장애물로 작용하고 있다. 이에 따라 본 연구보고서는 김정은 시대 북한의 사이버위협 능력과 특징을 식별하고 국제사회의 대응을 살펴보는 한편 이를 바탕으로 우리에게 필요한 정책들은 무엇인지 제시하고자 한다. 구체적으로 본 연구는 2장에서 김정은 시대 북한의 사이버 역량 및 주요 해킹 조직들을 소개하고, 북한 사이버공격의 특징을 ① 암호화폐 공격 ② 랜섬웨어 공격 ③ 국방산업 신기술 탈취 ④ 대북 · 대외전략 정보수집 ⑤ 코로나19 백신 기술 탈취 등 5가지로 분류하여 현황을 분석한다. 3장에서는 북한의 사이버위협에 대한 국제사회의 대응방안을 경제제재, 랜섬웨어 대응, 암호화폐 공격 대응의 측면에서 조명한다. 4장에서는 앞서 논의된 김정은 정권의 악의적 사이버 활동과 국제사회의 대응방안을 고려하여 우리의 합리적 대응방안을 제시하되, 보다 공세적인 대응방안의 필요성에 대한 고민을 국제협력 강화와 국내역량 강화라는 두 가지 측면에서 논의하고자 한다. 마지막으로 결론에서는 1장에서 4장까지의 논의를 정리하고 향후 예상되는 북한의 사이버위협은 어떠한 양상을 보일 것인지 전망한다.

핵심어

북한, 김정은 시대, 사이버공격, 암호화폐, 랜섬웨어

I

서론

1. 문제제기

2022년 5월 21일에 개최된 한미정상회담에서 가장 눈에 띄는 내용 중 하나는 한미 간 사이버 협력의 강화였다. 윤석열 대통령과 조 바이든(Joe Biden) 미 대통령이 발표한 공동성명에서 사이버보안, 사이버안보, 사이버공격 등 사이버와 관련한 단어는 총 12번이나 언급되었을 정도로 사이버보안은 양국 간 핵심의제로 부상하였다. 한미 정상은 특히 대북안보를 주제로도 북한 핵·미사일 프로그램에 대한 한미의 억제태세를 강조하는 데 그치지 않고 "북한으로부터의 다양한 사이버위협에 대응하기 위한 협력을 대폭 확대해나갈 것"임을 확인하였다.[1] 이는 북한의 사이버위협에 대해 동맹 차원에서의 대응이 필요하다는 데 양국이 인식의 공감대를 형성하였으며 후속 협력 조치를 할 것임을 시사한 것이었다.

또한 이와 같은 합의에 기반하여 2022년 7월 26일, 김성한 국가안보실장을 비롯한 우리 정부의 국가안보실 측과 앤 뉴버거(Anne Neuberger) 미 백악관 NSC 사이버·신기술 담당 부보좌관은 회동하여 한미 간 사이버안보 분야 협력을 확대해나가기 위한 방안에 대해 논의하였다. 양측은 진화하는 북한의 위협양상에 따라 국제사회의 대응 또한 달라져야 한다는 데 공감하고 사이버위협에 효과적으로 대응하기 위한 공동노력을 심화해나가기로 합의했다.

1 한미 정상회담(5.21.) 공동성명.

한미가 이처럼 북한의 사이버위협에 대한 경각심을 제고하게 된 것은 김정은 시대 북한의 사이버능력의 발전과 함께 정권 차원에서 이를 불법적으로 활용하는 사례가 늘어나고 있기 때문으로 볼 수 있다. 재래식 전력의 약화와 맞물려, 김정은 집권 이후 북한은 사이버능력을 핵 · 미사일과 함께 비대칭 전력 중 하나로 적극 활용하고 있으며 현재 북한의 사이버공격 능력은 세계 최고 수준인 것으로 평가되고 있다. 낮은 진입 비용과 높은 수익률, 책임규명의 어려움, 효과적인 억제방안 부족, 그리고 모니터링 기구의 부재 등이 김정은 정권이 사이버공격 능력 강화에 집중하도록 만드는 요인으로 보인다.[2] 북한은 자산 탈취, 군사 · 외교 기밀 유출과 같은 다양한 목적하에 세계 각국의 금융기관, 외국 정부, 군사기관 및 방위산업체, 에너지연구소 등을 대상으로 사이버공격을 광범위하게 감행하고 있다.

특히 북한이 불법적 사이버 활동을 통해 확보한 수익은 핵 · 미사일 능력을 지탱하기 위해 자금이 절실한 김정은 정권에 현금 공급망이 되어 비핵화를 위한 국제사회의 노력에 장애물로 작용하고 있다. UN 안보리 대북제재위원회 보고서와 미 정부는 북한의 사이버공격 능력이 주요 외화벌이 수단으로 자리 잡고 있음을 계속해서 지적하고 있다. 북한이 사이버공격을 통해 거둔 수입으로 핵 · 미사일 전력에 소요되는 비용을 충당함으로써 김정은 정권이 계속해서 대북제재를 무력화하고 있다는 것이다. 앤 뉴버거 미 백악관 NSC 사이버 · 신기술 담당 부보좌관은 "북한이 사이버 활동을 통해 미사일 프로그램에 필요한 재원의 최고 3분의 1을 충당하고 있다"라고 밝히기도 했다.[3]

실제로 김정은 시대 들어 북한 소행으로 추정되는 사이버공격에 관한 보도가 급격히 증가하고 있고, 특히 2010년대 중반 이후로는 경화 확보를 위한 대규모 사이버 사기 행위와 갈취 등이 빈번하게 포착되고 있다. 북한이 느슨하게 규제되는 가상자산 서버의 네트워크를 악용하여 불법적으로 획득한 가상자산을 법정화폐로 변환하여 수입을 확충하고 제재를 회피하고 있는 것으로 추정된다. 최근에는 암호화폐의 가격 하락에 따라 확보할 수 있는 외화의 총액이 줄어들었을 것으로 보임에도 북한은 사이버공격을 통한 외화벌이를 포기하지 못하는 것으로 보인다.

문제는 김정은 정권이 북한이 처한 대내 · 대외적 상황에 따라 앞으로도 책임소재가 불분명한 사이버공격의 특성을 적극적으로 활용하여 경제적 · 정치적 이익을 취하려 할 가능성이 크다는 것이다. 특히 미중경쟁의 심화, 코로나19로 인한 팬데믹 상황과 러시아-우크라이나 전쟁, 한국의 신정부 출범 등 복잡한 국제정세 속에서 북한은 사이버공간의 불안정성을 가중할 것으로 예상된다. 이미 러시아-우크라이나 전쟁과 미중경쟁에 따른 공급망 재편에 따라 자유민주주의 국가들과 권위주의 국가들 간 진영화 움직임이 두드러지게 나타나면서 북한은 사이버와 신기술 등 새로운 전략적 공간을 확장하려는 시도를 계속하고 있다. 세계 곡물 가

2 Stephanie Kleine-Ahlbrandt, "North Korea's Illicit Cyber Operations: What Can be Done?," 38 North, February 28, 2020, https://www.38north.org/2020/02/sklеineahlbrandt022820/ (검색일: 2022년 8월 13일).

3 강병철, "미 NSC 북, 사이버 활동으로 미사일 재원 3분의 1 충당," 연합뉴스, 2022년 7월 29일, https://www.yna.co.kr/view/AKR20220728184351071?input=1195m (검색일: 2022년 8월 13일).

격 상승, 외화부족과 유가상승은 북한의 식량부족 문제와 경제위기를 악화시키고 있으며 한국의 신정부 출범에 따른 남북관계의 긴장과 대결 가능성 고조는 김정은 정권에 새로운 대응전략의 필요성을 촉구하고 있다. 이에 따라 북한은 향후 사이버공간을 통한 해킹, 바이러스 유포 등은 물론 가짜뉴스와 허위조작 정보 유포, 랜섬웨어 등 다양한 사이버공격을 통해 군사·외교 기밀 유출을 시도하거나 불법적으로 외화수입 획득에 나설 것으로 예상된다.

북한의 사이버위협 수준이 국제사회의 안정을 해치는 요인으로 부상하면서 김정은 정권의 사이버위협에 대한 면밀한 분석을 바탕으로 한 대응방안 마련이 시급하다. 본 연구는 김정은 시대 북한의 사이버위협 능력과 특징을 식별하고 주요국의 대응을 살펴본 뒤, 향후 북한의 사이버위협을 최소화하기 위해 필요한 정책들은 무엇인지 제시하고자 한다. 본 연구는 북한의 사이버능력에 대한 기술적 내용에 집중하기보다는 공개된 자료들을 바탕으로 현재까지 밝혀진 김정은 시대 북한의 사이버공격의 양상과 특징에 대한 분석에 초점을 맞춘다.

구체적으로 본 연구는 2장에서 김정은 시대 북한의 사이버능력 및 공격 현황, 특징을 분석한다. 김정은 시대 북한의 사이버 역량 및 주요 해킹조직들을 소개하고, 북한 사이버공격의 특징을 ① 암호화폐 공격 ② 랜섬웨어 공격 ③ 국방산업 신기술 탈취 ④ 대북·대외전략 정보수집 ⑤ 코로나19 백신 기술 탈취 등 5가지로 분류하여 현황을 분석한다. 3장에서는 북한의 사이버위협에 대한 미국·EU·UN 등 국제사회의 대응방안을 소개한다. 구체적으로 본 연구는 국제사회의 대응을 경제제재, 랜섬웨어 대응, 암호화폐 공격 대응의 측면에서 조명한다. 4장에서는 북한의 사이버위협에 대한 한국의 대응방안을 제시한다. 앞서 논의된 김정은 정권의 악의적 사이버 활동과 국제사회의 대응방안을 고려하여 우리의 합리적 대응방안을 제시하되, 보다 공세적인 대응방안의 필요성에 대한 고민을 국제협력 강화와 국내역량 강화라는 두 가지 측면에서 논의하고자 한다. 마지막으로 결론에서는 1장에서 4장까지의 논의를 정리하고 향후 예상되는 북한의 사이버위협은 어떠한 양상을 보일 것인지 예측해 본다.

2. 선행연구 검토

북한의 사이버위협에 대한 객관적이고 실증적인 분석을 시도하는 것은 어려운 과제이다. 그 이유는 첫째, 사실상 국제정치학에서 사이버위협에 관한 이론적 연구가 부족한 데다, 둘째, 김정은 정권이 아직까지 사이버 관련 독트린이나 지휘체계를 공개한 바 없고, 셋째, 북한 소행으로 의심받는 사이버공격 역시 언론을 통해 보도되고는 있으나 김정은 정권에 의해 모두 부정당하고 있기 때문이다. 그리고 무엇보다 핵·ICBM 등 북한의 다른 비대칭 능력과 비교하였을 때 북한의 사이버위협에 관한 논의 자체가 크게 주목을 받고 있지 못하는 상황이다. 그러나 북한의 사이버공격에 의한 국제적 피해규모가 매년 증가하고 있는 시점에서 김정은 시대 북한 사이버공격의 특징을 종합적으로 분석한 연구는 반드시 필요하다고 할 수 있다.

북한의 사이버위협을 다룬 기존연구들은 다음과 같이 크게 세 가지 유

형으로 나누어 볼 수 있다. 첫째, 북한의 사이버 역량과 조직에 대한 일반적인 소개를 다룬 연구들이다.[4] 사이버공격을 주도하는 북한의 정찰총국에 대한 간략한 소개와 주요 해킹조직의 활동에 관한 설명들이 주를 이룬다. 둘째, 북한이 사이버공격에 활용하는 기술과 이와 관련한 일부 사례들을 분석한 연구들이다.[5] 스피어피싱, 랜섬웨어, DDoS, ATP 공격 등 북한의 해킹조직들이 주로 활용하는 사이버공격 기술 유형을 분석하고 공격의 대상과 목적에 대한 논의를 주로 한다. 셋째, 국제법적 관점에서 북한의 사이버위협에 대한 한국의 대응방안을 다룬 연구들이다.[6] 이들 연구들은 사이버공간이 갖는 한계와 국제법 체계 미확립에 따른 대응에 한계에 공감하고, 국제공조 강화와 국내 법제 정비를 요구하고 있다. 이 밖에도 북한의 사이버위협에 관한 연구들 중에서 위의 세 가지 내용 중 두 가지 이상을 동시에 다루고 있는 연구들도 있다.

선행연구들은 북한 사이버능력과 위협과 관련한 몇 가지 주요 이슈나 관심 분야를 중심으로 논지를 전개하고 있다. 그러나 김정은 집권 10년간 북한에 의한 사이버위협의 수준이 급격히 높아졌음에도 이에 대한 총체적 분석은 부족했다는 아쉬움을 남기고 있다. 본 연구는 김정은 시대 북한의 사이버 역량과 주요 조직들에 대한 논의뿐만 아니라 사이버공격이 국가전략의 변화와 어떠한 연계성을 갖고 변화하는지를 다룬다. 그뿐만 아니라 증대되고 있는 사이버위협에 대한 국제사회의 대응을 살펴보고, 한국이 추구해야 할 대응방안을 내적 역량 강화와 국제협력 강화의 측면에서 제시한다. 특히 트럼프 정부에서 제시된 미국의 선제방어(defend forward) 개념이 논란이 되고 바이든 정부하 사이버공격에 대한 미국의 적극적인 대응이 추진되는 상황에서 북한의 사이버위협에 대응한 한미의 공조방안은 어떠한 방향으로 확립되어야 할 것인지 논의한다.

4 대표적 기존연구로는 황지환, "북한의 사이버 안보 전략과 한반도: 비대칭적, 비전통적 갈등의 확산," 『동서연구』, 제29권 1호 (2017), pp. 139-159; 유동열, "북한의 사이버 위협 실태와 대응," 『전략연구』, 제28권 3호 (2021), pp. 7-36; 양철호 · 김윤영, "북한 사이버테러 조직의 역량 평가 고찰," 『한국민간경비학회보』, 제20권 5호 (2021), pp. 141-168.

5 정영애, "북한의 사이버공격 역량의 진화: 사이버공격 사례 분석을 중심으로," 『평화학연구』, 제20권 4호 (2019), pp. 125-143; 김진광, "북한의 사이버 공격 위협 분석 연구: 공격 기술의 유형 중심으로," 한국컴퓨터정보학회 학술발표논문집, 2020년 7월, pp. 107-110.

6 김윤영 · 양철호, "북한의 사이버테러에 대비한 법 · 제도 개선방안 연구," 『유럽헌법연구』, 제33호 (2020), pp. 355-384; 백상미, "북한의 대남 사이버공격에 대한 국제법적 검토와 이에 대한 한국의 대응전략," 『서울국제법연구』 제27권 2호 (2020), pp. 39-66.

II

김정은 시대 북한의 사이버위협: 능력과 특징

1. 북한의 사이버 역량 및 주요 조직

가. 북한의 사이버 역량

북한의 사이버전략이나 독트린, 지휘통제에 대해서는 아직 공식적으로 밝혀진 바가 없다. 그럼에도 불구하고 북한 정권이 김정일에서 김정은 시대로 이어지면서 내부적으로 사이버공격 능력에 대한 중요성이 날로 커지고 있는 것은 분명해 보인다. 2010년 김정일은 "현대전쟁은 기름전쟁, 알(탄약) 전쟁으로부터 정보전쟁으로 바뀌었다"라며 "정보전부대는 핵무기와 함께 나의 배짱이고 예비대"라고 강조하는 등 사이버전력의 중요성을 역설한 바 있다.[7] 김정은 역시 사이버전을 "핵·미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"으로 지칭하는 등 북한의 사이버능력을 핵심적인 비대칭 전력으로 분류하고 있다.[8]

북한이 사이버전력을 핵·미사일 전력과 함께 군사조직으로 분류하고 있는지는 불확실하다. 다만 현재까지 드러난 바에 따르면, 북한에 의한 사이버공격은 하나의 군 조직에 의해 주도되기보다는 다수의 무력단체와 정보기관에 의해 이루어지고 있으며 이들 기관은 조선노동당과 김정은의 지시를 따르는 것으로 확인되고 있다. 북한의 대표적인 사이버공격 담당기관으로 대남·대외 공작부서인 정찰총국을 꼽을 수 있다. 정찰총

7 김귀근, "김정일 "정보전부대는 나의 배짱이고 예비대"," 연합뉴스, 2011년 6월 28일, https://www.yna.co.kr/view/AKR20110628128400043 (검색일: 2022년 8월 13일).

8 이영종·윤호진, "김정은 "사이버전은 만능의 보검" 3대 전쟁수단 운용,"『중앙일보』 2013년 11월 5일, https://www.joongang.co.kr/article/13048072#home (검색일: 2022년 8월 13일).

국은 무기수출과 마약제조 및 거래, 위조지폐 생산 등을 해오기도 했는데 지난 십 년간 사이버공격을 주도하고 있는 것이 특징이다. 편제상 정찰총국은 총참모부 산하로 되어 있으나 총참모장이 아닌 김정은의 직접 지휘를 받는 독립부서로 볼 수 있다.[9]

북한 소행으로 의심되는 대부분의 사이버 작전은 정찰총국의 6개국 가운데 하나인 일명 '121국(별칭 '사이버전지도국')'에서 관할하는 것으로 추정된다. 121국은 허위정보와 사이버 범죄, 스파이 활동을 담당하는 6천여 명의 상근 사이버 요원 및 지원 인력을 보유한 것으로 알려져 있다. 해커들은 대다수가 특별한 성분 출신이라기보다는 금성학원 컴퓨터반 출신, 수학이나 컴퓨터에 소질을 보인 학생들로, 김책공업대학, 김일성종합대학 등에서 컴퓨터를 공부하고 사이버 요원으로 배치된다. 2020년 7월에 발표된 미 육군 보고서에 따르면 정찰총국의 121국에는 라자루스(Lazarus), 블루노로프(BlueNorOff), 안다리엘(Andariel) 등의 북한의 주요 해킹그룹들이 소속되어 있다. 소속 해커들의 활동 근거지는 북한이 아닌 해외로, 벨라루스와 중국, 인도, 말레이시아, 러시아 등 다양한 국가에서 사이버공격에 가담하고 있다.[10]

정찰총국 외에도 북한은 총참모부 산하 전자전 사령부를 비롯하여 여러 개의 하위 전자정보전 집단을 운용 중인 것으로 알려져 있다.[11] 최근

9 김일기 · 김호홍, 『김정은 시대 국가안보 기구』, INSS 연구보고서 2020-6 (2020), p. 61.

