한국경호경비학회 – 제54호(2018): 9–35

투고일 2018. 2. 10. 심사일 2018. 2. 26. 게재확정일 2018. 2. 28.

국내 관련 법과 비교 분석을 통한 국가사이버안보법안의 제정 필요성 연구

김 성 현·이 창 무

국내 관련 법과 비교 분석을 통한 국가사이버안보법안의 제정 필요성 연구*

김 성 현** · 이 창 무***

〈요 약〉

제 4차 산업혁명이 도래하고 있는 오늘날, 사이버공격은 초국가적인 형태로 민간과 공공 구분 없이 동시다발적으로 일어나고 있으며, 지난 2009년의 DDOS 사건을 포함하여 청와대, 언론, 금융기관 전산 시스템 마비 등 사이버 위협은 갈수록 심각성을 더하고 있다. 그러나 현재 우리나라는 사이버안보와 관련된 기본법이 존재하지 않고, 국내의 여러 법률에 관련 내용이 산재되어 있는 형편이다. 이는 사이버안보와 관련된 내용의 법 적용 및 판단 근거에 혼선을 초래할 수 있다. 이러한 상황을 극복하기 위해 2006년 '사이버위기 예방 및 대응에 관한 법률안'이 발의되었지만 폐기되었고, 이후 꾸준히 발의되었지만 기존 법률과의 중복문제 및 개인정보침해우려 등으로 번번이 통과가 무산되었다. 가장 최근 발의안은 '국가사이버안보법안'으로 2017년 1월 정부가 발의하였다. 이 법안은 사이버안보와 관련된 기본법의 부재를 해결하고, 사이버안보위기시의 대응 능력 강화 및 안보력 함양 등을 주요 내용으로 하고 있다. 따라서 본 연구는 '국가사이버안보법안'을 사이버안보와 관련된 국내의 기존법과 비교 분석을 통해 그 필요성을 고찰하고, 개선점을 제언함으로써 사이버안보 기본법으로서의 '국가사이버안보법안'의 올바른 제정에 기여하고자 한다.

주제어 : 사이버안보, 사이버공격, 사이버테러, 사이버안보 기본법, 사이버테러방지법, 국가사이버안보법안

* "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음"(IITP-2017-2014-0-00636)
** 중앙대학교 대학원 산업융합보안학과 (제1저자)
*** 중앙대학교 산업보안학과 교수 (교신저자)

목 차

Ⅰ. 서 론

1. 연구의 필요성

사이버공격이 초국가적인 형태와 그 피해가 극심한 오늘날, 세계는 사이버공격에 대한 대응체계를 법률과 조직 측면에서 강화하고 있는 추세다. 그러나 우리나라는 지난 DDOS 사건이나, 한수원, 국방부 등이 사이버공격으로 피해를 받았음에도, 사이버공격에 대한 법률적 대응체계는 미흡한 실정이다. 2006년 이래로 통과되지 못하고 있는 사이버테러방지법(통칭)이 대표적 예이다. 현재 우리나라는 사이버안보와 관련된 기본법이 존재하지 않고, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반 보호법」, 「국가사이버안전관리규정」 등에 부분적으로 산재해있어 법률의 적용 및 판단 근거에 혼선을 초래할 수 있다. 이를 극복하기 위해 사이버안보 기본법적인 성격으로서의 역할 뿐만 아니라 사이버안보력 함양을 위한 최고정책심의기구 및 사이버정보공유 등을 법적 근거로 마련하는 '국가사이버안보법안'이 2017년 1월 정부에 의해 발의되었다. 하지만 발의된 '국가사이버안보법안'이 기존의 국내법들과 상당한 중복이 있다는 문제 제기와 함께 사이버안보력 함양이라는 목적아래

무분별한 개인정보수집 등의 우려 제기로 국회에서 통과되지 못하고 계류 중이다.

반면 현재 미국은 국토안보법에 Cyber Security 항목을 규정하고 있으며, Cyber Security Act of 2015, Cyber Security Enhancement Act of 2014 등의 제정을 통해, 사이버정보공유 강화와 민·관 합동 사이버위기 대응, 사이버안보 교육 및 연구 등을 도모하고 있다. 또한 일본은 2014년 사이버시큐리티 기본법을, 중국은 2017년 사이버보안법을 제정하며 국가 차원에서의 사이버안보력 함양 및 법률의 체계화를 도모하고 있다(권오국, 석재왕, 2016). 이러한 상황 속에서 본 연구는 국회에 계류 중인 '국가사이버안보법안'이 우리나라의 사이버안보 기본법으로서 작용할 수 있다는 점에서 그 필요성을 인식하고, 꾸준히 제기되고 있는 문제점들을 개선할 수 있는 방안을 모색하고자 하였다. 특히 사이버안보 법률 제정과 관련하여 기존의 선행연구들은 단순히 법률의 부재를 이유로 그 필요성을 강조하였다면, 본 연구는 국내 다른 법과의 구체적인 비교 분석을 통해 현 법률체계의 문제점과 더불어 '국가사이버안보법안'제정에 필요한 개선방안을 제시하고자 한다. 이를 통해 우리나라의 사이버안보력 함양에 이바지 하고, 기존 사이버안보 관련 법률의 미비점을 개선하는데 기여하고자 한다.

2. 연구의 방법 및 범위

본 연구는 현재 국회에 계류 중인 '국가사이버안보법안'을 사이버안보와 관련된 기존의 국내법들과의 비교법적 분석을 통해 법안의 제정 필요성을 고찰해보고자 한다. 여기서 비교법적 분석이란, 법률간의 구체적 규정 내용을 비교해 보고 그 차이점을 고찰하는 방법을 의미한다. 통상적으로 법학에서는 비교법적 분석은 외국법과의 비교를 의미하나, 본 연구에서는 국내법들간의 제정 목적·적용대상·세부규정 조항 등을 비교 분석 하고자 한다. 이러한 비교법적 분석방법이 '국가사이버안보법안'의 시사점과 필요한 개선방안을 도출하는데 효과적이라는 점에서 본 연구의 주된 연구방법으로 채택하였다.

비교기준이 되는 '국가사이버안보법안'은 2017년 1월 정부에서 발의한 법안이다. 현재 발의 된 사이버테러방지 관련 법안은 2016년 5월 국회의원 이철우 의원이 대표 발의한 '국가 사이버안보에 관한 법률안'이 존재하며, 2017년 1월에 정부에서 일부 수정하여 발의한 '국가사이버안보법안'역시 국회에 계류 중이다. 발의된 두 법안의 내용이 거의 비슷하나 일부 수정 사항을 반영한 정부 측의 제안 법률안 인 '국가사이

버안보법안'을 본 연구에서는 주 연구대상 법안으로 설정하고자 한다.

