JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 9 : 1666~1673 Sep. 2017

국가 사이버안보를 위한 정책 연구

함승현 · 박대우*

Study on Policies for National Cybersecurity

Seung-hyeon Ham · Dea-woo Park*

Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, Korea

요 약

대한민국은 남한과 북한으로 분단되어, 군사적 대립과 사회적 갈등을 발생시키고 있다. 북한은 남한에 대해 사이버공격을 수행하고 있으며, 남한의 국방망을 해킹하였다. 사이버공간에서 세계 각국은 국경도 한계도 모호해지고 있으며, 사이버전쟁을 위한 사이버공격과 사이버테러는 점과 시간과 공간으로 연결된 디지털 컴퓨팅으로 작동된다. 국가 사이버안보를 위해서는 아젠다와 매뉴얼이 필요하다. 또한 국가 사이버안보 정책을 만들고, 수행 할 수 있는 국가 사이버안보 법률과 정책에 대한 연구가 필요하다. 본 논문은 현재 남북한 대치 상황의 사이버테러 상황과 세계의 사이버전쟁에 대한 피해를 연구한다. 또한 국내·외의 사이버안보 활동과 사이버전쟁 대응 아젠다와 매뉴얼과 신기술을 연구한다. 그리고 국가사이버안보 정책을 제시하여 '(가칭)국가사이버안보법'이 마련되도록 정책을 제안한다. 본 연구는 국가 사이버안보법과 정책의 기초자료로 활용될 것이다.

ABSTRACT

Republic of Korea is divided into South Korea and North Korea, creating military conflicts and social conflicts. North Korea is conducting cyberattacks against South Korea and has hacked South Korea 's defense network. In the world of cyberspace, the boundaries of the borders are becoming obscured, and cyberattacks and cyberterrorism for cyberwarfare operate with digital computing connected to points, time and space. Agenda and manual are needed for national cybersecurity. Also, it is necessary to study national cybersecurity laws and policies that can create and implement nationalcyber security policy. This paper investigates cyberterrorism situation in North and South Korean confrontation situation and damage to cyberwarfare in the world. We also study cybersecurity activities and cyberwarfare response agendas, manuals and new technologies at home and abroad. And propose national cybersecurity policy and propose policies so that '(tentative) The National Cybersecurity Law' is established. This study will be used as basic data of national cybersecurity law and policy.

키워드 : 사이버전쟁, 국가 사이버안보, 사이버보안 정책, 법정책

Key word : Cyberwarfare, National Cybersecurity, Cybersecurity Policy, Law & Policy

Received 30 June 2017, **Revised** 06 July 2017, **Accepted** 24 August 2017

* **Corresponding Author** Dea-woo Park(E-mail:prof_pdw@naver.com, Tel:+82-2-2059-2352)
Department of Convergence Technology, Hoseo Graduate School of Venture, Seoul 06724, South Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.9.1666 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

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

국가의 인프라에 대한 사이버공격(Cyberattacks)과 사이버테러(Cyberterrorism)는 사이버무기를 이용하여 공격받고 있다. 2009년, 2010년 스턱스넷(Stuxnet)과 듀크(Duqu) 등의 사이버공격 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. 사이버침해 사고로 인한 남한의 경제적 피해 규모는 연간 3조6000억원으로 추정된다. 이는 자연재해 국내 피해액 2조7000억원보다 훨씬 많은 금액이다[2].

세계의 분쟁지역은 물론 국가 간의 이익이 충돌하는 곳에서는 사이버테러가 발생하고 있다. 사이버테러는 국가 간 전쟁의 전초전으로서, 눈에 보이지 않는 사이버전쟁(Cyberwarfare)으로 확대되면서, 국민과 사회 및 국가의 안보에 큰 위협이 되고 있다[3].

사이버세계의 기술은 복잡·고도화되어가고 있고 시공간의 제약이 적으며, 국경이 모호한 사이버세계의 특징이 있다. 따라서 사이버범죄와 사이버테러에 대응하여 정부부처와 민간 단독으로 침해사고에 대응하기에는 한계가 있다[4].

