사이버안보 추진체계의 제도적 개선과제 연구

박상돈* · 김인중*

요 약

사이버공격은 단순 범죄의 차원을 넘어 테러의 성격을 보이고 있으며 국가안보를 위협하고 있다. 오늘날 사이버안보 위협 양상은 국가 기밀과 개인정보의 유출 및 확산, 기반시설 제어시스템에 대한 직접적인 공격의 현실화, 정치·사회적 목적을 지닌 핵티비즘 대두 등으로 나타나고 있으며, 한국의 경우는 남북분단에 따른 북한의 위협이라는 특수한 상황이 더해져 있다. 따라서 사이버공격을 국가안보적 측면에서 다루면서 사이버안보 추진체계를 점검하고 문제점을 확인하여 개선해야 한다. 정부는 국가 사이버안보 종합대책을 발표하는 등 노력을 기울이고 있으나 제도적으로 미흡한 점이 있다. 사이버안보 추진체계의 제도적 개선을 위한 과제로는 관계부처·기관 역할의 법적 근거 정비, 국가차원 합동대응 강화, 정보공유 체계 정립 및 활성화, 산업육성 및 인력양성을 통한 기반조성, 연구개발 강화를 통한 방어수단 확보 등이 있다. 이러한 과제를 해결하기 위해서는 관련 법률의 제·개정에 많은 관심을 기울이고 법제도 개선을 실천하여야 한다.

A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity

Sangdon Park* · Injung Kim*

ABSTRACT

Cyber attacks are threats to national security. Today, cybersecurity threats have various types, the theft or spread of privacy and national secret, the realization of direct attacks to infrastructure and the hacktivism with political or social objectives. Furthermore, There are special situations in South Korea because of North Korea's threats. Thus, It is necessary to handle cybersecurity as a kind of national security problem. It is a time to identify problems of governance system in cybersecurity and to improve related Acts and subordinate statutes. There are several tasks for legal improvement for governance system in cybersecurity. They are improving legal bases for the roles of the relevant authorities in cybersecurity, consolidating national joint response to cyber accidents, establishing and vitalizing information sharing system, constructing foundation of cybersecurity through industry promotion and manpower development, and acquiring defensive tools by enhancement research an development. In order to address these challenges, it is necessary to pay much attention to enactment and to revision laws and to practice legislative procedure.

Key words : 사이버안보 추진체계, 사이버안보 법제도, 국가 사이버안보 종합대책, Governance System in Cybersecurity, Cybersecurity Law, National Cyber Security Comprehensive Countermeasures

접수일(2013년 7월 11일), 수정일(1차: 2013년 9월 13일), 게재확정일(2013년 9월 23일)

* 한국전자통신연구원 부설연구소

1. 서 론

오늘날 사이버공격은 단순 범죄의 차원을 넘어 테러의 성격을 보이고 있으며 국가안보를 위협하고 있다. 이는 물리적 테러와 같은 정도의 위협으로 다가오고 있다. 미국 하원 국토안보위원회 위원장 Mike McCaul 의원은 2013년 4월 발생한 보스턴 폭탄테러를 언급하면서 “우리는 디지털 폭탄에 대해서도 스스로 무장을 갖출 필요가 있다.”라고 주장한 바 있다[1].

사이버공격은 그 파급력이 미치는 범위가 사이버공간 내에 한정되지 않고 물리적 공간에까지 영향을 미치고 있다. 그리고 공격 대상은 개인뿐만 아니라 사회, 나아가 국가 전체에까지 확대되고 있다. 이는 사이버공간에 대한 위협 문제를 국가안보 차원에서 바라보아야 하며, 보안의 문제에 그치는 것이 아니라 안보의 문제로 바라보아야 하는 지경에 이르렀다.

정부는 사이버안보 강화를 위한 계획과 대책들을 마련하고 시행하여 왔으나 2013년에도 3.20 사이버테러와 6.25 사이버공격이 발생하는 등 여전히 사이버안보가 위협받는 상황이 발생하고 있다. 그 원인으로는 추진체계가 아직 제대로 정비되지 못하고, 특히 이를 뒷받침하는 법제도적 개선이 제대로 이루어지지 않고 있는 점을 들 수 있다.

