https://doi.org/10.33778/kcsa.2020.20.5.019

한국의 사이버공격 비교 분석과 정책적 대응방안★

권 혁 천*, 이 용 준*, 박 원 형**

요 약

본 연구의 목적은 북한의 사이버 공격과 우리의 대응에 대해 노무현 정부 부터 문재인 정부까지 정부별로 비교 분석하는 데 있다. 현재 한반도는 미국, 중국, 러시아 등 다양한 이해관계가 상충되면서 새로운 세계질서의 주도권 다툼이 사이버상에서 충돌로 이어지고 있다. 사이버 공격의 속도는 빨라지고 위협의 수위는 높아지고 있다. 사이버 위협은 몇 가지 특징을 보이고 있다. 무엇보다 위협의 주체를 확인하거나 추적하기 어렵다는 점이다. 또한 정보통신기술의 발달로 공격기술이 지능화되어 이에 대응하는 수단을 마련하기도 쉽지 않다. 따라서, 국가사이버안보를 위해 지속적이고 선제적인 대응 역량을 제고하고, 국가간 또는 민간 전문가간의 국제협력과 같은 여러 행위자간의 거버넌스 구축이 필요하다.

Comparative Analysis of Cyber Attacks of Korea Government and Policy Countermeasures

Hyeokchun Kwon*, Youngjun Lee*, Wonhyung Park**

ABSTRACT

The purpose of this paper is to ccompare and analyze North Korean cyber attacks and our responses by government, from the Roh Moo-hyun administration to the Moon Jae-in administration. The current conflict of interests on the Korean peninsula, such as the United States, China, and Russia, is leading to a conflict for the leadership of a new world order in cyberspace. Cyber attacks are accelerating and threats are rising. Cyber threats exhibit several characteristics. Above all, it is difficult to identify or track the subject of the threat. Also, with the development of information and communication technology, attack technology has become more intelligent, and it is not easy to prepare a means to respond. Therefore, it is necessary to improve continuous and preemptive response capacity for national cybersecurity, and to establish governance among various actors, such as international cooperation between countries or private experts.

Key words : Cyber Attack, Korea Government, National Cyber Security Policy, Policy Countermeasures

접수일(2020년 11월 15일), 수정일(2020년 12월 22일), 게재확정일(2020년 12월 31일)

★ 본 논문은 2020년 건국대 박사학위논문 “북한의 사이버 공격양상 비교연구 : 노무현, 이명박, 박근혜 정부를 중심으로”를 수정/보완한 것임

* 극동대학교 사이버보안학과 강사(주저자)

* 극동대학교 사이버보안학과 조교수(공동저자)

** 상명대학교 정보보안공학과 부교수(교신저자)

1. 서 론

우리 정부가 국가차원에서 정보화를 추진한 이후 공공기관과 기업에서 실무를 수행하기 위해서 그리고 국민은 실생활을 위해 정보통신망과 정보시스템에 대한 의존도가 심화되고 있다. 세계 최고의 정보화 수준이 역설적으로 사이버 공격의 빌미를 주고 있다. 북한 사이버 공격의 주요사례는 2009년 청와대 등 국가기관의 공격, 2011년 3.4 사이버 공격 및 농협 전산망의 마비사태, 2013년 금융・방송사의 사이버 공격, 2014년 한국수력원자력의 내부문서 유출 사건, 2016년에 국방부의 군사기밀 유출 공격, 2017년 암호화폐거래소의 공격 등 국가・공공기관뿐만 아니라 일반기업까지 사이버 공격은 위협수준이 높아지고 다양하게 지속적으로 발생하고 있다. 이런 사이버 공격은 한국의 정치, 경제, 사회, 문화 등 국가 전반에 영향을 주며, 총체적인 국가 안보에 위협이 될 수 있는 사이버 공격들이다.

한편, 최근 4차 산업혁명을 맞아서 인공지능(AI), 사물인터넷(IoT), 빅데이터, 블록체인 등 새로운 기술의 등장으로 디지털 혁명을 넘어 초융합사회, 초연결사회, 초지능사회로 진입하면서 국가와 공공 기관, 기업 등의 업무를 효율적으로 처리할 수 있게 되었다. 그리고 차세대 이동통신기술인 5G, 스마트 폰 등 정보통신기술의 발전으로 국민들의 실생활이 더욱 더 윤택해지고 편리해졌다. 이에 반해 사이버 공격도 초지능화, 초고도화 되면서 새로운 보안 위협이 등장하고 증가하여 국가기관과 기업 그리고 국민 실생활에 큰 피해와 불편을 주고 있다. 이에 따라 급변하는 사이버 환경에 체계적이고 효율적으로 대응하기 위해 국가사이버보안의 정책 개선방안 마련과 실천이 더 이상 피할 수 없게 되었다. 지금 이 시간에도 북한은 사이버 요원들이 북한과 중국, 러시아, 홍콩 등 해외에서 우리의 국가기관망, 방송통신망, 금융망, 교통망과 민간 상용망 등을 대상으로 전방위적으로 사이버 공격을 전개하고 있다. 실제 북한과 해외거점에서 한국을 대상으로 해킹 시도 건수는 하루 평균 150만건에 달한다. 북한은 사이버 공간의 특성과 우리 법의 허점을 최대한 활용하여 사이버 공격을 하고 있다. 즉 시공간을 떠나 사이버 공격과 심리전을 시도하여 사회 혼란, 국론분열 등 국가안보를 위협하고 금전탈취 등 국부유출로 인한 사이버안보 위협은 더욱 치명적이다.