10 U.S. Army Headquarters, "North Korean Tactics," July 2020, p. E-2.

11 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: 2022년 8월 13일).

에는 통일전선부와 국가보위성도 사이버 해킹 활동에 참여하고 있다는 보도까지 나오고 있어 북한이 사이버 활동을 위해 다양한 조직을 탄력적으로 운용하고 있는 것으로 보인다.[12] 보도에 따르면, 통일전선부는 친북 성향 단체를 만드는 것을 목표로 대남 친북 관련 메시지를 웹사이트에 게시하는 프로파간다 활동을 벌여왔다. 반면 국가보위성은 방첩 활동에 집중하고 있으며 대표적으로 APT 37과 김수키(Kimsuky)가 탈북민 단체와 인도주의적 지원단체 등을 상대로 유사한 공격 활동을 벌이고 있다고 지적했다.[13] 이렇게 북한의 사이버공격 감행 단체가 증가하는 것은 북한이 사이버공격 능력을 탈북민, 학자, 정부, 언론, 금융기관, 제약회사 등 다양한 타깃에 대하여 방첩, 공작, 외화확보, 기술 · 정보 탈취 등 다양한 용도로 활용하고 있다는 것을 보여준다고 할 수 있다.

북한의 사이버능력에 대해서는 평가기관과 국가별로 다양하게 나타나고 있기는 하지만 대체적으로는 높은 수준이라는 평가가 내려지고 있다. 북한의 해킹 능력은 2009년 이후로 크게 성장했고 현재는 첨단의 사이버공격 능력을 보유하고 있으며 어떤 나라의 시설도 공격할 수 있을 정도로 능력을 갖춘 것으로 보인다. 또한 북한의 해킹 능력은 취약점이 발견되면 즉시 새 기술을 적용하는 데 매우 민첩한 것으로 알려져 있다.[14] 미국이 국가안보 위협으로 제시하고 있는 중국 · 러시아의 해킹 능력과

12 김영교, "북한 정찰총국 외에 통일전선부, 국가보위성도 사이버 해킹 관여," VOA, 2022년 3월 24일, https://www.voakorea.com/a/6498327.html (검색일: 2022년 8월 13일).

13 Ibid.

14 조상진, "북한 해킹조직, 외화탈취 위한 신종 랜섬웨어 4종 유포…금융 해킹 집중," 『VOA』, 2022년 5월 5일, https://www.voakorea.com/a/6557282.html (검색일: 2022년 8월 13일).

직접적인 수준을 비교하기는 힘들지만, 중 · 러가 산업 스파이나 정보 분야 탈취에 특히 뛰어난 것처럼 북한은 금융 분야 해킹 능력이 발달한 것으로 보인다.[15]

반면 북한의 사이버능력이 예상보다 떨어진다는 평가도 있다. 영국의 IISS(the International Institute for Strategic Studies)는 북한에 정교한 사이버 정보(intelligence) 능력이 없고 사이버보안 수준 또한 세계 최하위 수준에 불과하다며 북한의 전반적인 사이버능력을 가장 낮은 3그룹(Third-tier)에 포함하였다. IISS는 북한 당국이 주민들의 인터넷 접속을 엄격하게 통제하는 데다가 세계 인터넷망에 연결하기 위한 게이트웨이(gateway)를 중국 · 러시아 서비스 제공업체가 제공하는 극소수에 의존하여 사이버공격에 취약한 것으로 분석했다.[16] 반면 이러한 구식 인프라 덕분에 북한이 사이버 보복에 덜 취약하고 해커들의 활동 역시 해외에서 대부분 이루어져 제재가 효과를 거두기 어렵다고 보는 견해도 있다.[17]

북한의 사이버능력에 대해 일부 극과 극의 평가가 있기는 하나 전반적

15 Ibid.

16 The International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," IISS, February 2019, p. 125. 그러나 IISS의 보고서 발표 이후 미 국무부는 북한의 악의적 사이버 활동은 금융기관에 대한 심각한 사이버위협이자 사이버 간첩 위협으로, 북한이 파괴적인 사이버 활동을 수행할 능력을 보유하고 있다고 반박하였다. 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: 2022년 8월 13일).

17 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 (accessed: August 13, 2022).

으로 사이버공격 역량은 세계 최고 수준에 가까우며 주요 비대칭 전력 중 하나로 자리매김하고 있다는 사실을 부정하기는 어려워 보인다. 또한 북한의 이러한 사이버공격 능력은 김정은 시대 들어 빠르게 증가하여 국제사회에 심각한 위협으로 인식되고 있는 중이다. 북한의 핵 · 미사일 능력이 고도화됨에 따라 고강도 제재에 놓인 기간도 길어지면서 김정은 정권은 이를 우회하고 국제사회에 대항하기 위한 수단으로 사이버공격 능력 향상에 더욱 집중하는 것으로 보인다. 특히 △사이버공격의 낮은 진입 비용 △공격 성공 시 높은 잠재적 수익률 △사이버공격에 대한 책임 규명 한계 △효과적인 억제방안 부족 등 다양한 요인들은 김정은 정권이 사이버능력에 의존할 수밖에 없게 만드는 요인이 될 것이다.

실제로 미국 및 EU, UN 등 국제사회는 북한의 주요 해킹단체와 해커들에게 제재를 부과하고 북한 당국을 강하게 비난하고 있으나 사이버공간의 특성상 책임귀속을 증명하기 어렵기 때문에 북한 당국은 혐의를 쉽게 부정하는 한편 제재의 부당함까지 주장하고 있다. 2014년 소니픽처스(Sony Pictures) 영화사 해킹 사건의 배후로 북한이 지목되자, 외무성은 대변인 담화를 발표하여 터무니없는 여론으로 비방당하고 있다며 미국 측과 공동조사를 진행할 것을 주장했다.[18] 또한 2021년 한국항공우주산업(KAI)과 한국원자력연구원 해킹 사건들의 북한 배후설에 대해서도 북한은 "황당무계한 모략소동"이라며 "저열한 기술로 해킹을 당한 것"이라고 일갈하며 자신들의 소행임을 강하게 부정하였다.[19] 2022년 7월 20

18 조선중앙통신, 2014년 12월 20일.

19 "고질적 버릇, 상투적 수법," 『우리민족끼리』, 2021년 7월 12일.

일 뉴버거 미 백악관 국가안보회의 사이버 · 신기술 담당 부보좌관이 북한의 암호화폐 해킹에 대해 "국가를 가장해 수익을 추구한다는 측면에서 범죄집단"이라고 북한 정권을 평가하자 북한 외무성 대변인은 7월 23일 이에 대해 "도발적 망발"이라며 세계 유일무이한 범죄집단인 미국에 상응 조치를 하겠다고 발언하였다.[20]

나. 북한의 대표적인 사이버조직

북한의 대표적인 해킹조직으로는 라자루스, 블루노로프, 안다리엘, 김수키(Kimsuky, 탈륨(Thallium)) 등을 꼽을 수가 있다(〈표 1〉 참조).

〈표 1〉 북한의 주요 해킹조직

해킹조직	조직의 특징 및 활동	
라자루스 그룹 (Lazarus Group)	조직	▪ 정찰총국 산하조직으로 2007년 초 구성 추정 히든 코브라(Hidden Cobra), ATP 38와 동일 조직 추정
	활동 특징	▪ 2009-2014년까지 한국과 미국을 집중적으로 공격하였으나 2015년 이후에는 금전적 수익을 목적으로 공격 범위를 확장
	주요 타깃	▪ 암호화폐거래소, 은행, 언론사, 엔터테인먼트 기업 등 다양한 산업 분야와 방산 분야
	대표적 해킹 사례	▪ 2014년 소니픽처스 엔터테인먼트, 2017년 워너크라이 랜섬웨어 공격 배후 의심
블루노로프 (BlueNorOff)	조직	▪ 정찰총국 121국 산하조직으로 약 1,700명 안팎의 규모로 알려져 있으며 2014년 초 최초 활동 포착
	활동 특징	▪ 금전적 수익을 얻을 수 있는 곳만을 공격
	주요 타깃	▪ 글로벌 금융회사, 카지노, 암호화폐거래소, 금융 거래 소프트웨어 개발사 등
	대표적 해킹 사례	▪ 2016년 방글라데시 중앙은행 · 폴란드 금융감독원 해킹, 2018년 칠레 은행 해킹
안다리엘 (Andariel)	조직	▪ 정찰총국 121국 산하조직으로 약 1,600명 안팎의 규모로 2016년 최초 활동 포착
	활동 특징	▪ 무기개발 관련 정보 획득 및 경제적 이익 창출을 위한 해킹 활동
	주요 타깃	▪ 국내 방위산업체, 보안업체, 에너지연구소, 국방 관련 기구를 비롯한 도박게임, 여행사, 암호화폐거래소, ATM 기기 등
	대표적 해킹 사례	▪ 2016년 국방통합데이터센터 해킹, 2021년 KAI 해킹
김수키 (Kimsuky)	조직	▪ 정찰총국 산하조직으로 2010년 이래 활동한 것으로 추정 탈륨과 동일조직으로 추정되며, 2019년 MS가 인터넷 계정 도용 혐의로 미연방법원에 고소
	활동 특징	▪ 북한 정권의 글로벌 정보수집 임무를 담당일반적인 사회공학 전술, 스피어피싱[21],워터링 홀 공격 등을 사용해 피해자로부터 원하는 정보 색출
	주요 타깃	▪ 한국, 미국, 일본의 개인 및 싱크탱크, 정부조직의 전문가 (한반도 및 핵정책, 제재 관련 외교정책 및 국가안보 문제 관련), 탈북자
	대표적 해킹 사례	▪ 2020년 폴란드 정부 해킹, 2021년 6월 서울대병원 해킹, 2021년 한국원자력연구원 해킹

※ 출처: 필자 작성.

우선 라자루스 그룹은 2007년 초 설립된 것으로 추정되는 정찰총국 산하 해킹조직으로, 해외 정부와 금융기관, 방송매체들에 대한 사이버공격을 감행해왔다. 미 재무부에 따르면 라자루스 그룹은 정찰총국 제3국(제3 기술정찰국) 110 연구소 소속으로 창설되었으며 2007년 초에 활동이 포착되었다.[22] 라자루스 그룹이 관여한 대표적인 해킹 사건은 2014년 11월 소니픽처스 해킹 사건과 2016년 방글라데시 중앙은행 현금 탈취 사건, 2017년 5월 워너크라이(Wannacry) 랜섬웨어 사건 등이 있다. 라자루스 그룹이 유명해진 사건은 소니픽처스 해킹 사건으로, 김정은의 암살을 다룬 영화인 '인터뷰(The Interview)' 상영을 금지하라는

20 조선중앙통신, 2022년 7월 23일.

21 악성 첨부파일을 이메일에 포함하는 형태로 김수키의 공격에서 가장 많이 발견되는 방법이다.

22 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: 2022년 8월 13일). 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.

북한의 요구를 소니픽처스에서 들어주지 않자 이에 대한 보복으로 해킹을 감행하였다. 당시 해킹으로 미상영 영화, 이메일, 4,000명가량의 직원들의 신상정보 등이 유출되었다. 그러나 라자루스 그룹이 감행했던 가장 치명적인 해킹은 2017년 5월 워너크라이 랜섬웨어 사건일 것이다. 당시 라자루스 그룹은 150여 개국에 악영향을 끼치고 30만 대의 컴퓨터에 피해를 일으킨 것으로 알려져 있다. 이 해킹 사건으로 영국 국립보건원(NHS)의 1만 9천여 명의 진료 예약이 취소되고 국민건강보험에 1억 1,200만 달러 이상의 비용이 들었다. 라자루스 그룹은 최근에는 암호화폐 관련 사이트들을 대상으로 공격을 감행하고 있는 것으로 보고되고 있다.

라자루스 그룹의 하위기관으로 추정되고 있는 블루노로프와 안다리엘은 해외 금융기관을 대상으로 사이버공격을 감행하여 불법적 수입을 올린다는 공통점이 있다. 이들이 벌어들인 수입으로 김정은 정권은 핵・미사일 개발에 필요한 비용을 충당하는 것으로 알려졌다. 2020년 미 육군 보고서에 따르면 블루노로프는 총 1,700명 규모로, 네트워크 취약점과 시스템을 금전적 이익 취득이나 시스템 장악을 위해 악용하고 있다.[23] 블루노로프가 일반적으로 활용하는 해킹 기술로는 피싱(phishing), 백도어(backdoors), 워터링 홀(watering hole) 공격 등이 있다. 블루노로프는 금전적 이익에 초점을 맞추기 시작한 2014년부터 2021년까지 인도, 멕시코, 파키스탄, 필리핀, 대만, 한국 등 13개국 16개 기관에서 자금 탈취에 성공한 것으로 추정된다. 블루노로프가 감행했던 가장 악명높은 사이버공격은 라자루스 그룹과 협력하여 2016년 방글라데시 중앙은행에

23 U.S. Army, "North Korean Tactics," *Federation of American Scientists,* 2020, pp. E-1, E-2.

있는 뉴욕 연방준비은행(Fed) 계좌에서 8,100만 달러를 훔쳐낸 사건이었다.

안다리엘은 약 1,600명의 해커로 이루어진 조직으로 알려졌으며 소속 해커들은 적의 전산망에 대한 감시와 취약점 분석을 담당한다. 다른 정부, 인프라, 기업도 공격의 대상이지만 이들은 주로 한국을 표적으로 삼고 있는데, 여기에는 정부, 국방 및 모든 경제 관련 조직과 기관들, 인프라 등이 포함된다. 안다리엘은 현금인출기를 해킹해 은행 카드 정보를 빼내거나 해킹한 고객 정보를 암시장에서 판매하려 했으며, 현금을 훔치기 위해 온라인 포커 및 도박사이트를 해킹하는 독특한 악성코드를 개발해왔다. 안다리엘이 감행한 대표적인 해킹 사건은 2016년 9월 한민구 전 국방장관의 컴퓨터와 국방부 인트라넷에 침입하여 군사작전('작계 5015') 정보 탈취를 시도한 것이었다. 최근에는 블루노로프와 동시에 동일한 금융회사를 공격하기도 하며 금융권을 타깃으로 사이버공격을 지속적으로 감행하고 있는 것으로 확인되고 있으며, 가상자산과 암호화폐 거래소를 대상으로 수익 흐름을 혼란스럽게 만듦으로써 절도 행위를 시도한다. 안다리엘은 2019년 9월 라자루스 그룹, 블루노로프와 함께 미 재무부 해외자산통제실(Office of Foreign Assets Control: OFAC)의 특별제재 대상으로 지정되었다.[24]

2010년부터 활동한 것으로 알려진 김수키는 국제적인 정보수집 임

24 U.S. Department of the Treasury, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," September 13, 2019, https://www.home.treasury.gov/news/press-releases/sm7774 (accessed: August 13, 2022).

무를 담당하고 있다. 지능형 지속 공격(Advanced Persistent Threat: APT) 해킹조직으로 알려진 김수키는 2013년 러시아 정보보안업체가 해커의 이메일 계정인 '김숙향(kimsukyang)'이라는 이름으로 보고서를 발표하면서 존재가 확인되었다. 김수키는 한 · 미 · 일 정부 및 싱크탱크 등 여러 분야 전문가들을 상대로 한반도 관련 외교정책 및 안보문제와 관련하여 집합적인 정보활동을 벌이고 있으며 탈륨과 동일한 조직으로 추정되고 있다. 김수키는 한국 기자를 사칭하여 인터뷰나 방송 출연 요청 메일을 보내고 인터뷰 자료에 멀웨어, 악성코드 첨부 문서를 보내 열도록 유도한다. 김수키의 악명높은 활동으로 2014년 12월 한국수력원자력 해킹 사건을 들 수 있으며 근래에는 코로나19 관련 정보를 입수하기 위한 서울대병원 해킹 사건의 배후로 지목된 바 있다.

이 밖에도 북한의 해킹 집단으로 ATP 38, 평화의 수호자(Guardians of Peace), 히든 코브라(Hidden Cobra), 비글보이즈 등이 있으나 앞서 언급한 해킹조직들과 같은 해킹 수법을 활용하여 동일한 조직으로 추정되거나 의심받고 있다. 이외 북한의 악명높은 해커로 박진혁, 전창혁, 김일 등을 꼽을 수 있다. 이들 세 명은 2021년 2월, 전 세계의 은행과 기업을 상대로 13억 달러를 훔치려 한 혐의로 미 법무부에 기소되었다.[25] 박진혁의 경우, 라자루스 그룹의 일원으로 추정되며 북한 해커들의 위장회사라고 할 수 있는 '조선엑스포합영회사'에서 컴퓨터 프로그래머로 10년 이상 근무한 것으로 알려져 있다.[26] 그는 2016년 2월 방글라데시 중앙은행 해킹 사건에 연루된 것으로 알려져 있으며 미 방산업체 록히드 마틴(Lockheed Martin)사의 THADD에 대해서도 해킹을 시도한 것으로 드러났다. 박진혁은 2014년 소니픽처스 사이버공격에 연루된 혐의로 2018년 미 정부에 기소당한 바 있는데, 이는 미국이 사이버 범죄와 관련해 북한 공작원을 상대로 처음 기소한 사례가 되었다.

25 또한 이들이 훔친 돈의 자금세탁을 도운 캐나다 · 미국 이중 국적자인 갈렙 알라우마리(Ghaleb Alaumary)에게는 징역 11년 8개월이 선고되었고, 미 법무부는 알라우마리에게 피해자금 3천만 달러의 반환을 명령하였다.