비교대상 법 후보로서는 총 17개의 법률 및 대통령훈령을 검토하였다. 그 대상은 다음과 같다. 「국가사이버안전관리규정」, 「국가정보화 기본법」, 「군사기밀 보호법」, 「군형법」, 「개인정보 보호법」, 「보안업무규정」, 「부정경쟁방지 및 영업비밀보호에 관한 법률」, 「산업기술의 유출방지 및 보호에 관한 법률」, 「전기통신사업법」, 「전자금융거래법」, 「전자문서 및 전자거래 기본법」, 「전자서명법」, 「전자정부법」, 「정보보호산업 진흥에 관한 법률」, 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「형법」이다. 상기 총 17개의 법들을 검토한 결과 사이버안보와 관련된 법은 「국가사이버안전관리규정」, 「정보보호산업 진흥에 관한 법률」, 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」4개로 압축되었다. 특히 「전자정부법」의 경우 제56조(정보통신망 등의 보안대책 수립·시행)만이 사이버안보와 관련된 규정이었는데, 보안대책을 마련해야 한다는 내용이었을 뿐 구체적인 사항을 규정하지 않아 비교대상 법에서 제외하였다. 마찬가지로 「형법」역시 제314조(업무방해), 제347조의2(컴퓨터등 사용사기)만 컴퓨터 및 정보통신망 관련 규정사항이었으며, 그 내용이 구체적이지 않아 제외시켰다. 반면에 「정보보호산업의 진흥에 관한 법률」의 경우 정보보호 산업 진흥에 목적을 맞춘 법이기는 하나, 정보보호산업 진흥 그 자체로 사이버안보력 함양에 이바지 할 수 있고, 특히 일부 사항이 '국가사이버안보법안'과 밀접한 사항을 규정하고 있으므로 비교대상 법에 포함시켰다.

결과적으로 비교대상 법으로서 사이버안보와 관련된 3개의 법률과 1개의 대통령훈령을 선정하였다. 각각의 법률 및 훈령은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반 보호법」, 「정보보호산업 진흥에 관한 법률」, 「국가사이버안전관리규정」이다. 상기 법률 및 훈령의 목적 및 세부 규정내용을 비교 분석하고 '국가사이버안보법안'의 제정 필요성 및 개선점 제언을 도출해내는 것이 본 논문의 핵심 내용이다.

Ⅱ. 이론적 배경 및 선행연구

1. 이론적 배경

1) 사이버안보의 개념

사이버안보에 대한 명확한 개념 정의는 아직 존재하지 않는다. 일반적으로 안보를 사이버공간으로까지 확대한 것으로 볼 수 있다. 정용기(2016)는 사이버 안보 개념이 전통적 안보개념을 탈피한 포괄적 안보개념에서 시작된 개념임을 감안한다면, 사이버 안보는 사이버 공간에서 국가의 핵심적 가치체계가 내부적 · 외부적 세력으로부터 자유로운 상황을 의미하는 것으로 볼 수 있다고 하였다. 또 채재병(2013)은 사이버안보는 일반적으로 사이버위협으로부터 사이버공간을 보호하는 것으로, 사이버공간과 관련된 다양한 공격으로부터 국민생활과 국가안위 등을 안정적으로 유지방어하기 위한 수단들의 총체로 정의할 수 있다고 하였다. 한국인터넷진흥원(2011)에서는 사이버보안이라는 표현을 사용하고, 이를 '정보의 비밀성, 무결성 및 이용가능성을 유지하기 위하여 사이버공간의 공격으로부터 정보, 정보시스템 및 정보통신망을 보호하는 것'으로 개념화하고 있다. 국제전기통신연합의 사이버안보 정의는 사이버 환경과 조직 및 사용자의 자산을 보호하기 위한 다양한 도구, 정책, 기술 등을 모두 포괄하는 것으로 보고 사이버 환경의 관련 보안 위험으로부터 보호하고 달성하기 위해 노력하는 것으로 정의한다(ITU, 2008).

2) 사이버공격의 개념 및 특징

사이버공격에 대한 정의는 「국가사이버안전관리규정」 및 TTA(한국정보통신기술협회) 에서 규정하고 있다. 「국가사이버안전관리규정」에 따르면 사이버공격이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다. 또한 TTA(한국정보통신기술협회)는 사이버공격을 인터넷을 통해 다른 컴퓨터에 불법 접속하여 상대방에게 손상을 입히려는 행동이라 정의하고 있다. 이밖에 장신(2012: O. Hathaway, 2015에서 재인용)은 사이버 공격이란 정치적 목적 또는 국가 안보를 위해 존재하는 컴퓨터 네트워크의 기능을 저해하는 일체의 공격이

라고 정의하였다.

이러한 사이버공격의 특징은 사실상 테러리즘과 거의 흡사한 속성을 갖고 있다. 가장 두드러진 특징으로는 테러리즘과 마찬가지로 공격과 방어에 있어 비대칭성을 갖고 있다는 점이다. 이것이 사이버위협이 초기에 사이버테러라는 형태로 안보이슈화 되었고 현재에도 테러리즘의 영역에서 상당부분 다루어지고 있는 이유이기도 하다. 그리고 위협, 즉 공격의 주체가 국가·집단·개인 등으로 다양하고 그로 인한 피해가 막대하다는 점도 매우 유사한 점이다(채재병, 2013). 또한 정보통신망에 기반 한 사이버에서 발생하는 국가의 핵심적 가치 체계 침해는 기본적으로 그 파급력과 침해의 피해규모가 크다는 문제가 있다. 많은 비용과 국가적 지원 없이도 정보체계에 대한 지식만으로 사이버 위협과 무기를 개발할 수 있으며, 네트워크에 접근할 수 있는 소수인만 있어도 공격이 가능하다(정용기, 2016). 뿐만 아니라 사이버공격은 특정한 목표물에 대한 직접적인 피해뿐만 아니라 ICT 기술의 상호연계성으로 인해 다른 지역으로 그 피해가 확장될 수 있다. 특히 네트워크에 대한 보호대책과 구성원의 보안의식이 제고된 국가보다는 상대적으로 전산망과 보안의식이 취약한 지역에서 시작하여 우회하는 방식으로 공격을 수행하는 것이 일반적인 방법이다(박웅신, 2013: 정용기, 2016에서 재인용).

3) 사이버안보 관련 법안

사이버안보 관련 법안은 제일 처음 2006년 12월 공성진 의원 대표발의로 '사이버위기 예방 및 대응에 관한 법률안'이 발의되었으나 임기만료로 심사되지 못한 채로 폐기되었다. 이후 18대 국회에서 공성진 의원 대표발의로 '국가사이버위기관리법안'이 발의되어 정보위원회에서 2009년 4월에 상정되었으나 역시 법안심사소위에 이르지 못하고 임기만료로 폐기되었다. 19대 국회는 가장 활발하게 사이버 안보 관련 법안이 발의된 시기인데 2013년 3월 하태경 의원 대표발의로 '국가 사이버안전 관리에 관한 법률안', 2013년 4월에 서상기 의원 대표발의로 '국가사이버테러 방지에 관한 법률안', 2015년 5월 이철우 의원 대표발의로 '사이버위협정보 공유에 관한 법률안', 2015년 6월 이노근 의원 대표발의로 '사이버테러 방지 및 대응에 관한 법률안'이 제출되었다. 20대 국회에는 이철우 의원 대표발의로 '국가 사이버안보에 관한 법률안(2016. 5. 30)', 그리고 정부 발의안으로 '국가사이버안보법안(2017.1.3.)'이 제출되어 국회정보위원회의 심사 중에 있다(임진대, 2017). 2006년 첫 발의안을 시작으로 가장

최근인 2017년 정부 발의안까지 사이버안보 관련 법안 발의명과 그 제안이유를 정리하면 아래 <표 1> 과 같다.