따라서 사이버 위협으로부터 국민 실생활은 물론 국익과 국가안보를 위해 국가차원의 사이버보안전략을 수립하여 각 분야별 추진계획에 따라 불철주야 긴장을 유지하면서 이에 적극적 선제적으로 대응할 필요성이 있다. 따라서, 이 연구는 역대 정부별 북한 대남 사이버 공격과 대응에 대한 변천과정을 살펴보고 개선 방안을 도출하고자 한다[1][2][3].

2. 관련연구

국가 사이버안보는 국가기밀, 군사, 외교, 산업 등 국가안보 정보를 보호하는 것은 국가이익과 직결된 업무이다. 또한 국민의 안전한 생활에 직・간접적인 영향을 미치고 있기 때문에 사이버공격으로부터 국가 사이버안전을 지켜내기 위해 다양한 대응체계를 마련하고 있다. 아래 <표 1>은 국가 사이버 업무에 대한 기관별 주요 임무와 법적 근거이다[4][5].

<표 1> 기관별 주요임무와 법적 근거

기관명	관련법령 근거	주요임무
국가 정보원	・국가정보원법 ・정보통신기반보호법 ・전자정부법 ・국가사이버안전관리규정	・국가 정보보안 업무의 기획·조정 ・보안정책 수립·시행 ・국가·공공기관 사이버안보 업무 총괄
과학 기술 정보 통신부	・정보통신망 이용촉진 및 정보보호 등에 관한 법률 ・국가정보화 기본법 ・전자서명법 ・정보통신기반 보호법	・민간정보보호 정책의 수립·조정 ・주요정보통신기반시설 지정권고 총괄 ・민간분야 침해사고 예방・대응체계 구축 ・전자인증관련 정책수립・조정 ・정보보호산업 관련 주요 정책의 수립 ・민간정보보호 및 정보보호 산업업무 총괄
방송 통신 위원회	・정보통신망 이용촉진 및 정보보호 등에 관한 법률	・정보통신서비스 ・방송 관련 개인정보보호 정책
행정 안전부	・국가정보화기본법 ・전자정부법 ・개인정보보호법	・전자정부 사이버위협과 침해 선제적 예방 ・안전한 전자정부 구현 ・공공·민간 보유 개인정보 유출피해 방지 ・국민불안감 해소, 개인정보보호체계 강화
개인정 보보호 위원회	・개인정보보호법	・개인정보보호 총괄·조정 기능 강화 ・개인정보보호위원회의 개최 운영

국가 사이버안보는 국가비밀, 국방, 외교 등 국가안보 정보를 비롯하여 첨단기술 등의 산업기밀정보의 보호는 국익과 직결된 업무이다[6][7][8][9]. 한편, 북한은 선군정치 이념체계를 토대로 혁명역량 강화 등 국가목표를 달성하기 위해 ICT를 이용하여 사이버 공격 수행 능력을 강화하는 전략을 추진하고 있다. 이를 위해 사이버 공간을 적극적으로 활용하고 있다. 북한 사이버 공격에 영향을 미치는 사이버 환경 요인들을 사이버 대내 환경, 남북관계, 사이버 대외 환경으로 구분할 필요가 있다[10][11]. 북한체제의 폐쇄적인 속성상 정보기관과 권력기관의 조직편제와 임무 등을 파악하는 것은 매우 어렵다. 특히 비밀리에 운영되는 정찰총국과 같은 대남공작부서는 더욱 더 어려우며, 부서, 명칭, 기능 등이 수시로 변경되고 있다. 따라서 북한 사이버 관련 조직, 인원, 기술 등 실체 파악이 힘들다는 제한점을 전제로 한다[12][13].