26 이 조직은 중국 항구도시 다롄에 위치해 있으며 현재 미 재무부의 제재 대상에 포함되어 있다. 박진혁(Park Jin-hyok)은 다른 영어 철자 표기 Pak Jin-hek과 박광진(Park Kwang-jin)이라는 이름으로도 활동하였다. "라자루스 강도사건: 북한은 어떻게 최정예 해커부대를 만들어 냈나," BBC, 2021년 7월 8일, https://www.bbc.com/korean/international-57674041?xtor=AL-73-%5Bpartner%5D-%5Bnaver%5D-%5Bheadline%5D-%5Bkorean%5D-%5Bizdev%5D-%5Bisapi%5D (검색일: 2022년 8월 13일).

2. 김정은 시대 북한 사이버공격의 유형과 특징

가. 외화확보를 위한 암호화폐(cryptocurrency) 공격

북한의 사이버공격은 다방면에서 다목적으로 이루어지고 있지만 2010년대 중반 이후에는 가상자산 탈취에 주력하는 모습이 포착되고 있다. 전통적으로 북한이 현금을 확보하는 방법은 마약 거래나 멸종 위기 동식물 밀거래, 위조화폐 생산 등이었다. 그러나 암호화폐의 경우 거래내용을 암호화하여 실제 소유주의 신원이 노출되지 않아 도난 · 분실의 경우 익명성으로 인해 범인을 잡기 어렵다. 또한 해킹 공격에 특별한 비용이 들지 않는 데다 수익성이 높고 공격 출처를 추적하기 어려워 해커들은 적은 비용과 위험으로 더 많은 돈을 탈취할 수 있는 것이 특징이다. 김정은 정권은 이 같은 암호화폐 공격을 통한 장점을 충분히 인지하고 있는 것으로 보이며 이를 새로운 외화벌이 수단으로 정착시키고 있다.

북한은 투자자와 암호화폐거래소 모두에 대한 해킹을 통해 적은 노력과 비용으로 비교적 손쉽게 외화를 축적하고 있는 것으로 알려져 있다. 북한에 의한 암호화폐 공격과 피해규모는 해마다 증가하는 양상을 띠고 있는데, 2011년에서 2022년까지 발생한 암호화폐 해킹 사건 중 가장 많은 15건의 암호화폐 해킹을 북한에서 시도한 것으로 확인되었다. 다만 이는 UN 대북제재위원회에 의해 파악된 암호화폐 해킹 사례 건수일 뿐 실제로는 더 많은 피해 사례가 있을 것으로 추정되고 있다.[27]

북한은 암호화폐 공격을 통해 벌어들인 수입을 장기간 지속되는 고강도 제재를 회피하고 핵 · 미사일 프로그램의 확대 · 발전을 위한 자금을 마련하는 데 활용하고 있는 것으로 알려졌다. 특히 2016년 3월, UN 역사상 가장 강력한 것으로 알려진 대북제재 결의안 2270호의 통과로 인해 무기수출과 경제교역을 통한 외화수급에 심대한 차질이 생긴 이래 북한의 암호화폐 공격에 대한 의존도는 더욱 커졌다. 북한이 2017년부터 탈취한 암호화폐의 총가치는 16억 달러에 달할 것으로 추정되고 있다.[28]

UN 제재 감시 전문가패널 조정관 에릭 펜톤 보악(Eric Penton-Voak)은 김정은 정권이 제재를 회피하고 핵 · 미사일 프로그램에 자

27 임재섭, "암호화폐 해킹 시도, 북이 가장 많아...아일랜드 암화화폐 분석업체 설명," 『디지털타임스』, 2022년 6월 30일, https://http://www.dt.co.kr/contents.html?article_no=2022063002109958050002 (검색: 2022년 9월 8일).

28 홍제성, "북한, 전세계서 암호화폐 해킹 가장 많아...가치로 16억 달러," 연합뉴스, 2022년 6월 30일, https://n.news.naver.com/mnews/article/001/0013279239?sid=102 (검색일: 2022년 9월 26일). 반면 블록체인 분석업체 체이널리시스(Chainalysis)는 2017년부터 2020년까지 북한 해킹조직인 라자루스가 훔친 암호화폐 규모만 17억 5천만 달러라고 주장했다. 고준혁, "미 재무부 게임 '액시 인피니티' 암호화폐 도난, 북한 연루," 『이데일리』, 2022년 4월 15일, https://www.edaily.co.kr/news/read?newsId=01823686632296448&mediaCodeNo=257&OutLnkChk=Y (검색일: 2022년 9월 26일).

금을 조달하는 능력에 사이버공격이 "절대적으로 근본적(absolutely fundamental)"이 되었다고 밝혔으며, 2019년 제재 감시위원회는 북한이 사이버공격을 이용해 거둬들인 수입 20억 달러가 대량살상무기 프로그램에 투입되었다고 보고했다.[29] 또한 백악관 사이버보안 국가안보 부보좌관 앤 뉴버거는 북한이 훔친 암호화폐의 3분의 1이 미사일 프로그램에 활용되고 있다고 공식적으로 발언한 바 있다.[30]

김정은의 경제건설 및 애민행보가 잇따르면서 북한은 원산갈마관광지구와 평양종합건설 등 국가주도로 진행하는 각종 건설사업에 필요한 외화를 확보하기 위한 목적으로도 암호화폐 공격을 계속하였다.[31] 이 시기 북한이 감행한 대표적인 해킹 사건은 2018년 1월 일본 암호화폐거래소 코인체크의 자산 탈취 시도와 2018년 6월 국내 최대 암호화폐거래소 빗썸(Bithumb) 공격이었다. 라자루스 그룹이 빗썸 거래소와 이용자에게 악성파일이 담긴 이메일을 보내 약 189억 원가량의 돈을 탈취했을 것으로 추정되었다.32 또한 2018년 1월, 북한이 일본 암호화폐거래소 코인체크에서 탈취한 자산은 580억 엔(5,700억 원) 규모로 알려졌다.

또한 코로나19로 인한 국경봉쇄와 제재의 장기화로 외화수급과 자원

29 Josh Smith, "Crypto Crash Threatens North Korea's Stolen Funds as It Ramps Up Weapons Tests," Reuters, June 29, 2022, https://https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/ (accessed: September 26, 2022).

30 권성근, "미, 북 핵프로그램 자금 확보 위한 암호화폐 도적 빈도 높아져," 『뉴시스』, 2022년 8월 10일, https://www.newsis.com/view/?id=NISX20220810_0001973454 (검색일: 2022년 9월 26일).

31 박대로, "북한 해커들, 가상자산 해킹 2조원 빼돌려," 『뉴시스』, 2021년 12월 26일, http://www.newsis.com/view/?id=NISX20211207_0001679470&clD=10301&plD=10300 (검색일: 2022년 8월 13일).

32 북한은 앞서 2017년 2월 700만 달러, 2017년 7월 최소 700만 달러를 빗썸 해킹 공격으로 탈취했을 것으로 추정되었다.

조달에 차질이 생기면서 비글보이즈(Beagle Boys)를 비롯한 북한 해커 단체들은 금융기관에 대한 사이버공격과 암호화폐거래소에 대한 해킹을 시도하였다. 2020년 9월 북한의 해킹조직인 라자루스는 슬로바키아 암호화폐거래소인 이터베이스(Eterbase)에 침투해 540만 달러 상당의 암호화폐를 훔친 뒤 곧바로 전 세계 1위 암호화폐거래소인 바이낸스(Binance)에서 최소 24개의 익명계좌를 개설해 이를 환전한 것으로 알려졌다. 라자루스는 또한 2022년 3월, 블록체인 비디오 게임 '액시 인피니티(Axie Infinity)' 게임에 쓰이는 암호화폐 네트워크 로닌(Ronin)이 해킹당해 6억 달러가 넘는 암호화폐가 유출된, 금액 면에서 역대 최대인 이 사건의 배후로도 지목되었다. 이 밖에 2021년 싱가포르 암호화폐거래소인 쿠코인(KuCoin) 해킹 또한 북한 해커 소행으로 추정되고 있다.

암호화폐의 시장규모가 매해 커지고 있기 때문에 외화수입 확보를 위한 북한의 해킹 시도 역시 늘어날 수밖에 없을 것으로 보인다. 특히 최근 몇 년간 암호화폐가 가격 상승을 거듭했다는 점을 고려해볼 때, 김정은 정권은 암호화폐를 제재 회피뿐만 아니라 일종의 투자가치가 있는 금융자산으로 여기고 있는 것으로 판단된다. 2019년 북한은 대북제재의 돌파구로 암호화폐와 블록체인 등 첨단기술에 관심을 두고 평양에서 암호화폐 콘퍼런스를 개최하여 관련 기술의 국제적인 네트워크 구축 기회로 활용하려 시도하였다. 북한은 콘퍼런스 개최를 통해 해외 기술전문가들을 초청하여 북한 IT · 과학기술계 인사와 교류하고 암호화폐 기술을 이용하여 제재를 우회하는 방법을 확보하려 했던 것으로 알려졌다.[33] 이 밖에도 북한은 경제제재와 미국 중심의 글로벌 금융시스템에 대응하기 위해 자신들만의 암호화폐를 개발 중이며 중국과 협력할 가능성도 있는 것으로 확인되고 있다. 2019년 9월, 외신보도에 따르면 북한은 암호화폐, 채굴, 교환해킹 등에 많은 관심을 갖고 있으며 자체 가상화폐 개발 및 도입에 필요한 전문지식은 이미 갖춘 것으로 보인다.[34]

그러나 북한이 암호화폐를 통해 얻을 수 있는 이점에도 한계가 존재한다. 탈중앙집권적인 암호화폐의 특성상 가격변동이 빈번하게 일어나 해킹을 통해서 얻을 수 있는 금전적 수익에 편차가 발생하기 때문이다. 2021년 전 세계 암호화폐 해킹 피해 금액은 140억 달러(추정치)로 사상 최대규모였는데, 이는 암호화폐 가격 상승에 힘입은 것이었다.[35] 2022년 4월 1일에 발표된 UN 안보리 산하 대북제재위원회 전문가패널 보고서에 따르면 북한이 2021년 한 해 동안 암호화폐 해킹을 통해 벌어들인 수입은 4억 달러에 달한다. 그러나 북한이 암호화폐의 가치가 하락하는 현시점에서 훔친 암호화폐를 현금으로 전환한다면 얻을 수 있는 수익은 확연히 줄어들 것으로 보인다.[36] 또한 북한 해커들이 직면한 가장 큰 문제는 가상자산의 현금화로, 블록체인 분석업체인 체이널리시스

33 김민관, ""평양 암호화폐 국제콘퍼런스" 개최 가능성 점검," Weekly KDB Report, 2020년 2월 10일, p. 9.

34 David Gilbert, "North Korea Is Building Its Own Bitcoin," Vice, September 19, 2019, https://www.vice.com/en/article/9ke3ae/north-korea-is-building-its-own-bitcoin (accessed: September 9, 2022).

35 암호화폐 해킹에 따른 피해금액은 2018년은 17억 달러, 2019년은 45억 달러, 2020년은 19억 달러로 추정된다. Smiljanic Stasha, "Cryptocurrency Hacking Statistics," February 13, 2022, http://policyadvice.net/money/insights/cryptocurrency-hacking-statistics/ (accessed: September 7, 2022); MacKenzie Sigalos, "Crypto Scammers Took a Record $14 Billion in 2021," NBC News, January 7, 2022, https: https://www.nbcnews.com/tech/security/crypto-scammers-took-record-14-billion-2021-rcna11192 (accessed: September 7, 2022).

36 박대로, "북한 해커들, 가상자산 해킹 2조원 배돌려,"『뉴시스』, 2021년 12월 26. UN 안보리 산하 대북제재위원회 패널보고서에 따르면 북한은 훔친 암호화폐들을 중국의 비상장거래소를 이용해 실제 화폐로 환전하는 것으로 알려졌다.

(Chainalysis)에 따르면 북한이 해킹에 성공한 이후 현금화하지 못한 암호화폐는 2021년 말 1억 7,000만 달러어치였으나 암호화폐 가치가 하락하면서 은닉액이 6,500만 달러 수준으로 급감한 것으로 알려졌다.[37]

나. 다목적의 랜섬웨어(ransomware) 공격

랜섬웨어(ransomware)는 몸값(ransom)과 소프트웨어(software)의 합성어로, 컴퓨터 시스템을 잠그거나 데이터를 암호화해 접근을 제한하고 금전을 요구하는 악성 프로그램의 한 종류이다. 해킹을 해제하는 대가로 금전적 지불을 하는 것이 파일이나 기록의 복구를 보장할 수 없다. 또한 최근에는 이에 대한 금전적 지불 사례에 대해 제재 위험이 초래될 수 있어 권장하지 않는다. 북한은 랜섬웨어 공격을 통해 국가 핵심 인프라를 위협하고 금전을 갈취한 것으로 잘 알려져 있다. 특히 최근에는 경제난 극복을 위해 랜섬웨어 공격과 가상화폐에 대한 공격을 연계하여 더욱 발전시키고 있는 것으로 보인다.

북한이 감행한 것으로 알려진 랜섬웨어 공격 중 가장 피해가 컸던 사건은 2017년 5월 워너크라이 2.0 랜섬웨어 공격이었다. 마이크로소프트의 취약점을 이용한 사이버공격으로 인해 전 세계 150여 개 국가의 항공과 철도, 의료 네트워크가 마비되었으며, 북한은 이에 대한 복구 비용으로 비트코인 등을 요구한 것으로 알려졌다.[38] 북한의 워너크라이 랜섬웨어 공격으로 영국 국민보건서비스(NHS) 산하 병원 48곳이 피해를 당하였고 영국 일반 의료 행위의 약 8%가 마비되었던바, 2019년 5월 23일 제레미 헌트 영국 외무장관은 북한과 러시아 등이 악의적인 사이버공격을 감행하는 경우 제재를 가할 것임을 밝혔다.[39] 영국은 2021년 12월 16일 발표한 『국가사이버전략(UK National Cyber Strategy)』에서 워너크라이는 물론 낫페트야(NotPetya) 등과 같은 랜섬웨어 공격에 대해 영국 독자적인 경제제재를 부과할 것임을 천명하였다.[40]

영국에 근거한 국제사이버보안업체 NCC그룹은 2022년 8월 25일 발표한 '월례 위협 보고서'에서 북한 라자루스의 랜섬웨어 공격이 급증하였다고 분석하였다.[41] 한편 북한은 랜섬웨어 공격 등을 통해 획득한 가상화폐를 가상화폐 대체불가토큰(Non-Fungible Token: NFT)을 활용하여 돈세탁하고 있는 것으로 밝혀졌으며, 특히 2021부터 가상화폐 해킹과 랜섬웨어 공격을 연계하여 아시아 지역에서 금전 탈취 행위를 지속한 것으로 알려졌다.[42] 북한이 대규모 가상화폐 탈취 후 자금세탁 과정에서

37 Choe Sang-Hun and David Yaffe-Bellany, "How North Korea Used Crypto to Hack Its Way Through the Pandemic," The New York Times, July 1, 2022, https://https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html (accessed: September 8, 2022).

38 김상욱, "북한 사이버공격으로 핵개발 자금 마련, 연간 약 10억 달러," 『뉴스타운』, 2017년 10월 21일, https://www.newstown.co.kr/news/articleView.html?idxno=301943 (검색일: 2022년 8월 13일). 그러나 당시 확인된 정보로만 놓고 보면 지불된 피해금액은 한국돈 1억 원 미만으로 다른 유형의 피해에 비해 그리 크지 않은 편이었다.

39 최선영, "영국, 북한 · 러시아 등의 사이버공격에 제재할 것," 연합뉴스, 2019년 5월 24일, https://www.yna.co.kr/view/AKR20190524034600504 (검색일: 2022년 8월 13일).

40 HM Government, *National Cyber Strategy 2022. December* 2021, p. 32, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf (accessed: October 28, 2022).

41 조상진, "북한, '랜섬웨어' 공격 통한 외화 탈취 급증…'대체불가토큰' 활용 돈세탁도 증가," VOA, 2022년 8월 26일, https://www.voakorea.com/a/6716953.html (검색일: 2022년 9월 28일).

42 Ibid.

걸리는 시간과 날로 강화되고 있는 가상화폐 분야 규제에서 오는 손실을 최소화하고 현금확보를 신속히 하기 위하여 랜섬웨어 공격을 활용하고 있는 것으로 보인다.[43]

또한 북한 해커들은 2021년 '마우이'라는 이름의 변종 랜섬웨어를 이용해 미국 의료기관과 병원 등에 랜섬웨어 공격을 감행하여 미 법무부와 연방수사국(FBI)이 대응에 나서 피해액 50만 달러를 회수한 것으로 밝혀졌다.[44] 미 FBI는 CISA, 재무부와 더불어 2022년 7월 6일 '마우이' 랜섬웨어 주의보를 발령하였다.[45] 이 밖에 미국에 본부를 둔 사이버 보안업체 '트렐릭스(Trellix)'는 2022년 5월 3일 보고서를 통해, 북한 정찰총국 소속 해커와 연관이 있는 랜섬웨어 변종 악성코드의 집합 4개(BEAF, PXJ, ZZZZ and CHiCHi)를 식별하였다고 밝혔다.[46] 트렐릭스는 북한의 라자루스가 개발한 'VHD 랜섬웨어'와 이번에 새롭게 발견된 랜섬웨어의 소스코드 설계도가 상당 부분 유사하다고 하였다.[47] 최근에는 북한이 새로운 변이 랜섬웨어 4종을 아시아 지역에 유포한 정황이 포착되었다는 보도도 있었다.

43 Ibid.

44 함지하, "북한, 미 의료기관 겨냥 '변종' 랜섬웨어 공격…법무부 50만 달러 회수," VOA, 2022년 7월 20일, https://www.voakorea.com/a/6665412.html, (검색일: 2022년 9월 28일).

