남북통일을 대비한 국가사이버안보 정책 연구

함승현* · 박대우*

*호서대학교 벤처대학원

Research on National Cybersecurity Policy Preparing for the Reunification of North Korea and South Korea

Seung-hyeon Ham* · Dae-woo Park*

*Hoseo Graduate School of Venture

E-mail : h3040ms@hanmaul.net, prof_pdw@naver.com

요 약

대한민국의 남한과 북한이 평화통일을 위하여, 변혁과 개혁을 주도할 수 있고, 정책을 만들고 보완하고 협상하여, 실천 할 수 있는 사이버안보정책이 필요하다. 본 논문은 사이버전의 정의와, 해외의 사이버테러와 사이버전쟁 대응, 사이버전 대응 기술을 살펴본다. 남한과 북한의 대치 상황에서 사이버안보 활동을 분석하고, 남북통일을 대비한 사이버안보 정책을 연구한다. 본 연구는 사이버위협으로부터 안전한 사이버공간을 구축 및 운영으로 남북통일을 대비하여 합리적인 사이버안보 정책 및 법률의 방안을 제안한다.

ABSTRACT

The North and South Korea for the peaceful reunification of the Republic of Korea, to lead the transformation and reform, and to complement the policy making and negotiations, there is a need for cyber security policy to practice. This paper explores the definition and overseas cyber terrorism and cyber warfare correspondence, correspondence between the versions of the technology between versions. Analysis of cyber security activities in the North and South confrontation, and research the cyber security policy against the unification. In this study, we compared the unification to build and operate a secure cyberspace from cyber threats and cyber security policy suggestions for ways of rational and legal.

키워드

국가사이버안보, 국가사이버정책, 남북통일, 사이버전

I. 서 론

국가의 인프라를 구성하고 있는 교통, 통신, 가스, 전기, 수도, 원자력, 국방, 금융, 전자상거래 등의 정보자원들은 ICBM(Internet of Things, Cloud, Bigdata, Mobile)과 연결되고 있으며 기본적인 국민들의 실제 생활에 사용되고 있다. 국민들은 개인의 스마트폰과 ICBM으로 세계와 정보를 교류하고 이용하는, 국경 없는 사이버 세계로 발전하고 있다[1].

국가의 인프라에 대한 사이버 공격과 사이버 테러 무기로 실제 공격을 받고 있다. 2009년, 2010년 스턱스넷(Stuxnet)과 튜크(Duqu) 등의 사이버 공격 테러 무기(악성코드)가 이란의 핵시설을 마비시켰다. 또한 2012년 멕시코에서는 SNS를 통해 100만명 이상의 전국적 시위 선동으로 극한 대립이 발생했다. 2013년 미국의 F-35 전투기 관련 정보의 유출이 발생했다. '핵심 기반시설 보호 현황(Critical Infrastructure Protection Survey, CIP) 보고서'에 따르면 지난 5년간 정치적 의도를 가진 사이버 공격을 당했다. 또 ISACA의 2015 국제 사이버보안 실태 보고서에 따르면 응답자의 83%는 사이버 공격이 조직이 직면한 상위 3개 위협 가운데 하나라고 응답하고 있다. 사이버 침해사고로 인한 남함의 경제적 피해 규모는 연간 3조6000억원으로 추정된다. 이는 자연재해 국내 피해액 2조7000억원보다 훨씬 많은 금액이다[2].

국경이 모호한 사이버 세계의 역기능으로서 사이버 범죄와 사이버 테러가 발생하고 있다. 세계의 분쟁지역은 물론 국가 간의 이익이 충돌하는

곳에서는 사이버 테러가 발생하고 있다. 사이버 테러는 국가 간 전쟁의 전초전으로서 보이지 않는 사이버 세계로부터 사이버 전쟁으로 되면서 국민과 사회, 국가안보에 큰 위협이 되고 있다[3].

사이버세계의 기술은 복잡・고도화되어가고 있고 시공간의 제약이 적으며 발생하는 사이버 범죄와 테러에 대응하여 정부부처와 민간 단독으로 침해 사고에 대응하기에는 한계가 있다[4].

