사이버안보법 제정을 위한 국내 사이버안보 법률안 연구

박상돈* · 김소정*

요 약

오늘날 사이버공격은 국가안보를 위협하는 요소가 되고 있다. 최근의 사이버안보 정책으로서 국가 사이버안보 종합대책이 발표되었으나 현행 법제도에 의하면 온전한 법적 근거를 갖추고 그러한 대책들을 구현하기에는 어려운 부분이 있다. 현재 사이버안보 관련 법제도는 부문별로 별도의 법령이 적용되고 있으며, 이에 따라 사이버안보 추진체계도 분산되어 부문별 장벽에 의한 문제점들이 발생한다. 이러한 여러 가지 문제점들을 근본적으로 해결하기 위해서는 기존 법률의 개정보다는 새로운 사이버안보법의 제정이 더욱 적절한 방식이다. 한편 2013년에는 국회에서 사이버안보 강화를 위한 몇 가지 법률안이 발의되었다. 이 법률안들에 대한 분석을 통하여 바람직한 내용적 요소들을 도출하고, 이를 반영한 새로운 사이버안보법을 제정하는 것이 사이버안보 관련 법제도 정비의 실현 가능성을 높일 것이다. 향후 사이버안보법 제정 논의의 시발점이자 새로운 사이버안보법의 기초로 활용될 수 있다는 점에서 이 법률안들은 큰 의미가 있다.

A Study on Cybersecurity Bills for the Legislation of Cybersecurity Act in Korea

Sangdon Park* · So Jeong Kim*

ABSTRACT

Cyber attacks threaten the national security in this day and age. The government of the Republic of Korea recently released the National Cyber Security Comprehensive Countermeasures as a new cybersecurity policy. But current legal system cannot provide legal basis for the implementation of such measures. The current legal system related to cybersecurity is applied in each sector, thus the governance system in cybersecurity is separate. So there are many problems in the governance system in cybersecurity. To solve these problems fundamentally, it is righter to make a new cybersecurity law than to revise existing laws. Meanwhile, lawmakers proposed some bills in Congress to strengthen the cybersecurity in Korea in 2013. It will increase possibility of legislation of cybersecurity act to make a law through the analysis of these bills and to derive the essential elements from those. and to reflect these in the new cybersecurity act.

Key words : cybersecurity act, cybersecurity bills, National Cyberterror Prevention Act, National Cybersecurity Management Act, Act on the Protection of Information and Communications Infrastructure

접수일(2013년 11월 29일), 수정일(1차: 2013년 12월 10일), 게재확정일(2013년 12월 11일)

* 한국전자통신연구원 부설연구소

1. 서 론

오늘날 사이버공격은 단순 범죄의 차원을 넘어 테러의 성격을 보이는 경우가 증가하고 있으며 이러한 사이버공격은 국가안보를 위협하는 요소가 되고 있다. 사이버공격의 개념은 여러 가지로 제시된다. '지정된 목표의 손상을 위하여 이루어지는 사이버 무기의 공격적 사용'이라고 제시되기도 하고[1], 「국가사이버안전관리규정」 제2조에서의 정의와 같이 '해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위'라고 제시되기도 한다. 사이버공격의 개념 설명에 포함된 '사이버무기', '전자적 수단', '지정된 목표의 손상', '불법침입·교란·마비·파괴', '절취·훼손' 등의 용어들을 고려하면 사이버공격의 주요 요소는 국가와 사회의 주요 인프라로서 기능하는 정보통신 및 정보통신에 기반하는 유·무형의 각종 자산에 대한 손상이라는 점을 도출할 수 있다. 그리고 사이버안보는 이러한 손상이 국가안보에 영향을 미치는 경우와 관계되는 문제라고 할 수 있다. 제19대 국회에서 발의된 관련 법안에서는 사이버테러, 사이버안전 등의 용어를 사용하고 있는데, 후술하는 관련 법안들의 목적 및 용어의 정의 등을 고려하면 이들 법안 역시 본 논문에서 지칭하는 사이버안보를 대상으로 한다고 판단할 수 있다.