45 강영진, "미 정부 북한 해커 랜섬웨어 공격 주의보 발령,"『뉴시스』, 2022년 7월 7일, https://mobile.newsis.com/view.html?ar_id=NISX20220707_0001934071 (검색일: 2022년 9월 28일).

46 지정은, "북 해킹조직 연루 새 '변종 랜섬웨어' 4종 발견,"『자유아시아방송』, 2022년 5월 4일, https://www.rfa.org/korean/in_focus/food_international_org/cyberattack-05042022090614.html, (검색일: 2022년 9월 28일).

47 Ibid.

다. 국방력 발전을 위한 신기술 탈취

김정은 정권이 국가의 전략노선으로 경제핵무력병진노선을 실행하던 시기, 북한의 사이버공격은 주로 △핵실험 전후 사회적 혼란 조성 △투발수단 관련 국방 신기술 탈취 △미국과 국제사회에 대한 정치적 시위 △핵개발 재원 마련을 목적으로 감행되는 경향이 있었다. 특히 북한은 병진노선을 추진하면서 투발수단을 확장하려고 노력했는데 이와 관련하여 국방 신기술 탈취를 시도하였다.

2014년부터 2016년 초까지 북한은 SK네트웍스 서비스와 대한항공 등 정부로부터 수주받는 방산 관련 대기업들을 해킹하여 자료 4만여 건을 유출하였다. 북한은 이들 방산업체로부터 F-15 전투기 관련 정보를 빼내려 했던 것으로 알려졌다. 북한이 공군력이 육군과 해군에 비해 상대적으로 취약하다는 사실에 비추어 볼 때, 균형 있는 군사력의 발전을 위해 공군력을 발전시키려는 의도를 가지고 신기술 탈취를 시도했던 것으로 추정된다.

또한 북한은 2016년 4월 방산업체인 대우조선해양 해킹을 통해 3000t급 잠수함을 포함하여 이지스함과 잠수함 설계도 및 전투체계와 관련된 1-3급의 군사기밀 60여 건을 유출하였다. 해군 최대 수송함인 독도함을 건조한 방위산업체 한진중공업 역시 2016년 5월 10일 북한 소행으로 추정되는 해킹을 받은 것으로 드러났다. 북한은 2016년 3월 16일부터 8월 24일까지 4차례의 북극성-1형 시험발사를 강행하는 등 SLBM 성능향상에 주력하고 있었으며 전력화를 위해 미사일 발사관이 1

개인 신포급 잠수함보다 더 큰 잠수함을 필요로 하였다. 따라서 장기적으로 잠수함에 3발 이상의 SLBM을 탑재하기 위해 북한은 3000t급 잠수함 설계 기술에 대한 정보가 필요했던 것으로 보인다.

이 밖에 북한은 2014년 말부터 2015년 4월까지 한국수력원자력의 직원 이메일을 통한 사이버공격을 감행하여 원자력발전소의 도면과 기관의 조직도 등 기관 내부자료를 유출하는 한편 직원들의 이메일에서 빼낸 일반문서를 공개하고 원전을 중단시키겠다며 협박을 시도하였다. 해커들은 6차례에 걸쳐 85건을 해킹하고 유출된 정보를 블로그에 올리면서 돈을 요구하기도 했다. 조사 결과 김수키가 사용하는 악성코드의 IP와 9자리가 일치하여 북한 소행으로 추정되었다. 그러나 북한은 대남선전매체인 『우리민족끼리』를 통해 수사 결과가 "무뇌무능아의 엉터리 판단"이라며 해킹 배후설을 부인하였다.[48] 이 같은 북한의 행동은 국가 인프라 시설인 원전을 대상으로 사회불안을 야기하고 불안심리를 자극하려 했던 것으로 보인다.[49]

2021년 1월, 노동당 제8차 대회 사업총화보고에서 김정은은 국방력 강화와 경제발전을 향후 5년 동안 가장 중요한 과제로 내세웠다. 구체적으로 북한은 국방과학발전 및 무기체계개발 5개년계획의 실행에 들어갔으며 핵무기 고도화를 위한 신기술 탈취를 목표로 전방위적 사이버공격을 감행하였다. 2021년 6월, 북한은 잠수함과 이지스함을 건조하는 대

48 『우리민족끼리』, 2015년 3월 18일.

49 조원일, "'한수원 해킹' 결정적 단서는 없지만… "北 소행"," 『한국일보』, 2015년 3월 17일, https://www.hankookilbo.com/News/Read/201503171885878015 (검색일: 2022년 8월 13일).

우조선해양과 원자력 추진 잠수함에 필요한 소형 원자로 개발에 관여해 온 것으로 알려진 한국원자력연구원에 대한 해킹을 시도한 것으로 드러났다. 대우조선해양의 경우 총 세 번째 해킹을 당하는 것으로 이 중 두 번이 북한 소행인 것으로 확인되었다. 한국원자력연구원의 경우 2021년 5월 승인되지 않은 외부 IP가 연구원 내부망에 접속했던 점이 확인되었으며 이는 김수키의 해킹 서버와 연결되어 있었다.[50] 연구원은 북한의 해킹에 12일간 노출되었던 것으로 알려졌다.

또한 2021년 5월, 한국항공우주산업(KAI)에 대한 해킹으로 인해 KF-21 보라매 전투기와 한국형 다목적 기동헬기인 수리온 헬기 관련 기술이 유출되었는데 이 또한 북한 해킹조직인 김수키의 소행으로 추정되었다.[51] KF-21의 경우 2032년까지 120대를 실전배치할 계획으로 사업의 규모가 8조 원 정도에 달하는, 국내에서 진행된 무기개발 사업 중 가장 큰 것으로 꼽힌다. 따라서 KAI에 대한 해킹은 경제적 피해는 물론 국방과 안보에도 심각한 타격을 주는 것이었다. 2022년 4월 1일 발표된 UN 안보리 대북제재위원회 전문가패널 보고서에 따르면 북한은 2021년 9월과 2022년 1월 시험발사한 극초음속미사일(북한 주장) 개발에 필요한 기술적 정보를 사이버공격을 통해 절취한 것으로 추정되었다.[52]

50 북한의 해킹 소식이 국내에 알려지자 북한은 대남선전매체인 『우리민족끼리』를 통해 "동족에 대한 적대 의식이 골수에 찬 대결광신자들이 황당무계한 모략 소동을 벌이고 있다"라며 혐의를 부정하고 남한 정부를 비난하였다. 이수헌, "北 선전매체, '해킹 공격' 의혹에 '황당무계한 모략소동'(종합)," 『SPN 서울평양뉴스』, 2021년 7월 21일, www.spnews.co.kr/news/articleView.html?indxno=41026 (검색일: 2022년 10월 27일).

51 북한은 한국원자력연구원과 한국항공우주산업에 대한 해킹 보도에 대해 "어불성설이고 언어도단"이라며 혐의를 부정한 뒤 무슨 사건만 터지면 과학적이며 객관적 증거도 없이 북 소행으로 몰아간다고 비판하였다. 『우리민족끼리』, 2021년 7월 12일.

52 황인호, "일 언론, "북, 극초음속 미사일 기술 해킹으로 훔친 듯"," 『국민일보』, 2020년 4월 3일, http://news.

국방 신기술 탈취를 목표로 한 북한의 해킹은 남한만을 대상으로 한 것이 아니었다. 2020년 8월, 이스라엘 국방부는 북한의 해킹조직인 라자루스 요원들이 주요 방산업체들로부터 민감한 정보를 훔치려 시도하여 이를 차단했다고 밝혔다. 이스라엘 국방부는 라자루스가 주요 방산업체 직원들에게 접촉해 일자리를 제공한다는 명목으로 링크드인(LinkedIn)에 가짜 프로필을 만들어 구인 제안을 보냈으며 이 과정에서 직원들의 컴퓨터를 훼손하고, 회사 네트워크에 접속하여 민감한 보안정보를 얻으려 했다고 설명했다. 링크드인을 통해 취업제안을 미끼로 사이버공격을 감행하는 것은 라자루스의 전형적인 해킹 수법으로, 라자루스는 2020년 12월, 독일의 최대 방산업체인 라인메탈(Rheinmetall)과 장갑차의 변속기, 탄약 등을 제조하는 렝크AG(Renk AG)사 등의 직원들을 상대로 불법으로 군사기술 정보를 탈취한 것으로 알려졌다.[53] 북한은 대북제재로 인해 선진적 군사 강국들로부터 무기를 수입하거나 기술이전을 받을 수 없는 처지이기 때문에 지속적인 사이버공격을 통해 군사기술을 탈취하려 한 것으로 추정되었다.

라. 대북 · 대외전략 탐색을 위한 전문가 · 탈북자 해킹

김정은은 2018년 4월 20일 당중앙위 제7기 제3차 전원회의를 개최하여 기존의 전략노선인 경제핵무력병진노선의 승리를 선언하고 새로운 전략노선으로 사회주의경제건설 총력집중노선을 제시하였다. 북한은 경제핵무력병진노선이 완료됨에 따라 핵 · ICBM 시험의 모라토리엄을 선언하였으며 5월 24일 외신기자들이 지켜보는 가운데 풍계리 핵실험장을 폐쇄하였다. 남북 간에 화해 분위기가 무르익음과 동시에 싱가포르에서 북미정상회담 개최가 예고되었고 북한은 핵 · 미사일 관련 동향을 일절 노출하지 않았다. 북한은 대외적으로는 남북대화와 북미화해를 통해 대북제재의 완화를 꾀하고 이를 염두에 두고 경제개발에 집중하고자 했다. 이 시기 제재 해제와 이후 북한의 경제성장의 청사진을 그릴 필요가 있었던 김정은 정권은 남북대화와 북미대화에 앞서 한미 정부의 대북전략을 탐색하려는 목적으로 사이버공격을 활용하였다. 주요 공격 대상은 한국의 외교 · 북한 전문가들, 국회의원, 북한이탈주민들이었다.

2018년과 2019년에는 3차례 남북정상회담의 개최로 남북관계에 관심이 높아지면서 통일부 직원을 사칭한 북한 소행의 해킹 이메일이 증가하였다. 북한은 2018년과 2019년 문재인 정부의 대북전략을 탐색하기 위해 통일부를 대상으로 각 630건과 767건의 해킹을 시도한 것으로 알려졌다.[54] 북한은 2019년 2월 하노이 북미정상회담이 사실상 실패로 끝나면서 남북대화 역시 소강상태에 접어든 이후에도 한국 정부의 대북전략 탐색을 시도하기 위해 사이버공격을 감행하였다. 북한은 2019년 9월 국회 외통위, 정보위, 국방위 소속 국회의원들을 대상으로, 2019년 4월에는 북한 문제 관련 전문가집단에 대하여 사이버공격을 실시하였다. 또

kmib.co.kr/article/view.asp?arcid=0016935267&code=61131111&cp=nv (검색일: 2022년 8월 13일).

53 박희준, "북한 해커, 라인메탈 등 독일 방산업체 사이버공격," 『글로벌이코노믹』, 2020년 12월 20일, https://news.g-enews.com/ko-kr/news/article/news_all/20201220160913234 8c5557f8da8_1/article.html?md=20201220161514_U (검색일: 2022년 9월 26일).

54 배영경, "통일부 대상 사이버공격 2018년부터 급증…'피해는 없어'," 연합뉴스, 2021년 7월 7일, https://www.yna.co.kr/view/AKR20210707168701050 4 (검색일: 2022년 10월 27일).

한 2020년 6월 16일, 북한이 남북공동연락사무소를 일방적으로 폭파하여 남북관계에 긴장감이 감돌자 탈륨은 한국 정부의 대응전략을 파악하기 위해 2020년 7월 남한의 외교 · 안보 분야 종사자에 대한 사이버공격을 시도하였다. 북한은 2021년 5월 21일에 개최된 한미정상회담을 전후로도 스피어피싱을 대대적으로 감행하였다. 해커들은 '한글' 파일이나 'MS워드' 파일을 이용해 악성코드를 배포하는 방식을 주로 활용하였다. 해킹조직 탈륨은 통일부를 사칭하여 통일부가 발행하는 "월간북한동향"과 통일연구원의 "조선노동당 제8차 대회 분석" 자료와 같은 첨부파일의 URL을 이메일에 연결하여 공격하였다.

스피어피싱 방법을 활용한 북한의 해킹은 대선 기간과 신정부 출범 이후에도 계속되었다. 북한은 남 · 북 · 미 대화의 재개 가능성, 새로운 남한 정부의 대북정책 등 남한 정부의 대북 · 대외전략을 탐색하기 위해 사이버공격을 지속적으로 감행하는 것으로 보인다. 2022년 3월에는 통일부 관계자로 사칭해 대북 전문가들을 겨냥한 또 다른 해킹 시도가 있었으며 2022년 5월에는 국민의힘 태영호 의원실을 사칭한 해킹 메일이 의원실에서 주최한 토론회 참석자들을 대상으로 유포되었다. 메일에 첨부된 MS워드 문서는 사례비 지급 형태로 되어 있어 메일 수신자들이 의심을 덜 수밖에 없도록 만들었다. 이 사건은 토론회 후 사례비 지급을 한다는 통상적인 행사 절차를 파악하고 있다는 것을 보여주는 것으로, 북한의 해킹 수법이 사회공학적으로도 진화하고 있음을 시사하였다.

그뿐만 아니라 북한이탈주민들을 상대로 한 스피어피싱 사례들이 발견되고 있으며 이 역시 북한이 배후인 것으로 추정된다. 해킹조직은 "제

20기 북한이탈주민 자문위원 대상 의견수렴_설문지.hwp"라는 악성파일을 첨부하여 탈북민들에게 의견을 수렴하는 것처럼 위장하여 공격을 시도하였다. 이 같은 북한의 해킹 시도들이 반복적으로 발생하면 정상적인 행정업무까지 매번 확인을 거쳐야 하는 등 행정의 비효율성이 초래되며 사회 전반에 불신 분위기를 형성하게 된다는 문제점이 있다.[55]

마. 코로나19 대응을 위한 원천기술 확보

북한은 2020년 코로나19 바이러스가 전(全) 세계적으로 확산함에 따라 낙후된 의료체계를 고려하여 외국인 입국 제한과 국경봉쇄, 주민들의 이동통제로 대응하였다. 이러한 이동 제한은 유증상자 30일 격리, 이동금지, 평양 진입 제한 등 다소 극단적으로 느껴지는 조치들을 포함하고 있었다. 그러나 이러한 봉쇄를 지속하기에는 북한 경제의 내구성이 한계에 다다를 수도 있었다. 김정은 정권은 제재 장기화, 수해, 코로나19에 따른 '삼중고'에 직면하였으며 경제난을 극복하기 위해 사이버공격 능력을 활용하였다.

우선 코로나19 백신과 치료제 원천기술을 얻기 위해 국내외 제약회사에 해킹을 시도하였다. 김정은 정권은 대외적으로 북한 내 코로나19 감염자가 없다고 발표하였으나 백신과 치료제 원천기술에 접근하기 위해 2020년부터 화이자, 아스트라제네카, 존슨앤존슨, 노바백스, 셀트리

55 기획취재팀, "토론회 개최한 태영호 의원실 사칭 북한 해킹 메일 공격 포착됐다," 『보안뉴스』, 2022년 5월 20일, https://www.boannews.com/media/view.asp?idx=106924&kind= (검색일: 2022년 8월 13일).

온, 제넥신, 신풍제약 등 한국뿐만 아니라 미국 · 영국 등 글로벌 제약사에 대한 해킹을 시도했던 것으로 확인되었다. 그러나 북한 스스로 백신을 개발하여 보관할 만한 능력이 부족하기 때문에 해킹 시도는 백신 기술 탈취를 통한 자체적인 백신 생산을 목적으로 하기보다 북한 내부 상황에 맞는 백신 제품이 무엇인지 확인하기 위함이었을 것으로 추측되었다.[56] 크리스토퍼 레이(Christopher Wray) 미 FBI 국장 역시 상원 법사위원회 청문회 제출 보고서에서 북한이 미국의 백신 연구를 겨냥한 사이버 작전을 진행해왔다고 확인했다.[57]

북한은 공식적으로 코로나 환자가 '0'이라고 주장하고 국제사회로부터 백신 수급조차 극구 거부하는 등 외부의 도움을 철저히 차단하였다. 그러나 실제로는 코로나19 발병 이후부터 국제사회의 바이러스 발생 동향에 많은 관심을 기울이는 한편 백신과 치료제 관련 정보를 얻기 위해 세계의 제약사와 병원 등을 상대로 광범위하게 사이버공격을 시도하였다는 사실이 드러났다. 2021년 6월에는 북한 해킹조직인 김수키가 서울대병원 서버 1대와 업무용 PC 62대를 해킹하여 환자 정보 6,969건을 유출한 것으로 알려졌다. 서울대병원뿐만이 아니라 다른 국가기관 및 병원에 대한 북한의 대규모 침해 시도도 드러났다. 다행히 국내 제약회사들의 경우 북한의 해킹 시도를 사전에 포착하고 미리 방지한 덕분에 기밀사항이 유출되는 피해는 겪지 않은 것으로 확인되었다.

56 김지영, "'코로나 0명'이라더니…북한은 왜 '화이자 해킹' 시도했나," 『머니투데이』, 2021년 2월 18일, https://news.mt.co.kr/mtview.php?no=2021021715345891578 (검색일: 2022년 8월 13일).

57 김승욱, "FBI "북한, 해킹으로 코로나19 백신 기술 탈취 시도," 2022년 8월 5일, https://www.yna.co.kr/view/AKR20220805016000504?input=1195m (검색일: 2022년 8월 13일).