사이버범죄와 사이버테러는 현실에서 국가질서에 혼란을 야기 시키며, 국민의 행복을 파괴한다. 사이버테러는 사이버전쟁으로 확대하기 위한 기반 작업이다. 현재 수행되고 있는 국가 간의 전쟁을 분석해 보면, 제4차 세계대전은 사이버전쟁으로 촉발될 것이다.

사이버전쟁을 위한 사이버공격과 사이버테러는 점과 시간과 공간으로 연결된 디지털 컴퓨팅(digital computing)으로 작동되며, 국가 안보 및 국민의 안전을 파괴하는 행위의 결과로 나타난다.

특히 북한의 비대칭전력으로서 남한에 대한 사이버공격은, 공격원점지 파악의 어려움과 사이버공격이 눈에 보이지 않는 점을 이용하여, 사이버전쟁을 목적으로 사이버테러를 확대할 수 있는 실정이다.

국가 사이버안보(National Cybersecurity)를 책임지는 국방망, 전장망은 사이버로 연결되어 정보통신을 하고 있으며, 사이버보안(Cybersecurity)은 국가 사이버안보의 필수적인 요소이다. 따라서 국방망, 전장망을 지키기 위한 사이버안보 조직과 예산이 있어야 하며, 사이버전시 상태로 확대 될 때, 사이버전 수행을 위한 근거가 되는 ‘(가칭)국가사이버안보법’과 제도가 반드시 필요하다.

현재 북한과 해외로부터 빈번하게 발생되고 있는 사이버공격-사이버테러-사이버전쟁에 대응하는 국가 차원의 아젠다(Agenda)와 사이버대응 매뉴얼(Manuals)과 신기술에 대한 연구가 필요하다.

또한 사이버공격-사이버테러-사이버전쟁에 능동적으로 대응하기 위한 수행조직과 예산을 투입 할 수 있는 근거인, 국가 사이버안보를 위한 법제도에 대한 연구가 필요하며, 본 논문에서는 국가 사이버안보를 위한 정책을 제안하고 법제도를 연구한다.

본 연구의 결과는 국가 사이버안보 정책을 바탕으로 ‘(가칭)국가사이버안보법’의 내용을 정립하는 기초자료로 활용될 것이다.

Ⅱ. 관련 연구

2.1. 사이버전쟁의 정의

“사이버전쟁”이란 사이버공격 및 사이버테러를 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. 국외 사이버테러와 사이버전쟁의 대응

국외 사이버테러와 사이버전쟁의 대응은 정부 주도로 이루어지고 있다.

미국은 사이버사령부가 모든 사이버전쟁에 대한 컨트롤타워 역할을 수행하여 민·관·군 기관의 지원을 받고 있으며, 육군·해군·공군에 다음에 제4전장으로 사이버전장을 규정하여 우주군과 함께 국가 안보를 위한 사이버전에 대응하고 있다.

중국은 인민해방군 총참모부가 사이버전쟁을 기획, 실행하며 민간기구를 통제하여 국가관리 차원의 광통신망과 IP를 제공받고 있다[5]. 2017년 개편된 중국의 인민해방군 체계는 육군·해군·공군·로켓군에 이어 전략지원부대를 구성하여 사이버전·전자전·군사용 인공위성 운용·사이버군·우주군의 임무를 수행하며, 해커 약 10만명을 운영하여 전 세계의 인터넷과 통신을 감청하고 해킹하여, 사이버 작전을 수행하는 임무를 수행하고 있다. 보이지 않는 세계에서 발생하는 사이버테러는 보이는 세계에서 발생하는 물리적 전쟁과 마찬가지로 대응을 해야 한다[6].

Ⅲ. 사이버공격 분석과 대응 활동 분석

3.1. 남북대치 상황에서 사이버공격 분석

북한은 조선인민군 총참모부 예하 정찰총국에서 사이버테러를 총괄하여 우수한 인력양성 및 사이버전쟁 연구를 지원받으면서, 비대칭 전력으로서 사이버공격과 사이버테러 및 사이버전쟁을 수행하는 것으로 분석되고 있다.