이에 따라 사이버안보위협 현황을 진단하고 사이버안보 추진체계 개선과제를 법제도적 측면에서 검토하는 것이 필요한 시점이다.

2. 사이버안보위협의 현황

2.1 사이버안보 위협의 대두

사이버안보 위협 양상은 다음과 같다.

첫째, 오늘날 국가 기밀과 개인정보가 사이버공간을 통해 유출되고 및 공개되기를 원하지 않는 정보가 널리 확산되는 경우가 증가하고 있다. 중국 해커의 소행으로 추정되는 미국의 주요 무기시스템 설계안 해킹이 대표적인 사례이다[2].

둘째, 에너지·수자원·교통 등 대다수 국민의 일상생활과 밀접한 관련이 있고 국가적인 중요성을 지닌 기반시설 제어시스템에 대한 직접적인 공격이 현실화되었다. 이는 스턱스넷과 같은 고도화된 컴퓨터 바이러스 등장이 만들어낸 결과이다. 스턱스넷은 이란 원자력 발전소를 마비시키는 등 그 위력을 과시하였으며, 유사 악성코드인 듀큐도 등장하면서 산업기반시설 보안에 우려가 높아지고 있다[3].

셋째, 공격자 개인의 흥미 충족 또는 금전 탈취 등의 목적이 아니라 정치·사회적 목적을 지닌 사이버위협이 증가하여 핵티비즘이 대두되고 있다. 핵티비즘은 인터넷이 일반화되면서 새로 생겨난 정치적·사회적 행동주의이며, 단순하게 보안 시스템을 무력화해 해킹실력을 과시하던 것에 그치지 않고 목적을 이루기 위해 적극적이고 다양한 활동을 벌이는 것이 특징이다. 해커집단 어너니머스는 대표적인 핵티비즘 단체 중 하나이다[4].

2.2 한국의 사이버안보 위협 상황

한국은 전세계적으로 사이버공격의 주요 관련국으로 추정되는 중국, 러시아 등과 인근에 있는 지리적 위치에 있으며, 이에 따라 이들 국가와 국익이 얽혀있는 관계에 있다. 또한 남북 분단이라는 특수한 상황하에 북한이라는 주적과 마주하고 있다. 이에 국가안보와 밀접한 관련이 있는 사이버공격이 종종 발생하고 있다. 최근 3년간 발생한 국가안보 위협 공격의 주요 사례는 다음과 같다.

2011년 3월 3.4 디도스 공격이 발생하여 국내 40여 개 주요기관의 인터넷 웹사이트에 접속 장애가 있었다. 경찰은 북한의 소행으로 밝혀진 바 있는 2009년의 7.7. 디도스 공격 당시 사용된 것과 동일한 IP가 사용된 점을 확인하여 북한의 소행으로 추정된다고 발표했으며[5], 해외의 보안업체도 공격대응능력을 정찰하기 위한 북한의 소행으로 보인다는 보고서를 발표한 바 있다[6].

같은 해 4월에는 농협 전산망 마비 사건이 발생하였다. 전산망 관리업체 직원의 노트북을 좀비PC로 활용하여 농협 전산망 마비되었으며, 검찰 조사결과 북한 정찰총국이 주도한 사이버테러로 확인되었다. 좀비PC가 된 노트북을 통해 농협 전산망에 접근하고 최고관리자의 비밀번호 등을 유출한 뒤, 노트북에 공격 명령 파일을 설치해 실행한 것으로 알려졌다[7].

2012년 2월에는 기반시설 제어시스템에 대한 공격

시도가 적발되어, 북한 공작원과 접촉해 디도스(DDoS) 공격용 악성코드가 숨겨진 게임 프로그램을 국내로 들여와 유통한 혐의가 있는 내국인이 기소되었다. 용의자는 북한 정찰총국 공작원과 만나는 등 연락을 주고받으며, 불법 사행성 프로그램 제작 및 개발비 명목으로 수천만원 지불하였고, 자신의 인터넷 게임 서버가 북한의 디도스 공격에 활용되는 것을 알면서도 싼값에 게임 프로그램을 개발하기 위해 프로그램을 의뢰한 것으로 밝혀졌다. 검찰은 북한 공작원이 2,700여대의 컴퓨터에 악성코드를 감염시켜 좀비PC로 만든 뒤 인천공항 등에 사이버테러를 하려 한 사실을 확인하였다[8].