정부는 국가 사이버안보 종합대책을 발표하였으나 현행 법제도상 법적 근거를 갖추고 구현하기에는 어려운 부분이 없지 않다. 한편 2013년 제19대 국회가 출범하면서 사이버안보 추진체계를 개선하고자 하는 법률안들이 다수 발의되었다. 본 논문에서는 이들 법률안을 사이버안보 법률안이라고 칭하고, 이러한 입법 활동에 의하여 향후 갖추어질 것으로 기대되는 법률을 사이버안보법이라고 칭하기로 한다. 사이버안보 법률안은 사이버안보 추진체계의 개선에 대한 법적 근거 제공이라는 점에서 큰 의미가 있다고 본다. 본 논문에서는 바람직한 사이버안보법을 통하여 개선되어야 할 주요 과제들을 살펴보고, 그러한 과제의 해결에 필요한 요소의 존재 여부를 기준으로 하여 2013년에 제19대 국회에서 발의된 사이버안보 법률안을 평가하고자 한다.

2. 사이버안보법의 주요 과제

사이버안보법의 핵심적인 기능은 사이버안보 활동을 이끌어나가는 추진체계를 규율하고 법적 근거를 제공하는 것이다. 따라서 현재의 관련 법제도를 개선하기 위하여 사이버안보법에 반드시 반영되어야 하는 우선순위에 있는 주요 과제는 사이버안보 추진체계의 제도적 개선과제와 부합한다고 할 수 있다. 사이버안보 추진체계의 제도적 개선과제를 중심으로 하여 사이버안보법의 주요 과제들을 살펴보면 다음과 같다[2].

첫째, 관계부처·기관 역할의 법적 근거 정비이다. 국가 사이버안보 종합대책에 의한 추진체계에서 청와대가 컨트롤타워를 담당하고 국가정보원이 실무를 총괄한다고 정하였으나, 관계 부처·기관의 역할에 법률상 적절한 수준으로 정해져 있지 않으며, 상당 부분은 대통령훈령인 「국가사이버안전관리규정」에 의존하고 있다. 이는 관계 부처·기관의 집행력을 미약하게 하고 특히 민간부문에 대한 대국민 효력을 발휘하는데 한계를 발생시킨다. 따라서 법률상 관계부처·기관이 수행하는 사이버안보 활동의 법적 근거를 명확히 정하고, 대통령훈령 등에 규정한 내용들을 법률의 형식으로 하여 다시 규정해야 한다.

둘째, 국가차원의 합동대응 강화이다. 현재 사고대응을 위한 합동대응시 공공부문과 민간부문의 체계가 별개이고, 정보통신기반시설의 체계는 이와 또 별개로 구성되어 있다. 공공부문은 「국가사이버안전관리규정」에 의하여 국가정보원 주도의 민·관·군 합동대응반 또는 범정부적 사이버위기 대책본부, 민간부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의하여 미래창조과학부가 주도하는 민·관합동조사단, 주요정보통신기반시설은 「정보통신기반 보호법」에 의하여 정보통신기반보호위원회가 주도하는 정보통신기반침해사고대책본부가 합동대응을 수행한다. 사이버공격에서 부문별로 다른 형태의 합동대응을 법률에 정하는 것은 합동대응의 의미를 무색하게 한다. 따라서 국가차원의 합동대응을 일원화하고 그에 따른 관계부처·기관의 역할을 명확히 법률에 정할 필요가 있다.

셋째, 정보공유 체계 정립 및 활성화이다. 현재 부문별로 별개의 법령에서 정보공유 체계를 규정하고 있기 때문에 공공부문과 민간부문의 정보공유체계가 다르고, 정보통신기반시설의 정보공유체계는 이와 또 별개

이다. 그 결과 부문별로 정보공유체계를 관장하는 기관이 다르고, 공공부문과 민간부문 및 주요정보통신기반시설의 정보공유체계가 일원화되어 있지 않기 때문에 정보가 원활히 교류되지 않을 소지가 있다. 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.

넷째, 산업육성 및 인력양성을 통한 기반조성이다. 현재 관련 법률에서 정한 인력양성 관련 내용은 안보적 관점이 결여되어 있거나 선언적 수준에 그치고 있다. 산업육성 관련 내용은 주로 「정보통신산업 진흥법」에서 지식정보보안산업 육성에 관하여 정하고 있으나, 대부분 지식정보보안 컨설팅전문업체의 지정에 관한 내용이기 때문에 산업육성 전반에 대한 구체적인 추진체계가 결여되어 있다. 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.