3. 정부별 사이버공격 대응 방식

북한의 사이버 공격에 대한 한국의 대응방식은 북한에 역공격 등 적극적인 대응보다는 사태 수습을 위한 정책적으로 추진되었다. 즉 북한의 대형 사이버 공격이 발생할 때마다 정부의 대응 및 대책이 마련되어 시행되었다. 대부분의 대응과 대책은 사후약방문식으로 사건 발생 이후에 땜질식으로 추진되었다. 2003년부터 2017년까지 대남 사이버 공격에 대한 대응과 대책을 노무현・이명박・박근혜 정부 등 3개 정부별로 구분하여 논의 한다.

3.1 노무현 정부

노무현 정부에는 인터넷을 이용하는 인구가 2천 600만 명을 초월하고, 초고속인터넷 가입 1천만 가구를 넘어선 세계 최강의 인터넷 인프라를 갖추었다. 그럼에도 불구하고 해킹, 바이러스 등에 대한 대책이나 대비가 미흡하였다. 즉 인터넷 인프라 구축 분야에 성장 주도형으로 적극 추진하고 사이버보안 투자에는 미흡한 시기였다. 참여정부 기간 중에 북한의 사이버 공격 목표는 주로 국가 및 공공기관에 공격이 집중되었다. 게다가 우리나라 주요 국가시설에 대한 망 분리가 완벽하게 이루어지지 않은 시점이었다.

우리나라는 정부차원에서 국가정보화사업을 적극 추진하여 정보화 강국이 되었다. 인터넷 보급률과 회선 속도의 증대로 이뤄낸 초고속 인터넷 1위의 명예를 보유할 수 있었다. 반면에 국내 기업들 중에서 몇몇 대기업과 주요 금융권을 제외한 대부분의 기업들의 경우 보안 책임자가 한직이고 여러 업무를 겸직함으로써 사이버보안과 바이러스 감염 대책 등에 집중할 수 없는 것이 현실이었다. 특히 정부와 실무기관에서 필요한 보안패치를 배포했음에도 불구하고 설마하는 인식 부족으로 보안사고가 재발하는 등 보안의식 부재가 가장 심했던 기간이였다. 이는 기업 이익 창출에만 최우선 시 하고 사이버보안은 매우 무관심했던 시기였다. 우리나라는 2003년에 초고속 인터넷 가입자만 1,000만 명, 10가구당 7가구가 초고속 인터넷을 사용하는 나라였다. 그만큼 인터넷을 실무와 실생활에 긴요하게 활용하였다. 그러나 1.25 인터넷 대란으로 인터넷 강국의 이면에 허약한 정보보호 수준은 모래 위의 성이었다는 사실을 깨닫게 해 주었다.

따라서 정부는 2003년 1.25 인터넷 사고를 계기로 2003.12에 한국인터넷진흥원에 ‘인터넷침해사고대응지원센터’를 운영하였다. 이는 국가적으로 인터넷 침해사고에 대처하기 위해 설치된 사이버 공격 대응 기구로 민간 정보통신망을 상시 관제하는 센터이다. 조직은 ①분석대응팀, ②네트워크 모니터링팀, ③침해사고대응협력팀으로 구성되었다. 특히 네트워크 트래픽을 24시간 모니터링하고 유관기관 간 정보공유를 통해 인터넷망의 이상 징후를 조기에 탐지・분석하는 역할을 담당하였다. 그리고 이상 징후 발생 직후 대국민 예보와 함께 경보를 발령하고 침해사고 복구 관련 기술과 노하우를 지원토록 하였다. 또한, 2004년 정부는 국가정보원 산하에 ‘국가사이버안전센터’를 설치하였다. 주요임무는 국가 정보통신망을 직접 관리하고 ‘인터넷침해사고 대응지원센터’, ‘국방정보전대응센터’, ‘보안관제센터’, ‘정보공유분석센터(ISAC)’, ‘컴퓨터침해사고대응팀’ 등 국내외 사이버 침해사고 대응 기관들과 협력해 각종 공격징후를 탐지하고 위협정보를 종합적으로 분석하여 관련기관에 안전대책을 제공하고 있다. 국내 사이버 테러 대응체계는 청와대 국가안전보장회의(NSC)의 ‘사이버안전정책조정회의’