같은 해 6월에는 중앙일보에 대한 해킹 사건 발생한 바 있다. 공격자들은 중앙일보의 홈페이지를 변조하고 고양이 사진을 게시하였다. 또한 신문제작 시스템의 데이터가 삭제되어 신문 제작에 차질이 발생하였다. 경찰은 신문제작시스템과 보안시스템 접속기록, 악성코드, 공격에 이용된 국내 경유지 서버 2대와 10여개국으로 분산된 경유지 서버 17대 등을 분석한 결과 사이버테러 공격의 진원지로 북한을 지목했다. 경찰 조사결과, 북한 체신성 IP를 통해 중앙일보 사이트에 집중적인 접속이 시작된 시점은 같은 해 4월 21일로, 북한이 대규모 대남 규탄 집회를 열고 일부 언론사 등에 특별행동을 감행하겠다고 한 시기와 일치한다[9].

2013년 3월에는 3.20 사이버테러가 발생하여 주요 방송사 및 금융기관에 대한 사이버테러가 발생하였다. 또한 같은 달 대북보수단체 홈페이지 자료 삭제, YTN 계열사 홈페이지 자료서버 파괴 등 일련의 사건이 연이어 발생하였다. 이들 공격은 고난도 기술을 적용하여 국내 전력·금융·통신망을 목표로 이루어졌으며, 북한 내부에서 국내 공격경유지에 수시 접속한 흔적이 발견되었다. 민·관·군 합동대응팀은 3.20 사이버테러가 북한 정찰총국의 소행으로 추정된다는 조사결과를 발표하였다[10].

같은 해 6월에는 6.25 사이버공격이 발생하여 청와대와 국무조정실의 홈페이지가 위변조되고, 일부 언론사 홈페이지의 서버가 멈추거나 접속 불가상태에 빠지는 등 총 16개 기관에서 피해가 발생하였다. 이 사건은 6.25 전쟁 발발 63주년이자 정전 60주년의 6월 25일에 대대적인 해킹 공격이 나타났다는 정황상 남북한의 긴장관계와 무관하지 않을 것이라는 관측이 제기된 바 있다[11].

한국의 사이버공간 의존도를 감안하면, 북한의 사이버위협으로 인한 국가적 위기 발생의 가능성을 배제할 수 없다. 지금까지의 위협양상이 동시다발적으로 발생한다면 그 파급력이 클 수 있다. 따라서 사이버공격을 국가안보적 측면에서 바라보고 사이버안보 추진체계를 점검하고 문제점을 확인하여 개선해야 한다.

3. 사이버안보 추진체계 현황과 정부의 개선 노력

3.1 기존의 추진체계

한국의 현행 사이버안보 추진체계를 살펴보면 일상적 상황에서는 분산관리 방식을 적용하여 민(미래창조과학부)·관(국가정보원)·군(국방부)의 분야별로 역할을 분산하고, 국가안보 사안에 대해서는 국가정보원이 총괄하는 중앙통제방식을 적용하는 방식이다.

한국의 현행 관련 법률에 따른 추진체계는 분야별·보호대상별로 별개의 법령이 적용되고 있다. 현재 공공부문과 민간부문을 막론하고 주요정보통신기반시설에 대하여는 「정보통신기반 보호법」이 적용되며, 그 외에는 공공부문은 「국가사이버안전관리규정」, 민간부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 적용된다. 이와 같이 내용이 각 부문마다 상이한 법령들이 적용되고, 추진체계가 별도로 구성되어 있으며, 각 법률마다 주무부처도 다르다[12].

