Jeju Peace Institute 제주평화연구원

JPI PeaceNet

사이버공간의 혼돈 속 한반도 사이버평화를 위한 과제

나 용 우
통일연구원

[기획자 註] 사이버공간은 근대 국가의 경계, 영토를 넘어서는 국제정치 질서의 새로운 영역이다. 국제질서는 근대 주권 국가의 영역을 초월해 이뤄지는 것이다. 문제는 국제사회에서 사이버 공간의 확대에 따른 부정적 영향이다. 인류는 기술 탈취, 해킹 등 새로운 사이버 안보 위협에 직면했다. 이제 국제정치에서 평화는 현실 공간뿐만 아니라 사이버 공간에서도 요구된다. 특히 남북 남계에서도 북한의 남한에 조직적 해킹이 크게 우려할 만한 수준이다. 남북한 간 사이버 안보 문제를 분석하고, 사이버 공간에서의 한반도 평화의 길을 모색하고자 한다. [기획: 이재준 연구위원(junlee@jpi.or.kr)]

1. 사이버공간의 변화 양상

인류는 정보통신기술(ICT)의 발전에 따라 사이버공간을 새롭게 탄생시켰다. 이 새로운 공간은 전통적인 국가의 통제에서 벗어나 개인(행위자)들의 자유로운 정보 교환을 위해 시작되었지만, 점차 현실 세계와 밀접하게 결합되면서 기존 국가 및 지역간 지리적 혹은 공간적 분리됨을 상쇄시켜 전 세계를 서로 연결하고 있다. 이제 가상공간과 현실세계가 융합된 소위 메타버스(Metaverse) 시대로까지 확장되고 있다. 이러한 기술의 발전 속에서 인간의 삶은 더욱 편리하고 풍요로워지고 있지만, 그와 함께 새로운 위협들로부터 개인 및 공동체의 안전이 위태로워지는 상황도 더욱 증가하고 있다. 10월 15일 데이터센터 화재로 인해 발생되었던 카카오서비스 접속 장애 사태는 이를 단적으로 보여준 사례였다. 우발적 사건으로 발생한 일이 국가, 사회공동체에 이처럼 큰 피해를 줄 수 있다면, 특정한 정치적 의도를 갖고 사이버공격을 할 경우 더욱 심각한 위협이 될 수 있다.

사이버공격은 디도스(DDos) 공격이나 악성 프로그램 유포, 첨단기술 및 정보 절취 등 기술적 유형 외 랜섬웨어나 암호화폐 해킹 등 금전 탈취를 목적으로 하는 유형도 증가하고 있다. 러시아의 우크라이나 침공 이후에 빈번하게 발생하고 있는 디지털 미디어를 이용한 가짜뉴스의 생성이나 허위정보 유포 등 사이버 선전선동도 새롭게 중요한 위협으로 등장하고 있다. 사람들의 일상적 생활에 활용되고 있는 로봇이나 드론 등 새로운 첨단 디바이스에 대한 사이버 위협까지 그 범위가 더욱 확대되고 있다.

개인을 대상으로 정보 및 금전 탈취를 목적으로 했던 초기의 사이버위협은 이제 개별 해커

혹은 해커조직, 국제 테러조직에 의한 주요 국가 기반시설 및 인프라에 대한 공격으로 확대되고 있다. 그런데 더욱 심각한 문제는 사이버공격의 주체로 국가가 전면에 나서고 있다는 점이다. 즉 사이버공격을 행하는 비국가행위자의 배후였던 국가들이 직접 공격이나 위협행위를 감행함으로써 권력정치(power politics)가 사이버공간에서 더욱 갈등을 심화시키고 있다는 것이다.