북한은 세계 수준의 사이버전쟁 능력을 보유하고 있으며, 핵심 비대칭 전력으로 사이버전쟁사를 육성하고 있다. 북한은 사이버전쟁을 핵미사일과 함께 핵심 비대칭 전력으로 이용하여, DDoS, 지능형 지속공격(Advanced Persistent Threat APT), 역추척 방지 등 다양한 공격수단 보유하여 사이버전쟁의 종합능력은 세계5위 수준으로 판단하고 있다[7].

남한에서는 2009년 7.7 DDoS 공격, 2011년 3.4 DDoS 공격, NH농협전산망 마비, 2012년 중앙일보사고, 2013년 3.20 사이버테러로 인한 KBS, MBC, YTN, 신한은행, NH농협 등에 대한 APT공격으로 사이버테러가 발생하여, 대량의 컴퓨터가 작동이 마비되어 피해가 발생하였고, 전국규모의 은행전산망 마비사태가 발생하였고, 2013년 6.25 사이버테러 청와대 홈페이지가 해킹되어 '통일대통령 김정은'의 문구가 게시되었고, 2014년 1월 롯데카드, KB국민카드, NH농협카드 등 3사의 약 8500만명 개인정보유출사건, 2014년 5월 KT에서 약 1200만명 개인정보유출사건이 발생하였다. 2014년 12월 한국수력원자력이 관리하는 '원전안전해석코드(SPACE)'와 같은 원자력 핵심기술이 포함된 원전자료가 해커로부터 유출되었다[8].

또한 2015년 세월호 사고와 함께, 안드로이드 악성앱과 악성 루머를 퍼뜨렸으며, 2015년 5월 인터파크의 약 2500만 건 회원정보를 탈취하였고, 2016년 8월 국방통합데이터센터(DIDC)의 백신중계서버가 해킹공격을 받아 남한의 국방망을 해킹하였다.

북한은 비대칭전력으로 남한에 대한 사이버공격을 감행한다. 사이버공격도 기반시설에 대한 중단 및 파괴를 통해, 전통적 전쟁과 마찬가지로 사상자가 발생할 수 있고, 정보시스템과 주변 장치들을 못 쓰게 하면서 전체 기반시설에 심각한 장애를 가져다 줄 수 있기 때문이다[9].

3.2. 남한의 국내 · 외 사이버안보 활동

남한의 사이버안보는 평시에 국가정보원을 중심으로 컨트롤타워를 구성하고 있다. 국군사이버사령부가 사이버전쟁을 대비하여 활동하고 있다. 정부기관의 사이버시스템에 관해서는 행정자치부가 맡고 있으며, 민간분야는 인터넷진흥원(KISA)를 중심으로 하는 미래창조과학부가 사이버보안 분야를 담당하고 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 사이버이슈 관련 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. 서울 총회에서는 '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, 사이버공격과 범죄에 대응할 수 있는 견고하고 효과적인 파트너십의 필요성, 사이버 역량강화 필요성을 연설하였다[10].

3.3. 세계 각국의 사이버공격과 피해

세계 각국은 자국의 이익을 위해 국경 없는 사이버공격을 수행하고 있으며, 갈등이 커질 때에는 사이버테러와 사이버전쟁을 수행하고 있다.

각국의 사이버전 역량을 비교/분석 할 수 있는 명확한 기준이 없어 적을 알 수 있는 각국의 사이버전 역량을 알기에는 상당히 제한적이다[11].

북한과 같은 공산주의는 정부주도로 사이버공격을 포함한 작전을 수행하고 있으며, 민주주의를 표방하고 있는 국가들도 자국의 이익을 위해서 군과 정보기관을 중심으로 작전을 수행하고 있다.

표 1은 사이버공격으로 인한 세계 각국의 피해 내용을 표시하였다.