각종 사고에서 대응상 문제점이 나타나고 추진체계의 문제점이 지적됨에 따라 2011년부터 국가정보원·방송통신위원회·국방부·행정안전부·금융위원회 등 15개 관계부처·기관이 참여하여 수립한 국가사이버안보 마스터플랜에 의해 국가정보원 중심으로 민·관·군 합동대응체계 정립을 추진한 바 있다. 이에 따라 국가사이버안전센터를 중심으로 관계부처·기관간 협력·공조와 민간 전문가 참여를 확대하는 한편, 국가정보원의 컨트롤타워 기능과 부처별 역할을 명확히 하기로 하였다[13]. 국가사이버안보 마스터플랜은 관계부처·기관이 합동으로 논의하여 현행 법제도에 의한 추진체

계를 확인하고 어느 기관이 중심축 역할을 수행할지에 대한 합의를 이끌어냈다는 점에서 의미가 있다고 평가할 수 있다. 그러나 법제도 정비와 같은 후속조치가 미흡함에 따라 국가 전체적인 역량을 집결하는 효과가 기대만큼 이루어지지는 못하였다고 평가할 수 있다. 이에 따라 추진체계 개선을 위한 새로운 노력들이 다시 시도되고 있다.

3.2 정부의 추진체계 개선 노력

3.2.1 국가사이버안전 전략회의의 논의

3.20 사이버테러가 발생함에 따라 2013년 4월 정부는 국가정보원장 주관하에 국가사이버안전 전략회의를 개최하여 사건의 후속 조치와 사이버안전 강화 방안을 논의했다. 주요 내용은 다음과 같다. 첫째, 범정부 차원의 사이버안전 수행체계 개선·보완책으로서 청와대가 컨트롤타워 역할을 수행한다. 둘째, 민·관·군 합동대응팀'의 역할 및 기능을 강화하고, 사이버위기 상황 조기경보·전파체계를 점검·보완하며, 국가사이버안보전략을 마련한다. 셋째, 금융분야를 포함하여 민간분야의 보안대책을 강화한다[14].

3.2.2 국가사이버안보 종합대책 발표

국가사이버안전 전략회의에서 논의한 바를 현실화함과 동시에 6.25 사이버공격이 발생에 따른 대책을 보완하여 정부는 2013년 7월 국가사이버안보 종합대책을 발표하였다. 주요 내용은 다음과 같은 4대 전략(PCRC)이다[15].

첫째, Prompt, 즉 즉응성 강화이다. 사이버안보 컨트롤타워를 청와대가 맡고, 실무총괄은 국정원이 담당하며, 관계 중앙행정기관이 소관분야를 각각 담당토록 하는 대응체계를 확립한다.

둘째, Cooperative, 즉 유관기관 스마트 협력체계 구축이다. 국가차원의 '사이버위협정보 공유시스템'을 2014년까지 구축하고, 이를 토대로 민간 부문과의 정보제공·협력을 강화한다.

셋째, Robust, 즉 견고성 보강이다. 2017년까지 집적정보통신시설(IDC)·의료기관 등을 포함한 주요정보통신기반시설을 확대하고 국가기반시설에 대해 인터넷망과 분리·운영하는 한편, 전력·교통 등 테마별로 특화된 위기대응훈련을 실시한다.

넷째, Creative, 즉 창조적 기반 조성이다. 다양한 인력양성 프로그램을 추진하여 2017년까지 사이버 전문인력 5,000명을 양성하고, 10대 정보보호 핵심기술 선정과 연구개발의 집중적 추진으로 기술 경쟁력을 강화한다.

3.2.3 평가

2011년 국가사이버안보 마스터플랜의 수립 시기부터 정부는 사이버위협이 국가안보상 중대한 문제가 될 수 있다는 것을 이미 인식한 바 있다. 그리고 그러한 문제의식의 연장선상에서 국가사이버안보 종합대책이 이루어졌다고 할 수 있다.

국가사이버안보 종합대책은 추진체계 개선을 위한 타당한 대책들을 다수 제시하고 있으나 현행 법제도상 법적 근거를 갖추고 구현하기에는 어려운 부분이 없지 않다. 따라서 사이버안보 추진체계의 제도적 개선 과제를 구체적으로 확인하고 향후 법제도 개선에 반영할 필요가 있다.