이렇듯 사이버위협이 그 빈도와 강도가 심화되며 증가하는 것은 사이버공간이 갖는 근본적인 특성에서 기인하는 것이다.[1] 첫째, 사이버공간은 지리적 특성, 물리적 공간(territory)을 초월함으로써 무정부적 공간성을 띠게 된다. 국가 관할권 혹은 주권이 미치는 영역이어야 하는지에 대해 상이한 입장을 갖기 때문에, 사이버공간에서의 합의된 국제규범을 만들어내기 어렵게 된다. 둘째, 공간 내 행위자가 자신의 신분을 감출 수 있는 익명성이 보장됨에 따라 은밀하게 활동할 수 있다. 기존 테러 행위와 달리 사이버위협을 가한 행위자들의 귀속을 특정짓기 어렵기 때문에, 목적 달성을 위해 은밀한 공격을 감행할 유인이 충분하다. 마지막으로 물리적 공간에서의 역량을 사이버공간에서 효율적으로 역전시킬 수 있는 가능성이 열려 있다. 얼마나 큰 경제력, 군사력을 갖고 있는지가 국가의 역량을 결정하는 전통적인 공간과 달리 사이버공간에서는 고도의 네트워크로 연결된 사회, 공동체가 소규모의 시스템 오류나 저강도의 사이버공격에 의해 오히려 엄청난 피해를 겪게 되는 소위 '기술진보의 역설(a paradox of technological advance)' 을 산출할 수 있다. 결국 사이버공격은 재래식 국력의 불균형을 단번에 역전시킬 수 있는 효율적인 수단이 될 수 있다.

2. 북한의 사이버역량 실태와 사이버위협 수준

북한의 사이버능력은 더 이상 실행 가능성의 차원에서가 아니라 한국의 안보를 실질적으로 위협하고 있다. 북한은 사이버공간을 중요한 전략공간으로 인식하고 있으며, 이에 따라 자신의 사이버역량을 전통적인 군사전략에 결합해 활용하는 중요한 전력수단으로 이용하고 있다. 다시 말해서, 남북간 안보 갈등이 사이버공간으로까지 그대로 투사되고 있는 것이다. 군사, 경제, 사회문화 등 다양한 영역에서 남북관계의 변화에 따라 협력이 이루어지기도 했었지만, 사이버공간은 남북관계의 변화 속에서 협력의 공간으로 단 한 번도 다루어지지 않았다는 특징도 있다.

북한은 남북간 국력의 차이를 극복하는 전략으로 사이버공간을 적극 활용하고 있다. 이미 김정일은 "20세기 전쟁은 기름전쟁이고 알탄 전쟁이라 한다면, 21세기 전쟁은 정보전쟁"이라 언급했고, 김정은도 "핵미사일과 함께 우리 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"이라고 천명한 바 있다. 사이버전력을 핵, 미사일과 함께 인민군대의 3대 핵심수단으로 제시하며,[2] 소위 '사이버전사' 육성에 적극적으로 나서고 있다. 이렇듯 사

1) 나용우, "초연결융합시대와 사이버안보: 사이버공간의 안보화와 한국의 사이버안보 강화 방안," 『Journal of North Korea Studies』 제3집 2호(2017), pp. 32-33.

이버능력을 강화함으로써 미래 사이버전 대비, 첨단과학 및 군사기술의 탈취, 대남 공작 및 외화 획득 등의 다양한 전략적 목표를 달성하기 위한 효과적인 수단으로 활용하고 있다. 앞서 언급되었듯, 낮은 진입비용과 높은 효율성, 책임귀속의 어려움 및 억지수단의 제한 등 사이버공간의 특성을 활용해 북한은 사이버역량을 강화하고 있는 것이다.

북한의 사이버전력 체계에서 가장 중추적 역할을 하는 기관은 정찰총국 산하의 기술정찰국이다. 특히 기술정찰국 '110연구소'는 종래의 121국과 100연구소를 통합한 부서로 정찰총국의 사이버공작을 전담하는 부서로 알려지고 있다.[3] 사이버전력의 규모는 약 3,000~6,000명 수준으로 추정되고 있다. 세계적으로 악명을 떨치고 있는 라자루스(Lazarus)를 비롯해, 천리마, 블루노르프, 안다리엘, APT37/38, 김수키 등이 북한의 대표적 해킹조직들이며, 이들은 대부분 정찰총국의 지휘를 받아 활동하고 있다.

북한의 사이버 위협은 1) 사이버 해킹(정보 탈취), 2) 사이버심리전, 3) 사이버테러, 4) 사이버 간첩, 5) 금전 탈취 등 다양한 형태로 이루어지고 있다. 북한은 이들 조직들을 활용해 한국에 직접적인 공격을 단행한 바 있다. 2009년 7.7 DDos 공격을 시작으로 2011년 3월 청와대, 국정원 및 금융기관을 대상으로 DDos 공격, 2011년 4월 농협 전산망 해킹, 2012년 6월 중앙일보 해킹, 2013년 3월 방송사 및 금융기관 해킹, 2014년 12월 한국수력원자력 해킹, 2015년 국회, 청와대 등 해킹 시도, 2016년 12월 국방통합데이터센터(DIDC) 해킹, 2017년 암호화폐거래소 빗썸 해킹, 2019년 청와대 및 안보관계자 해킹, 2021년 대우조선해양 및 한국원자력연구원 해킹 등의 여러 차례 사이버공격을 감행해왔다.