2022년 5월, 북한은 최초로 코로나19 환자 발생 사실을 인정하고 정치국 회의를 소집하여 대책 마련에 착수하였다.[58] 북한은 최대비상방역체계를 가동하여 코로나19에 대응하였으나 백신이나 치료제가 일반 주민들에게까지 공급되었다는 보도는 찾아보기 힘들었다. 북한은 민간요법과 일반 의약품에 의존하고 고려약(북한식 한약)까지 선전하는 한편, 투명성이 의심되는 확진자 수를 매일 공개하면서 상황이 나아지고 있음을 선전하였다. 이후 북한은 8월 10일 김정은 주재로 "전국비상방역총화회의"를 개최하여 코로나19의 종식을 선언하였으며 북한은 백신 접종 없이 방역전쟁에서 승리하였다고 자축하였다.

58 2022년 4월 25일 조선인민혁명군 창건 90주년 기념일을 맞이하여 열린 열병식을 계기로 코로나19가 확산한 것으로 추정되었다.

Ⅲ

북한 사이버위협에 대한 주요국 대응

1. 진영화와 경제제재

4차 산업혁명과 코로나19 바이러스로 인한 디지털 전환의 가속화, 그리고 미중경쟁은 사이버공간에서 미국을 비롯한 서방 국가들과 북한, 중국, 러시아 등의 권위주의 국가들 사이의 진영화를 격화시키고 있다. 특히 우크라이나 전쟁은 자유민주적 시장경제 질서와 보편적 가치를 중요시하는 서방 국가들과 러시아의 국가 배후 해커 또는 친러시아 성향의 해커들 사이의 대립과 갈등을 사이버공간으로 확장하고 있다. 미국과 서방은 러시아에 대해서는 우크라이나 침공을 이유로, 중국에 대해서는 기술 탈취와 지적재산권 침해를 이유로, 북한에 대해서는 금융기관에 대한 공격과 암호화폐 탈취를 통한 제재 회피와 핵능력 증강을 이유로 자유시장경제와 국제평화에 타격을 가하였다고 비난하고 있다.

이 같은 사이버공간의 진영화는 상대 진영에 대한 경제제재와 수출통제는 물론, 같은 진영을 중심으로 한 사이버 합동훈련이나 정보공유의 강화로 나타나고 있다. 미국의 경우 바이든 대통령이 2021년 4월 15일 러시아의 악의적 사이버 활동 관여를 포함한 불안정한 국제적 활동을 지속시키거나 심화하는 행동에 대해 비용을 부과하겠다는 행정명령에 서명하였다.[59] 또한 미국 상무부 산업안보국(Bureau of Industry and Security: BIS)은 2021년 10월 20일 악의적인 사이버 활동에 사용될

59 The White House, "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021,https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (accessed: September 30, 2022).

가능성이 있는 특정 품목의 수출, 재수출, 국내 전송에 관한 규제를 강화한다고 발표하였는데, 이로 인해 무기수출 규제 대상국인 중국이나 러시아 등과의 거래는 원칙적으로 금지되었다.[60]

북한의 악의적 사이버 활동에 대해서 서방은 경제제재를 강화하고 있다. 대표적으로 미국과 EU의 사례를 들 수 있다. 미국은 악의적 사이버 활동 또는 외국에 위치한 사람의 감독하에 이루어진 악의적 사이버 활동으로 미국의 국가안보, 외교정책 및 경제에 비정상적인 위협을 야기하는 경우 제재를 부과하는 것이 보편적이다. 악의적 사이버 활동에 대한 제재는 특히 오바마 대통령이 2015년 4월 1일에 발표한 행정명령 제13694호에 근거한다. 2020년 10월 1일, 미국 재무부 해외자산관리국(Office of Foreign Assets Control: OFAC)은 랜섬웨어 피해 기업이 공격자에게 랜섬웨어 해제를 위해 대가를 지불하는 것이 법규 위반이 되어 미 연방정부로부터 벌금을 부과받을 수 있다는 권고안을 발표하였다. 랜섬웨어 공격자가 북한, 쿠바, 우크라이나의 크림지역, 이란, 시리아 등 OFAC가 규제하는 국가 또는 사람이었을 경우가 대상이 된다. 또한 금융기관, 보험회사, 사고 대응회사 등이 피해 기업에 지불을 촉진했을 경우도 규제 대상이 된다.[61] 2021년 2월 17일, 미 국무부 대변인은 정례브리핑에서 "대북정책 검토를 진행하면서 북한의 악의적 활동과 위협을 총체적으로 고려할 것"이라며 "우리가 주의 깊게 평가하고 주시하고 있는 북한의 악성 사이버 활동도 여기에 포함된다."라고 밝혔다.[62]

유럽연합(European Union: EU)은 미국만큼 광범위하고 적극적인 제재를 하지 않지만 사이버공격에 대한 제재를 시행하고 있다. 2020년 7월 30일, EU는 처음으로 사이버공격을 이유로 경제제재를 단행하면서 러시아와 중국의 개인 6명과 기관 2곳을 비롯하여 북한의 조선엑스포합영회사를 제재 대상 명단에 올려놓았다.[63] 해당 제재는 2021년 5월, 1년 연장 결정이 내려졌다. 제재 대상 기관과 개인은 EU 입국이 제한되며 자산이 동결된다. 북한의 조선엑스포합영회사 소속 해커들은 2017년 워너크라이 랜섬웨어 공격, 2017년 폴란드 금융 감독청 해킹, 2014년 소니픽처스 영화사 해킹, 2016년 방글라데시 중앙은행 사이버공격 등을 감행한 것으로 알려져 있다. EU는 조선엑스포합영회사의 사이버공격으로 EU와 회원국이 지대한 피해를 입었다고 주장하였다. 특히 2017년 워너크라이 2.0 랜섬웨어 사건은 EU 내 기업을 포함한 세계 정보시스템에 상당한 지장을 일으켜 시민들과 기업의 경제활동과 필수서비스 유지에 악영향을 초래하였다고 지적하였다.

60 Federal Register, "Information Security Controls: Cybersecurity Items," October 21, 2021, https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items (accessed: September 30, 2022).

61 U.S. Department of The Treasury, "Ransomware Advisory," October 1, 2020, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001 (accessed: August 13, 2022).

62 함지하, "국무부 "대북 정책 재검토, 사이버 활동 등 위협 고려…미국 위협 줄이는 데 초점"," VOA, 2021년 2월 18일, https://www.voakorea.com/a/korea_korea-politics_state-briefing-about-north-korean-cyber-attacks/6056276.html (검색일: 2022년 10월 19일).

63 Council of the EU, "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/ (accessed: October 19, 2022). 앞서 EU는 사이버 공격자(개인 또는 국가기관, 기업)에 대해 자산동결과 여행금지 등의 제재를 부과하는 법규(Council Decision 2019/797 and Council Regulation No. 2019/796)를 2019년 5월 22일에 통과시킨 바 있다.

EU의 사이버 대북제재는 미국의 사이버 제재와 비교할 때 정교하다고 평가하기는 어렵지만 여행금지와 자산동결이라는 제재 유형과 중국, 러시아, 북한 등 제재 대상에 있어서 미국의 제재와 유사성을 보인다. 특히 조선엑스포합영회사의 경우 EU의 제재 대상인 동시에 미국의 제재 대상이기도 하여 향후 EU와 미국 정부가 북한과 중국, 러시아 등 공동의 사이버위협 국가들에 대해 제재 협력을 할 수도 있을 것으로 기대된다.[64]

2. 랜섬웨어 대응 강화

북한은 미국과 UN 안보리의 경제제재가 강력하게 유지되고 있는 상황에서 부족한 외화를 조달하기 위해 랜섬웨어 공격을 확대 · 지속할 것으로 보인다. 북한의 대표적인 해커조직인 라자루스 그룹은 2017년 워너크라이 랜섬웨어 사건에 관여하여 150여 개국에 악영향을 미치고 30만 대의 컴퓨터에 피해를 야기한 바 있다. 2020년 코로나19 대유행으로 랜섬웨어는 위장형 공격과 원격접속(RDP) 등을 통한 공격 등으로 변화 · 발전하고 있는데, 북한 해커 그룹들은 더 많은 금전적 이득을 위하여 랜섬웨어 공격에 다양한 변화를 시도하고 공격 대상과 범위도 확대할 것으로 예상된다.

날이 갈수록 심각해지는 랜섬웨어 공격에 대해 각국은 공동 대응의 필요성을 강조하는 한편, 국가별로 대응방안을 강화하고 있다. 사이버위협

64 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 (accessed: April 22, 2022).

에 공동으로 대처할 수 있는 플랫폼은 부재하지만, 북한 등 주요 국가배후 해킹 세력들이 가하는 랜섬웨어 위협 대응과 관련하여 가장 대표적인 다자협의체는 G7이라고 할 수 있다. G7 사무국은 2021년 12월 15일부터 16일까지 랜섬웨어 범죄 네트워크에 대처하기 위한 임시 포럼을 개최하였다. 이 포럼에는 유럽평의회, 유럽위원회, 유럽연합 사이버보안청(European Union Agency for Cybersecurity: ENISA), 유로폴, 인터폴, 국제자금세탁방지기구(Financial Action Task Force: FATF) 금융활동전담반, G7 사이버 전문가 그룹, UN 약물범죄사무소(United Nations Office on Drugs and Crime: UNODC) 등에서 고위관리들이 참가하였다. 이 포럼에서는 랜섬웨어 범죄의 조직화, 정책적 개입, 암호화폐 대응, 회복력 향상 등이 중점적으로 논의되었다.[65] 이어 2022년 6월 13일, 영국 콘월에서 열린 G7 정상회담의 공동선언문은 랜섬웨어 피해를 줄이기 위한 G7 국가들의 공동 행동에 대한 의제를 다루었다. G7 국가들은 랜섬웨어에 공동으로 대처하며 랜섬웨어 범죄집단에 대해 책임을 묻는 한편, 러시아에 대해 랜섬웨어 방지를 위한 행동에 나설 것을 촉구하였다.

이처럼 국제사회는 점차 랜섬웨어 위협에 대응하여 국제공조를 강화하는 방안을 논의하고 있다. 미국은 이러한 공동 대응의 필요성을 주도하고 있는 국가라고 볼 수 있는데 미국 백악관 국가안보실은 2021년 10월 13일부터 14일까지 이틀에 걸쳐 '랜섬웨어 대응 이니셔티브' 화상회

65 Government of UK, "G7 Interior and Security Senior Officials' Meeting on Ransomware," December 24, 2021, https://www.gov.uk/government/publications/g7-interior-and-security-senior-officials-meeting-on-ransomware (accessed: October 27, 2022).

의를 개최하였다. 이 회의에는 영국과 호주는 물론 유럽 · 중동 · 아프리카 · 아시아 등에서 30개국 이상이 참가하였다. 참여국들은 랜섬웨어가 세계적인 규모로 경제와 안보를 위협하고 있다는 데 인식을 같이하고 공동 대응을 위해 노력하기로 하는 공동성명을 발표하였다. 이 공동성명에는 랜섬웨어 공격으로부터의 회복력 강화와 법 집행 당국의 랜섬웨어 범죄자 추적과 단속을 위한 외교적 협력의 추진 등이 포함되었다.[66] 공동성언문에는 랜섬웨어 위협을 가하는 특정 국가에 대한 언급은 없었지만, 미국이 러시아, 중국, 북한 등에 의한 랜섬웨어 공격에 대한 국제공조 태세를 확립하기 위해 회의를 개최한 것이란 분석이 제기되었다.

랜섬웨어 대응을 위한 국제공조는 다자협력뿐만 아니라 양자협력 차원에서도 논의되고 있다. 2022년 5월 21일에 개최된 한미정상회담에서는 윤석열 대통령과 미국 바이든 대통령이 사이버안보에 있어 한미 동반자 관계를 확장하기로 합의하면서 랜섬웨어 공격 대처를 위한 사이버 실무자 회의(working group)의 설립에 동의하였다. 이를 통해 북한 랜섬웨어 위협에 대한 공동 대응의 기반이 마련될 것으로 보인다. 또한 2021년 7월 9일 바이든 대통령과 푸틴 러시아 대통령은 러시아 기반 랜섬웨어 해킹그룹인 레빌(REvil)의 소행으로 알려진 카세야 랜섬웨어 사건(Kasey VSA ransomware attack)에 대해 전화통화를 나누었다. 바이든은 푸틴에게 직접 전화를 걸어 러시아에서 활동하는 랜섬웨어 집단

66 Anne Neuberger, "Update on the International Counter-Ransomware Initiative," U.S. Department of State, October 15, 2021, https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative (accessed: August, 13, 2022).

을 압박하는 조치를 취할 필요가 있다고 강조하였다.[67] 이 통화 이후 러시아 해킹그룹 레빌의 활동은 잠잠해졌고 다크웹에서 이들의 웹사이트 또한 사라졌는데, 이는 러시아 당국의 압력에 따른 것으로 해석되고 있다.[68]

또한 일부 국가들은 개별적으로 랜섬웨어 대응방안을 강화하고 있는데 미국과 영국이 주목할 만하다. 미국 정부의 경우 암호화폐로 랜섬웨어 대가(몸값)를 지급하는 경우 정부에 보고하도록 하고, 암호화폐의 익명성을 제한할 수 있도록 암호화폐거래소와 금융기관으로 하여금 암호화폐 거래에 대해 보고나 등록 조치 등을 시행하도록 압박하고 있다. 나아가 랜섬웨어 관련 정보를 제공한 사람에 대한 보상을 통해 민간의 협력을 기반으로 랜섬웨어에 적극적으로 대응할 것으로 보인다. 즉, 미국의 주요 산업에 대한 랜섬웨어 공격의 중단 또는 공격자 등의 처벌에 기여하는 정보를 제공하는 경우 1,000만 달러까지 보상할 수 있도록 한다는 계획이다. 랜섬웨어가 국가안보 최우선 위협이 되었기 때문에 국제테러에 대응하기 위해 설립된 국무부의 '정의를 위한 보상(Reward for Justice)' 프로그램의 하나로 랜섬웨어 공격 관련 정보를 제공할 시 포상금을 지불한다는 것이다.[69]

67 장영은, "바이든의 경고 먹혔나…러시아 랜섬웨어그룹 돌연 사라져," 『이데일리』, 2021년 7월 14일, https://www.edaily.co.kr/news/read?newsId=03480086629114520&mediaCodeNo=257 (검색일: 2022년 10월 1일).

68 David E. Sanger and Julian E. Barnes, "Biden Makes a New Push in Fight against Ransomware, Including a $10 Million Reward," The New York Times, July 15, 2021, https://www.nytimes.com/2021/07/15/us/biden-reward-ransomware.html (accessed: October 19, 2022).

69 Joseph Marks, "The Cybersecurity 202: The Biden administration is stepping up the fight against ransomware," The Washington Post, July 15, 2021, https://www.washingtonpost.com/politics/2021/07/15/cybersecurity-202-biden-administration-is-stepping-up-fight-against-ransomware/ (accessed: October 19, 2022).

영국 정부는 심각한 랜섬웨어 피해를 경험한 이후 2021년 12월 발표한 『국가사이버전략 2022 (National Cyber Strategy 2022)』에서 랜섬웨어 공격이 더욱 정교해지고 있으며 심각한 피해를 야기하고 있다고 인식하고 있다.[70] 특히 랜섬웨어 공격을 2021년 영국이 직면한 가장 심각한 사이버위협으로 인식하였으며[71] 암호화폐가 랜섬웨어 공격에 활용되고 있는 상황을 우려하였다.[72] 영국은 이 전략에서 러시아와 중국으로부터 발생하는 사이버공격을 탐지하고 차단하기 위하여 파트너들과 협력하였는데, 특히 조직범죄 집단에 의해 감행되고 있는 서방을 향한 랜섬웨어 공격이 대부분 러시아에 근거를 두고 있다고 결론지었다.[73] 『국가사이버전략』을 통해 영국 정부는 랜섬웨어에 보다 효과적으로 대응하기 위해 기존 정부정책과 운영 방식을 검토할 것임을 천명하였다. 아울러 랜섬웨어 대응을 위한 각종 활동을 전개하고 민간 및 국제 파트너들과 협력할 것을 표명하였다.

3. 암호화폐 대응 강화

앞서 2장에서 살펴본 바와 같이 북한은 역대 최고 수준의 대북제재 속에서 핵 · 미사일 프로그램의 지속과 확장을 위해 암호화폐 관련 사이버

70 HM Government, *UK National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK*, December 2021, p. 24, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (accessed: October 27, 2022).

71 Ibid.

72 Ibid., p. 30.

73 Ibid., p. 26.

공격을 지속하였다. UN 안보리 대북제재위 전문가패널 보고서는 북한이 2021년 암호화폐거래소와 투자회사에 대한 7건의 사이버공격을 통해 총 4억 달러 상당의 암호화폐를 훔친 것으로 추정하였다. 보고서는 북한이 불법적으로 확보한 암호화폐를 농축우라늄(HEU) 생산을 포함한 핵 · 미사일 개발에 쓴 것으로 보았다. 한 UN 회원국에 따르면 북한은 영변 핵실험 실험용 경수로의 외부 공사를 완료하고 내부 개조를 진행하고 있는 것으로 확인되었다.[74] 또한 패널들은 북한이 암호화폐거래소에 대한 사이버공격으로 획득한 암호화폐를 핵 · 미사일 기술 개발을 위한 주요 수입원으로 삼았다고 주장했다.[75]

미국 블록체인 정보분석업체 체이널리시스(Chainalysis) 보고서에 따르면 북한은 2018년 이후 해킹을 통해 해마다 2억 달러어치 이상의 암호화폐를 탈취하고 있는 것으로 조사되었다.[76] 이 보고서에 따르면 북한이 확보한 암호화폐 가운데 이더리움의 비중이 58%로 가장 높았고, 비트코인 비율은 20%로 2017년(100%)의 5분의 1로 줄었으며, 나머지 알트코인(비주류 암호화폐)이 22%를 차지했다고 한다. 북한은 암호화폐거래소와 투자회사를 피싱, 악성코드 등으로 공격해 코인을 빼돌린 뒤 자신들이 관리하는 지갑으로 옮기는 방식을 주로 사용하였다. 다양한 코인을 섞어 여러 차례 세탁하고 디파이(DeFi) 플랫폼을 사용하는 등 수법

74 조현의, "UN "북 해커조직 김수키, IAEA · KAI 해킹"," 『아시아경제』, 2022년 2월 8일, https://view.asiae.co.kr/article/2022020810211910643 (검색일: 2022년 8월 13일).