4. 사이버안보 추진체계의 제도적 문제와 개선과제

4.1 관계부처·기관 역할의 법적 근거 정비

국가 사이버안보 종합대책에 의한 추진체계에서 청와대가 컨트롤타워를 담당하고 국가정보원이 실무를 총괄한다고 정하였으나, 현재의 법제도상 이를 뒷받침하기에 다소 부족한 점이 있다. 현재 사이버위협 문제에 관하여 국가정보원의 주요 규범으로서 적용되는 「국가사이버안전관리규정」은 법률 또는 법률을 구체화하는 시행령이나 시행규칙이 아닌 대통령훈령으로서 행정기관 내부에만 효력이 있고, 그 적용범위를 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망으로 명시하고 있어 민간부문의 정보통신망과 정보통신기반시설을 제외하고 있기 때문에[16] 실무 총괄의 근거로는 한계가 있다는 지적이 제기될 수 있다.

일찍이 18대 국회에서 국가사이버위기관리법안이 발의되어 이러한 법적 근거 미비를 해소하려는 시도

가 있었으나 입법에 실패한 바 있다. 한편 관계부처·기관들이 합동으로 국가사이버안보 마스터플랜을 마련하면서, 사이버위협 대응을 보다 효율화하기 위해 관련 법령의 정비를 추진하기로 하였으나 여전히 지지부진한 상태이다.

이와 같이 관련 법령의 정비가 미진함에 따라 집행력이 미약하고 대국민 효력을 발휘하기에 한계가 있어 왔다. 이러한 문제는 사이버안보에서 기본법 역할을 하는 법률의 부재가 근본 원인이다. 이는 단지 담당기관의 역할 문제에서 그치지 않으며, 이하에서 논의하는 여러 가지 다른 법제도적 개선과제가 파생되는 주요 원인으로 작용한다. 따라서 법률상 관계부처·기관이 수행하는 사이버안보 활동의 법적 근거를 명확히 정하고, 대통령훈령 등에 규정한 내용들을 법률의 형식으로 하여 다시 규정해야 한다.

4.2 국가차원 합동대응 강화

현행 법령에 의하면 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반을 설치·운영할 수 있으며, 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우에는 관계 중앙행정기관의 장과 협의하여 범정부적 사이버위기 대책본부를 구성·운영할 수 있다[16]. 한편 미래창조과학부는 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다[17]. 이와 별개로 정보통신기반보호위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부를 둘 수 있다[18].

이러한 법령 규정상 사고대응을 위한 합동대응시 공공부문과 민간부문의 체계가 별개이고, 정보통신기반시설의 체계는 이와 또 별개로 구성되어 있다. 사고발생시 공공부문은 국가정보원 주도의 민·관·군 합동대응반, 민간부문은 미래창조과학부가 주도하는 민·관합동조사단, 주요정보통신기반시설은 정보통신기반보호위원회가 주도하는 정보통신기반침해사고대책본부가 합동대응을 수행한다.

현재 국가정보원을 중심으로 18개 기관이 참여하는 민·관·군 합동대응팀을 구성·운영중이나 대통령훈령인 「국가사이버안전관리규정」에 근거하고 있어 임무·기능 및 권한에 한계가 있다.

따라서 국가차원의 합동대응을 강화하고 그에 따른 관계부처·기관의 역할을 명확히 법률에 정할 필요가 있다. 민·관·군 합동대응팀 운영을 법률에 규정하여 명확한 법률상 근거를 마련해야 한다.

4.3 정보공유 체계 정립 및 활성화

현재 사이버안보를 총괄하는 법률이 없고 부문별로 정보보호를 정한 법률들이 산재하여 정보공유 체계가 불완전한 상태이다. 법령 규정상 정보공유체계가 공공부문과 민간부문의 체계가 별개이며, 정보통신기반시설의 체계는 이와 또 별개이다.

현행 법령에 의하면 공공부문의 경우 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가정보원장에게 통보하여야 한다. 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 보안관제센터를 설치·운영하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 국가정보원 등 다른 중앙행정기관의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다. 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다[16]. 민간부문의 경우 주요정보통신서비스 제공자, 집적정보통신시설 사업자, 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자는 침해사고 관련 정보를 미래창조과학부나 한국인터넷진흥원에 제공하여야 하고, 침해사고가 발생하면 정보통신서비스 제공

자, 집적정보통신시설 사업자는 즉시 그 사실을 미래창조과학부나 한국인터넷진흥원에 신고하여야 한다[17]. 주요정보통신기반시설의 경우 주요정보통신기반시설 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 그 사실을 통지하여야 하고, 금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 취약점 및 침해요인과 그 대응방안에 관한 정보 제공, 침해사고의 실시간 경보·분석체계 운영을 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다[18].