다섯째, 연구개발 강화를 통한 방어수단 확보이다. 현재 연구개발 관련 규정은 개발가능한 모든 연구개발 분야에 대해 규율하지 못하고 있다. 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.

3. 사이버안보 법률안 발의 동향

3.1. 법률안 발의 현황 개요

제19대 국회에서는 사이버안보 추진체계의 전면적인 개선을 위한 새로운 법률 제정이 추진되고 있으며, 이러한 새로운 법률로서 '국가 사이버테러 방지에 관한 법률안'과 '국가 사이버안전 관리에 관한 법률안'이 발의되어 있다. 한편 새로운 법률의 제정이 아닌 기존 법률의 개정으로 사이버안보를 개선하는 형태로는 '정보통신기반 보호법 일부개정법률안'이 발의되어 있다.

'국가 사이버테러 방지에 관한 법률안'은 제안이유에서 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 하는 것을 입법의 목적으로 제시한다[3]. 특징으로는 국가정보원 중심의 사이버테러 방지체계를 구성하고, 악성프로그램에 대한 조치, 기술이전, 국제협력, 포상, 벌칙 등 현행 「국가사이버안전관리규정」에서 다루지 않는 사항을 다수 추가하여 규율한다는 점이다.

'국가 사이버안전 관리에 관한 법률안'은 제안이유에서 사이버안전을 확보하며 국가의 안전보장과 국민의 이익에 이바지하는 것을 입법의 목적으로 제시한다[4]. 특징으로는 정책심의를 국무총리 소속 회의에서 수행하고 실행은 국가정보원을 중심으로 수행한다는 점이다.

'정보통신기반 보호법 일부개정법률안'은 제안이유에서 대규모 침해사고 발생에 대한 신속하고 적극적인 대응시스템을 구축함으로써 국가의 안전과 국민생활의 안정을 보장하는 것을 입법의 목적으로 제시한다[5]. 특징으로는 대규모 침해사고 대응체계를 미래창조과학부로 일원화한다는 점이다.

3.2. 각 법률안의 주요 내용

3.2.1. 국가 사이버테러 방지에 관한 법률안

적용 범위는 사이버테러 방지 및 위기관리에 관한 사항이며, 다른 법률에 특별한 규정이 있는 경우에는 해당 법률을 적용한다. 다만, 사이버위기가 발생할 경우에는 다른 법률에 우선하여 적용한다(안 제3조). '사이버테러'란 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 절취·훼손·왜곡전파 하는 등 모든 공격행위를 의미하며, '사이버위기'란 사이버테러로 인하여 국가·사회기능에 심각한 지장을 초래하거나 피해가 전국적으로 확산될 가능성이 있는 경우를 의미한다(안 제2조). 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련정보를 상호 공유

하기 위하여 민·관 협의체를 구성·운영할 수 있으며(안 제5조), 국가사이버테러 방지 및 위기관련 기본계획을 수립하고 이에 따라 시행계획을 작성하여 사이버테러 방지 및 위기관리에 관한 업무를 수행하는 책임기관의 장에게 배포한다(안 제7조). 책임기관의 범위에는 국가기관, 지방자치단체, 공공기관, 주요정보통신기반시설 관리기관, 집적정보통신시설사업자, 주요정보통신서비스제공자, 국가핵심기술을 보유한 기업체나 연구기관, 방위사업체 및 방위사업 관련 전문연구기관 등을 포함한다(안 제2조). 또한 사이버테러에 대한 국가차원의 종합적이고 체계적인 대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둔다(안 제9조)[3].

책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁한다(안 제12조)[3].

중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 피해가 중대할 경우 관계 중앙행정기관의 장 및 국가정보원장에게 그 결과를 통보한다(안 제13조). 국가정보원장은 사이버테러에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취한다(안 제15조). 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등을 위하여 관계 기관 및 전문인력이 참여하는 사이버위기대책본부를 구성·운영할 수 있다(안 제16조)[3].