북한의 사이버공격은 한국에 그치는 것이 아니라 글로벌 차원에서 이루어지고 있다. 특히 코로나19 이후 국경봉쇄와 대북제재의 장기화로 인해 해외로부터의 외화 확보에 차질이 생기면서 이를 대체하기 위한 수단으로 최근 사이버 금전 탈취에 집중하고 있는 것으로 보인다. 실제 UN 대북제재위원회 전문가패널 보고서에서는 북한이 2020년~2021년 중반까지 북아메리카, 유럽, 아시아 등 최소 3곳의 가상화폐거래소로부터 총 5천만 달러 이상 탈취했다고 적시했다.[4] 또한 지난 2월 블록체인 데이터 플랫폼 기업 체이널리시스의 "2022 가상자산 범죄 보고서" 에서도 북한과 연루된 해킹과 자금 탈취가 꾸준히 증가했고, 2017년~2021년 49차례 해킹을 통해 총 10억 달러 규모의 자산을 탈취했으며, 이 중 아직 세탁되지 않은 가상자산도 1억 7,000만 달러에 이를 것으로 추정하였다.[5]

이렇듯 북한은 한국과 국제사회를 상대로 사이버 정보 및 금전 탈취에 집중하고 있으나, 더욱 우려되는 것은 북한이 자신들의 공세적인 사이버 역량을 군사안보와 직접 결합할 경우

2) 임종인 외, "북한의 사이버전력 현황과 한국의 국가적 대응전략," 『국방정책연구』, 제29권 제4호(2013), p.15.

3) 유동열, "북한의 사이버 위협 실태와 대응," 『전략연구』, 통권 제84호(2021), p.13.

4) ""북, 작년에 가상화폐 4천800억원 훔쳐…중국에 석탄 불법 수출"(종합)," 『연합뉴스』, 2022/04/02.https://www.yna.co.kr/view/AKR20220401003951072?section=nk/news/all (검색일: 2022.5.16.).

5) 김소정, "북한의 가상자산 탈취 대응을 위한 한·미 협력 고려사항," 『이슈브리프』 제395호 (서울: 국가안보전략연구원, 2022), p.3; 김보미, "김정은 시대 북한 사이버 위협의 특징과 대응방안," <정보세계정치학회 추계학술대회 자료집>, p.279.

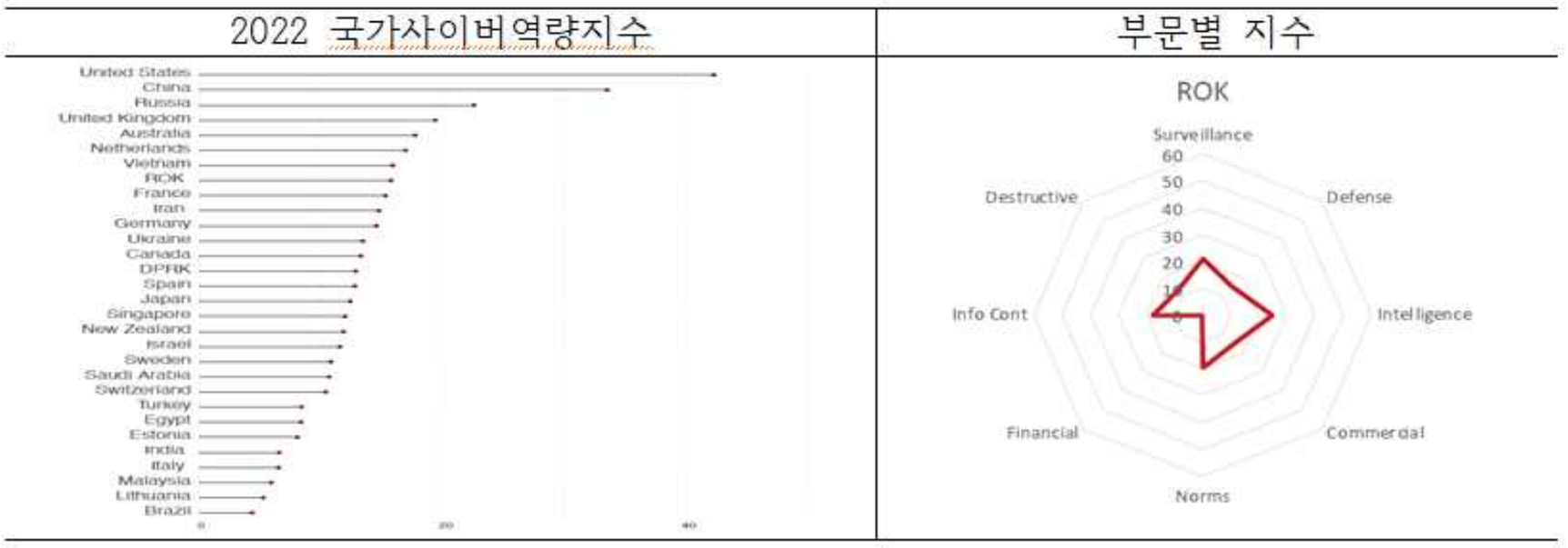
현재 위협보다 그 파괴력이 더욱 치명적일 수 있다는 점이다. 한국과 미국의 군사 작전계획이 전달되는 과정을 해킹을 통해 저지시키거나, 교란하는 방식으로 정보 및 지휘통제 시스템을 무력화시킬 뿐 아니라, 한미 양국의 시스템을 역이용해 아군에게 공격하도록 조정할 수도 있을 것이다.