를 중심으로 공공 부분에는 국가정보원의 ‘국가사이버안전센터’, 경찰청의 ‘사이버 테러대응센터’가 담당하였다. 민간 부분에는 한국인터넷진흥원의 ‘인터넷침해대응센터’가 담당하고, 국방 부분에는 국방부의 ‘국방정보전대응센터’가 담당하는 등 역할을 분담하고 있다. 따라서, 우리 정부의 대응은 국가사이버안전센터와 인터넷침해사고대응지원센터를 설치하고 관련지침을 마련하여 신속히 대응하였다. 특히 참여정부 기간에 북한의 사이버 공격이 시작 단계였지만 1.25대란은 우리의 인터넷 취약점을 정확히 파악 후 공격하였다. 반면에 우리 정부는 외부공격에 대한 방어대책이 마련되어 있지 않아서 국민 불편 등 피해가 상상외로 컸고 많은 교훈도 얻었다. 따라서 2005년 1월에는 국가사이버안전에 관한 조직체계와 운영에 대한 사항을 규정하고, 사이버안전 업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 하는 ‘국가사이버안전관리 규정’을 제정하였다. 즉 국가사이버안전체계의 수립과 개선, 유관기관 간 역할과 임무 조정 등 국가사이버안전에 관한 사항을 심의하기 위한 ‘국가사이버안전전략회의’를 설치하고, 전략회의의 효과적 운영을 위한 ‘국가사이버안전대책회의’를 구성함으로써 사이버안전 관리체계가 확립되었다. 2006년 8월에 ‘국가 사이버안전 위기대응 통합훈련’은 1968년 을지연습을 시작한 이래 처음 실시하였다. 이 훈련은 전쟁 이외의 각종 위기에 대해 국가의 통합적인 대응 능력을 확인하기 위한 것이다. 특히 국가 사이버 공격 또는 위기상황 발생에 대비하고 준비태세를 점검하기 위해 민・관・군이 공동으로 참여하는 합동연습으로 실시되었다.

3.2. 이명박 정부

2008년 1월 인터넷쇼핑몰인 옥션 해킹으로 1,000만 명의 개인정보를 유출하는 피해를 입었다. 옥션 해킹사태 이후 정보보호 대응의 필요성 인식하여 2008. 7. 22 행안부 주관으로 ‘정보보호중기종합계획’을 마련하였다. 2010년까지 제도개선 및 인프라 조성을 통해 사회안전망을 구축할 계획을 세웠다. 또한 2008년에 국방, 외교, 행정 등 10대 핵심부문의 보안관제센터를 설립하였다.

2009년 7.7 DDoS 공격 이후 국가정보원장의 주재로 ‘국가사이버안전전략회의’를 개최하였다. 이는 대외 사이버 공격이 국가 안보를 위협하는 것으로 인식하여 사이버공격의 대응역량을 강화하기 위해 ‘범정부 사이버위기 종합대책’을 마련하여 시행하였다. 핵심 내용은 사이버 안보 거버넌스 시스템을 확립하고 부처별 책임과 역할을 규정하였다. 또한 대국민 언론창구를 방통위로 일원화하고, DDoS의 대피소 구축 및 대응장비를 설치하는 것이었다.

2010년 1월에 국방부는 국방 사이버전의 기획, 계획, 시행, 연구・개발 및 부대 훈련에 관한 업무를 수행하기 위하여 국방부장관 소속으로 ‘국군사이버사령부’를 설립하였다. 2011년 3.4 DDoS와 농협 사이버 공격을 계기로 실효적인 대응을 추진토록 ‘국가 사이버안보 마스터플랜’을 마련하여 시행하였다. 주요내용은 민・관・군 ‘사이버위협합동대응팀’을 구축하여 운영하고, 업무망과 인터넷망을 분리하였으며, S/W 보안 취약점을 진단하는 제도 시행 및 외주업체의 보안을 강화하였다.

3.3. 박근혜 정부

정부는 2013년 3·20 전산망 대란과 6·25 사이버 공격을 통해 각종 사이버위협으로부터 범국가 차원의 역량을 결집하여 효율적으로 대응하기 위해 ‘국가사이버안보 종합대책’ 을 마련·시행하였다. 또한 사이버 역량을 한 곳으로 통합하는 필요성을 인식하고 청와대는 컨트롤타워 역할을 맡고 국가정보원은 총괄토록 하였다. 즉 청와대 중심으로 사이버안보 컨트롤타워를 일원화토록 정립하여 평시에는 ‘미래전략수석’이 담당하고, 위기 시에는 ‘국가안보실’이 담당하며 상황발생 할 경우 청와대와 국가정보원에 동시 전파토록 하였다. 그리고 청와대에 ‘사이버안보비서관실’을 신설하고 주요 통신 기반시설 보호체계를 강화하는 등 ‘국가 사이버안보 종합대책’을 마련하였다.

2014년 소니픽쳐스사 공격 사건을 계기로 미국은 북한을 공격자로 지목하고 북한을 사이버 공격에 대한 제재를 가하였다. 미국 정부가 북한의 사이버 공격 행위자 즉 북한 해커 박진혁, 조선엑스포, 정찰총

국 등을 대상으로 제재를 가하는 것은 이번이 처음이다. 특히 수사단계에서 우리 정부와 함께 사이버 공격정보의 공유 등 한·미 간 국제공조를 하였다.