75 정영교, "유엔, 北, 작년 사이버공격서 번 돈으로 미사일 기술 증강," 『중앙일보』, 2022년 2월 6일, https://www.joongang.co.kr/article/25045877 (검색일: 2022년 10월 1일).

76 임현우, "北, 작년 암호화폐 4억 달러 해킹…이더리움이 58%," 『한국경제』, 2022년 1월 16일, https://www.hankyung.com/economy/article/2022011617971 (검색일: 2022년 10월 19일.).

또한 고도화되었다. 디파이는 이용자 정보를 수집하지 않아 법 집행 당국의 추적에 따른 자산동결 위험이 없다는 장점이 있다. 이는 라자루스 그룹이 주도한 것으로 추정되고 있다. 북한은 2017년부터 2021년까지 해킹한 암호화폐 중 1억 7,000만 달러어치는 현금화하지 않고 그대로 보유 중인 것으로 파악되고 있다.[77]

한편 미국은 북한의 금전적 효과를 노린 사이버공격에 대해 기소와 제재, 경보 발령 및 보고서 발간, 카운터해킹 등으로 다양한 방식으로 대응하고 있다. 미 법무부는 2020년 12월 북한 정찰총국 소속 해커 전창혁 · 김일 · 박진혁 등을 미국 및 멕시코 · 폴란드 · 파키스탄 · 베트남 · 몰타 등 전 세계의 은행과 기업, 암호화폐거래소 등에 대한 사이버공격으로 13억 달러 규모의 현금과 암호화폐를 절취하려고 시도한 혐의로 기소하였다.[78] 이들은 '크립토뉴로 트레이더(CryptoNeuro Trader)' 앱을 통해 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 있다. FBI는 2021년 2월 17일 세계적 사이버공격과 금융범죄에 대한 책임을 물어 이들의 사진을 담은 공개수배 전단을 공개하였다.[79] 박진혁의 경우 북한으로 돌아간 지 이미 수년이 지

77 Ibid.

78 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: 2022년 10월 19일).

79 Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and (accessed: August 13, 2022).

났기 때문에 법무부나 FBI가 실제로 그를 체포하거나 법원에 출석시킬 방법은 사실상 없었다. 다만 북한의 악명높은 해커들을 기소하고 사진과 실명을 공개한 행위는 북한 사이버 범죄 근절에 대한 미국 정부의 강력한 의지를 보여준 것으로 평가할 수 있다.

또한 미국의 사이버안보 관련 기관들은 북한의 금융 공격에 특화된 보고서를 발간하는 한편 북한의 사이버공격에 대한 경각심을 높이는 경보를 발령하고 있다. 2020년 8월 26일, FBI와 CISA(Cybersecurity and Infrastructure Security Agency) 등 미국 정부기관들은 북한 해커들이 전 세계 은행들에 불법 접속해 불법 송금과 현금자동입출금기(ATM)를 통한 불법 인출을 시도하고 있다는 경보를 발령한 바 있다.[80] 또한 CISA는 2020년 5월 12일 북한 해커들이 사용하는 악성코드 3개에 대한 분석 보고서도 발간하였다. CISA와 사이버사령부, 연방수사국(FBI) 등이 작성에 참여한 보고서는 북한 해커가 사용하는 악성코드의 개요와 대응 권장 사항, 피해경감 대책 등이 정리되어 있다.[81] 그뿐만 아니라 2020년 4월 15일 미국 국무부, CISA, 재무부, 연방수사국(FBI) 등은 북한의 사이버위협에 대한 인식 제고를 위해 새로운 지침서를 발표하였다.

80 Cybersecurity 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 (accessed: August 13, 2022).

81 Cybersecurity 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 (accessed: August 13, 2022). ; Cybersecurity and Infrastructure Security Agency, "North Korea Cyber Threat Overview and Advisories," https://www.us-cert.gov/northkorea (accessed: August 13, 2022).

이 지침서는 과거 북한의 사이버공격 활동, 대책을 위한 권장 사항 등이 정리되어 있다. 특히 북한 해커들이 금융기관을 대상으로 하고 있다는 점을 지적하면서 경계를 촉구하였다.[82]

그뿐만 아니라 최근 미국은 보다 적극적인 대응을 시도하고 있는데, 북한이 해킹에서 벌어들인 불법 자금을 다시 회수하는 카운터해킹(counter-hacking) 방법을 활용하는 것이다. 미국은 북한이 2022년 3월 블록체인 비디오 게임 '액시 인피니티'에서 훔친 암호화폐 중 3,000만 달러 이상을 회수한 것으로 알려졌다. FBI 수사관들은 첨단 블록체인 모니터링 도구와 중앙집중식 암호화폐거래소 간 협력을 기반으로 라자루스의 암호화폐 현금화 시도를 파악해 거래를 동결하고 도난 암호화폐 일부를 회수할 수 있었다.[83]

이 외에도 미 정부는 랜섬웨어 공격에 암호화폐로 몸값을 지불한 경우에도 금액을 압류하고 회수하는 성과를 올렸다. 2022년 7월, 미 법무부는 캔자스주의 한 병원이 랜섬웨어 공격을 당해 라자루스 그룹에 몸값으로 지불한 50만 달러를 회수했다고 밝혔다. 법무부와 FBI는 피해사실을 접수하고 수사를 통해 북한이 훔친 돈이 연계된 중국 자금세탁 조직에

82 Cybersecurity and Infrastructure Security Agency, "Alert (AA20-106A) Guidance on the North Korean Cyber Threat," June 23, 2020, https://www.us-cert.gov/ncas/alerts/aa20-106a (accessed: August 13, 2022).

83 Dustin Volz, "U.S. Recovers Over $30 Million in Cryptocurrency Stolen by North Korean Hackers," The Wall Street Journal, September 8, 2022, https://www.wsj.com/articles/u-s-recovers-over-30-million-in-cryptocurrency-stolen-by-north-korean-hackers-11662648600 (accessed: September 1, 2022).

흘러 들어간 것을 확인하고 금액을 압류한 뒤 병원과 의료센터 피해자들에게 돌려주었다.[84]

이처럼 북한의 진화하는 사이버공격에 맞서 미국의 대응방안도 적극적이고 전방위적으로 진행되고 있는 것으로 보이며, 북한은 암호화폐 공격 성공 이후 자금회수 과정에서 미국과 밀고 당기는 줄다리기를 할 것으로 예상된다.

84 Department of Justice, "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and Their Conspirators," https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors (accessed: September 1, 2022).

Ⅳ

우리의 대응방안

1. 국제적 협력 확대

가. 핵 · 미사일 개발과 연계된 사이버공격과 암호화폐 대응 강화

북한의 사이버공격은 남한과 주변국에 대한 무력도발을 전후로 하여 사회적 혼란을 초래하기 위해 이루어지거나 핵개발에 필요한 정보를 탈취하기 위해 감행되었으며, 핵 · 미사일 프로그램의 발전을 위한 외화획득의 수단으로 이루어졌다. 한국은 북한이 핵실험과 탄도미사일 발사 등 무력도발의 감행 전후로 사회적 혼란을 야기하기 위해 감행하는 북한의 사이버공격에 대한 경계태세를 강화하는 동시에 북한의 사이버공격 동향과 관련한 정보를 미국과 서방은 물론 국제사회와 공유할 필요가 있다. 특히 2022년 상반기부터 신정부 출범을 겨냥한 북한의 무력시위가 사이버공간으로 확산할 가능성이 농후하기 때문에 이에 대해 국제사회와 더불어 대비할 필요가 있다. 구체적으로 예를 든다면, 북한이 물리적 도발과 사이버공격을 동시에 감행할 가능성이 높은 만큼 한미연합훈련을 실시할 때 한미사이버연합훈련도 강도 높게 실행하는 것을 고려할 필요가 있다.

또한 북한은 암호화폐와 금융기관에 대한 사이버공격으로 핵개발을 지속하기 위한 외화를 획득하였기 때문에, 국제사회와 더불어 북한의 불법 자금 차단방안을 모색하여야 한다. 국제사회와 협력을 통해 북한 출신 해커들에 대한 수사와 기소는 물론 해킹에 가담한 북한 기업소, 기관 및 단체에 대한 경제제재를 단행할 수 있을 것이다. 아울러 국제사회와 협력하여 북한 해커들이 암호화폐를 일반 화폐로 환전한 기관이나 단체를 찾아내 경제제재를 내릴 수도 있다.

2022년 8월 11일, 북한 라자루스 그룹이 탈취한 4억 5,500만 달러 상당의 암호화폐를 토네이도 캐시(Tornado Cash)라는 업체를 활용하여 돈세탁 창구로 활용한 사실이 밝혀졌다.[85] 따라서 이 토네이도 캐시라는 업체를 제재 대상으로 지정해야 한다는 목소리가 높다. 미 재무부는 이미 2022년 8월 토네이도 캐시를 특별지정 제재 대상(Specially Designated Nationals: SDN) 목록에 추가하고 이 조치가 부패나 범죄 활동에 사용될 자금세탁을 목적으로 믹서를 이용하려는 범죄에 대한 억제책으로 작용할 수 있을 것으로 기대한다고 발표하였다.[86]

한편 2022년 2월 1일 유로폴은 암호화폐의 범죄 이용에 관한 보고서를 발표하였다. 이 보고서는 법 집행기관으로 하여금 암호화폐의 부정 이용에 적극적으로 대처하도록 지원하기 위해 작성되었다. 동 보고서는 법 집행기관이 암호화폐 대응에 있어 직면한 과제를 정리하고 대응 사례와 방법 등에 대한 상세한 정보를 제공하고 있다.[87] 우리 정보당국과 법 집행 당국도 유로폴과의 협력을 통해 북한의 암호화폐 공격 기법과 대응 사례 및 방법 등에 대한 정보를 제공할 필요가 있다.

우리 정부는 암호화폐로 대가(몸값)를 요구하는 랜섬웨어 퇴치를 위해

85 박형주, "북한 가상화폐 세탁에 이용되는 '렌 브릿지' 제재해야…'환전 네트워크' 압박 필요," VOA, 2022년 8월 12일, https://www.voakorea.com/a/6698148.html (검색일: 2022년 8월 14일).

86 그러나 암호화폐 분야 엔지니어 및 투자자들 6명은 이와 관련하여 탈중앙화된 오픈소스 소프트웨어인 토네이도 캐시를 제재 대상 주체로 지정할 권리가 없다는 이유를 들어 미 재무부를 상대로 소송을 제기한 상태다. 토네이도 캐시로 촉발된 암호화폐의 탈중앙성과 이에 대한 규제에 대한 법적 논쟁이 앞으로 더욱 치열해질 것으로 예상된다.

87 Europol, "Cryptocurrencies: Tracing the Evolution of Criminal Finances," January 27, 2022, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (accessed: October 19, 2022).

국제사회가 추진하는 북한의 사이버 범죄자와 해커 집단에 대한 공개수배, 기소와 소추 등에 적극 참여할 필요가 있다. 우리의 경우 미국 및 우크라이나와 협력하여 우크라이나 경찰이 2021년 6월 16일 미국과 우리나라에 랜섬웨어 공격을 감행한 6명의 범죄자를 체포하고 18만 5,000달러에 이르는 대가(몸값)를 압수하도록 지원한 경험이 있다.[88]

북한을 포함한 랜섬웨어 공격에 대해 국제사회가 우리 정보기관 및 법 집행기관에 대해 적극적인 협력을 요청할 것으로 보이므로 이에 대한 준비가 필요하다. 특히 북한 랜섬웨어 공격 관련 정보의 공유와 수사 및 소추에 필요한 사항에 관한 협조를 구할 가능성이 크므로 이에 대비할 필요가 있다. 북한 해커 그룹들은 더 많은 금전적 이득을 위하여 랜섬웨어 공격에 다양한 변화를 시도하고 공격 대상이나 범위도 확대할 것으로 전망된다. 따라서 북한의 랜섬웨어 공격을 국제사회와 함께 지속적으로 탐지하고 모니터링할 필요가 있다.

나. 사이버 글로벌 중추국가로서의 역할 수행

미중경쟁과 러시아-우크라이나 전쟁으로 진영화가 심화하고 있는 상황에서 한국은 사이버위협에 대응하여 미국 및 서방국가들과 협력을 강화함으로써 진영화에 참여하고 있는 것으로 볼 수 있다. 우선 한국은 2022년 5월 5일 북대서양 조약기구(NATO)의 사이버방위센터

88 Jim Heintz and Frank Bajak, "Ukraine Police Seize Cash in Raid on Major Ransomware Gang," AP, June 17, 2021, https://apnews.com/article/europe-ukraine-technology-hacking-a56fc6b3d1cd79ffd987e721bf558985 (accessed: October 19, 2022).

(Cooperative Cyber Defence Centre of Excellence: CCDCOE)의 정회원으로 가입하였다. 한국은 NATO의 비회원국으로서 사이버방위센터의 정회원이 된 다섯 번째 국가이며 아시아 국가로서는 처음이다. 사이버방위센터 정회원은 총 32개국으로, NATO 회원국들로 이루어진 27개 후원국과 NATO 비회원국들로 구성된 5개 기여국이 있다. 한국은 핀란드, 오스트리아, 스웨덴, 스위스와 더불어 CCDCOE의 기여국(Contributing Participants)으로 참여하게 되었다.

또한 한국은 2022년 5월 개최된 한미정상회담에서 자유민주적 가치에 기초하여 미국과 사이버안보 전반에 걸쳐 적극적으로 협력하기로 합의하였다. 구체적으로 한미는 국가 배후의 사이버공격 등을 포함하여 북한으로부터의 다양한 사이버위협에 대응하기 위한 협력을 대폭 확대하기로 하였다. 또한 한미는 핵심 · 신흥 기술과 사이버안보 협력을 심화하고 확대하기로 합의하면서, 민주주의 원칙과 보편적 가치에 맞게 기술을 개발, 사용, 발전시킬 것을 약속하였다. 그뿐만 아니라 한미는 사이버 적대세력 억제, 핵심 기반시설의 사이버보안, 사이버 범죄 및 이와 관련한 자금세탁 대응, 암호화폐 및 블록체인 애플리케이션 보호, 역량 강화, 사이버 훈련, 정보공유, 군 당국 간 사이버 협력을 강화하기로 하였다. 사이버공간에서의 여타 국제안보 현안에 관한 협력을 포함하여, 지역 및 국제 사이버 정책에 관한 한미 간 협력 또한 지속적으로 강화할 예정이다.

이처럼 NATO 사이버방위센터 회원 가입과 한미 간 사이버 공조 강화는 사실상 한국이 사이버공간에서 미국 및 서방과 공조하는 입장을 선택한 것으로 보인다. 한국은 사이버공간에서의 진영화 참여를 통해 북한

의 사이버공격에 적극적으로 대응해 나갈 필요가 있다. 이를 위해 북한의 사이버공격이 밝혀진 경우 진영 내 국가들과 공동성명을 적극적으로 발표하여 북한이 사이버공격에 나서지 않도록 유도하여야 한다. 또한 한국은 북한의 사이버공격으로 추정되는 사건들에 대해 디지털포렌식과 기술적 분석 기술을 통해 책임귀속할 수 있는 증거를 수집하여 공유해야 한다. 그뿐만 아니라 한국은 국제사회에 대해 북한의 사이버공격 유형과 특징에 대한 기술적 분석을 제공하고 북한 사이버공격 관련 정보를 공유하여야 하며, 북한 사이버공격에 대한 위기경보체계를 국제사회와 공동으로 가동할 필요가 있다.

다른 한편으로 우리는 진영화 참여로 발생할 수 있는 불이익을 최소화하기 위해 우리 안보와 국민의 안전을 수호하기 위해 국제 사이버위협에 대응하고 있다는 점을 어필할 필요가 있다. 즉, 진영 외부에 대해서는 전 세계 인류 공통의 문제인 사이버공격을 해결하고 사이버공간의 안전성 확보를 위해 진영화에 참여하였음을 강조하고, 진영 내부에서는 우리의 강점인 기술적 지원을 실행하고 경험과 정보의 공유를 통해 글로벌 중추국가로서의 역할을 수행해야 할 것이다. 구체적으로 중견국들의 공통 이해관계를 기반으로 한 중견국 협의체 구성을 제안하고 우리의 사이버안보 경험을 공유한다면 실질적인 결과를 달성할 수 있을 것으로 보인다.

중견국들은 사이버공간의 패권 다툼보다는 안전한 사이버공간의 유지와 이용을 주된 관심사로 하고 있다. 미국과 중국의 대립으로 사이버공간에서의 국제규범 창출이나 지속적 협력체계 구축은 지난한 일이 되어가고 있다. 그렇지만 미국과 중국 이외의 한국, 호주, 인도, 캐나다, 영

국, 프랑스, 독일 등은 사이버공격으로 인한 피해의 방지와 공동 대응에 관한 이해관계를 공유하고 있다. 비록 미국과 중국이 참여하지 않기 때문에 현실 국제질서에서 큰 힘을 발휘할 수 없는 한계가 있을 수 있지만, 중견국 협의체에서 사이버안보와 관련된 각종 통계 지수를 발표하고, 전문가 회의를 개최하며 인력 양성과 공동 교육 등을 실행한다면 중견국들의 적극적인 참여를 유도할 수 있을 것으로 보인다. 또한 중견국협의체를 기반으로 사이버공격 대응 매뉴얼이나 가이드라인의 작성, 사이버공격 및 방어 관련 정보공유 체계의 설립 등도 시도해볼 수 있을 것이다.