3. 한국의 사이버역량 강화와 남북 사이버협력: 한반도 사이버평화를 위한 과제

이렇듯 북한의 사이버능력은 나날이 높아지고 있는 상황인데 반해, 한국의 사이버역량은 어떠한지 살펴 볼 필요가 있다. 2020년 기준 한국은 초고속 인터넷 광섬유 비중, 모바일 브로드밴드 이용량, 인터넷 다운로드 속도 등 인프라 측면에서 회원국 중 1위이며, 인터넷 이용자 비율은 95%로 OECD 7위 수준이며, ICT 관련 특허 비중은 53.9%로 OECD 회원국 중 1위 등 사이버 인프라 및 활용 부문에서 세계적인 수준이다.[6)]

2020년부터 하버드대 과학국제문제벨퍼센터가 발표하고 있는 국가사이버역량지표(NCPI)에 따르면, 한국의 종합적인 사이버역량은 30개 대상국들 중 세계 7위로 발표되었다. 8개 기준 중 사이버방어, 사이버공격, 금융 부문에서 주요 선진국들에 비해 상대적으로 낮은 수준을 보였다.

<그림> 2022 국가사이버역량지수와 한국 부문별 지수[7)]



한국의 사이버역량 중 인프라 및 활용 부문에서 세계적인 수준이지만, 사이버방어 역량이 부족하기 때문에 북한을 비롯한 세계적인 해킹그룹으로부터의 공격에는 매우 취약한 상황이다. 앞서 살펴보았듯, 북한으로부터 중요한 군사 및 기술정보는 물론 금전 탈취를 여러 차례 경험했다는 것은 이를 잘 보여주는 것이다. 따라서 한국의 사이버역량 강화를 위한 방안들을 우선적으로 강구해야 한다.

6) 주오이시디 대한민국대표부, "OECD 디지털경제전망(Digital Eonomy Outlook) 2020 주요내용," p. 1. https://overseas.mofa.go.kr/oecd-ko/brd/m_20806/view.do?seq=229 (검색일: 2022.11.14.).

7) Julia Voo, Irfan Hemani & Daniel Cassidy, National Cyber Power Index 2022 (Cambridge, MA: Belfer Center for Science and International Affairs, 2022), p. 10; p. 23.

지난 2019년 4월 「국가사이버안보전략」을 채택하고, 국가사이버안보 기본계획을 수립해 시행하고 있으나, 정작 사이버안보와 관련한 통합적 기본법은 아직까지 제정하지 못하고 있다. 미국, 일본, 러시아, 중국 등 주요 선진국들이 점증하는 사이버위협에 효과적으로 대응하기 위해 사이버안보 법제를 채택해왔음에도 불구하고, 북한이라는 실질적 사이버위협을 직면하고 있는 한국이 아직도 '사이버안보 기본법'을 채택하지 못한 상황은 상당히 우려스럽다. 물론 「국가정보원법」 개정[8]과 국가안보실 사이버안보비서관 신설로 정부 차원에서 사이버 위협에 적극적으로 대처하려는 움직임은 있으나, 효과적인 안보위협에 대응하기 위해서는 체계적이고 통합적인 '국가사이버안보기본법'을 제정하는 것이 필요하다.