〈표 1〉 사이버안보 관련 법안 발의

법 안	제안 이유
사이버위기 예방 및 대응에 관한 법률안 (공성진 의원 대표발의, 2006.12.28.)	정부와 민간부분을 포함한 국가차원에서 사이버공격을 사전 탐지하고 정보를 공유할 수 있는 체계를 구축함으로써 사이버위기 발생을 예방하고 사이버위기가 발생하였을 경우에는 효율적으로 대처할 수 있는 체계의 구축 및 대응활동 등을 명확히 규정함으로써 사이버위기로 인한 피해확산을 방지하고 이를 조기에 극복하고자 함
국가 사이버위기관리법안 (공성진 의원 대표발의, 2008.10.28.)	정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함
국가 사이버안전 관리에 관한 법률안 (하태경 의원 대표발의, 2013.03.26.)	국가차원에서 사이버안전에 관한 기본계획을 수립·시행하도록 하고, 국무총리 소속으로 국가사이버안전전략회의를 두어 국가 사이버안전에 관한 중요사항을 심의하도록 하며, 사이버위기 대응 훈련·사이버위기경보 발령·사이버공격으로 인한 사고의 통보 및 조사 등에 관한 법적 근거를 담은 법률을 제정함으로써 사이버안전을 확보하며 국가의 안전보장과 국민의 이익에 이바지하고자 함
국가 사이버테러 방지에 관한 법률안 (서상기 의원 대표발의, 2013.04.09.)	정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버테러를 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함
사이버위협정보 공유에 관한 법률안 (이철우 의원 등 22인, 2015.05.19.)	사이버위협을 신속히 차단하여 피해를 최소화하는 등 효과적으로 대처할 수 있도록 공공·민간이 함께 사이버위협정보를 공유·분석하는 등 협력을 활성화하여 사이버위협을 조기 탐지·전파할 수 있는 체계를 구축하고자 함
사이버테러 방지 및 대응에 관한 법률안 (이노근 의원 대표발의, 2015.06.24.)	사이버테러를 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응하기 위한 범국가적인 차원의 사이버테러 방지 및 대응 체계를 구축하고자 함
국가 사이버안보에 관한 법률안 (이철우 의원 등 122인, 2016.05.30.)	정부와 민간이 함께 협력하여 국가차원의 체계적이고 일원화된 대응 체계를 구축하고, 이를 통해 사이버공격을 사전에 탐지하여 사이버위기 발생가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응 할 수 있도록 함
국가사이버안보법안 (정부 발의, 2017.01.03.)	공공 및 민간 영역의 구분 없이 광범위하게 발생하는 사이버공격으로 인하여 막대한 경제적 피해와 사회 혼란이 유발되고 있는바, 국가안보를 위협하는 사이버공격을 신속히 차단하고 피해를 최소화하기 위하여 국가사이버안보를 위한 조직 및 운영에 관한 사항을 체계적으로 정립하려는 것

2. 선행연구

사이버안보 기본법과 관련하여 구체적인 분석 및 제언을 하는 선행연구는 찾아볼 수 없었고, 주로 사이버안보법의 부재를 이유로 사이버안보법의 필요성 및 사이버안보 역량 강화 정도에 대해 역설한 연구가 대부분이었다. 다음 <표 2>는 사이버안보 관련 선행연구를 검토 및 정리한 결과로, 해당 연구에서 주장하고 있는 핵심 내용이 각 주제 항목에 해당되면 기호 ○로 표시 하였다.

〈표 2〉 사이버안보 관련 선행연구 정리

연구자	주요내용	사이버안보 기본법제정	사이버 안보 역량 강화	사이버 컨트롤 통합 타워 설치	민 · 관 사이버 정보 공유 협력	사이버인력 양성 교육
김도승 (2017)	국가차원에서 사이버안보력 강화를 위한 법적 과제 제시	○	○	○	○	
김문성 (2016)	민 · 관 협력을 위한 사이버안보 관련 법률 정비 및 통합 사이버 컨트롤타워 설치 강조	○	○	○	○	
김재광 (2017)	사이버안보 위협에 대한 법제적 대응방안	○	○			
박상돈 · 김인중 (2012)	사이버보안 법률 제정 필요성과 민 · 관 협력체계 강조	○	○		○	○
성용은 · 윤병훈 (2016)	사이버테러 방지 관련 단일 법률 제정의 필요성 강조	○	○	○		
신재헌 · 김용현 (2016)	사이버 안보위협에 대한 법률적 · 체계적 대응방안 제시	○	○	○	○	
정영도 · 정기석 (2016)	북한의 사이버공격 대응을 위한 사이버테러방지법 제정 및 민 · 관 협력체제 구축 강조	○	○		○	○
정준현 (2015)	국가사이버안전법제 측면에서 통합 사이버컨트롤타워와 법제정의 필요성 강조	○	○	○		

검토해 본 선행연구 모두가 공통적으로 사이버안보 기본법 및 역량 강화의 필요성을 역설하였다. 더불어서 통합 사이버컨트롤 타워 설치 문제나, 민·관 사이버 정보 공유 및 협력의 중요성도 주장하였다. 특히 김도승(2017), 김문성(2016)은 현재 민간과 공공이 이원화 되어있는 우리나라의 사이버대응체계를 지적하면서 통합적인 사

이버컨트롤타워 설치를 주장하였고, 이에 대한 법적 근거를 마련하는 의미에서도 사이버안보 기본법이 필요하다 보았다. 그러나 기존의 법률이나 제도에서의 구체적인 분석 및 제언은 이루어지지 않았고, 큰 틀에서의 방향성만 제시하였다. 또한 박상돈과 김인중(2012), 정영도와 정기석(2016)은 사이버 전문 인력 양성 및 교육, 연구투자에 대한 필요성도 지적하였다. 그러나 현재 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의거 한국인터넷진흥원을 필두로 사이버 관련 전문인력 양성 및 교육이 이루어지고 있다는 점에서, 오히려 이에 대한 개선점을 제시할 필요가 있었다. 더불어서 '국가사이버안보법안'내에서도 비슷한 내용을 규정하고 있기에 법률의 중복 규정내용에 대한 해결책 제시도 필요했다. 이외에도 사이버공간 보호책임을 부과하는 사이버책임기관지정, 사이버안보를 지원하는 전문기업 등의 지정 필요성도 사이버안보를 위한 필요한 부분이지만 선행연구에서 이 부분을 다루지 못하였다.

이처럼 기존의 연구들은 추상적으로 사이버안보 기본법의 부재 및 사이버 역량강화를 위한 법률 제정의 필요성만 언급하였을 뿐, 구체적인 법률에 관한 분석 및 개선점 제시는 이루어지지 않았다. 특히 기존법률의 규정 조항을 토대로 비교 분석하여 사이버안보법의 필요성을 강조한 것이 아닌, 기존 법률 자체의 제정 목적에만 의거한 사이버안보 기본법 필요성 역설이었기에 설득력 측면에서 부족한 부분이 있었다. 이러한 선행연구들은 현재 국회에 계류 중인 '국가사이버안보법안'의 통과를 위한 실질적인 해결방안이 될 수 없기에, 본 연구는 사이버안보 관련 국내 법률과의 구체적인 비교 분석을 통해 법안의 필요성을 고찰하고 실질적인 개선점을 제언한다는 점에서 그 의의가 있다고 하겠다.

Ⅲ. 사이버안보 관련 국내법과의 비교 분석

1. 국가사이버안보법안 분석

2017년 1월 3일 정부에서 발의된 '국가사이버안보법안'은 23개 조문과 1개의 부칙으로 구성되어 있다. 본문은 6개의 장으로 구성되어 있으며, 제1장 총칙을 시작으로 제2장 사이버안보 추진기구, 제3장 사이버안보 예방활동, 제4장 사이버안보 대응활동, 제5장 보칙, 제6장 벌칙으로 이루어져있다.