3.4. 사이버전쟁 대응 아젠다와 매뉴얼 및 신기술

북한으로 추정되는 사이버공격과 사이버테러가 남한의 안전을 위협하고 있고, 세계 각국도 자국의 이익을 위해 국경 없는 사이버전쟁을 벌이고 있다.

따라서 남한은 사이버테러와 사이버전쟁에 대한 대응정책을 발굴하고 국가 사이버안보를 위한 아젠다를 마련하여 매뉴얼식의 대응을 해야 한다.

대한민국은 사이버테러와 사이버전쟁에 대응하는 컨트롤타워를 대통령 직속의 상설위원회 (가칭)국가사이버안보위원회를 두고, 사이버수석과 외교안보수석과 국군사이버사령부와 국가정보원 및 KISA와 전문가 집단들이 실시간 대응을 할 수 있어야 한다.

국가 사이버안보를 위한 대응체제를, 실시간 상설조직으로 구축하고, 국군과 정부와 공공기관 그리고 민간의 클러스터로 구성된 사이버전쟁 대응 전문인력과 전문기술을 연구하여 확보하고 신기술을 계속 개발하여야 한다.

사이버전쟁장은 은닉성, 익명성을 가진 사이버무기로 침투가 발생된다. 사이버전쟁장의 특성은 평시와 전시, 전방과 후방, 시간과 공간의 구분이 모호하고, 물리적 실제에게 피해를 나타내야 만, 전장으로 인식되므로, 사이버침투가 발생하면 즉시 사이버전쟁 대응 매뉴얼이 작동되어야 한다.

사이버공격과 사이버테러가 발생하게 되면, 평시(1단계)-주의(2단계)-경계(3단계)-테러(4단계)-전시(5단계)의 단계별로 대응 매뉴얼을 민·관·군 별로 만들고 민·관·군의 매뉴얼 별로 대응하여야 한다.

만약 사이버테러(4단계)-전시(5단계) 단계가 발령되면 민·관·군은 합동으로 작전을 전개해야 하며, 사이버

Table. 1 Worldwide damages caused by cyberattacks

year	Operation Country	Contents of damage caused by cyber attack
2016	Russia	US Democratic National Committee (DNC) Information Disclosure
2015	China	US federal officials 21.5 million information outflows
2014	Russia	US White House Computer network Penetration
2014	North Korea	US Sony Pictures attack • Information leak
	USA	North Korea Labor Newspaper Website Paralysis
2013	North Korea	Korean Broadcasters • Financial Institutions 3.20 • 6.25 Cyberterror
2012	Iran	US financial firm attacks Israeli government
2011	North Korea	Korea NH Agricultural Cooperation Network Paralysis
2010	USA	Iran Stuxnet nuclear uranium facility destruction
2008	Russia	Gurusia homepage tampering, DDoS attack paralysis
2007	Israel	Syria's air defense network neutralized
2007	Russia	Estonian DDoS attack Internet paralysis
2001	USA	Iraq information system, command communication network disablement
1993	USA	Disabling Serbian network infrastructure
1991	USA	Iraq war information network, disturbance of air defense network, psychological war

전쟁(5단계)이 발령되면 대통령의 직접적인 지시를 받는 국군사이버사령부와 합동참모본부에서 직접 작전을 수행해야 한다.

사이버테러가 발생하여도 인터넷 네트워크와 물리적 망(network)분리가 되어 안전하다고 강조하나, 내부자에 의한 정보유출이나 신기술과 사회공학적방법이 적용된 사이버공격에 대응하기에는 미흡하며, 신기술에 의한 취약점이 발견되기도 한다.

실제로 남한의 네트워크에 대한 물리적 망분리 상황에서도 한국수력원자력(2014년), 국방망(2016년)이 북한으로 추정되는 해킹공격을 당했으며 취약점이 발견되었다.