이와 같이 부문별로 정보공유체계를 관장하는 기관이 다르고, 공공부문과 민간부문 및 주요정보통신기반시설의 정보공유체계가 일원화되어 있지 않기 때문에 정보가 원활히 교류되지 않을 소지가 있다. 국가사이버안보 종합대책에서 제시한 국가차원의 정보공유시스템 구축은 적절한 대책이지만 현행 법제도를 근거로 하여서는 조화롭게 이루어지지 않을 소지가 많다. 따라서 공공기관간, 민간기업간, 그리고 공공과 민간을 모두 아울러 정보공유가 원활이 이루어질 수 있도록 부문별 구분없이 정보수집·분석 역량을 갖춘 기관이 책임지는 정보공유 체계를 수립하고 정보공유의 활성화를 제도적으로 보장할 필요가 있다. 단일 체계에 의한 보안관제센터 운영과 관리, 그리고 그러한 보안관제센터를 통해 수집된 정보가 신속히 전파되고 경보발령에도 활용되도록 법률에 규정해야 한다.

4.4 산업육성 및 인력양성을 통한 기반조성

현재 관련 법률에서 정한 인력양성 관련 내용은 안보적 관점이 결여되어 있거나 선언적 수준에 그치고 있다. 민간부문의 경우는 인력양성에 관하여 비교적 구체적으로 정하고 있으나, 그 대상을 정보통신망 응용서비스의 개발에 필요한 기술인력 양성이라고 규정하여[17], 보안에 초점을 맞추지는 않았다. 또한 주요정보통신기반시설 보호의 경우 단지 전문인력 양성에 관한 시책을 강구한다고 정할 뿐이다[18].

따라서 관련 기업 및 교육기관 등의 의견을 수렴하여 보다 실질적인 정책효과를 구현할 체계를 마련할 필요가 있다. 산업육성 및 인력양성을 책임지고 담당할 정부부처와 유관기관을 법률상 명시하고 어떠한 절차를 통해 추진할 것인지 정해야 한다.

4.5 연구개발 강화를 통한 방어수단 확보

현재 연구개발 관련 규정은 개발가능한 모든 연구개발 분야에 대해 규율하지 못하고 있다. 민간부문의 경우 미래창조과학부는 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 관련 연구기관으로 하여금 연구개발·기술협력·기술이전 또는 기술지도 등의 사업을 하게 할 수 있으며, 정부는 해당 연구기관에 비용의 전부 또는 일부를 지원할 수 있고, 이에 관하여 필요한 사항은 대통령령으로 정한다[17]. 그러나 이는 보안 관련 연구개발에 초점을 맞춘 것은 아니며, 법률이 위임한 사항들을 대통령령에서 별도로 정한 바가 없다. 따라서 연구개발·기술협력·기술이전 또는 기술지도 등의 사업을 실행하기 위한 구체적인 방법에 대한 규정이 없고 실효성이 부족하다. 한편 정부는 민간부문에 의한 정보통신망 응용서비스의 개발을 촉진하기 위하여 재정 및 기술 등 필요한 지원을 할 수 있다고 규정하고 있으나[17], 이 역시 보안보다는 정보통신망 이용촉진에 초점을 맞추고 있다. 「정보통신기반 보호법」과 「국가사이버안전관리규정」은 보안에 초점을 맞추어 연구개발 규정을 두었으나, 그 적용범위가 「정보통신기반 보호법」은 기반시설, 「국가사이버안전관리규정」은 공공분야로 범위가 한정된다[16][18].

지능화·고도화되고 있는 사이버공격에 대응하기 위하여 범국가적 연구개발 체계를 마련하고 연구개발 여건을 제도적으로 보장해야 한다. 연구개발을 담당할 정부출연연구기관을 법률상 지정하거나 정부의 지원을 받을 수 있는 연구기관의 자격요건을 정하는 것도 검토할 필요가 있다.

5. 결 론

사이버안보를 위한 추진체계는 통합적으로 재구성되어야 한다. 이를 위하여 담당기관이 수행하는 역할의 법적 근거를 정비하는 것을 출발점으로 하여 사이버안보 강화에 필요한 각종 요소들의 개선을 추진하고 법제화하여야 한다.