제1장 총칙에서는 법안의 목적 및 용어정의, 국가의 책무, 다른 법률과의 관계에 대해 규정하고 있다. 현재 사이버공격에 대응하고 사이버안보 역량 강화를 위한 통합적인 기본법이 없는 상태이기에, 본 법안의 제정목적을 알 수 있다. 또한 주목해야 할 점은 '사이버안보', '사이버공간'등의 용어정의를 했다는 점인데, 그동안 우리나라에서 법률로써 정의된 바가 없기 때문이다. 기존의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 '정보통신망'이라는 개념과 매우 유사하긴 하나 '정보통신망'은 물리적 형태가 존재하지만, 본 법안에서 규정하고자 하는 '사이버공간'은 실체가 물리적으로는 존재하지 아니한다는 점에서 차이가 있다. 또한 '국가사이버안보법안'을 사이버안보에 관하여서는 다른 법률에 우선 적용한다는 점을 밝히며 기존의 타 법률과 내용이 중복되거나 법 적용의 우선순위 다툼에 있어서 명확한 정리를 통해 법안의 법적 안전성과 효과성을 도모하고자 하였다.

제2장 사이버안보 추진기구에서는 국가사이버안보 정책에 대한 최고심의기구, 책임기관 및 지원기관, 사이버안보 전문기업 및 연구기관을 규정하고 있다. 우선 최고심의기구로서 국가사이버안보위원회를 설치하고 회의의 장은 국가안보실장을 임명한다. 또한 실무위원회를 설치하여 국가안보실과 국가정보원의 공무원을 공동위원장으로 규정하여, 실무위원회 내에서의 견제와 균형 및 협력을 가능하도록 하였다. 책임기관 및 지원기관 규정은 사이버공간을 보호하는 책임을 지는 기관을 명시하고, 지원기관으로 하여금 필요시 기술적 지원을 하도록 하였다.

제3장 사이버안보 예방활동에서는 사이버안보 기본계획의 수립, 사이버안보 실태평가, 사이버위협정보의 공유 및 위기대응 훈련을 규정하였다. 본 법안에서는 3년마다 사이버안보 기본계획을 수립 및 시행하도록 하였는데, 주로 국내 다른 법률에서는 기본계획을 5년 또는 10년으로 중장기인 경우가 일반적이다. 즉 사이버안보 기본계획 주기를 3년으로 정함으로써 사이버공간의 급변하는 생태계를 대비하고자 하는 것으로 보인다. 또한 사이버안보 실태평가를 매년 하도록 하였고, 사이버위협정보의 공유를 규정하면서 사이버공격을 받았을 시 피해를 최소화 할 수 있도록 하였다. 특히 공유된 사이버위협정보의 오남용을 제거하기 위해 정보의 사용은 필요한 최소한의 범위내로 제한하고 있고, 국민의 권리가 침해되지 않도록 기술적·관리적·물리적 보호조치를 마련하도록 규정하고 있다.

제4장 사이버안보 대응활동에서는 사이버공격의 탐지 및 사고조사, 사이버위기경보의 발령 및 조치, 사이버위기 대책본부 구성 등을 규정하고 있다. 이 제4장은 기존

대통령훈령인 「국가사이버안전관리규정」과 대부분 중복된다. 다만 이러한 내용을 대통령훈령이 아닌 법률로서 규정하여 법적 강제성과 위반 시 처벌을 부과할 수 있다는 것에 의의가 있다고 하겠다.

제5장은 보칙 부분으로 비밀엄수의무, 포상, 국방 분야에 대한 특례, 개인정보처리에 관한 내용을 규정하고 있다. 이 법안에 근거한 사이버안보 활동으로 취득된 정보 및 비밀을 유지하도록 하여 법적 안정성을 도모하였고, 특히 개인의 사생활침해 등에 대한 우려를 해소하기 위해 「개인정보 보호법」제58조제4항을 준용토록 하는 점은 주목해야 할 부분이다.

마지막 제 6장은 벌칙 부분으로 사이버안보에 필요한 업무 시 발생되는 불법이나 부당한 행위에 대한 벌칙 및 과태료를 규정하고 있다. 기존에 실질적으로 사이버안보관련 업무의 근간이었던 「국가사이버안전관리규정」에서는 사이버안보 활동시의 불법 및 부당행위에 벌칙 및 과태료를 규정하고 있지 않아 처벌근거가 미흡하였다. 이에 본 법안이 관련 부분을 규정하면서 사이버안보에 필요한 업무에서의 발생 가능한 불법 및 부당한 행위를 금지하였다.

지금까지 정부가 입법 발의한 '국가사이버안보법안'을 분석해 보았으며 내용을 요약하면 <표 3>과 같다.

〈표 3〉 국가사이버안보법안 요약

구분	국가사이버안보법안 (정부입법案 17.1.3)
구성	본문23조, 부칙2조
사이버안보체계	국가사이버안보위원회 : 안보실
	국가사이버안보실무위원회 : 안보실 · 국정원(공동 운영)
사이버안보활동	기본계획 수립 · 시행 : 국정원
	시행계획 작성 · 배포 : 상급책임기관(중앙부처, 광역지자체 · 교육청, 국회 · 법원 등)
	실태평가 : 국정원(합동평가단 운영)
	보안관제센터 설치 : 책임기관
	사이버위협정보공유센터 설치 : 국정원-책임기관 간 자율적 정보공유
	사고조사 : 상급책임기관(일반 사이버공격), 국정원(안보위협 사이버공격)
	대응훈련 : 상급책임기관(소관영역), 국정원(통합)
	경보발령 : 국정원, 중앙행정기관(분야별)
	대책본부 : 상급책임기관, 국정원
	전문기업 지정 · 관리 : 미래부

구분	국가사이버안보법안 (정부입법案 17.1.3)
사이버안보 .기반조성	포상 : 국정원
	벌칙 : 공유정보 부정사용, 자료삭제, 비밀 미엄수, 직무목적 외 사용 시 5년 이하, 5천만원 미만
	과태료 : 사이버공격으로 인한 사고를 미신고시 1천만원 이하
	개인정보 보호법 제58조 제4항 준용

〈출처: 임진대, 2017: 국가 사이버안보에 관한 법률 · 국가사이버안보법안 검토보고 47쪽 재구성〉

분석내용을 통해 알 수 있는 점은 이 법안이 국민과 국가의 사이버공간의 안보를 위한 중대한 법안이라는 점과, 이 법안으로 인하여 발생가능한 개인정보의 침해라든지 권력집중화를 최소화하고자 관련 사항을 세부적으로 규정하고자 했다는 점이다. 따라서 사이버 정보공유의 문제로 인한 사생활침해, 특정 기관의 권력 집중화의 문제로 이 법안을 반대하는 것은 부적절하다고 보인다. 특히 북한 및 초국가적인 사이버공격은 한수원 사태나 세계를 떠들썩하게 했던 랜섬웨어 등의 문제를 통해 충분히 그 피해의 심각성을 인식할 수 있었다. 따라서 사이버안보에 관련된 기본법을 제정할 필요가 있으며, 이를 통해 발생 가능한 사이버공격으로부터 국민과 국가의 안녕을 수호할 필요가 있다.

2. 사이버안보와 관련된 법의 비교 분석

1) 각 법의 총칙 비교

현재 국내의 기존법률에서 '사이버'또는 '사이버안보'라는 단어는 전무한 상황이고, 대통령훈령인 「국가사이버안전관리규정」에서만 '사이버안보'를 다루고 있다. '사이버'라는 단어 자체가 외래어이기는 하나, 사이버테러·사이버공격·사이버안보 등이 이미 우리사회는 물론 전 세계적으로 자주 사용되고 있는 만큼 충분히 국내의 법률에서 논의되어야 할 사항이다. 따라서 우리나라가 사이버안보와 관련된 사항이 법률에 규정되어 있지 않다는 점은 납득하기 어려운 점이다. 이에 본 연구 서론의 연구방법에서 언급되었듯이, 총 17개의 법을 검토하여 사이버안보와 관련된 4개의 법을 선정하였다. 선정한 법은 「국가사이버안전관리규정」(대통령 훈령), 「정보보호산업의 진흥에 관한 법률」, 「정보통신기반 보호법, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이며, '국가사이버안보법안'과 비교 분석해 기존 국내법들의 사이버안보

관련 허점을 고찰하고 '국가사이버안보법안'의 필요성을 강조하고자 한다.