정부는 사이버위기관리에 필요한 연구개발·산업육성·인력양성·국제협력 등 필요한 시책을 추진할 수 있으며(안 제19조, 제20조, 제21조 및 제22조), 사이버테러 기도에 관한 정보를 제공하거나 사이버테러를 가한 자를 신고한 자에 대하여 포상금을 지급할 수 있다(안 제24조)[3].

한편 사이버위협정보를 정당하게 사용하지 않은 경우, 사이버테러 관련 자료를 손상시킨 경우, 직무상 비밀을 누설한 경우 등에는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 보안관제센터를 구축하지 아니한 경우 등에는 2천만원 이하의 과태료에 처할 수 있다(안 제25조 및 제26조)[3].

3.2.2. 국가 사이버안전 관리에 관한 법률안

사이버안전 관리에 관하여 다른 법률에 우선 적용되며, 정한 바가 없는 경우 「재난 및 안전관리 기본법」 및 「정보통신기반 보호법」 등에 따른다(안 제3조). '사이버안전'이라 함은 사이버공격으로부터 정보통신망을 보호함으로써 정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 의미한다(안 제2조). 국가 사이버안전에 관한 중요사항을 심의하기 위하여 국무총리 소속으로 국가사이버안전전략회의를 두고(안 제6조), 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속으로 국가사이버안전센터를 둔다(안 제7조)[4].

국가정보원장은 국가 사이버안전에 관한 정책을 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관과의 협의를 거쳐 국가사이버안전기본계획을 수립하며(안 제5조), 국가 차원의 사이버위기 발생에 대비하여 사이버안전에 관한 업무를 행하는 사이버안전관리책임기관이 참여하는 사이버위기 대응 훈련을 실시한다(안 제9조). '사이버위기'란 사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 의미한다(안 제2조). 사이버안전관리책임기관의 범위에는 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무 처리 기관, 중앙행정기관, 지방자치단체 및 공공기관, 주요정보통신기반시설 관리기관, 국가핵심기술을 보유한 기업체나 연구기관 등이 포함된다(안 제2조)[4].

중앙행정기관, 지방자치단체, 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 보안관제센터를 설치·운영하며(안 제11조), 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우 국가정보원장에게 통보한다(안 제13조). 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향 및 피해규모 등을 고려하여 수준별 사이버위기경보를 발령할 수 있다(안 제12조)[4],

국가정보원장은 사이버공격으로 인하여 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있으며, 사이버공격으로 인한 피해가 심각하다고 판단

되는 경우나 심각 수준 이상의 사이버위기경보가 발령된 경우에 관계 중앙행정기관의 장과 협의하여 사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위한 범정부적 사이버위기 대책본부를 구성·운영한다(안 제14조)[4].

3.2.3. 정보통신기반 보호법 일부개정법률안

대규모 전자적 침해행위에 대한 국가차원의 종합적이고 체계적인 대응을 위해 미래창조과학부장관 소속으로 국가정보통신기반보호센터를 두며(안 제4조의2), 관리기관에 대한 주요정보통신기반시설보호대책 이행여부의 확인, 관리기관에 기술적 지원, 주요정보통신기반시설 지정 권고 등을 하는 주체를 미래창조과학부장관과 국가정보원장등에서 미래창조과학부장관으로 일원화한다(안 제5조의2, 제7조 및 제8조의2). 미래창조과학부장관은 대규모 침해사고에 체계적·효율적으로 대응하기 위하여 대규모 침해사고 대응훈련을 실시한다(안 제11조의4)[5].

관리기관의 장은 대규모 전자적 침해사고로부터 정보통신기반시설을 보호하고 신속·정확하게 대응하기 위해 대규모 침해사고 대응대책을 수립·시행하며(안 제11조의2), 대규모 전자적 침해사고에 즉시 대응조치를 할 수 있는 기구로서 보안관제센터를 설치·운영한다(안 제11조의3)[5].

미래창조과학부장관은 침해사고에 따른 파급영향과 피해규모 등을 고려하여 수준별 경고를 발령할 수 있으며(안 제11조의5), 관리기관의 장은 전자적 침해행위가 발생한 경우 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시한다(안 제14조의2)[5].