사이버 범죄와 테러는 현실에서 국가질서에 혼란을 야기하며, 국민행복의 파괴와 국가안보 및 국민의 안전을 파괴하는 사이버 전쟁 사태로 확대될 수 있는 실정이다.

사이버 테러와 사이버 전쟁 위협의 증대로 인한 국민에게 정신적・물리적 피해가 발생한다. 특히 남북한으로 대치되고 있는 현상에서, 남북한이 통일 되었을 때를 대비한 국가 차원에서 사이버 테러와 사이버 전쟁을 컨트롤 할 수 있는 시스템이 필요하다.

본 논문에서는 남북한이 통일 되었을 때를 대비한 체계적인 사이버안보 정책에 관한 연구를 한다. 국가 사이버안보의 정책과 법의 구체적 내용을 정립한다. 통일 후에 대한민국 국가가 세계 속에 기술 발전을 토대로 한 국가와 국민을 위한 국가사이버안보에 관한 정책을 연구한다.

Ⅱ. 관련 연구

2-1 사이버전(Cyber Warfare) 정의

사이버 공간에서 다양한 사비어 수단을 사용하여 상대 정보자산을 교란, 거부, 파괴하여 상대의 정보체계를 마비시키기 위해 전・평시 사이버 도메인에서 이루어지는 무형의 공격이나 방어 활동이다.

“사이버전쟁”이란 사이버범죄및테러를 통하여 군사적 목적달성을 위한 국가인프라파괴, 지휘통제전, 군사정보전, 전자전, 미디어심리전, 해킹전, 경제정보전 등의 국가와 국민의 안전에 위해를 가하는 물리적●전자적●경제적●정신적●인적 전쟁수행을 말한다[5].

2-2 해외의 사이버테러와 사이버전쟁 대응

해외의 사이버 테러와 전쟁과 대응은 정부 주도로 이루어지고 있다.

미국은 사이버 사령부가 모든 사이버전에 대한 컨트롤타워 역할을 수행하여 민간・관료・군 기관의 지원을 받고 있다.

중국은 인민해방군 총참모부가 사이버전을 기획, 실행하며 민간기구를 통제하여 국가관리 차원의 광통신망과 IP를 제공받고 있다[5].

2-3 사이버전 대응 기술

사이버 테러와 전쟁을 위한 실시간 대응을 위한 대응체제 구축하고, 민간 영역과 정부 공공기관의 사이버전 대응 기술이 요구된다.

사이버 테러와 전쟁은 인터넷 네트워크를 물리적으로 분리되어 안전하다고 강조하나, Stuxnet과 같이 내부자에 의한 정보유출이나 사이버공격 대비 미흡하다.

사이버전을 위한 다음과 같은 새로운 사이버공격 패턴과 기술에 대비하여야 한다.

. 전자공격을 위한 EMP 공격 방호시설 구축
. 전파교란을 위한 GPS, 전자교란, 통신 재밍
. 고기밀성의 암호장비
. 해킹 역추적 기술
. 사이버 공격의 원점지 식별 및 타격
. 해외 국가와 사이버 동맹 및 정보공유 강화
. 주변국과 사이버정책과 기술 수집 및 분석
. 사이버전을 수행한 결과분석 및 시나리오
. 사이버전 정책과 기술 분석

Ⅲ. 남북대치 상황에서 사이버안보 활동

3-1. 남북대치 상황에서 사이버 공격 분석

남한에서는 2009년 7.7 DDoS 공격, 2011년 3.4 DDoS 공격, NH농협전산망 마비, 2012년 중앙일보 사고, 2013년 3.20 사이버테러로 인한 KBS, MBC, YTN, 신한은행, NH농협 등에 대한 APT(Advanced Persistent Threat)공격으로 사이버테러가 발생하여, 대량의 컴퓨터가 작동이 않되어 피해가 발생하였고, 전국규모의 은행전산망 마비 사태가 발생하였고, 2013년 6.25 사이버테러 청와대 홈페이지가 해킹되어 ‘통일대통령 김정은’의 문구가 게시되었고, 2014년 1월 롯데카드, KB국민카드, NH농협카드 등 3사의 약8,500만명 개인정보유출사건, 2014년 5월 KT에서 1,200만명 개인정보유출사건이 발생하였다. 2014년 12월 한국수력원자력이 관리하는 ’원전안전해석코드(SPACE)‘와 같은 원자력 핵심기술이 포함된 원전자료가 해커로부터 유출되어, 국민의 자산침해뿐만 아니라, 국가의 인프라에 대한 사이버테러와 공격으로 인한 국민들에게 피해와 불안감을 가중시켰다[6].