'국가사이버안보법안'과 비교대상 법의 총칙(목적, 용어정의, 다른 법률과의 관계)을 요약정리해보면 다음 <표 4>와 같다.

〈표 4〉 사이버안보 관련 법규의 목적, 정의, 법률간 관계

	목적	용어정의	다른 법률과의 관계
국가사이버안보 법안	국가안보를 위협하는 사이버공격을 예방하고, 사이버위기에 신속하고 적극적으로 대처함으로써 국가의 안전 보장 및 국민의 이익 보호에 이바지함을 목적으로 함	사이버공간 사이버공격 국가안보위협 사이버공격 사이버안보	사이버안보에 관하여는 다른 법률에 우선하여 이 법을 적용
국가사이버안전 관리규정 (대통령 훈령)	국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버 공격으로부터 국가정보통신망을 보호함을 목적으로 함	사이버공격 사이버안전 사이버위기	대통령 훈령으로 법률보다 하위 개념
정보보호산업의 진흥에 관한 법률	정보보호산업의 진흥에 필요한 사항을 정함으로써 정보보호산업의 기반을 조성하고 그 경쟁력을 강화하여 안전한 정보통신 이용환경 조성과 국민경제의 건전한 발전에 이바지함을 목적으로 함	정보보호 정보보호산업 정보보호기업	정보보호산업에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따름
정보통신기반 보호법	전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 함	정보통신기반시설 전자적 침해행위 침해사고	×
정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 함	정보통신망 정보통신서비스 침해사고 개인정보	정보통신망 이용촉진 및 정보보호등에 관하여는 다른 법률에서 특별히 규정된 경우 외에는 이 법으로 정하는 바에 따름

각 법률 및 훈령의 목적을 살펴보면, 기존 법률들은 정보통신망 또는 전자적 침해행위를 대비한 목적으로 법률이 제정되었는데, 이는 '국가사이버안보법안'에서 정의

한 ‘사이버공간’과 일맥상통한 부분이기에 비슷한 개념으로 볼 수 있다. 다만 국제사회를 더불어 국내에서도 자주 사용되는 사이버테러, 사이버안보라는 단어들을 고려한다면, 직접적으로 ‘사이버’라는 단어를 법률의 이름 및 목적 부분에서 사용함으로써 용어의 이해도를 높이고 법률의 목적을 강조할 수 있을 것이다.

다음으로 용어 정의부분을 살펴보면, ‘국가사이버안보법안’은 기존의 국내법들이 규정하고 있지 않았던 ‘사이버공간’, ‘사이버공격’, ‘사이버안보’등을 명확하게 규정함으로써 용어 개념을 정립하고 오용 및 혼선을 방지하였다. 또한 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정의하고 있는 ‘침해사고’같은 경우 사이버공격으로 인한 침해사고라고 인식될 정도의 직관성을 띄지 않고 있다. 더불어서 기존 법률들은 국가의 사이버 안보를 위한 ‘사이버안보’에 관한 개념정립 역시 전무하다는 점이 주목해야 할 부분이다.

다른 법률과의 관계부분은 특히나 ‘국가사이버안보법안’의 필요성을 여실히 보여주는 대목인데, 각각이 모두 일반법적 성격을 지님으로써 법률의 적용 및 판단 근거에서 혼선을 초래할 수 있다. 반면 ‘국가사이버안보법안’은 사이버안보에 관한 기본법으로 작용하고자하기에 법률적 판단 및 적용의 혼선을 최소화 할 수 있다.

2) 각 법의 내용 비교

‘국가사이버안보법안’의 법률 규정 내용을 기준으로 각각 이에 상응하는 내용이 다른 법률 및 훈령에서 규정하고 있는가에 대한 분석을 하고자 한다. 이를 통해 기존 국내법들의 사이버안보와 관련된 허점을 고찰하고 ‘국가사이버안보법안’의 필요성을 고찰해 보고자 한다.

아래 <표 5> 는 ‘국가사이버안보법안’의 각 조항을 기준으로 비교대상 법인 「국가사이버안전관리규정」, 「정보보호산업의 진흥에 관한 법률」, 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 관련 내용을 규정하고 있는가에 대한 비교 분석 결과표이다. ‘국가사이버안보법안’에서 규정한 내용을 각각의 비교대상 법에서 규정하고 있으면 해당 조항을 명시하였고, 규정하고 있지 않으면 기호 ×를 표시하였다.

〈표 5〉 사이버안보 관련 법 비교 분석

	국가사이버안보법안	국가사이버안전관리규정 (대통령 훈령)	정보보호산업의 진흥에 관한 법률	정보통신기반 보호법	정보통신망 이용촉진 및 정보보호 등에 관한 법률
사이버 안보 추진 기구	제5조 (국가사이버안보위원회)	제6조 (국가사이버안전전략회의) 제7조 (국가사이버안전대책회의) 제8조 (국가사이버안전센터)	제5조 (정보보호산업 진흥계획 수립)	제3조 (정보통신기반보호위원회) 제4조 (위원회의 기능)	제4조 (정보통신망 이용촉진 및 정보보호에 시책의 마련)
	제6조 (책임기관)	×	×	제5조 (주요정보통신기반시설 보호 대책의 수립)	제51조 (중요 정보의 국외유출 제한)
	제7조 (지원기관)	×	×	제7조 (주요정보통신기반시설의 보호지원)	제52조 (한국인터넷진흥원)
	제8조 (사이버안보 전문기업)	×	제23조 (정보보호 전문서비스 기업의 지정 · 관리)	×	×
	제9조 (사이버안보 연구기관)	제15조 (연구개발)	제11조 (정보보호산업의 융합 촉진) 제14조 (기술개발 및 표준화 추진)	제24조 (기술개발 등)	제6조 (기술개발의 추진)
사이버 안보 예방 활동	제10조 (사이버안보 기본계획의 수립)	제5조 제2항 (국가사이버안전정책 · 관리) 제9조 (사이버안전대책의 수립 · 시행)	×	×	×
	제11조 (사이버안보 실태평가)	제9조 제4항 (사이버안전대책의 수립 · 시행)	×	제9조 (취약점의 분석 평가)	제45조의3 제3항 제2호 (정보보호 최고책임자의 지정)
	제12조 (사이버위협정보의 공유)	제10조 (사이버공격 관련 정보의 협력) 제14조 제1항 (전문기관 간 협력)	×	제16조 (정보공유 · 분석센터)	×
	제13조 (사이버위기 대응 훈련)	제9조의2 (사이버위기대응 훈련)	×	×	제52조 제3항 제4호 (한국인터넷진흥원)
사이버 안보 대응 활동	제14조 (사이버공격의 탐지 등)	제10조의2 (보안관제센터의 설치 · 운영)	×	제16조 제1항 제2호 (정보공유 · 분석센터)	제48조의4 제1항 (침해사고의 원인 분석)
	제15조 (사이버공격으로 인한 사고의 통보 · 조사)	제10조 (사이버공격 정보의 협력) 제12조 (사고통보 및 복구) 제13조 (사고조사 및 처리)	×	제13조 (침해사고의 통지)	제48조의4 제2항 (침해사고의 원인 분석)
	제16조 (사이버위기경보의 발령 · 조치)	제11조 (경보 발령)	×	제16조 제1항 제2호 (정보공유 · 분석센터)	제48조의2 제1항 제2호 (침해사고 대응)
	제17조 (사이버위기 대책본부의 구성 · 운영)	제13조 제3항 (사고조사 및 처리)	×	제15조 (대책본부의 구성)	제48조의4 제2항 (침해사고 원인 분석)
보칙	제18조 (비밀 엄수의 의무)	×	제32조 (비밀유지)	제27조 (비밀유지의무)	제66조 (비밀유지)
	제21조 (개인정보 처리 등)	×	×	×	×
벌칙	제22조 (벌칙)	×	제40조 (벌칙)	제28조~제29조 (벌칙)	제70조~제74조 (벌칙)
	제23조 (과태료)	×	제41조 (과태료)	제30조 (과태료)	제76조 (과태료)