국방분야의 주요정보통신기반 보호의 이행 여부, 경보발령, 사고조사 등에 대하여는 국방부장관이 업무를 수행할 수 있도록 특례를 둔다(안 제27조의3)[5].

4. 사이버안보 법률안 비교 및 평가

4.1. 새로운 법률의 제정과 기존 법률의 개정 비교

사이버안보법 정비방식의 형태는 기존 법률의 개정보다 새로운 법률의 제정이 효과적이라고 판단된다. 기존 법률은 부문별로 적용범위와 추진체계가 고착화된 상태이기 때문에 이를 개정하는 것은 오히려 새로운 법률의 제정보다도 더 곤란한 문제일 수 있으며, 부문별로 분산된 추진체계로 인하여 발생하는 여러 문제점의 근본적인 해결책이 될 수 없다. 새로운 법률로 사이버안보 추진체계의 큰 틀을 개편하고, 기존 법률은 평시에 부문별로 특화된 사이버안보활동의 법적 근거로 활용하는 것이 합리적이다. 따라서 개정의 형식을 취하는 법률안은 논의의 실익이 적기 때문에 이하에서는 '정보통신기반 보호법 일부개정법률안'은 논외로 하고 '국가 사이버테러 방지에 관한 법률안'과 '국가 사이버안전 관리에 관한 법률안'을 대상으로 하여 사이버안보법의 주요 과제 해결 여부를 비교하고자 한다.

4.2. 사이버안보법의 주요 과제 해결 여부 비교

4.2.1. 관계부처·기관 역할의 법적 근거 정비 여부

사이버안보 추진체계를 주도하는 역할은 실제로 활동에 필요한 정도의 역량을 갖추고 있고 국가안보와 밀접한 관련이 있는 기관이 수행하는 것이 바람직하다. 추진체계의 주도기능은 정책총괄기능과 실무총괄기능으로 세분화할 수 있다. 정책총괄기능과 실무총괄기능의 구성방법은 하나의 기관에 집중시키는 형태와 분리시키는 형태의 두 가지가 있다. '국가 사이버테러 방지에 관한 법률안'은 국가사이버안전전략회의와 국가사이버안전센터를 모두 국가정보원장 소속으로 하여 정책총괄기능과 실무총괄기능을 국가정보원에 집중시키는 형태이다. '국가 사이버안전 관리에 관한 법률안'은 국가사이버안전전략회의를 국무총리 소속으로 하고 국가사이버안전센터는 국가정보원장 소속으로 하여 정책총괄기능은 국무총리실, 실무총괄기능은 국가정보원으로 분리하는 형태라고 할 수 있다. 국가사이버안보 종합대책에서 밝힌 청와대의 컨트롤타워 역할 수행도 정책총괄기능과 실무총괄기능을 분리시키는 형태라고 판단된다. 국가 사이버안보 종합대책 발표 이후 개정된 「국가사이버안전관리규정」에서도 여전히 국가정보원의 실무총괄기능이 유지되고 있기 때문이다.

정책총괄기능과 실무총괄기능을 하나의 기관에 집중시키는 형태가 기능의 집적에 따른 효율성은 가장 높을 것이다. 그러나 특정 기관에 권한과 책임이 집중되는 것을 지양하려 하는 정책적 고려를 반영해야 하는 상황이라면 정책총괄기능과 실무총괄기능의 담당

기관을 분리시키는 형태를 취하는 것을 검토할 수 있다고 본다. 정책총괄기능과 실무총괄기능의 담당기관을 분리시키는 형태라면 정책총괄기능을 국무총리실보다는 대통령실이 담당하도록 하여 컨트롤 타워의 위상을 승격하고 부처 간 업무 조정 및 통제를 용이하게 하는 것이 상당한 타당성을 지닌다고 할 수 있다[6].

정책총괄기능과 실무총괄기능의 분리여부를 막론하고 실무총괄기능은 반드시 기술적 역량을 갖춘 기관이 수행하여야 한다. 따라서 청와대가 실무총괄기능을 담당하기에는 현실적으로 무리가 있다고 본다. 한편 단지 기술적 역량의 보유에 그치는 것이 아니라 다른 유관기관과의 협력을 능동적으로 주도할 수 있는 지위에 있고 안보 문제를 적절히 다룰 수 있는 기관이 적합하다고 할 수 있다.