정부는 2014년 한수원 사이버 공격 이후에 안전한 사이버공간이 필요하다고 인식하여 2015년 3월에 '국가사이버안보태세 역량강화방안'을 발표·시행하였다. 특히, 청와대 국가안보실의 사이버안보 컨트롤타워 기능을 대폭 강화하였다. 또한 중앙행정기관과 지방자치단체, 주요 공공기관에 사이버 보안을 담당하는 전담조직을 신설 또는 기존 조직을 확대하는 등 사이버 보안 전담조직을 확충하였다.

상기 본문의 내용을 토대로 정부별 북한의 사이버 공격과 한국의 대응 양상을 종합 비교 분석한 내용은 아래 <표 2>와 같다.

<표 2> 정부별 사이버공격과 대응 양상 비교

정부	주요 공격	공격목적	정부별 대응
노무현 정부	2003 1.25 2004전산망	인터넷마비 경제적타격 정보탈취	국가사이버안전센터, 인터넷 침해사고대응지원센터 설치 국가사이버안전관리규정제정 국가사이버위기대응통합연습
이명박 정부	굳 인터넷 7.7 디도스 농협전산망	전산망마비 기밀탈취	국가차원 보안관제체계구축 국가전산망보안관제지침규정 국가사이버위기종합대책, 국가사이버안보마스터플랜 마련 국군사이버사령부 신설
박근혜 정부	3.20전산망 한수원전산망 국방부전산망	기밀탈취 기간망침투 사회혼란 금융탈취	국가사이버안보종합대책 및 국가사이버안보태세역량강화방안 마련 사이버분야 위기관리 표준매뉴얼 준비 한·미 국제공조 정보공유

지금부터는 노무현정부, 이명박정부, 박근혜정부에서 문재인정부(2017.5-2019)를 추가하여 정부별로 북한의 사이버 공격 유형, 정부별로 한국의 대응 방식을 비교하여 어떤 변화와 특징이 있는지 분석하였다. 또한 보수(이명박·박근혜정부)와 진보(노무현·문재인정부) 정권으로 구분하여 북한의 공격과 한국의 대응 양상을 알아보고 북한의 비대칭전력 중에 하나인 북한 핵실험과 사이버 공격과의 어떤 함수 관계가 있는지도 분석하였다.

4. 한국의 사이버공격 비교 분석

4.1 4개 정부별 한국의 대응 방식 비교

북한은 본격 핵실험을 시작한 2006년부터 2017년까지 실시하였다. 북한의 핵실험과 대남 사이버 공격과의 상관관계를 분석하기 위해 핵실험 전후 기간에 발생한 북한의 사이버 공격사례를 정리한 내용은 <표 3>과 같다. 따라서 노무현·이명박·박근혜·문재인정부 등 정부별, 핵실험일자별로 대남 사이버 공격과의 상관관계를 비교 분석 한다.

2006.10.9.일부터 2017.9.3.일까지 6차례 실시한 북한의 핵실험이 사이버공격과 어떤 관계가 있는지 살펴보았다. 먼저 핵실험 전후로 사이버공격이 발생하였으며 공격대상은 정부기관, 언론사, 금융기관 등이었다. 핵실험 전후로 사이버공격 대상이 청와대, 국방부, 통일부, 국회 및 외교·안보 등 정부기관이 많았다. 우리 정부의 정보 즉 지휘부와 외교안보 정보를 집중 수집하였다. 언론사는 국민 여론을 살피고, 금융기관은 세계적으로 대북제재로 수입원이 부족하여 금전탈취를 목적으로 했을 것으로 판단된다. 북한의 사이버공격 특징 중의 하나는 핵실험을 시도했을 때 7.7 DDoS, 3.20 인터넷 대란, 6.25사이버공격, 국방부 5015작계 유출 등 대형 사이버공격이 발생한 점이다. 북한이 사이버 공격을 본격적으로 시작한 2009년부터는 2차 핵실험에서 6차 핵실험까지 각각 2번의 사이버공격이 있었다. 특히 4차 핵실험에는 사이버공격이 4번으로 가장 많았다. 박근혜정부 기간인 2016년 1월 6일 북한의 4차 핵실험 전후로 북한 확인 또는 추정의 사이버공격이 지속적으로 포착되었다. 특히 2016년 1월 박근혜 대통령이 북한 핵실험과 관련해 대국민 담화와 기자회견 당일 13일에도 북한의 사이버 공격 시도가 있었다. 즉 13일 오후 4시 20분경에는 국가·공공기관을 대상으로 청와대를 사칭한 악성메일이 유포된 정황이 포착됐다. 이정규(sntongil12@daum.net), 이용주(returnkk@daum.net) 등이 발신자 계정정보이며 메일제목은 '[국가안보실] 북한 4차 핵실험 관련 대응방향 의견 수렴'과 '청와대 외교안보실입니다. 북한 4차 핵실험 관련' 등이다. 또한 북한의 사이버전사 계정으로 추정되는 메일을 통해 국가안보실을 공격하고 북한 4차 핵실험 관련 내용을 사칭해서 스피어피싱 공격을 진행한 징후가 포착되었다. 방산업체를 공격한 조직 역시 2015년 말부터