상기 <표 5>로 정리된 비교 분석 결과를 '국가사이버안보법안'에서의 각 장에 따른 순서로 고찰해보고자 한다. 우선 '국가사이버안보법안'에서 제2장에 해당하는 사

이버안보 추진기구 분야는 제5조(국가사이버안보위원회), 제6조(책임기관), 제7조(지원기관), 제8조(사이버안보 전문기업), 제9조(사이버안보 연구기관)가 해당된다. 먼저 제5조의 정책심의기구와 관련해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 별다른 심의기구를 두고 있지는 아니하고, 과학기술정보통신부장관 또는 방송통신위원회에서 필요한 제반사항을 마련하도록 하고 있기에 전문성 및 사이버안보에 대한 집중도가 떨어질 우려가 있다. 「정보통신기반 보호법」의 경우 정보통신기반보호위원회가 존재하기는 하나 주요정보통신기반시설에 대한 사항만을 담당하기에 사이버안보에 관한 총체적인 관리가 어렵다. 「정보보호산업의 진흥에 관한 법률」에서는 정보보호 산업 진흥에 관한 사항을 중점적으로 다루고 있기 때문에 사이버안보 정책에 관한 심도 있는 정책을 기대하긴 무리가 있다. 「국가사이버안전관리규정」에서만 국가사이버안전전략회의, 국가사이버안전대책회의, 국가사이버안전센터 등을 규정하고 사이버안전에 관한 전략 및 정책의 구축을 규정하고 있지만 대통령훈령만으로는 부족함이 있다. 제6조 책임기관 부분은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반 보호법」 각각에서 중요기술 및 이를 보관하고 있는 기관 등에 조치를 취하도록 하고 있고, 「국가사이버안전관리규정」에서는 이와 같은 내용을 정하고 있지 아니하다. 제7조(지원기관)의 경우 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 한국인터넷진흥원을 설립하도록 하고 정보보호산업 정책 지원 및 관련 기술 개발 등을 담당하도록 하고 있고, 「정보통신기반 보호법」에서는 전문기관의장에게 필요시 기술적 지원을 요청할 수 있도록 하였다. 이외 「정보보호산업의 진흥에 관한 법률」이나 「국가사이버안전관리규정」에서는 관련 조항에 대한 내용은 없었다. 제8조(사이버안보 전문기업)는 사이버공간을 보호하기 위하여 사이버안보 전문기업을 지정·관리할 수 있는 조항으로 오직 「정보보호산업의 진흥에 관한 법률」에서만이 규정하고 있었다. 사이버공간을 위한 사이버안보 전문기업을 지정한다는 것은 전문성 있는 기업들을 포섭한다는 것을 의미하고, 이는 민·관 협력의 장이 될 수 있다. 따라서 매우 중요한 사항이지만, 대부분의 법률에서 관련 규정이 없다는 점은 현재의 사이버안보에 관한 협력체계의 미흡함을 여실히 보여준다. 제9조(사이버안보 연구기관)의 경우엔 비교대상 법 모두에서 비슷한 사항을 규정하고 있다. 주요 기술의 개발을 위한 연구지원 및 연구기관은 사이버안보 또는 정보통신망의 발전을 위한 필수적인 요소로 관련사항이 있다는 점은 다행스러운 부분이다.

다음 제3장에 해당하는 사이버안보 예방활동 분야는 제10조(사이버안보 기본계획), 제11조(사이버안보 실태평가), 제12조(사이버위협정보의 공유), 제13조(사이버위기 대응훈련)이다. 제10조(사이버안보 기본계획의 수립)는 사이버안보에 관한 총체적인 기본계획을 수립 및 시행한다는 점에서 매우 중요한 조항이다. 이와 관련해서 사이버안보에 관한 기본계획을 수립하는 규정사항은 오직 대통령훈령인 「국가사이버안전관리규정」에서만 존재했다는 점은, 사이버안보에 관한 중요성 인식 부재를 여실히 보여주는 대목이다. 제11조(사이버안보 실태평가)는 사이버안보 전반에 걸친 실태를 평가하고 이를 향후 예산·인사 등에 반영 및 활용하도록 하고 있다. 비교대상법 모두 비슷한 사항을 규정하고 있었지만, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 경우엔 정보통신서비스 제공자에만 국한되어 있었고, 「정보통신기반보호법」의 경우 역시 주요정보통신기반시설에만 국한되어있다. 결국 사이버안보에 관한 종합적인 실태평가 및 피드백이 제대로 이루어질 수 없는 법률 구조를 가지고 있었고, 이는 사이버안보에 관한 선순환 구조 형성의 어려움이 되고 있다. 제12조(위협정보 공유)는 사이버위협정보공유센터를 설치하고, 각종 위협으로부터 대응체계를 구축하는 것으로써 사이버공격에 대비한 필수적인 요소이다. 이와 관련해서 「정보통신기반보호법」에서 비슷한 사항을 규정하고 있긴 하지만 금융·통신 등 정보통신기반시설에만 국한되어 있기에 한계가 존재한다. 「국가사이버안전관리규정」에서만이 이 사항을 규정하고 있지만 대통령훈령이기에 강제성을 띄고 필요한 정보공유 형태가 수립되기 어려움이 존재한다. 특히나 미국, 일본 등은 이미 사이버안보를 위한 민·관 위협정보 공유체계가 매우 잘 정비되어있고, 위협정보만을 위한 법률을 따로 제정하는 등 그 중요성이 커지고 있기에, 우리나라 역시 반드시 관련 사항이 법률로써 규정되어야 한다. 제13조(사이버위기 대응 훈련)는 사이버위기 시에 적절한 대응 체계를 정비하는 내용인데, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서만이 비슷한 사항을 규정하고 있다.

다음 제4장은 사이버안보 대응활동과 관련된 내용으로 제14조(사이버공격의 탐지), 제15조(사이버사고의 통보 및 조사), 제16조(사이버위기경보 발령 및 조치), 제17조(사이버위기 대책본부 구성·운영)가 해당된다. 제14조와 관련하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 침해사고의 원인 분석 등을 위하여 관련 사항을 규정하고 있지만, 정보통신서비스 제공자 및 운영하는 자에만 국한되어 있다는 한계가 있다. 다만 「정보통신기반 보호법」에서는 정보공유·분석센터를 구축·운영

하도록 하고 있어 '국가사이버안보법안'과 비슷한 내용을 이미 규정하고 있다. 이러한 점은 향후 법률의 적용 및 판단 근거에 혼선을 초래하기에 하나의 법률에 통일되게 규정해놓는 것이 좋다. 제15조는 사고의 통보 및 조사의 경우 대부분의 법률이 관련 사항을 규정하고 있었다. 그러나 마찬가지로 각각의 법률에서 이와 같이 중첩된 내용이 규정되어 있으면 법률의 적용 및 근거 판단에 혼선을 초래할 수 있기에 관련 사항을 하나로 통합해 규정할 필요가 있다. 제16조는 사이버위기경보의 발령 및 조치에 관한 사항으로, 「국가사이버안전관리규정」, 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 비슷한 내용을 규정하고 있었다. 다만 각각의 법이 규정하고 있는 대상은 상이한 부분이 있었으나, '국가사이버안보법안'은 국가 차원의 통합적이고 체계적인 구조를 구축하고자 한다는 점이 주목해야할 부분이다. 제17조 위기대책본부의 구성 및 운영에 있어서도 마찬가지로 각각의 법에서 관련사항을 규정하고 있었고, 이 역시 그 대상은 각각 법의 제정 목적에 맞춰서 다른 부분이 존재했다.