4.2.2. 국가차원 합동대응 강화 여부

'국가 사이버테러 방지에 관한 법률안'은 사이버테러 방지 및 위기관리에 관한 업무를 수행하는 책임기관의 범위에 기존의 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「국가사이버안전관리규정」의 주요 적용대상들을 모두 포함시켰다. 이에 따라 부문별 장벽을 없앤 추진체계가 구축될 수 있는 기반을 마련하는데 용이하다. 반면에 '국가 사이버안전 관리에 관한 법률안'은 사이버안전에 관한 업무를 행하는 사이버안전관리책임기관의 범위에 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 주요 적용대상들을 제외하여, 부문별 장벽을 완전히 없애지 못하였다는 문제점을 지니고 있다.

한편 '국가 사이버테러 방지에 관한 법률안'은 민·관 협의체의 구성·운영 근거를 명시하고 있으며 국가사이버안전센터 내 민·관·군 합동대응팀의 설치·운영 근거도 명시하고 있다. 아울러 일정 수준 이상의 경보가 발령된 경우에는 사이버위기 대책본부를 구성·운영하도록 하고 있다. 반면에 '국가 사이버안전 관리에 관한 법률안'은 민·관 협의체의 구성·운영은 정하고 있지 않으며, 국가사이버안전센터 내 민·관·군 합동대응팀의 설치·운영 근거와 사이버위기 대책본부의 구성·운영 근거만을 명시하고 있다. 따라서 '국가 사이버테러 방지에 관한 법률안'이 상대적으로 범국가적 협력을 더 강조한 것으로 평가할 수 있다. 또한 사이버위기에 대응하기 위한 대책본부에 민간과 군이 함께 참여할 수 있음을 명시한 '국가 사이버테러 방지에 관한 법률안'이 단계별 사이버안전관리 업무의 효율적 수행에 유리하다[6]. 특히 '국가 사이버안전 관리에 관한 법률안'은 국방부문의 경우 상당부분 적용을 제외하는 특례를 두고 있는데 이는 추진체계를 실제로 운용함에 있어서 합동대응의 효과를 반감시키는 결과를 가져올 수 있다.

따라서 범국가적 협력체계는 '국가 사이버테러 방지에 관한 법률안'에 준하여 구성하는 것이 바람직하다. 다만 동 법률안에서 민·관 협의체의 구성·운영을 대통령령에 위임하고 있는데, 대통령령 제정시 충분한 논의를 거쳐 내실있는 협의체를 구성하는 과제는 별도로 남게 된다. 민·관 협의체를 구성·운영을 통하여 민·관 협력을 실질적으로 활성화시킬 수 있는 방안을 마련하여야 한다.

4.2.3. 정보공유 체계 정립 및 활성화 여부

'국가 사이버테러 방지에 관한 법률안'은 보안관제센터를 국가기관과 지방자치단체 및 공공기관뿐만 아니라 주요정보통신기반시설과 민간 정보통신망도 대상으로 하여 설치하도록 하고, 사이버위협정보통합공유체계를 구축·활용할 수 있도록 하여 정보를 탐지하고 공유하는 체계의 일원화를 달성했다고 평가할 수 있다. 반면에 '국가 사이버안전 관리에 관한 법률안'은 현행 「국가사이버안전관리규정」과 마찬가지로 중앙행정기관과 지방자치단체 및 공공기관만을 대상으로 보안관제센터를 설치하도록 하여 정보를 탐지하고 공유하는 체계의 일원화를 달성하지 못했다. 이는 현재의 정보공유체계가 가진 문제점을 그대로 답습하도록 할 우려가 있다.

생각건대 사이버안보 위협상황에 빠르게 대처하기 위해서는 다방면의 신속한 정보의 탐지와 공유가 필수적이기 때문에 정보공유체계를 일원화하는 법적 근거가 반드시 마련되어야 한다.