3-2. 남한의 사이버안보 활동

대한민국인 남한은 평시에 사이버안보는 국가정보원을 중심으로 컨트롤타워를 구성하고 있다. 국군사이버사령부가 사이버전을 대비하여 활동하고 있다. 정부기관의 사이버시스템에 관해서는 행정자치부가 맡고 있으며, 민간분야는 KISA를 중심으로 하는 미래창조과학부가 사이버보안 분야를 맡고 있다.

남한의 사이버안보를 위한 해외와의 협력은 다음과 같다.

남한은 러시아(2014년 5월), 호주(2014년 8월), 인도(2015년 1월), 일본(2015년 10월), 중국(2015년 10월), 사우디(2016년 1월), EU(2016년 6월), 체코(2016년 6월), 독일(2016년 6월), 미국(2016년 6월) 등과 사이버정책 협의회를 개최하여, 국가 상호간 사이버협력 및 국제 사이버안보를 위한 협력을 도모하고 있다.

또한 UN 정보안보 정부전문가그룹(GGE: Group of Governmental Experts on Information Security)과 1차(2004년~2005년), 2차(2009년~2010년) 및 4차(2014년~2015년)에 걸쳐, 국가 간 사이버안보 규범 문제를 논의하고 있다.

아세안지역포럼(ARF)을 통해 2012년 9월 서울에서 관련 세미나를 개최하고, 2013년 9월, 2014년 3월, 2015년 7월에 개최된 ARF 차원의 사이버 이슈관련 워크숍의 사이버안보 Work Plan을 2015년 8월 ARF 외교장관회담에서 채택하였다.

세계 사이버스페이스 총회에서는 2011년 런던, 2012년 부다페스트 총회에 참석 하였고, 2013년 서울 사이버스페이스 총회(2013년 Seoul Conference on Cyberspace)를 개최하였다. 서울총회에서는 '개방되고 안전한 사이버공간을 통한 글로벌 번영(Global Prosperity Through an Open and Secure Cyberspace)'이라는 주제로, 사이버공간 관련 제반 이슈에 대한 논의하였고, 2015년 헤이그 총회에서 남한의 외교부장관은 국제규범 논의와 신뢰구축 노력의 병행 필요성, 사이버 공격과 범죄에 대응할 수 있는 견고하고 효과적인 파트너십의 필요성, 사이버 역량강화 필요성을 연설하였다.

3-3. 북한의 사이버안보 활동

북한은 조선인민군 총참모부 예하 정찰총국에서 사이버 테러를 총괄하여 우수한 인력양성 및 사이버전 연구를 지원받으면서 비대칭 전력으로서 총체적인 사이버 전쟁을 수행할 수 있는 것으로 알려져 있다.

북한은 세계 수준의 사이버전 능력을 보유하고 있으며, 핵심 비대칭 전력으로 사이버전사를 육성하고 있다. 북한은 사이버전을 핵미사일과 함께 핵심 비대칭 전력으로 이용하여, DDoS, 지능형 지속(APT) 공격, 역추척 방지 등 다양한 공격수단 보유하여 사이버전의 종합능력은 세계5위 수준으로 판단하고 있다.

Ⅳ. 남북통일을 대비한 국가사이버안보 정책

4-1. 남북통일을 대비한 국가사이버안보 전략

남북한 통일 후의 사이버안보를 위해서는 외국과의 국제공조를 수행해야 한다. 사이버안보를 위한 규범을 식별하고, 사이버범죄와 사이버테러에 대한 법안과 정책을 마련하여 집행하고, 국가사이버안보를 위한 공격과 방어가 시스템적으로 수행되어야 한다.

4-2. 남북통일을 대비한 국가사이버안보 정책과 법률

남북통일을 대비한 사이버안보 정책과 법률 제안의 주요 방안은 다음과 같다.