사이버전쟁을 위해서는 새로운 사이버공격 패턴과 기술에 대비하여야 한다. 전자공격을 위한 EMP 공격(Electromagnetic Pulse attack) 방호시설 구축, 전파교란을 위한 GPS(Global Positioning System), 전자교란, 통신 재밍, 양자 암호화(Quantum Cryptography)와 같은 고기밀성의 암호장비, 해킹 역추적 기술, 사이버공격의 원점지 식별 및 타격, 해외 국가와 사이버 동맹 및 정보공유 강화, 주변국과 사이버정책과 기술 수집 및 분석 등 전문적이고 경험적인 실전 기술을 개발하고, 실전에 운용할 수 있도록 대비해야한다. 또한, 국군은 사이버무기체계를 갖추고, 사이버무기를 다룰 사이버전사와 사이버전 전문가를 양성하여야 한다.

Ⅳ. 국가 사이버안보를 위한 법 · 정책

실제로 사이버테러와 사이버전쟁에 대응하기 위해서는 국가 사이버안보를 위한 '(가칭)국가사이버안보법'이 국회에서 통과 되어야 하며, 법을 뒷받침하기위한 정책과 제도가 만들어져야 한다.

'(가칭)국가사이버안보법'과 같은 법률과 제도가 뒷받침이 되어야 만, 사이버테러와 사이버전쟁에 대응하고, 임무를 수행하는 예산과 조직이 확보되는 근거 법률이 된다.

4.1. 국가 사이버안보를 위한 전략

현재 국가 사이버안보를 총괄하는 법률이 없고 부문별로 정보보호를 정한 법률들이 산재하여[12] 국가적 사이버안보의 정책과 입안을 위한 국가 사이버안보의 용어와 원칙의 정립이 필요하다.

국가의 인프라를 담당하는 주요정보통신기반시설뿐만 아니라 국민의 생활과도 직접 연결되는 사이버인프라의 기술과 운영의 표준화를 위한 가이드라인과 용어의 정립이 필요하다.

또한, 국가에 대한 사이버테러 위협 대응 및 관리를 위해 관련된 사이버테러 및 국가 정보의 운영에 대한 컨트롤타워를 통한 일관된 실시간 사이버대응이 필요하다. 즉 현실세계로 연결된 사이버공간에 대한 사이버테러를 현실세계의 대한 테러와 동일한 수준으로 대응하고 법적 효력과 당위성을 발생시킬 수 있는 실시간 대응시스템에 대한 컨트롤타워의 역할이 필요하다.

국가 정보공유 체계 정립위해서는 사이버공격과 사이버범죄, 사이버테러와 사이버무기 기술 정보는 물론 사이버취약점 정보까지 정보를 보안등급 별로 구분하고, 보안 관리를 하여, 사이버안보를 위한 정보의 저장과 배포 및 공유와 확산을 위한 국가 사이버안보 정보공유 체계를 정립해야 한다.

국가사이버안전관리규정상 국가정보원 역할의 법령상 근거가 공공망에 한정하므로, 국가사이버안보 차원의 사이버위협정보 공유의 확대 및 규정 이 필요하다.

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

현재 국가사이버안보 합동 대응으로 대한민국은 평시에 사이버보안은 국가정보원을 중심으로 18개 기관이 참여하는 민·관·군 합동대응팀을 구성·운영 중이다.

하지만, 대통령훈령인 '국가사이버 안전관리규정'에 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 사이버안보 대응에는 한계가 있다.

따라서 국가차원의 사이버안보 합동대응을 강화하고 관련 유관기관과 연계기관의 역할을 정책과 매뉴얼식의 총체적인 대응에 필요한 국가 사이버안보 합동 대응이 필요하다.

더불어 국가 사이버안보를 위해서는 외국과의 국가사이버안보 공조 대응을 위해, 사이버버공격, 취약점, 기술, 전문가, 수사 및 처벌에 대한 국제 공조를 수행하

여, 세계 각국과 사이버안보를 위한 규범을 식별하고, 사이버범죄와 사이버테러 및 사이버전쟁에 대비한 국제 공조가 필요하다.