다음 제5장은 보칙 부분으로 제18조(비밀 엄수의 의무), 제19조(포상), 제20조(국방분야에 대한 특례), 제21조(개인정보 처리) 가 해당된다. 제18조는 비밀유지에 관련된 내용으로, 업무상 취득된 모든 정보는 비밀유지가 되어야 한다는 내용이다. 비교 법 모두에서 이를 규정하고 있었지만, 법 규정 내용이 사이버안보와 모두 관련 있는 것은 아니였고, 사이버안보 관련 업무에 대한 모든 사항을 포함할 수 없었기에 해당 규정은 허점이 존재했다. 또한 주목해야 할 점은 사실상 기존의 국가 사이버활동 근간이었던 「국가사이버안전관리규정」에 이러한 비밀유지 규정이 되어있지 않았다는 점이다. 일반적으로 대통령 훈령은 벌칙규정이 존재하지 않는 것처럼, 「국가사이버안전관리규정」역시 벌칙규정이 존재하지 않다. 이에 비밀유지의무 및 위반시 벌칙 규정 등이 존재하지 않는 허점이 있었다. 따라서 '국가사이버안보법안'에서는 이러한 업무상 취득정보의 비밀유지의무를 규정함으로써 정보유출로 발생 가능한 문제를 최소화 하였다. 제19조(포상 등)와 제20조(국방 분야에 대한 특례)는 사이버공격에 대한 탐지 및 대응 등에 기여한 자에 대한 포상과, 전시의 경우 이 법이 군사작전을 지원하기 위해 수행되어야 한다는 내용으로, 관련 법률간의 비교 분석이 모호하다는 점에서 생략하기로 한다. 제21조의 경우는 개인정보처리에 관한 내용을 규정한 것으로서 본 법안에서 매우 중요한 부분이다. 특히나 '국가사이버안보법안'이 통과되지 못하고 계류 중에 있는 원인 중 하나로서, 사이버안보를 위한 목적 하에 무분

별한 개인정보의 수집을 우려하였기 때문이다. 그러나 '국가사이버안보법안'에서는 이러한 우려를 종식시키기 위해 사이버안보를 위하여 처리되는 개인정보는 「개인정보 보호법」 제58조제4항을 준용하도록 하여 필요최소한의 수집과 수집된 정보의 안전한 관리를 위한 기술적·관리적·물리적 보호조치를 하도록 하고 있다. 따라서 '국가사이버안보법안'은 구체적으로 개인정보보호법 일부를 준수하도록 하는 내용을 규정함으로써 무분별한 개인정보침해가 일어나지 않도록 하였고, 수집된 정보의 안전한 보안조치도 마련하였다.

마지막 제6장은 벌칙부분으로 제22조(벌칙), 제23조(과태료)가 규정되어 있다. 그동안 사이버안보 활동의 근간이었던 것은 「국가사이버안전관리규정」이었지만, 벌칙 및 과태료 조항이 없다. 따라서 관련내용이 반드시 필요한 부분이었고, '국가사이버안보법안'에서 이를 규정하였다. 비교대상의 법률의 경우 벌칙 및 과태료 부분이 존재하지만 이 역시 법률의 모든 내용이 사이버안보와 관련된 것은 아니였기에 그 연관성은 미비했다. 따라서 '국가사이버안보법안'에 사이버안보와 관련된 벌칙 및 과태료 부분을 규정함으로써, 본 법안의 부당한 오남용을 방지하였고, 필요한 법적 강제성을 부과하여 사이버안보 기본법으로서 작용하도록 하였다.

3) 소결 및 정책적 제언

지금까지 '국가사이버안보법안'을 사이버안보와 관련된 국내 다른 법들과 비교 분석하였다. 비교 분석결과 사이버안보 기본계획이나 위협정보의 공유, 사이버안보 전문기업 등과 같은 반드시 필요한 사항이 기존 법률에서는 존재하지 않았다. 기본계획의 경우 사이버안보에 관련된 전반적이고 총체적인 국가계획을 설립하고, 이에 수반되는 여러 정책을 규정하는 것으로서 사이버안보의 큰 틀을 구조화한다는데 의의가 있다. 그러나 이러한 기본계획을 법으로서 규정하는 내용이 존재하지 않았기에 반드시 필요한 상황이다. 사이버위협정보공유의 사항은 미국, 일본 등을 비롯하여 국제적으로 중요한 이슈로 부각되고 있고, 관련 법률이 따로 제정되고 있는 상황이다. 더불어 사이버공격이 단순히 정부기관에만 국한되는 것이 아닌, 민간에도 다양한 형태로 발생되기 때문에 관련 정보의 공유와 이를 통한 협력 대응 체계 구축을 위한 근거 법률이 존재해야 할 필요성이 있다. 또한 사이버안보 전문기업 등을 지정하고, 사이버공간을 보호하기 위한 지원구조를 공식화 한다면 사이버대응 전문성의 증대효과도 얻을 수 있다.

반면 어떤 부분은 이미 기존 법률에 제정되어 있는 부분도 존재하여 법률의 적용 및 판단 근거에 혼선을 초래할 여지도 있었다. 정책심의기구같은 경우 각 법률마다 정책기구를 신설하도록 하고 있었는데, '국가사이버안보법안'의 경우 국가사이버 안보 정책에 대한 최고심의기구로서의 지위를 규정하였기에 다른 정책심의기구와의 관계에 있어 명확한 구분이 필요하였다. 또한 관련 사항의 연구 및 연구기관 역시 각각의 법이 모두 규정하고 있었는데, 너무 많은 연구기관이 난립하면 오히려 작업의 능률이 떨어질 수 있고, 제대로 된 관리가 어려울 수 있다. 따라서 통합된 연구기관을 설립하여 관리를 일원화하고 연구능률 향상을 도모해야 할 것이다. 실태평가나 사고 대응과 관련해서는 대부분의 법에서 규정하고 있었기에 이에 관한 정리도 필요하다. 특히 사고대응의 경우 각각의 법이 사고 발생 경보와 대응 및 조사까지 모두 규정하고 있었는데, 자칫 사고 대응에 있어 혼선이 초래될 수 있다. 이에 '국가사이버안보법안'에서는 국가차원의 일원화 된 통보 및 조사 체계를 구축하도록 함으로써 사고대응의 효율성을 극대화하고자 하였다. 따라서 다른 법률에서 중첩되거나 혼선을 초래할 우려가 있는 규정사항들은 '국가사이버안보법안'을 사이버안보 기본법으로 적용시키기 위해 관련 내용 삭제 또는 개정이 필요하다.

이처럼 '국가사이버안보법안'은 기존의 법률에서 규정하지 않았던 사이버안보와 관련된 총체적인 내용을 담았다. 즉 사이버안보와 관련된 기본법적인 성격을 지님으로서 기존 법률에서의 부족함을 채워주고, 여러 법률로 산재해 있는 사이버 안보 관련내용 판단에 있어서 혼선 역시 줄이고자 하였다.