4.2.4. 산업육성 및 인력양성을 통한 기반조성 여부

'국가 사이버테러 방지에 관한 법률안'은 정부가 산업육성에 관하여 시책을 수립·시행할 사항들을 열거하고 연구기관이 필요한 업무를 수행할 수 있는 근거를 명시하고 있다. 또한 동 법률안은 정부가 인력양성에 관하여 시책을 강구할 사항들을 열거하고 있다. 이는

관련 분야의 기업체, 학계의 전문가들이 공청회 등에서 사이버 테러를 방지하기 위한 인력의 부족, 체계적인 연구의 부족, 각 기관·업체들간 협력의 부족, 사이버 테러 대응과 관련한 인프라 구축의 필요성 등을 주장해 온 바를 반영한 것으로 보인다[6]. 한편 '국가 사이버안전 관리에 관한 법률안'은 산업육성에 관한 내용은 정한 바 없으며, 인력양성에 관해서는 정부가 시책을 강구할 사항들을 열거하고 있다. 양 법률안을 비교하면 산업육성의 보장은 '국가 사이버테러 방지에 관한 법률안'만이 실질적인 추진체계를 명시하고 있으며, 인력양성의 보장은 양 법률안 모두 구체적인 추진체계는 드러나지 않는 수준이다. '국가 사이버테러 방지에 관한 법률안'이 상대적으로 더 충실하게 산업육성 및 인력양성 추진체계를 규정하고 있으나 인력양성에 관한 내용은 더욱 구체적이어야 실효성이 확보될 것으로 보인다. 이는 대통령령의 형식으로도 가능할 것으로 본다.

또한 산업육성 및 인력양성의 보장은 산업계에 대한 직접적인 지원책도 필요하지만 보안제품 사용을 활성화하여 관련 산업의 시장규모 자체를 증대시키는 것도 필요하다. 특히 기업들의 보안제품 사용을 일상화하도록 유도하는 것이 시장의 확대와 그에 따른 인력수요 증가에 효과적이다. 따라서 기업들이 보안제품을 사용하지 않고 사이버공간에 대한 안전조치의무를 소홀히 한 경우 법적으로 불이익을 받도록 하는 것을 검토할 필요가 있다[7].

4.2.5. 연구개발 강화를 통한 방어수단 확보 여부

'국가 사이버테러 방지에 관한 법률안'은 정부가 연구개발에 관하여 시책을 추진할 사항들을 열거하고 연구기관이 필요한 업무를 수행할 수 있는 근거를 명시하고 있다. 한편 '국가 사이버안전 관리에 관한 법률안'은 기술 연구 및 개발에 관해서 정부가 시책을 강구한다고만 하여 매우 간단한 선언적 규정만을 두고 있다. 양 법률안을 비교하면 '국가 사이버테러 방지에 관한 법률안'이 실질적인 추진체계를 명시하여 상대적으로 더 바람직한 수준으로 연구개발을 보장하고 있다.

다만 동 법률안에서 연구개발에 관한 절차·방법 등 세부사항은 국가정보원장이 따로 정하도록 하고 있는데, 세부사항을 정함에 있어 충분한 논의를 거쳐 내실있는 연구개발 추진체계를 수립하여 제도화하여야 한다. 미국의 경우는 연구개발에 관하여 별도의 법률을 제정하여 연구개발에 대한 강력한 지원을 추진하는 체계를 구체적으로 정하고 있다[8]. 법률에서는 입법의 편의상 기본적인 근거가 되는 정도로만 정해도 무방할 것이나 하위법령에서는 연구개발의 효과를 높일 수 있는 추진체계와 연구개발 프로그램의 내용들을 구체적으로 정하여 제도화할 필요가 있다.

4.3. 법률안의 의의 및 과제

제19대 국회에 발의되어 있는 법률안들은 사이버안보 강화를 위한 입법을 시도한다는 점에서 큰 의미를 지닌다. 현 시점에서는 각 국회에 발의된 법률안의 장점을 취하고 더욱 발전시켜서 소관 위원회 대안 등의 형식을 취하여 바람직한 사이버안보법을 도출하는 것이 비교적 용이한 입법 방법이라고 할 수 있다.