따라서 사이버안보 추진체계 개선 과제를 해결하기 위한 법제도 개선이 적극적으로 추진되어야 한다. 이러한 필요성은 이전부터 다수의 관련 연구를 통하여 제기되어 왔으며, 2013년 상반기부터 국회에서 '국가 사이버테러 방지에 관한 법률안', '국가 사이버안전 관리에 관한 법률안', '정보통신기반 보호법 일부개정법률안' 등이 발의되어 법제도를 개선하려는 실제적인 움직임이 나타나고 있다. 사이버안보 추진체계의 제도적 개선을 위해서는 사이버안보의 중요성과 추진체계의 제도적 정비의 필요성에 대한 관심을 높여야 한다. 그리고 국회에서 보다 많은 논의를 활발히 수행하고 각계각층의 의견을 수렴하는 한편, 입법에 필요한 절차를 진행해나가야 한다. 그러한 과정을 통해서 법제도 정비를 위한 구체적 방안을 도출하고 관련 법률의 제·개정을 추진하는 것이 필요하다.

참고문헌

[1] Ryan Gallagher, "Lawmakers Cite Boston Bombing, WikiLeaks "Hacking" as Reasons to Pass CISPA", Slate, 2013.4.19.

[2] 정빛나, "中, 美 첨단 무기시스템 설계도 20여개 해킹", 연합뉴스, 2013.5.28.

[3] 김희연, "스턱스넷 등 산업기반시설 해킹 위협 증가", ZDNet Korea, 2011.12.7.

[4] 김희연, "사이버 시위대 등장, '핵티비즘'의 시대", ZDNet Korea, 2011.11.21.

[5] 허정헌, "경찰 "3·4 디도스 공격도 北 소행 추정"", 한국일보, 2011.4.7.

[6] 김동훈, "3.4 디도스 공격, 대응력 정찰위한 北소행", 한국경제, 2011.7.6.

[7] 전성훈·송진원, "檢 "농협 해킹은 北 정찰총국 소행"", 연합뉴스, 2011.5.3.

[8] 이재림, "北정찰총국 대남 디도스공격 코드 반입 30대 기소", 연합뉴스, 2012.6.28.

[9] 박용주, "경찰 "작년 중앙일보 해킹 北소행"…도발 위협후 공격", 연합뉴스, 2013.1.6.

[10] 김주성, "정부 "3·20 해킹은 북한 소행 추정…수법 일치"", 연합뉴스, 2013.4.10.

[11] 최인영, "정전 60주년에 해킹…'사이버 6·25전쟁' 불안", 연합뉴스, 2013.6.25.

[12] 김민식·박상돈·권헌영·김일환·임종인, "통합적 사이버 위기관리 체계의 필요성에 관한 연구 : 미국과 한국의 제도 및 정책 비교를 중심으로", 「정보·보안 논문지」 제9권 제1호, 한국사이버테러정보전학회, 2009.3.

[13] "정부, 「국가 사이버안보 마스터플랜」 수립", 방송통신위원회 보도자료. 2011.8.8.

[14] ""3.20 사이버테러' 관련 국가 사이버안전 전략회의 개최", 미래창조과학부 보도자료, 2013.4.11.

[15] "정부, 「국가 사이버안보 종합대책」 수립", 미래창조과학부 보도자료, 2013.7.4.

[16] 「국가사이버안전관리규정」

[17] 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

[18] 「정보통신기반 보호법」

[저 자 소 개]

박 상 돈 (Sangdon Park)

2002년 성균관대학교 법학과(학사)
2004년 성균관대학교 법학과(석사)
2010년 성균관대학교 법학과 박사과정 수료
2008년~현재 한국전자통신연구원 부설연구소 연구원

email : sdpark@ensec.re.kr

김 인 중 (Injung Kim)

2006년 성균관대학교 전기전자 및 컴퓨터공학부(박사)
1992년~1999년 국방과학연구소 선임연구원
2000년~현재 한국전자통신연구원 부설연구소 책임연구원(실장)
現 충남대학교 겸임교수
現 2013년 세계사이버스페이스총회 자문위원

email : cipher@ensec.re.kr