2016년 1월 13일까지 활동한 정황이 포착되었으며 정보수집용 악성코드로 공격을 시도하였다. 2017년 5월 문재인 정부 출범에 따라 ICT 분야 행정조직을 과학기술정보통신부로 개편하였다. 과학기술정보통신부는 사이버보안 강화를 통한 국민불안 해소를 국정과제로 정하였다. 또한 안전한 사이버 환경을 조성하기 위하여 국내 인터넷을 365일 24시간 상시 모니터링 중이다. 2017년 6월에 빗썸, 9월에 코인이즈, 12월에 유빗(구 야피존) 등 3곳의 암호화폐거래소를 대상으로 공격하였다. 공격 목적은 코인이즈와 유빗은 금융탈취이며 빗썸의 경우 고객정보를 해킹(3만여 명)하였다. 공격 기법은 3곳 모두 APT와 랜썸웨어 방법으로 공격하였다. 또한 2017년 9월에 SI업체의 서버 등을 공격하기도 하였다. 결론적으로 북한이 핵실험을 실시한 전후로 북한 추정의 사이버공격은 한국의 내부 동향정보를 수집하여 여론을 우호적으로 조성하기 위해 은밀하게 진행하였다.

<표 3> 정부별 북한 핵실험과 사이버 공격 비교

정부	핵실험		사이버 공격		특징
	차수	일자	공격 일자	공격기관	
노무현 정부	1	2006. 10.9	2006.2	청와대, 정부기관	
이명박 정부	2	2009. 5.25	2009.3	육군사령부	국정원 결과 보고
			2009.7	청와대, 정부기관	7.7 DDoS 공격
	3	2013. 2.12	2013.3	언론사, 금융기관	3.20 인터넷 공격 민·관·군 합동
			2013.6	청와대, 정부기관, 언론·방송사	6.25 사이버 공격 시스템 등 파괴 정부, 민관군합동 3.20 공격 유사
박근혜 정부	4	2016. 1.6	2015.10	청와대, 국회, 통일부	서버해킹, 북한추정
			2016.1.13.~14	청와대	경찰발표, 북한제작 악성코드 유사
			2016.2	이니텍 금융기관	코드서명인증서 탈취
			2016.3	외교·안보 인사 등 정부기관	스마트 폰 해킹
	5	2016. 9.9	2016.8	대우조선	서버해킹 국회 국방위
			2016.9	국방부 국방통합데이터센터	서버해킹 작계5015 등 유출 국방부 발표 중국 선양 IP
문재인 정부	6	2017. 9.3	2017.4~12	한국은행 등 금융기관, 암호화폐 거래소 4곳	악성코드 유포 서버해킹 금전탈취 정보유출
			2017.9	SI업체	서버해킹 국정원 조사

4.2 정권별 북한의 핵실험과 사이버 공격과의 상관관계

보수(이명박·박근혜정부)와 진보(노무현·문재인 정부) 정권으로 구분하여 북한 핵실험과 사이버 공격을 비교하여 정리한 내용은 <표 4>와 같다. 북한이 실시한 핵실험 총 6차례 중에서 보수정권 4번, 진보정권 2번으로 보수가 두 배 많았다. 핵실험 시간적 간격은 1차에서 4차까지는 대부분 약 3년 정도 소요 되었으며, 박근혜정부인 5차는 8개월, 문재인정부의 6차는 1년 만에 핵실험을 실시하였다. 특히 6차까지 핵실험 전후로 사이버 공격을 총 13번 발생하였다. 사이버 공격 횟수는 보수정권은 10번, 진보정권은 3번으로 보수정권 기간에 3배 이상 많이 발생하였다. 결국 보수정권에 핵실험과 사이버 공격이 많았다는 증거이다. 이는 북한은 평화와 포용정책을 펼친 진보정권보다는 적대적 관계를 유지했던 보수정권에 더 왕성하게 핵개발과 사이버 역량을 키우고 공격하는데 집중하였다고 볼 수 있다.