◈ 국가 정보공유 체계 정립

국가사이버안보를 총괄하는 법률과 부문별로 정보보호를 정한 법률들이 산재하여 정보공유 체계 불완전하므로 국가정보공유 체계를 정립해야 한다.

국가사이버안전관리규정상 국가정보원 역할의 법령상 근거가 공공망에 한정하므로, 국가사이버안보차원의 사이버위협정보 공유의 확대 및 규정이 필요하다.

국가의 공공기관, 민간기업, 그리고 공공과 민간의 정보공유가 원활이 이루어질 수 있도록 컨트롤타워 중심의 정보공유 체계와 정보교환 및 정보공유 보안 프로토콜이 정립되어야 한다.

. 기존의 국가 법률의 정보공유체계에 국가정보원, 미래창조과학부, 법무부, 국방부, 안전행정부 등의 범정부적 사이버범죄 및 사이버테러 대책에도 정보를 제공하는 규정이 필요하다.

◈ 국가 사이버테러 위협 대응

현실세계로 연결된 사이버공간 위협을 현실세계 위협과 동일한 수준으로 실시간 대응시스템이 필요하다. 국가에 대한 사이버테러 위협 대응 및 관리를 위해 관련된 사이버테러 및 정보의 운영기관에 대한 컨트롤타워와 정보공유에 대한 실시간 일관된 사이버대응이 필요하다.

◈ 국가 사이버안보 용어와 원칙 정립

현재 국가사이버보안을 총괄하는 법률이 없고 부문별로 정보보호를 정한 법률들이 산재하여 범국가적 사이버안보의 원칙과 수행을 위한 원칙과 용어의 정립이 필요하다.

국가인프라를 담당하는 정보통신기반시설 뿐만 아니라 국민의 사회 시설에도 연결되는 사이버 인프라의 국가사이버안보를 위한 원칙과 용어의 정립이 필요하다.

국가사이버안보를 위한 정책과 법률의 제정을 위한 부문별 법률 체계가 필요하다.

◈ 국가 사이버안보 합동 대응

현재 대한민국은 평시에 사이버보안은 국가정보원을 중심으로 18개 기관이 참여하는 민・관・군 합동대응팀을 구성・운영 중이다. 하지만, 대통령훈령인 국가사이버 안전관리규정에 근거하고 있어서 국가사이버안보를 위한 임무・기능 및 권한에는 한계가 있다.

급속하게 발전하는 사이버안보의 기술과 사이버안보의 인프라를 위한 인터넷 네트워크를 스캔하고, 탐지하는 것만으로는 국가사이버안보를 위한 실시간 대응에는 한계가 있다. 따라서 국가차원의 사이버안보 합동대응을 강화하고 관련 유관기관과 연계기관의 역할을 정책과 매뉴얼 식의 총체적인 대응에 필요한 국가사이버안보 정책과 법률의 연구와 제정이 필요하다.

◈ 국가 사이버사령부 운영과 정책

통일된 대한민국의 대통령 소속으로 사이버안보 컨트롤타워를 두고, 국방부 직속으로 사이버사

령부를 두고, 국방 사이버전의 기획 및 계획 수립, 국방 사이버전의 시행, 국방 사이버전을 수행할 전문 인력의 육성과 기술 개발, 국방 사이버전을 대비한 부대 훈련, 국방 사이버전 유관기관 사이의 정보 공유 및 협조체계 구축, 그 밖에 국방 사이버전과 관련된 사항을 수행[7]하도록 해야 한다.

국군사이버사령부령의 입법을 통해 헌법 제5조 '국가의 안전보장과 국토방위의 신성한 의무를 수행' 하기 위한 확고한 기반을 마련한다.

▶ (국군사이버사령부 설치법)제정으로 민·관·군 통합 사이버전 수행의 기반 마련 및 정부의 예산을 확보한다.

▶ (조직운영·편제) 임무형 T/F중심의 운영을 통해 신속한 국가사이버전의 수행이 가능하다.

▶ (인사) 실질적인 인사권(임용, 해임, 전출 등) 및 탄력적 조직 운영권을 부여한다.