또한 사이버위협에 대응하는 국제적 차원의 협력도 모색해야 한다. 윤석열 대통령은 금년 5월 바이든 대통령과의 한미정상회담에서 북한발 사이버위협에 대응하기 위한 협력 확대에 합의했고, 이런 차원에서 지난 10월 미국 사이버사령부가 주관한 사이버플래그(Cyber Flag) 훈련에 우리 군 사이버작전사령부을 중심으로 처음 참여했다. 이렇듯 북한과 글로벌 차원의 사이버위협에 대해 한미 사이버워킹그룹을 중심으로 협력하는 것이 효과적인 방안이다. 지난 5월 한국은 비나토회원국으로서 나토 사이버방위센터(CCDCOE)에 가입하여, 라키드쉴드 훈련(Exercise Locked Shields)에 참가하는 등 국제적 사이버안보협력을 강화하고 있다.

마지막으로 기술적 차원의 대응체계도 구축해야 할 것이다. 사이버위협에 대한 취약성을 감소시키기 위해 사이버위협에 대한 모니터링과 조기경보시스템, 취약성 평가 및 신속위기대응 체계 구축 등을 통해 북한발 사이버위협에 효과적으로 대응해야 한다.

전통적 안보구조가 사이버공간에 그대로 투영되는 현 상황에서 한반도 사이버평화를 구축하기 위해서는 무엇이 필요할 것인가? 북한이 사이버위협을 통해 얻는 이익을 최소화하거나 협력에서 얻는 이익을 확대하는 것이 가장 효과적일 것이다.

북한이 사이버역량 중 공격능력을 제외하고 인프라, 디지털경제, 거버넌스 측면에서 매우 취약한 상황이다. 인트라넷-인터넷 분리 정책을 통해 사이버공간에서의 안전을 유지하고 있으나, 대외개방이 본격화될 경우 북한 역시 향후 외부 세력으로부터 사이버공격에 노출될 수 밖에 없다. 따라서 사물인터넷(IoT) 등 첨단 정보통신기술의 노하우를 갖고 있는 한국과의 협력은 북한에게도 상당한 이익을 제공할 수 있다.

사이버공간에서도 남북간 상호 불신이 크고, 저비용-고효율로 인해 북한의 사이버공격 유인이 크다. 따라서 남북간 사이버평화를 위한 협력은 제도적 그리고 공유이익적 차원에서 구상해야 할 것이다. 우선 제도적 차원에서 사이버공간에서 상호 적대행위를 중지하는 협약(가칭 '남북 사이버평화협정')을 체결하는 것이다. 현재 남북관계 경색으로 9.19 군사합의가 사실상 사문화되고 있는지만, 그럼에도 군사분야 합의서 체결은 남북간 군사안보차원에서 화해협력의 물꼬를 열었다는 의미가 있다. 남북 사이버평화협정 체결로 상호간 사이버위

8) 「국가정보원법」 제4조 제1항 제1호 마목

협을 최소화하거나 억지할 수 있다. 이익의 차원에서는 남북간 사이버안보 기술의 공동연구 및 개발을 고려할 수 있다. 특히 김대중 정부 시기 남북은 정보통신협력을 추진했던 경험을 다시 되살려서 북한에게 협력을 통한 이익을 제시하는 것이 중요하다. 사이버 인재 양성을 포함한 기술 공동연구 및 개발을 남북이 함께 한다면, 사이버공간에서의 평화를 만들어나갈 수 있다. 이렇듯 한반도 사이버데탕트는 궁극적으로 남북관계의 정상화와 한반도의 지속가능한 평화에 기여할 것이다.

저자소개

나용우 박사는 성균관대학교 정치외교학과에서 학사, 석사, 박사학위를 취득했으며, 성균관대학교 좋은민주주의연구센터 선임연구원, 조지타운대학교 평화안보연구소 방문연구원으로 근무하였다. 현재 통일연구원 인도협력연구실 부연구위원으로 재직하고 있다. 주요 연구분야는 남북교류협력, 신흥안보, 동북아 국제관계 등이다.

2022년 12월