2019년 8월에 UN 안보리 대북제재위 보고서는 “북한이 최근 3년간 최소 17개국 금융기관과 암호화폐거래소를 대상으로 35차례에 걸친 사이버 공격을 통해 20억 달러를 탈취했으며, 한국이 10건으로 최대 피해국”이라고 밝힌 바 있다. 또한 UN 기밀 보고서에서 “북한은 세계 금융기관과 암호화폐거래소를 상대로 사이버공격을 통해 대량파괴무기(WMD) 개발 자금을 조달한다”고 발표하였다. 이에 북한은 “UN 보고서가 북한이 감행했다는 과학적 근거도 없다"며 반박까지 하였다. 게다가 북한이 자체 암호화폐를 개발 중인 것으로 알려졌다. 북한이 스스로 암호화폐를 구축하는 이유는 세계 금융 시스템의 간섭을 피하면서 UN, 미국 등 국제 제재를 피하고, 정권유지 자금을 창출할 수 있기 때문이다. 북한이 국내 암호화폐거래소를 대상으로 집중적으로 사이버 공격에 집중하는 이유를 분석한 결과 보안체계가 타 금융권보다 상대적으로 취약하기 때문이다. 북한의 사이버 공격기관도 진보정권에서는 정부기관과 금융기관 등으로 한정되어 있지만 보수정권은 청와대, 국회, 국방부, 통일부 등 정부기관, 언론·방송사, 금융기관

및 민간기업 등 다양하게 분포되어 있었다. 이는 진보정권에서는 정보수집과 금융절취가 주목적이었으며, 반면에 보수정권에서는 민・관・군 등 여러 기관에서 기밀절취, 여론수집 및 금전탈취 등 다양한 목적으로 공격하였다.

북한의 사이버 공격 규모면서도 보수정권은 7.7 DDoS, 3.20 인터넷 대란 등 대규모로 사이버 공격을 하였다. 진보정권은 사전에 목표 기관을 정하고 그 목적에 부합되게 사이버 공격을 시도하였다. 그리고 북한의 공격양상은 보수정권에서 공격적이고 사회 이슈화, 정부 불신을 야기하였으나 진보정권에서는 가능한 조용히 은밀하게 추진하였다. 국내외의 금융기관을 대상으로 사이버 공격을 통해 외화를 획득하여 핵・미사일 개발비로 사용하였거나 통치자금으로 충당했을 것이다. 또한, 2018년 남북정상회담, 평창동계올림픽 등 화해 무드에도 북한의 사이버 공격은 지속되었다.

<표 4> 정권별 북한 핵실험과 공격특징 비교

정권	핵실험	공격 기관	공격 목표	공격 특징
보수 정권	4회	정부기관 기반시설 금융기관 언론사	전산망마비 기밀탈취 기간망침투 금융탈취	사건 대형화 사회 이슈화 국가혼란 대규모・공격적
진보 정권	2회	정부기관 공공기관 금융기관 민간기업	인터넷마비 경제적타격 정보탈취 금융탈취	사회혼란 외화벌이 은밀한 공격

5. 결 론

우리는 노무현 정부부터 문재인 정부까지 사이버 공간에서 북한으로부터 2003년 1.25 인터넷 대란, 2009년 7.7 DDoS, 2013년 3.20 전산망 대란, 2014년 한수원 전산망 공격, 2016년 국방부 내부망 공격, 2017년 암호화폐거래소 공격 등 북한의 크고 작은 사이버 공격을 받았다. 앞으로 이런 위협은 얼마든지 발생할 수 있다. 전자정부 시대에 만약 전쟁이나 핵이라도 등장한다면 순식간에 모든 시스템이 마비될 수 있다. 우리의 국가통신망과 정보시스템이 중단됐다면 그 자체가 혼란이다. 바이러스나 DDoS 공격만으로도 온 국가가 혼란과 마비상황이 발생하였다. 이 보다 더한 사태가 발생한다면 국가안보 위기가 올 것이다. 생각만 해도 소름이 돋는 끔직한 일이다.

미래의 전쟁은 예전과 달리 사이버전이 될 것이다. 앞선 IT기술력을 바탕으로 상대의 전산시스템을 마비시킨 후에 물리적인 방법으로 공격한다. 미국은 98년 코소보전에서 사이버 공격으로 세르비아의 방공망과 보안관제 시스템을 성공적으로 마비시켰다. 또한 미국은 이라크전에도 동일하게 먼저 사이버공격을 하고 난 뒤에 전통적 전쟁을 수행하였다.