▶ (인재 충원(확대) 및 교육) 전문성, 기민성 및 충성심 등을 겸비한 인재의 적시·적소 충원으로 통합 사이버전에 적합한 최적의 인재 POOL 구성 및 정원 확대(선발권) 충원 후 전문기관(학교, 연구소)연계 및 해외 활동을 통한 지속적 인재 양성교육을 수행한다.

▶ (처우개선)24시간 사이버전 수행 및 관련 연구 활동에 전념할 수밖에 없는 직무 특성상 우수 인재의 처우 개선 필요(별도 수당 지급 법제화)하다.

▶ (사업 예산 보장) 사이버전 특성상 은밀성, 익명성 및 적시성(24시간)을 위한 영외 활동 보장 및 관련 경비의 지원이 필요(특수 사업비 집행 법적 제도화)하다.

▶ (정보요구권) 사이버테러와 전쟁 시 대비 신속한 피·아 식별을 위한 유관기관에 정보요구 시 최단시간 자료 제공을 의무화할 필요가 있다.

◈ 국가 사이버인프라 보안의 조직 구성

대통령령이 정하는 사이보안보 수석을 중심으로 중앙행정기관의 1급~2급에 해당되는 독립부서의 사이보안보국을 만들어 운영한다.

◈ 국가 사이버 인프라의 범죄 처벌 규정 정비

사이버범죄와 사이버테러의 은밀화, 조직화, 대형화에 따라 사후적 대응만으로는 국가인프라와 국민의 실생활보호에는 한계가 있다.

따라서 원격지에서 범죄 혐의가 의심되면, 정보통신망 수색 및 범죄단서 포착(온라인수색), 해킹을 수사방법으로 역이용하는 방안을 마련해야 한다.

국가 사이버 인프라에 대한 취약점을 악용하거나, 악성코드 감염(좀비)PC 확산 방지를 위한 처벌 규정의 정비가 필요하다. 즉 국가 사이버 인프라에 대한 악성코드(사이버범죄 및 사이버테러의 불법 범행도구)의 제작·보유에 대한 처벌 규정의 정비가 필요하다.

그리고 국가사이버 인프라의 정보통신망을 이용한 국민과 공공기관 상대의 사이버사기와 사이버범죄의 수시 업데이트 및 트랜드 분석을 통한 규정의 보안이 필요하다.

사이버범죄의 디지털 증거 확보와 절차에 대한 적법성을 부여하고, 감염PC의 인터넷 접속 차단 및 백신 설치 유도, 인터넷 사업자의 로그보존 의무 명시 등의 규정의 보완이 필요하다.

Ⅴ. 결 론

본 연구는 사이버위협으로부터 안전한 사이버공간을 구축 및 운영으로 남북통일을 대비하여 남과 북의 현 상황을 살펴보고, 합리적인 정책방안을 제안한다.

대한민국의 통일을 위해 변혁과 개혁을 주도할 수 있고 정책을 만들고 보완하고 협상하여, 실천할 수 있는 사이버안보정책이 필요하다.

남북한이 평화통일이 되고, 남한과 북한이 협상테이블에 앉아 소통하고 조율하고 보완하면서, 통일 후의 사이버안보 정책을 갖는다면, 대한민국과 세계가 함께 발전하는 사이버안보 강국을 바탕으로 한반도는 세계적인 사이버강국으로 탄생될 것이다.

참고문헌

[1] 박대우, '국가 사이버 안보 정책 보고서', 국가 사이버안보정책포럼, 2012년 12월

[2]박대우, "국가 사이버안보에 관련 법률 제안", 국회, 2013.5.14.

[3] 박대우, '국가 사이버 안보정책 포럼', 국회, 2014년7월18일

[4] 박대우, 글로벌이코노믹스, "국가 사이버안보에 관한 법률의 당위성", 2016.09.07.

[5] Dea-woo Park, "Draft of National Cybersecurity Act", International Journal of Security and Its Applications Vol.9, No.11, pp. 105-112, Nov. 2015.

[6] Dea-woo Park, Jin Shin, "A Comparative Study of the Proposed National Cyber-terror Prevention Act", International Journal of Security and Its Applications Vol.9, No.10, pp.267-274, Sep. 2015.

[7] 국군사이버사령부령[국방부 시행 2015.2.16.] [대통령령 제26101호, 2015.2.16., 일부개정]