다. 북한의 사이버공격 관련 정보공유

우리 정부는 김정은 시대 북한의 사이버공격의 유형과 특징, 분석을 담은 백서를 정기적으로 발간하고 해외 주요 국가들과 공유할 필요가 있다. 북한 사이버위협 백서에 특히 최근 가장 주목받고 있는 북한의 암호화폐 공격 기법과 이에 대비하기 위한 기술적 조치는 물론, 범죄 추적과 몰수 관련 정보가 포함된다면 북한의 사이버공격으로 인해 피해를 입은 경험이 있거나 잠재적 피해 대상인 국가들에 큰 도움이 될 것으로 보인다. 가령 2014년 11월 소니픽처스 해킹으로 심각한 피해를 경험한 미국은 물론 2017년 5월 워너크라이 2.0 랜섬웨어 공격으로 의료체계의 심각한 마비를 경험한 영국과 EU 국가들의 관심을 끌 수 있을 것이다. 장기적으로 북한 사이버위협 백서는 이들과 북한 사이버위협에 따른 공동대응 방안을 수립하는 데 중요한 참고자료가 될 것이다.

그뿐만 아니라 한국은 미국의 CISA, NSA, 영국의 국가사이버안보센터(National Cyber Security Centre: NCSC) 등과 더불어 북한의 사이버위협 정보와 기술적 대응 방법을 공유하고, 북한의 사이버공격을 규탄하는 공동성명의 발표도 고려할 필요가 있다. 또한 북한의 사이버공격이 초국가적으로 진행되는 만큼 위기 감지 시 각국이 수집한 정보를 바탕으로 공동 사이버 경보를 발령할 수도 있을 것이다.

2. 국내적 역량 강화

가. 북한의 사이버공격에 대한 회복력 강화

북한은 핵무력 고도화를 위한 신기술 탈취, 민생경제 지원, 남북대화 탐색 등을 위해 남한에 대한 전방위적 사이버공격을 감행하고 있으며 우리의 대응에도 일부 한계가 노정되고 있는 상황이다. 사이버공격에 대해 북한의 소행이라는 명백하고 확실한 직접적인 증거(clear and convincing evidence)의 제시가 어려운 데다 가해 당사자로 의심되는 북한이 이를 부인하면서 사이버공격의 책임을 부담하기 곤란한 현실적 어려움이 존재한다.

바이든 정부는 사이버공격에 대하여 사이버적 수단과 비사이버적 수단을 사용하여 실질적인 비용을 부과함으로써 사이버공격에 신속하게 비례하여 대응할 것이라고 선언한 바 있다. 이를 바탕으로 볼 때, 트럼프 정부가 '선제 방어(defend forward)'라는 예방적 선제 사이버공격을 주장했던 것처럼 바이든 정부 또한 강력한 비사이버적 수단을 적극 활용함

으로써 사이버위협에 대응하려 할 것으로 보인다.[89] 디지털 정밀 전쟁 시대에 사이버공격은 무력 행사의 하나로 전쟁의 명분(casus belli)을 제공하여 자위권 행사를 가능하게 하므로,[90] 물리적 공격이 가능하다는 이론적 기반하에 공세적 사이버안보 정책을 추진할 가능성도 완전히 배제하기는 어렵다.[91]

그러나 만약 미국이나 국제사회가 북한의 사이버공격에 대해 물리적 타격까지 고려하게 된다면 한국 정부는 이를 자제시키고 기술적 지원을 통한 갈등 관리에 주력하는 것이 바람직할 것으로 보인다. 무엇보다 우리는 사이버위협에 무력으로 대응하는 방법을 택하기보다 사이버위협을 사전 탐지하고 모니터링하여 예방하여 취약성을 감소시키는 현실적 대응방안을 채택하는 것이 바람직하다. 사이버공격에 대한 모니터링과 조기경보체계, 취약성 평가, 신속한 위기대응체계 가동 및 복구 등을 통해 위협, 취약성 및 결과 발생을 감소시킴으로써 사이버공격에 효과적으로 대응할 필요가 있다. 아시아유럽정상회의(ASEM), 아세안안보포럼(ARF), G20 등을 통해 북한의 사이버공격이 관리되도록 회원국들과 협력하고 이들에 대한 기술적 지원을 확대하는 것이 하나의 구체적 방안이 될 수 있을 것이다.

89 The White House, *Interim National Security Strategic Guidance*, March 2021. p.18.

90 Yevgeny Vindman, "Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is," LAWFARE, January 26, 2021. https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it (accessed: October 19, 2022).

91 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: October 19, 2022).

또한 경제제재, 비난성명 발표 참여 등을 통해 북한의 사이버공격에 대한 억지가 일정 부분 발휘되도록 하여야 한다. 특히 미국과 서방이 물리적 수단을 사용하는 경우 명백성, 인도성, 비례성 및 필요성 등 국제법 원칙을 준수하여야 함을 강조하고 사용 자제를 유도하여야 한다. 아울러 북한의 금융기관과 암호화폐거래소 등에 대한 해킹 공격은 더욱 거세질 것으로 보이는바, 이를 지속적으로 모니터링하고 피해를 차단하기 위한 기술적 지원을 강화할 필요가 있다.

올바른 대응방안 마련을 위해서는 위협평가 역시 객관적이고 주기적으로 실행되어야 한다. 미국의 경우, 국가정보국장은 매년 의회에 국가안보에 관한 연례보고서(Annual Threat Assessment)를 보고하고 있다.[92] 2006년부터 시작된 위 위협평가는 최소한 1개의 공개 혹은 비기밀 세션을 포함하여야 하고, 해당 연도에 미국 정보공동체가 평가한 비기밀의 고도 위협에 관련 문서를 공개하여야 한다. 국가정보국(DNI)은 2021년 4월 13일 '2021년도 국가안보 위협 연례보고서'를, 2022년 3월 8일 '2022년도 국가안보 위협 연례보고서'를 각각 의회에 제출하였다. 우리도 이와 유사하게 국가정보원이 미국 국가정보실의 선례를 참고하여 국가안보 위협평가를 실행하고 국회에 보고하는 것을 고려해볼 수 있다. 이 경우 미국이 세계위협과 지역위협으로 대변하여 보고서를 작성한 것을 참조하되 우리 실정에 적합한 보고가 되도록 하여야 한다. 즉, 북한 위협, 대외위협, 신안보 위협 등으로 보고서를 구성할 필요가 있다. 특히

92 Robert S. Litt, Remarks, "U.S. Intelligence Community Surveillance One Year After President Obama's Address," 3 NAT'L SEC. L.J. 210 (2015), p. 218.

지구화와 세계화의 역기능으로 새롭게 등장하면서 전 지구적 피해를 야기하고 있는 신안보 위협의 경우 사이버, 감염병, 기후변화, 신기술, 에너지 등이 포함되도록 하여야 한다.

마지막으로 사이버위협 대응 관련, 정책과 법률 정비에도 노력을 기울여야 할 것이다. 문재인 정부의 『국가사이버안보전략』이 발표된 2019년 4월 이후 4차 산업혁명 기술의 고도화, 코로나19 발생 및 대응, 우크라이나 전쟁 등으로 사이버안보 환경이 급격하게 변화하였다. 북한의 사이버공격의 유형과 기술도 진화하였다. 또한 사이버안보 문제가 정상회담의 의제로 논의되는 등 국제협력을 통해 해결하여야 할 전 세계적 문제가 되었다. 신정부는 이와 같은 비대면 디지털 초연결 사회로의 전환이라는 시대적 변화와 안보 환경의 변화 등을 고려하여 『국가사이버안보전략』을 다시 정립하여야 할 것으로 보인다. 또한 이 전략이 구체적으로 실행될 수 있도록 「사이버안보기본법」 제정 등 관련 법제의 정비도 조속히 이루어져야 할 것으로 보인다.

나. 랜섬웨어 공격과 암호화폐 부정 이용에 대한 대응 강화

미국은 '주요기반시설 사이버 침해사고 보고법(CIRCIA of 2022)'을 통해 랜섬웨어 대가(몸값)을 지불한 경우 24시간 이내에 보고하도록 의무화하였다.[93] 우리 '정보통신기반보호법'은 주요 정보통신 기반시설의 관리기관장으로 하여금 침해사고가 발생하여 소관 주요 정보통신 기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관,

93 Cyber Incident Reporting For Critical Infrastructure Act of 2022.

수사기관 또는 인터넷진흥원 등에 그 사실을 통지하도록 규정하고 있다. 우리의 법제는 구체적인 시간을 명시하지 않고 있는바, 미국의 입법례를 참고하여 시간을 구체적으로 규정하는 것을 검토하여야 한다. 또한 우리 법제는 침해사고만을 통지의 대상으로 하고 있는바, 미국의 입법례를 참고하여 랜섬웨어 대가 지불에 대한 통지 의무화 도입을 고려하여야 한다. 특히 미국의 경우 주요 기반시설의 대부분을 민간이 운영하고 있다는 점에서 주요 정보통신 기반시설로 지정되지 않은 민간의 통지나 보고를 강제할 수 있는 입법적 개선을 모색할 필요가 있다. 아울러 민간의 보고를 강제하는 경우 보고한 민간기업 등에 대해, 미국 사이버보안정보공유법(Cybersecurity Information Sharing Act of 2015)을 참고하여, 소송으로부터 면책받을 수 있는 권리를 부여할 필요가 있다.

랜섬웨어 대금 지급에 대한 익명성을 차단할 수 있도록 암호화폐거래소 등에 대한 감독과 규제도 정비할 필요가 있다. 암호화폐거래소와 금융기관으로 하여금 암호화폐 거래에 대해 보고나 등록 조치 등을 시행하도록 검토하여야 한다. 또한 랜섬웨어 대가 지급에 따른 기업과 지방자치단체의 피해를 경감시키고 민관협력을 강화하기 위한 각종 조치를 실행할 필요가 있다. 금융기관으로 하여금 보다 현실에 적합한 사이버안보 보험을 개발하여 시장에서 채택될 수 있도록 독려하고, 기업과 지방자치단체에 대해서는 사이버안보 보험에 가입하도록 적극적으로 유도할 필요가 있다. 다만 사이버안보 보험 가입으로 기업들의 랜섬웨어 대응에 대한 경각심이 축소되지 않도록 유의하여야 한다. 미국의 사례와 우리의 간첩신고 보상제 등을 참고하여 랜섬웨어 신고자 또는 결정적 제보자 등에 대한 포상금을 지급하는 방안을 검토할 필요도 있다.

앞에서 살펴본 바와 같이 북한은 미국과 유엔의 대북제재가 강력하게 유지되고 있는 상황에서 부족한 외화를 조달하기 위해 랜섬웨어 공격을 확대 · 지속할 것으로 예상되므로 주의가 요망된다. 북한 해커 그룹인 라자루스는 2017년 워너크라이 랜섬웨어 사건에 관여하여 150여 개국에 악영향을 미치고 30만 대의 컴퓨터에 피해를 야기한 바 있다. 2020년 코로나19 대유행으로 랜섬웨어는 위장형 공격과 원격접속(RDP) 등을 통한 공격 등으로 변화 · 발전하고 있다. 북한 해커 그룹들은 더 많은 금전적 이득을 위하여 랜섬웨어 공격에 다양한 변화를 시도하고 공격 대상이나 범위도 확대할 것으로 전망된다. 따라서 북한의 랜섬웨어 공격에 대해 지속적으로 탐지하고 모니터링할 필요가 있다.

V

결론

2022년 9월 28일, 미국 하버드 대학교 벨퍼센터(Belfer Center)는 각 국가별로 사이버능력을 측정하여 '국가 사이버 역량 지표 2022(National Cyber Power Index 2022)'를 발표하였다. 해당 지표에 따르면 북한은 암호화폐 해킹 등의 사이버공격 역량에 힘입어 사이버 금융 분야에서 1위를 기록하여 종합 14위를 차지하였다. 북한을 전반적으로 사이버 강국으로 평가할 수는 없지만 사이버공격 능력만큼은 매우 위협적이라고 볼 수 있는 것이다.

이 같은 북한의 위협적인 사이버공격 활동은 고도로 정치화된 북한 사회의 특성상 국가 주도로 이루어지고 있다. 김정은 시대 북한은 사이버 능력을 만능의 보검으로 정의하고 새로운 비대칭 전력의 하나로 간주하면서 국가 차원에서 해커들을 양성하였다. 정찰총국 산하에는 6천여 명의 사이버 상근요원이 배치되어 있으며, 이들은 중국을 비롯하여 전 세계를 무대로 활동하고 있다. 북한 해커들의 사이버공격은 다방면에서 다목적으로 전개되고 있으나 최근에는 주로 외화확보를 위한 암호화폐 관련 공격, 랜섬웨어 공격, 국방산업 신기술 탈취, 대북 · 대외전략 탐색을 위한 전문가 · 탈북자 해킹, 코로나19 대응을 위한 원천기술 확보 등의 이유로 사이버공격을 감행하고 있다.

이 중에서도 특히 눈여겨보아야 할 북한의 사이버공격은 암호화폐 해킹이다. 암호화폐의 가격이 상승을 거듭하고 시장이 확장된 2010년대 중반 이후로 김정은 정권의 암호화폐 해킹 공격은 크게 증가하였다. 암호화폐 해킹의 경우 수익성이 높은 데 반해 특별한 비용을 필요로 하지 않고 공격 출처를 추적하기 어려워 책임추궁을 당하거나 보복당할 확률

이 낮다. 북한은 불법적 외화소득원을 찾는 과정에서 이 같은 암호화폐에 주목하고 매력을 느낀 것으로 보인다. 최근 암호화폐 가격은 폭락을 거듭하고 있으나 뚜렷한 외화수입 대체재를 찾을 수 없는 북한으로서는 암호화폐 해킹을 통한 외화확보에 매달릴 수밖에 없을 것으로 예상된다. 가격 하락에도 불구하고 암호화폐 시장은 계속 확장세에 있어 다시 가격 상승이 일어난다면 해킹을 통해 상당한 수준의 수입을 확보할 수 있기 때문이다.

따라서 북한은 앞으로도 경제제재를 우회하고 핵미사일 프로그램을 지탱하기 위한 재정 수입의 대안으로 암호화폐 해킹에 집중할 것으로 전망된다. 앞서 2019년 4월 북한은 대북제재의 돌파구로 암호화폐와 블록체인 등 첨단기술에 관심을 두고 '평양 블록체인 · 가상화폐 콘퍼런스'를 개최하여 논란을 야기한 바 있다. 그뿐만 아니라 북한은 경제제재와 미국 중심의 글로벌 금융 시스템에 대처하기 위해 자신들만의 암호화폐를 개발 중인 것으로 알려졌으며 중국과 협력할 가능성도 있는 것으로 확인되었다.[94] 북한의 암호화폐 해킹과 관련하여 우려스러운 점은 북한이 불법적으로 취득한 암호화폐를 통해 제재를 회피하여 중 · 러 등 전통적 우호협력국과 은밀히 무역거래를 시도할 수도 있다는 점이다. 이러한 우려가 현실이 된다면 대북제재의 틈새가 커지고 북한을 비핵화로 유도하기 위한 우리의 노력이 결실을 맺지 못할 가능성이 커진다.

94 David Gilbert, "North Korea Is Building Its Own Bitcoin," Vice, September 19, 2019, https://www.vice.com/en/article/9ke3ae/north-korea-is-building-its-own-bitcoin (accessed: September 8, 2022).

우리 정부는 북한에 의한 사이버위협과 관련하여 내적 역량 강화와 국제공조 강화라는 두 가지 방향으로 대응방안을 수립하여 실행하고 있다. 내부적으로는 국가사이버안보전략 수립과 사이버안보기본법 제정, 인터넷-인트라넷 분리정책, 사이버위협 정보공유 시스템 가동, 기업 보안 위반 시 제재 등을 실행하고 있다. 그러나 북한의 사이버위협에 대한 대응이 대부분 내부 역량 강화에 초점을 맞추고 있고 사이버보안 문제의 책임을 피해를 입은 기업에만 책임을 물리도록 되어 있어 북한에 대한 적극적 대응이 부족할뿐더러 정부가 사이버문제에 대한 심각성을 회피하려 한다는 지적도 많다. 사실 책임귀속이 어려운 사이버공격의 특성과 남북관계의 구조적 특수성으로 인해 한국 정부가 북한의 사이버위협에 독자적으로 대응하기 어려운 측면이 있었다.

따라서 사이버위협 관련 정보공유를 포함하여 국제공조를 강화해나간다면 북한으로부터의 사이버공격의 피해를 줄이는 데 도움이 될 수 있을 것으로 기대된다. 우리나라는 2022년 6월 비회원국임에도 NATO의 사이버방위센터의 정식 멤버가 되는 한편 2022년 5월 한미정상회담을 통해 사이버안보 전반에 걸쳐 미국과 공동 대응하기로 합의하면서 북한의 사이버위협에 대응할 수 있는 양자 및 다자협력의 틀을 마련하였다. 2022년 10월, 우리 군은 처음으로 미국 사이버사령부가 주관하는 다국적군 연합 사이버 방어훈련인 '사이버플래그(Cyber Flag)'에 최초로 참여하게 되었다. 이번 훈련 참여를 토대로 우리 군의 사이버전 역량을 강화하고 상호 간 파트너십 구축에 도움이 될 수 있을 것으로 보인다.

우리 정부는 사이버공간의 안전성 확보를 위해 다자 및 양자협력을 강

화해나가기로 하였음을 강조하고 우리의 장점인 기술적 지원을 실행하고 협력 국가들과 경험과 정보를 공유함으로써 위협을 줄여나갈 수 있도록 노력해야 할 것이다. 구체적으로는 북한 사이버위협 보고서 공동발행, 북한 배후의 해킹 사건에 대한 공동 수사, 공동 위기경보 발령, 추진하는 북한의 사이버 범죄자와 해커 집단에 대한 공개수배, 기소와 소추 등에 참여하거나 관련 정보공유와 수사 및 소추에 필요한 사항에 관한 협조 등의 방안으로 협력해나갈 수 있다. 또한 실전과 유사한 모의훈련을 공동으로 실시하여 참여하고 위기대응체계를 마련해 사이버위협에 능동적으로 대처하는 자세가 필요하다.