2000년 초부터 북한의 사이버 공격은 국가・정부기관, 공공기관, 방산업체, 금융기관, 언론사, 민간기업 등을 가리지 않고 전방위적으로 발생하고 있다. 북한의 사이버 공격에 대해 체계적이고 효율적으로 대응하기 위해서는 관·군·민이 유기적으로 협력하여 법·제도를 개선하고, 전문 인력을 육성하며, 정보보호 예산 확보와 최첨단 기술을 개발하는 등의 지속적인 노력이 필요하다. 또한 인공지능 등 최신기술이 접목된 전문성과 신뢰성 있는 보안관제서비스와 모의해킹 서비스를 제공할 수 있는 환경이 조성되어야 한다. 향후에는 스마트폰이나 업무용 PC 등 다양한 기기들의 보안이슈가 많이 발생할 것으로 예상된다. 이에 능동적으로 대응하기 위해서는 기술적 보안뿐만 아니라 정보보안 교육을 통해 보안의식을 제고하는 등 관리적 보안과 함께 도덕적 윤리적으로 무장한 전문가를 양성하는 것도 더욱 중요하다. 그리고 사이버 공격은 예고하고 오지 않는다. 언제 어떤 방법으로 누구에게 공격해 올지 모르는 사이버 공격에 대비하여 철저한 준비태세가 필요하다. 한수원 전산망 공격 등 대규모 북한사이버공격이 발생할 때마다 「국가사이버테러방지법」제정을 지속적으로 요구하였으나 여야의 의견차이로 국회에서 계류하다가, 결국 법안 모두 임기만료로 폐기되었다. 이런 범국가적 사이버 보안 원칙의 부재를 해결토록 사이버보안 정책의 거시적 원칙을 국가 차원에서 정하고, 이를 관련 법률로 정하는 것이 필수적이다. 사이버 공격이 국가안보의 위협으로 부상하였다. 이에 대비하고 국가안전을 보장하기 위해 국가전략을 구상할 필요

가 있다. 2019년 4월 문재인정부에서 사이버안보 정책의 장기적 비전과 목표를 담고 있는 최상위 지침서인 '국가사이버안보전략'을 대한민국정부 최초로 수립하였다. 9월에는 세부지침인'국가사이버안보 기본계획'이 발표되었다. 이는 우리 국가 최초로 국가차원의 사이버 위협에 효율적으로 대응하기 위해 전략 체계가 마련되었다는 데 큰 의미를 두고 싶다.

참고문헌

[1] 윤재석. "국가 사이버보안 전략 수립과 개선을 위한 참조 모델 개발", 한국융합보안학회, 2016.

[2] 국가정보원, 2020 국가정보보호백서, 한국인터넷진흥원, 2020.

[3] 강정호·김회동·김순수·유진철, "국외 주요국과 북한의 사이버전 수행전략 및 기술 비교분석을 통한 대응방향". 『보안공학연구논문지』. Vol 13 No4., 2016.

[4] 권문택, "북한의 비대칭 전략 '사이버 기습공격'에 대한 대책 연구". 『정보·보안 논문지』. 제10권 제4호., 2010.

[5] 권안도, "북한의 사이버전 능력이 비대칭 전력인가?". 『군사논단』., 2017.

[6] 권오국·석재왕, "주요국의 사이버테러 대응체계와 시사점 분석-미국, 영국, 독일 사례를 중심으로" 『한국경호경비학회』. 제49호., 2016.

[7] 김문성, "사이버테러 국가대응체계 구축방안 : 법률체계와 조직체계를 중심으로". 『평화학연구』. 제17권 1호., 2016.

[8] 김상배, "사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계". 『국제지역연구』. 24(3)., 2015.

[9] 김승주, "북한의 사이버 공격과 우리의 대응". 『북한연구소』. 통권 516호., 2014.

[10] 김승주, "전방위적으로 시도되는 북한 사이버 테러 실상". 『북한연구소』., 2017.

[11] 김양현, "북한의 대남 사이버테러 사례 연구". 『한국테러학회보』., 2014.

[12] 김연준·김상진, "사이버테러대응방안에 관한 연구". 『융합보안 논문지』 제16권제3호., 2015.

[13] 김윤영, "북한 대남 심리전 변천 양상과 전망". 『북한연구소』. 통권 535호., 2016.

〔저자소개〕

권 혁 천(Hyeokchun Kwon)

1987년 2월 충북대학교 계산통계학과 (이학사)
1996년 12월 국방대학교 전자계산학과(국방과학석사)
2020년 2월 건국대학교 안보재난관리학과(정책학박사)
2020년 3월 ~ 현재 극동대학교 사이버보안학과 강사
email: kwhc2429@kdu.ac.kr

이 용 준 (Youngjoon Lee)

1999년 2월 강남대학교 컴퓨터학과 (공학사)
2001년 2월 숭실대학교 컴퓨터공학과 (공학석사)
2005년 2월 숭실대학교 컴퓨터공학과 (공학박사)
2020년 4월 ~ 현재 극동대학교 해킹보안학과 조교수
email: yjlee@kdu.ac.kr

박 원 형 (Wonhyung Park)

서울과학기술대학교 산업정보시스템공학과 (공학사)
서울과학기술대학교 정보산업공학과 (공학석사)
경기대학교 정보보호학과 (이학박사)
성균관대학교 컴퓨터교육학과(박사수료)
전) 극동대학교 사이버보안학과 부교수/학과장
현) 상명대학교 정보보안공학과 부교수
email : whpark@smu.ac.kr