사이버안보무기와 운영체제 기술 연구개발도 필요하다. 사이버기술과 사이버인프라의 발달과 함께, 사이버공격은 지능화되고 사회공학적방법을 동원한 조직적인 APT 공격으로 공격목표와 공격대상에 따라서 고도화 전문화 되고 있다. 따라서 사이버무기도 맞춤형 공격에 대응하는 맞춤형 방호형으로 연구개발 되어야 한다. 특히 사이버무기와 사이버방호를 위한 운영체제는 실시간으로 작동되어야 하므로, AI(Artificial intelligent)을 활용한 사이버공격-방호 자가 학습 및 기술의 집적화를 해야 한다. ICT 기술의 발전과 사이버응용 범위의 확대에 따라 제4차 산업혁명의 IoT, Drone, AI 등을 활용한 맞춤형 목표물 선정과 사이버무기 운영체제에 대한 맞춤형 방호시스템을 갖추기 위한 기술 연구개발에 예산과 조직을 확보하여야 한다.

사이버안보 전문 인력 양성은 사이버안보에 관한 가장 중요한 요소이며, 사이버무기를 개발하고 운영하고 통제하고 방호할 수 있는 가장 중요한 요소가 사이버안보 전문 인력이다. 따라서 사이버안보 전문 인력의 양성은 가장 필수적인 요소이며, 초등학교 방과 후 특기수업, 중·고등학교 인재 발굴 및 대학 학부에서 전문 인력 부사관-사관제도로 전문 인력이 양성되어 국군에서 주특기 전사로 근무하면서 경험과 기술을 확대한다. 군 간부는 대학원과정에서 사이버안보의 정책과 제도를 연구하여, 석사-박사를 보유한 사이버안보의 전문가와 사이버전사로서 전문 인력을 양성한다.

전문 인력을 양성 시, 국군사이버사령부 운영과 정책으로는 국방부 직속으로 국군사이버사령부를 두고 합동참모본부와 국방 사이버전쟁의 기획 및 계획 수립, 국방 사이버전쟁의 시행, 국방 사이버전쟁을 수행할 전문 인력의 육성과 기술 개발한다.

평시에는 사회의 군의 사이버범죄와 연관된 기술들을 습득하여 처리하고, 경계경보 이상에서는 민·관·군의 합동으로 사이버테러에 대한 방호를 한다. 최종적으로 국방 사이버전쟁을 대비한 부대 훈련, 국방 사이버전쟁 유관기관 사이의 정보 공유 및 협조체계 구축하여, 국방 사이버테러와 사이버전쟁을 수행한다.

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

- ▹(국군사이버사령부 설치법)제정으로 민·관·군 통합 사이버전쟁 수행의 기반 마련 및 정부의 예산을 확보한다.
- ▹(조직운영·편제) 임무형 T/F중심의 운영을 통해 신속한 국가사이버전쟁의 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 사이버전쟁에 적합한 최적의 인재 POOL구성 및 정원 확대(선발권) 충원 후 전문기관(학교, 연구소)연계 및 해외 활동을 통한 지속적 인재 양성교육을 수행한다.
- ▹(처우개선)24시간 사이버전쟁 수행 및 관련 연구 활동에 전념할 수밖에 없는 직무 특성상 우수 인재의 처우 개선 필요(별도 수당 지급 법제화)하다.
- ▹(사업 예산 보장) 사이버전쟁 특성상 은밀성, 익명성, 적시성(24시간)을 위한 영외 활동 보장 및 관련 경비의 지원(특수 사업비 집행 법적 제도화)이 필요하다.
- ▹(정보요구권) 사이버테러와 전쟁 시 대비 신속한 피·아 식별을 위한 유관기관에 정보요구 시 최단시간 자료 제공을 의무화할 필요가 있다.

또한 국가사이버(안보) 조직의 구성으로 대통령 직속으로 장관급의 사이버위원회를 구성하고, 사이버수석과 외교안보수석을 중심으로 사이버위원회 산하에 중앙행정기관의 1급~2급에 해당되는 독립부서의 사이보안보국을 만들어 운영한다.

사이버범죄와 사이버테러의 은닉화, 조직화, 대형화에 따라 사후 대응만으로는 국가인프라와 국민의 실생활보호에는 한계가 있다.