앞에서 살펴본 바와 같이 2013년 발의된 사이버안보 법률안들은 사이버안보법이 담아야 할 요소들을 상당부분 반영하였으나 세부 사항들은 불완전한 부분을 내포하고 있다. 전체적인 구성은 '국가 사이버테러 방지에 관한 법률안'이 사이버안보법의 주요 과제 해결에 필요한 요소들을 적절히 포함하고 있으나 구체적인 내용은 보완이 필요한 부분이 없지 않다. 따라서 향후 국회의 입법과정에서 '국가 사이버안전 관리에 관한 법률안' 등 다른 법률안과 각계의 의견을 참고하여 본 논문에서 지적한 보완사항들을 수정하는 것이 필요하다. 또한 다른 사항에 관한 추가적인 의견이 제시된다면 이에 대한 조정과 합의도 이루어져야 한다.

5. 결 론

법제도 정비가 수반되지 않은 사이버안보 정책은 법적 근거의 부실 및 파생되는 문제점들로 인하여 실효성을 확보하기 어렵다. 따라서 사이버안보 관련 법제도의 대대적인 정비를 추진하여 현행 사이버안보 관련 법제도의 문제점들을 해결하고 법제도 전체의 체계성을 확보하는 것이 필요하다.

사이버안보 관련 법제도의 정비는 기존 법률의 개정보다는 사이버안보 관련 기본법의 지위를 갖는 사이버안보법을 제정하면서 관계부처·기관 역할의 법적 근거 정비, 국가차원 합동대응 강화, 정보공유 체계 정립

및 활성화, 산업육성 및 인력양성을 통한 기반조성, 연구개발 강화를 통한 방어수단 확보 등의 주요 과제들을 해결할 수 있는 내용을 갖추도록 하여야 한다. 따라서 사이버안보법은 이러한 과제들의 해결에 필요한 요소들을 빠짐없이 다루는 동시에, 각 요소별로 구체적인 내용의 타당성을 함께 갖추어야 한다. 지금까지는 국회 등 유관기관에서 사이버안보법에 대한 구체적인 논의가 미진한 점이 없지 않았다. 2013년도에 발의된 사이버안보 법률안들은 제19대 국회 개원 이후 국회에서 이루어지는 사이버안보법 논의의 시발점이라는 점에서, 그리고 그러한 논의를 거친 후 구현될 것으로 기대되는 새로운 사이버안보법의 기초가 될 수 있다는 점에서 큰 의미를 지닌다고 할 수 있다.

참고문헌

[1] Karl Frederick Rauscher, Valery Yaschenko (ed.), Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, EastWest institute, Information Security Institute of Moscow State University, 2011.

[2] 박상돈/김인중, “사이버안보 추진체계의 제도적 개선과제 연구”, 융합보안 논문지 제13권 제4호, 한국융합보안학회, 2013. 9.

[3] 국가 사이버테러 방지에 관한 법률안(서상기의원 대표발의), 2013. 4. 9.

[4] 국가 사이버안전 관리에 관한 법률안(하태경의원 대표발의), 2013. 3. 26.

[5] 정보통신기반 보호법 일부개정법률안(정청래의원 대표발의), 2013. 7. 4.

[6] 정보위원회 수석전문위원, “국가 사이버테러 방지에 관한 법률안(서상기의원 대표발의), 국가 사이버안전 관리에 관한 법률안(하태경의원 대표발의) 검토보고서”, 2013. 6.

[7] 정준현, “정보보안산업육성정책과 관련 법률”, 국가 사이버테러 위기 대응과 정보보안산업 육성 법률개정안, 새누리당 중앙위원회 정보과학분과, 2013. 5.

[8] 박상돈/김인중, “한국과 미국의 사이버보안 단계별 법제도 비교 연구”, 융합보안 논문지 제12권 제4호, 한국융합보안학회, 2012. 9.

[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 정책연구실 연구원

email : sdpark@ensec.re.kr

김 소 정 (So Jeong Kim)

1998년 8월 부산대학교 사학과(학사)
2001년 2월 경희대학교 평화복지대학원 동북아학(석사)
2006년 2월 고려대학교 정보보호대학원 정보보호정책학과(박사)
2004년~현재 한국전자통신연구원 부설연구소 정책연구실 선임연구원

email : sjkim@ensec.re.kr