정보통신 기술을 기반으로 하는 사이버공간이 점차 확장됨에 따라 우리 사회는 한층 편리해졌다. 그러나 디지털 전환이 가속화되면서 사이버위협 요인 또한 진화하고 있다. 조직화된 국가배후의 사이버공격은 보다 치밀하고 강도를 더해가고 있으며 사회적 혼란을 야기하는 수준을 넘어 자유민주주의를 위협하는 수준에 이르고 있다. 우리 혼자만의 힘으로는 점차 심각해지는 사이버위협으로부터 안전을 담보할 수 없다. 북한의 공세적이고 조직화된 사이버공격에 대한 대응책으로 우리의 자체적인 역량 강화는 물론이거니와 동맹과 우방국들과의 협력을 통해 사이버안보 역량을 제고하고 공동 대응하는 방법을 적극적으로 강구해야 할 것이다.

Abstract

Characteristics of North Korean Cyberthreats and Countermeasures: Focusing on the Kim Jong Un Era

Bomi Kim

Il-Seok Oh

(Institute for National Security Strategy)

Along with the rapid development of North Korea's cyber capabilities during the Kim Jong Un era, the number of cases of illegal use of cyber capabilities at the regime level is increasing. Since Kim Jong Un took his power, North Korea has been widely using cyber capabilities as one of its asymmetric forces along with nuclear and missile programs. North Korea has been conducting cyberattacks on financial institutions, foreign governments, military and defense companies, and energy research institutes around the world for various purposes such as asset theft and leakage of military classified information. In particular, North Korea's profits obtained through malicious cyber activities serve as a cash supply chain for the Kim Jong Un regime, which desperately needs funds to support its nuclear and missile programs, which is an obstacle to international efforts for denuclearization. Accordingly, this research aims to identify North Korea's cyberthreat capabilities and characteristics in the Kim Jong Un era, and examines security countermeasures of the international community, while suggesting what policies we need to establish based on this. Specifically, in Chapter 2, the study introduces North Korea's cyber capabilities and major hacker groups in the Kim Jong Un era, analyzes the characteristics of North Korea's cyber attacks into five categories: cryptocurrency attacks, ransomware attacks, stealing of new technologies in the defense industries, collecting information on foreign policy related to North Korea, and securing COVID-19 vaccine technology. Chapter 3 sheds light on the international community's countermeasures against North

Korea's cyber threats in terms of economic sanctions, ransomware countermeasures, and cryptocurrency attack countermeasures. Chapter 4 presents our rational countermeasures considering the malicious cyber activities of the Kim Jong Un regime and the international community's countermeasures, but discusses the need for more aggressive countermeasures. Finally, the future prospects of North Korea's cyber threats are predicted in the conclusion.

Keywords

North Korea, Kim Jong Un era, cyber attack, cryptocurrency, ransomware

참고문헌

1. 국내문헌

「국가정보원법」 제4조 제1항 제1호 마목.

「국가정보원법」 제4조 제1항 제4호.

『국방백서 2018』. 서울: 국방부, 2018.

강영진. "미 정부 북한 해커 랜섬웨어 공격 주의보 발령." 『뉴시스』. 2022년 7월 7일. https://mobile.newsis.com/view.html?ar_id=NISX20220707_0001934071 (검색일: 2022년 9월 28일).

고준혁. "미 재무부 게임 '액시 인피니티' 암호화폐 도난, 북한 연루." 『이데일리』. 2022년 4월 15일. https://www.edaily.co.kr/news/read?newsId=01823686632296448&mediaCodeNo=257&OutLnkChk=Y (검색일: 2022년 9월 26일).

권성근. "미 북 핵프로그램 자금 확보 위한 암호화폐 도적 빈도 높아져." 『뉴시스』. 2022년 8월 10일. https://www.newsis.com/view/?id=NISX20220810_0001973454 (검색일: 2022년 9월 26일.).

기획취재팀. "토론회 개최한 태영호 의원실 사칭 북한 해킹 메일 공격 포착됐다." 『보안뉴스』. 2022년 5월 20일. https://www.boannews.com/media/view.asp?idx=106924&kind= (검색일: 2022년 8월 13일).

김귀근. "김정일 "정보전부대는 나의 배짱이고 예비대"." 연합뉴스. 2011년 6월 28일. https://www.yna.co.kr/view/AKR20110628128400043 (검색일: 2022년 8월 13일).

김문경. "과거와 다른 핵-경제 병진...한미에 공 넘긴 북." YTN. 2021년 1월 14일. https://www.ytn.co.kr/_ln/0101_202101140025017924 (검색일: 2022년 8월 13일).

김민관. ""평양 암호화폐 국제콘퍼런스" 개최 가능성 점검." Weekly KDB Report. 2020년 2월 10일. pp. 8-10.

김상욱. "북한 사이버공격으로 핵개발 자금 마련, 연간 약 10억 달러." 『뉴스타운』. 2017년 10월 21일. https://www.newstown.co.kr/news/articleView.html?idxno=301943 (검색일: 2022년 8월 13일).

김성진. "북한, 소니 영화사 해킹 배후설은 조작." KBS. 2014년 12월 5일. https://news.kbs.co.kr/news/view.do?ncd=2978823 (검색일: 2022년 8월 13일).

김일기 · 김호홍. 『김정은 시대 국가안보 기구』, INSS 연구보고서 2020-6 (2020).

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: 2022년 8월 13일).

김지영. "'코로나 0명'이라더니...북한은 왜 '화이자 해킹' 시도했나." 『머니투데이』. 2021년 2월 18일, https://news.mt.co.kr/mtview.php?no=2021021715345891578 (검색일: 2022년 8월 13일).

김지원. IAEA "북한, "핵 프로그램에 전력 증. 매우 유감"…북핵 감시 강화." 『경향신문』. 2021년 9월 20일. https://m.khan.co.kr/world/world-general/article/202109201957001#c2b (검색일: 2022년 8월 13일).

김진광. "북한의 사이버 공격 위협 분석 연구: 공격 기술의 유형 중심으로." 한국컴퓨터정보학회 학술발표논문집 (2020년 7월). pp. 107-110.

"라자루스 강도사건: 북한은 어떻게 최정예 해커부대를 만들어 냈나." BBC. 2021년 7월 8일. https://www.bbc.com/korean/international-57674041?xtor=AL-73-%5Bpartner%5D-%5Bnaver%5D-%5Bheadline%5D-%5Bkorean%5D-%5Bbizdev%5D-%5Bisapi%5D (검색일: 2022년 8월 13일).

문동희. "정찰총국 인사조치에 대남 사이버공격 강화 우려…어떤 부서길래." 『데일리

NK』. 2020년 9월 23일.

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: 2022년 8월 13일).

박대로. “북한 해커들, 가상자산 해킹 2조원 빼돌려.”『뉴시스』. 2021년 12월 26일. http://www.newsis.com/view/?id=NISX20211207_0001679470&clD=10301&plD=10300 (검색일: 2022년 8월 13일).

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: 2022년 8월 13일).

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: 2022년 8월 13일).

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: 2022년 8월 13일).

박형주. “북한 가상화폐 세탁에 이용되는 ‘렌 브릿지’ 제재해야…‘환전 네트워크’ 압박 필요.” VOA. 2022년 8월 12일. https://www.voakorea.com/a/6698148.html (검색일: 2022년 8월 14일).

박희준. “북한 해커, 라인메탈 등 독일 방산업체 사이버공격.”『글로벌이코노믹』. 2020년 12월 20일. https://news.g-enews.com/ko-kr/news/article/news_all/20201220161609132348c5557f8da8_1/article.html?md=20201220161514_U (검색일: 2022.9.26.).

배영경. “통일부 대상 사이버공격 2018년부터 급증…‘피해는 없어’.” 연합뉴스. 2021년 7월 7일. https://www.yna.co.kr/view/AKR20210707168701050 4, (검색일: 2022년 10월 27일).

신진우 · 최지선. “미, ‘북 사이버공격’ 맞대응 나섰다…전담 모니터링 요원 배치.”『동아일보』. 2021년 7월 16일. https://www.donga.com/news/Politics/article/all/20210716/107979812/1 (검색일: 2022년 8월 13일)

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: 2022년 8월 13일)

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: 2022년 8월 13일).

양철호 · 김윤영. “북한 사이버테러 조직의 역량 평가 고찰.”『한국민간경비학회보』. 제20권 5호 (2021), pp. 141-168.

오다인. “EU, 첫 사이버 제재 이행… 북한 조선 엑스포 등 개인 6 · 기관 3곳.”『전자신문』. 2020년 7월 31일. https://m.etnews.com/20200731000135 (검색일: 2022년 8월 13일).

유동열. “북한의 사이버 위협 실태와 대응.”『전략연구』. 제28권 3호 (2021), pp. 7-36.

이수헌. “北 선전매체, ‘해킹 공격’ 의혹에 ‘황당무계한 모략소동’(종합).”『SPN 서울평양뉴스』. 2021년 7월 21일. www.spnews.co.kr/news/articleView.html?indxno-41026 (검색일: 2022년 10월 27일).

이영종 · 윤호진. “김정은 “사이버전은 만능의 보검” 3대 전쟁수단 운용.”『중앙일보』 2013년 11월 5일. https://www.joongang.co.kr/article/13048072#home (검색일: 2022년 8월 13일).

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: 2022년 8월 13일).

임재섭. “암호화폐 해킹 시도, 북이 가장 많아…아일랜드 암화화폐 분석업체 설명.”『디지털타임스』. 2022년 6월 30일. https://http://www.dt.co.kr/contents.html?article_no=2022063002109958050002 (검색: 2022년 9월 8일).

임현우. “北, 작년 암호화폐 4억 달러 해킹…이더리움이 58%.”『한국경제』. 2022년 1월 16일. https://www.hankyung.com/economy/article/2022011617971 (검색일: 2022년 10월 19일.).

장영은. “바이든의 경고 먹혔나…러시아 랜섬웨어그룹 돌연 사라져.”『이데일리』. 2021년 7월 14일. https://www.edaily.co.kr/news/read?newsId=0348008

6629114520&mediaCodeNo=257 (검색일: 2022년 10월 1일).

정영교. “유엔, 北, 작년 사이버공격서 번 돈으로 미사일 기술 증강.” 『중앙일보』. 2022년 2월 6일. https://www.joongang.co.kr/article/25045877 (검색일: 2022년 10월 1일).

조상진. “북한 해킹조직, 외화탈취 위한 신종 랜섬웨어 4종 유포…금융 해킹 집중.” 『VOA』. 2022년 5월 5일. https://www.voakorea.com/a/6557282.html (검색일: 2022년 8월 13일).

조원일. “‘한수원 해킹’ 결정적 단서는 없지만… “北 소행”.” 『한국일보』. 2015년 3월 17일. https://www.hankookilbo.com/News/Read/201503171885878015 (검색일: 2022년 8월 13일).

조현의. “UN “북 해커조직 김수키, IAEA · KAI 해킹”.” 『아시아경제』. 2022년 2월 8일. https://view.asiae.co.kr/article/2022020810211910643 (검색일: 2022년 8월 13일).

지정은. “북 해킹조직 연루 새 ‘변종 랜섬웨어’ 4종 발견.” 『자유아시아방송』. 2022년 5월 4일. https://www.rfa.org/korean/in_focus/food_international_org/cyberattack-05042022090614.html, (검색일: 2022년 9월 28일).

최선영. “‘영국, 북한 · 러시아 등의 사이버공격에 제재할 것.” 『연합뉴스』. 2019년 5월 24일. https://www.yna.co.kr/view/AKR20190524034600504 (검색일: 2022년 8월 13일).

하윤해. “미, 6800억원 탈취한 북 해킹그룹 3곳 제재, 정찰총국이 배후.” 『국민일보』. 2019년 9월 15일. http://news.kmib.co.kr/article/view.asp?arcid=0013711916&code=61131111&cp=nv (검색일: 2022년 8월 13일).

함지하. “국무부 “대북 정책 재검토, 사이버 활동 등 위협 고려…미국 위협 줄이는 데 초점”.” VOA. 2021년 2월 18일, https://www.voakorea.com/a/korea_korea-politics_state-briefing-about-north-korean-cyber-attacks/6056276.html (검색일: 2022년 10월 19일).

홍제성. “북한, 전세계서 암호화폐 해킹 가장 많아…가치로 16억 달러.” 연합뉴스. 2022년 6월 30일. https://n.news.naver.com/mnews/article/001/0013279239?sid=102 (검색일: 2022년 9월 26일).

2. 북한문헌

『우리민족끼리』.

『조선중앙통신』.

3. 영어문헌

Council of the EU. “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/ (accessed: October 19, 2022).

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

Cybersecurity 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 (accessed: August 13, 2022).

Cybersecurity 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 (accessed: August 13, 2022).

Cybersecurity and Infrastructure Security Agency. “North Korea Cyber Threat Overview and Advisories.” https://www.us-cert.gov/northkorea (accessed: August 13, 2022).

Department of Justice. “Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and Their Conspirators.” https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors (accessed: September 1, 2022).

Department of Homeland Security. National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2013.

Department of Justice. "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators." https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors (accessed: September 1, 2022).

Department of Justice. "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe." February 17, 2021. https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and (accessed: August 13, 2022).

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/ (accessed: October 4, 2021). => 삭제.

Federal Register. "Information Security Controls: Cybersecurity Items." October 21, 2021. https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items (accessed: September 30, 2022).

Europol. "Cryptocurrencies: Tracing the Evolution of Criminal Finances." January 27, 2022. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (accessed: October 19, 2022).

Gilbert, David. "North Korea Is Building Its Own Bitcoin." Vice. September 19, 2019. https://www.vice.com/en/article/9ke3ae/north-korea-is-building-its-own-bitcoin (accessed: September 8, 2022).

Government of UK. "G7 Interior and Security Senior Officials' Meeting on Ransomware." December 24, 2021. https://www.gov.uk/government/publications/g7-interior-and-security-senior-officials-meeting-on-ransomware (accessed: October 29, 2022).

Heintz, Jim and Frank Bajak. "Ukraine Police Seize Cash in Raid on Major Ransomware Gang." AP. June 17, 2021. https://apnews.com/article/europe-ukraine-technology-hacking-a56fc6b3d1cd79ffd987e721bf558985 (accessed: October 19, 2022).

HM Government. *National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK.* December 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf (accessed: October 28, 2022).

Lewis, James Andrew. "Toward a More Coercive Cyber Strategy." CSIS Report. March 10, 2021. https://www.csis.org/analysis/toward-more-coercive-cyber-strategy (accessed: October 19, 2022).

Litt, Robert S. "U.S. Intelligence Community Surveillance One Year After President Obama's Address." 3 NAT'L SEC. L.J. 210 (2015), p. 218.

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.

Marks, Joseph. "The Cybersecurity 202: The Biden administration is stepping up the fight against ransomware." The Washington Post. July 15, 2021. https://www.washingtonpost.com/politics/2021/07/15/cybersecurity-202-biden-administration-is-stepping-up-fight-against-ransomware/ (accessed: October 19, 2022).

Neuberger, Anne. "Update on the International Counter-Ransomware Initiative." U.S. Department of State. October 15, 2021. https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative (accessed: August 13, 2022).

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/ (accessed: April 29, 2022).

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 (accessed: April 29, 2022).

Sanger, David E and Julian E. Barnes. "Biden Makes a New Push in Fight against Ransomware, Including a $10 Million Reward." The New York Times. July 15, 2021. https://www.nytimes.com/2021/07/15/us/biden-reward-ransomware.html (accessed: October 19, 2022).

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 (accessed: August 13, 2022).

Sang-Hun, Choe and David Yaffe-Bellany. "How North Korea Used Crypto to Hack Its Way Through the Pandemic." The New York Times. July 1, 2022. https://https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html (accessed: September 8, 2022).

Sigalos, MacKenzie. "Crypto Scammers Took a Record $14 Billion in 2021." NBC News. January 7, 2022. https: https://www.nbcnews.com/tech/security/crypto-scammers-took-record-14-billion-2021-rcna11192 (accessed: September 7, 2022).

Smith, Josh. "Crypto Crash Threatens North Korea's Stolen Funds as It Ramps Up Weapons Tests." Reuters. June 29, 2022. https://https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/ (accessed: September 26, 2022).

Stasha, Smiljanic. "Cryptocurrency Hacking Statistics." February 13, 2022. http://policyadvice.net/money/insights/cryptocurrency-hacking-statistics/ (accessed: September 7, 2022).

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. (accessed: August, 13, 2022).

The White House. "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." April 15, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (accessed: September 30, 2022).

U.S. Army Headquarters. "North Korean Tactics." July 2020. https://irp.fas.org/doddir/army/atp7-100-2.pdf (accessed: April 29, 2022).

U.S. Department of The Treasury, "Ransomware Advisory." October 1, 2020. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001 (accessed: August 13, 2022).

Vindman, Yevgeny. "Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is." LAWFARE. January 26, 2021. https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it (accessed: October 19, 2022).

Volz, Dustin. "U.S. Recovers Over $30 Million in Cryptocurrency Stolen by North Korean Hackers." The Wall Street Journal. September 8, 2022. https://www.wsj.com/articles/u-s-recovers-over-30-million-in-cryptocurrency-stolen-by-north-korean-hackers-11662648600 (accessed: September 1, 2022).

INSS 연구보고서 2022-03

북한 사이버위협의 특징과 대응방안:
김정은 시대를 중심으로

발행처 사단법인 국가안보전략연구원
발행인 한석희
주소 06295 서울시 강남구 언주로 120 인스토피아 빌딩
전화 02-6191-1000 (Fax. 02-6191-1111)
홈페이지 http://www.inss.re.kr
인쇄일 2023년 2월
발행일 2023년 2월
편집 한국학술정보(주)
ISBN 979-11-89781-82-8
979-11-89781-79-8 (세트)
가격 비매품