공격 전조현상을 분석해야 하고, 공격 침해사고가 발생되면, 정보통신망 수색 및 범죄단서 포착하여 원격지에서 온라인수색을 통해 사이버해킹을 수사방안을 마련해야 한다.

국가 사이버인프라에 대한 취약점을 악용하거나, 악성코드 감염(좀비)PC의 확산 방지를 위한 처벌 규정의 정비가 필요하다.

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, 감염 PC의 인터넷 접속 차단 및 백신 설치 유도, 인터넷 사업자의 로그보존 의무 명시 등의 규정의 보완이 필요하다.

육군·해군·공군·해병대의 무기체계는 각 군과 합동참모본부를 통해 사이버로 연계되어 있으며, 국군의 모든 행정망, 국방망, 전장망도 사이버로 연계되어 있다. 따라서 물리적 전쟁을 계획하거나, 수행하거나, 작전을 하려면 반드시 사이버군이 필요하며, 미국, 중국과 마찬가지로 사이버전장을 규정하고 사이버무기의 개발과 운영 및 사이버작전을 수행하여야 한다.

국군도 사이버군을 정규편성하고, 사이버전장에 대비한 전용 Secure Network Protocol을 운영하여, 4차 산업혁명의 기술들을 응용하여 사이버방호를 해야 하며, 사이버무기를 제도화하여 분기별로 점검하고, 연구 및 기술개발을 통해 실전에 배치하고, 사이버전투에 대한 시뮬레이션을 진행하고 사이버기술을 발전시켜야한다.

4.2. '(가칭)국가사이버안보법'[5]의 제안

국가 사이버안보를 위한 '(가칭)국가사이버안보법'의 주요 방안은 다음과 같다.

◈ 국가 사이버안보에 관한 법률(안)

박대우는 2013년 5월 14일에 국회 발표에서 국가사이버안보에 관한 법률(안)을 제안[2]하였으며, 2015년에도 법률안의 당위성을 주장하였다.

'(가칭)국가사이버안보법'은 다음과 같다.

(목적) 이 법은 국가차원에서 사이버공격과 사이버테러를 탐지하고, 사이버테러 및 전쟁 발생 가능성을 조기에 차단하며, 사이버테러 및 전쟁 발생 시 국가 사이버안보 역량을 결집하여 신속히 대처함으로써 국가와 국민의 안전보장과 이익보호에 이바지함을 목적으로 한다.

(정의) 다른 법률과의 관계, 국가사이버안보위원회의 설치, 민·관·군 협의체의 구성, 조직 운영 및 예산 편성, 국가사이버테러 및 전쟁관리종합계획 수립 등, 사이버테러 및 전쟁관리지침 이행 확인 및 보고, 사이버안보대응센터의 구축운영, 대응활동, 사고조사, 훈련, 사이버테러경보의 발령, 사이버테러대책본부의 구성, 연구개발 및 기술이전, 전문인력양성 및 인력확보, 정보분석 및 공유와 정보확산, 국제협력, 비밀엄수의 의무, 포상, 벌칙을 제1조부터 제21조까지 제안[5]한다.

4.3. 국가 사이버안보와 관련된 법률 개정 필요항목

'(가칭)국가사이버안보법'이 국회에서 통과되고 시행된다면, 관련하여 다음의 법률과 항목들도 개정되어야 효율적인 국가 사이버안보를 이룰 수 있다.

개정해야 할 관련 내용은 다음과 같다.

- 정보저장·분배·공유·확산 체계 정립.
- 사이버테러 위협 대응 강화.
- 국가차원 합동대응 강화.
- 국군사이버사령부령(안) 입법.
- 정보통신기반 보호법 시행령 개정(안).
- 형사소송법 개정(안).
- 적극적 사이버범죄 단서 수집 근거(안).
- 실체법 규정 정비.
- 악성코드 방지법 제정 검토.

Ⅴ. 결 론

본 논문은 북한과 해외로부터 사이버공격을 분석하고, 현재 법률이 정한 주요정보통신기반시설 보호를 위하여, 안전한 사이버공간 구축 및 운영을 위한 국가 사이버안보 전략을 연구하였다.

사이버테러와 사이버전쟁에 대한 피해의 연구를 통해, 국내·외의 사이버안보 활동과 사이버전쟁 대응 아젠다와 매뉴얼의 필요성 및 신기술을 나열하였다.

국가 사이버안보 전략으로 국가 사이버안보 용어와 원칙 정립, 국가 사이버테러 위협 대응, 국가 정보공유체계 정립, 국가 사이버안보 합동 대응, 외국과의 국가 사이버안보 공조 대응, 사이버 안보무기와 기술 연구개발, 사이버안보 전문 인력 양성, 국군사이버사령부 운영과 정책, 국가 사이버인프라 보안의 조직 구성, 국가 사이버 인프라의 범죄 처벌 규정 정비, 물리적 전쟁과 사이버전쟁의 연계를 연구하였다. 또한 (가칭)국가사이버안보법과 관련된 법률 개정(안)을 연구하였다.

본 논문은 세계적인 사이버강국으로 탈바꿈하기 위한 기초자료로 활용될 것이다.

REFERENCES

[1] D. W. Park, “National Cybersecurity Policy Report,” National Cyber Security Policy Forum, Dec. 2012.

[2] D. W. Park, “National Cybersecurity Law Proposal,” National Assembly, May 14, 2013.

[3] D. W. Park, “National Cybersecurity Policy Forum,” National Assembly, July 18, 2014.

[4] D. W. Park, Global Economics, “Necessity of National Cybersecurity Law,” Sep. 07, 2016.

[5] D. W. Park, “Draft of National Cybersecurity Act,” *International Journal of Security and Its Applications*, vol. 9, no. 11, pp. 105-112, Nov. 2015.

[6] C. Y. Choi, D. W. Park, “The Analysis of the APT Prelude by Big Data Analytics,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 20, no. 6, pp. 1129-1135, Jun. 2016.

[7] Ministry of National Defense, “Presidential Decree”, No. 26101, Feb. 16, 2015.

[8] D. W. 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.

[9] I. J. Kim, “Cyber security strategy against cyber threat,” National Security Research Institute, Blue Today, [Internet]. Available: http://www.bluetoday.net/news/articleView.html?idxno=11112.

[10] S. H. Ham, D. W. Park, "National Cybersecurity Policy Preparing for the Unification of North Korea and South Korea", *in Proceeding of Conference on Korea Institute of Information and Communication Engineering*, KOREA, vol. 20, no. 2, pp. 185-190, Oct. 2016.

[11] C. S. Park, Y.S. Park, “A Study on the Improvement of Capability Assessment and the Plan for Enhancing Cyber Warfare Capability of Korea”, *Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, no. 5, pp. 1251-1258, May 2015.

[12] S. D. Park, I. J. Kim, “A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity,” *Convergence Security Journal Korea Information Assurance Society*, vol. 13, no. 4, pp.3-10, Sep. 2013.

함승현(Seung-hyeon Ham)

2006.08 서울디지털대학교 행정학 전공 행정학사
2010.02 가천대학교 전자거래학 전공 공학석사
2015.03 ~ 현재 : 호서대학교 벤처대학원 융합공학과 박사과정
2012.11 ~ 2017.07 대한민국예비역부사관총연합회 수석부회장
2013.03 ~ 2017.06 민주평화통일자문회의 자문위원
2013.03 ~ 현재 : 민주평화통일자문회의 자문위원
1982.09 ~ 현재 : 서울교통공사
※관심분야 : 국가사이버안보, 사이버전쟁

박대우(Dea-woo Park)

1998년 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 : 숭실대학교 겸임교수
2006년 : 정보보호진흥원(KISA) 선임연구원
2007년 ~ 현재 : 호서대학교 벤처대학원 교수
※관심분야 : 사이버안보, Hacking, Forensic, CERT/CC, 침해사고 대응, e-Discoverty, 네트워크 보안, 스마트폰 보안