Ⅳ. 결 론

오늘날 사이버공격은 국내뿐만 아니라, 초국가적으로 발생되며 고도화 되고 있다. 과거 DDOS 공격이나 한수원, 국방부 해킹 등이 바로 그것이며, IS 나 알카에다 등의 테러단체 역시 미국의 정부 및 금융기관 등에 사이버테러를 감행하고 있다. 이러한 상황 속에서 미국을 비롯한 일본, 중국 등은 사이버안보에 관한 독립된 법률을 제정하고 사이버안보력 함양을 도모하고 있다. 반면 우리나라는 2006년 '사이버위기 예방 및 대응에 관한 법률안'을 시작으로, 가장 최근인 2017년 발의된 '국가사이버안보법안'까지 기존법률과의 중첩문제, 사생활 침해우려, 정보공유문제 등으로 지금까지

도 여전히 국회에서 통과되지 못하고 계류 중에 있다.

이에 본 연구는 사이버안보 기본법이 필요하다는 인식아래, 현재 국회에 계류 중인 '국가사이버안보법안'을 기존 사이버안보와 관련된 국내법들과 비교 분석을 통해 고찰해봄으로써, 법안 제정의 필요성을 강조하고 향후 필요한 개선점을 제시하고자 하였다. 비교대상 법을 선정하기 위해 국내의 17개의 법률 및 훈령을 검토하였고, 결과적으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반 보호법」, 「정보보호산업의 진흥에 관한 법률」, 「국가사이버안전관리규정」(대통령 훈령) 4개를 선정하여 '국가사이버안보법안'과 비교 분석 연구를 진행하였다.

연구 결과로는 사이버안보 기본계획, 위협정보의 공유, 사이버안보 전문기업 지정 등의 중요한 사안이 기존의 국내 법률에서 규정되어 있지 않았고, 이는 '국가사이버안보법안'제정의 필요성을 알 수 있었다. 특히 사이버안보 기본계획 같은 경우 사이버안보와 관련된 총체적인 국가계획을 설립한다는 면에서 상당히 중요한 내용이며, 사이버위협정보의 공유 역시 민·관 정보 공유를 통한 효과적인 사이버 위협 대응 구조를 형성할 수 있다는 점에서 필요하다. 또한 사이버안보와 관련된 전문적인 법률이 전무하다는 점에서 '국가사이버안보법안'의 제정은 필요하다고 볼 수 있다.

그러나 일부 다른 법들과 중첩되는 내용도 있었는데, 정책심의기구 및 연구 기관 등은 비교대상 법에서 모두 규정하고 있었기에 이로 인한 혼선 및 비효율화를 초래할 수도 있었다. 따라서 정책심의기구의 경우 '국가사이버안보법안'에서 규정하는 심의기구를, 국가사이버안보와 관련된 최고정책심의기구로의 명확한 구분이 필요해 보였다. 또한 연구기관 역시 각 법마다 규정하고 있기 때문에, 연구기관 난립으로 인한 재정적·능률적인 비효율화를 초래할 수도 있다. 이에 사이버안보와 관련된 연구기관을 통합하고 관련 규정을 일원화하여 체계적이고 효과적인 연구 환경을 조성할 필요가 있다.

이처럼 '국가사이버안보법안'은 현재 사이버안보와 관련된 법률이 전무한 상황에서 사이버안보의 기본법적인 성격으로서 작용할 수 있는 필수적인 법안이라고 할 수 있다. 특히 현재 사이버안보와 관련된 사항이 대통령훈령인 「국가사이버안전관리규정」에 대부분 의거하고 있다는 점에서도 이 법안의 필요성을 여실히 보여주고 있다. 다만, 본 법안이 분석결과처럼 기존 법률과의 일부 중첩되는 부분은 해결되어야 할 문제로 보이며, 기본법으로서의 지위 역시 확실하게 보장받아야 법적 안정성과 효력을 다 할 수 있을 것으로 보인다.

본 연구의 한계점으로는 각각의 비교대상 법들의 제정 역사와 맥락, 입법과정 등에 대한 상세한 분석을 토대로 연구가 진행되지는 못했다는 점이 있다. 이러한 기존 국내법에 대한 전반적인 배경의 분석을 토대로 연구가 이루어졌다면 사이버안보 관련 법률의 보다 심도 있는 비교 분석 연구가 이루어졌을 것이다. 따라서 이는 향후 연구과제로 다뤄야 할 것으로 보인다.

끝으로 현재 우리나라가 사이버안보와 관련된 법률이 전무한 상황에서 본 연구에서 제시한 개선방안을 감안해 '국가사이버안보법안'이 제정된다면, 사이버안보 기본법으로 작용하여 대한민국의 사이버안보력 함양에 크게 기여할 것으로 기대된다.

참고문헌

권오국, 석재왕 (2016). 주요국의 사이버테러 대응체계와 시사점 분석 -미국·영국·독일 사례의 비교를 중심으로-. **한국경호경비학회지, 49**, 185-214.

김도승 (2017). 국가 사이버안보의 법적 과제. **미국헌법연구, 28**(2), 99-130.

김문성 (2016). 사이버테러 국가대응체계 구축방안 : 법률체계와 조직체계를 중심으로. **평화학연구, 17**(1), 161-184.

김재광 (2017). 사이버 안보위협에 대한 법제적 대응방안. **법학논고, 58**, 145-177.

박상돈, 김인중 (2012). 한국과 미국의 사이버보안 단계별 법제도 비교 연구. **융합보안논문지, 12**(4), 33-40.

박웅신 (2013). **복합적 위험사회에서 사이버 테러 규제방안에 대한 연구**. 법제처 미래융합법제 연구보고서, 177.

신재헌, 김용현 (2016). 사이버 상의 안보위협에 대한 대응방안. **한국경찰연구, 15**(3), 75-104.

윤병훈, 성용은 (2016). 한국 사이버테러 방지를 위한 효과적 대응방안. **융합보안논문지, 16**(2), 11-17.

임진대 (2017). **국가 사이버안보에 관한 법률안·국가사이버안보법안 국회정보위원회 수석전문위원 검토보고서**. 국회 정보위원회,

장신 (2015). 사이버공격과 Jus in Bello. **국제법학회논총, 60**(4), 199-226.

정영도·정기석 (2016). 북한 사이버공격에 대한 대응방안에 관한 연구. **융합보안논문지, 16**(6-1), 43-50.

정용기 (2016). 우리나라의 사이버 안보 위협현황과 대응방안. **경찰학논총, 11**(4), 189-215.

정준현 (2015). 국가사이버안전법제의 방향에 관한 연구. **법학논총, 39**(4), 277-317.

채재병 (2013). 안보환경의 변화와 사이버안보. **정치정보연구, 16**(2), 171-193.

한국인터넷진흥원 (2011). **사이버 보안법제 선진화 방안 연구**. 방송통신정책연구 11-진흥-라-02, 292.

ITU Recommendation. (2008). Overview of Cybersecurity, *ITU X-1205,* 2.

O. Hathaway el al. (2012). The Law of Cyber-Attack. *ICalifornia Law Review, Inc., 100(4),* 817-885.

■ 법

「국가사이버안전관리규정」(대통령훈령 제316호)

「국가정보화 기본법」(법률 제14905호)

「군사기밀 보호법」(법률 제13503호)
「군형법」(법률 제14183호)
「개인정보 보호법」(법률 제14839호)
「보안업무규정」(대통령령 제28211호)
「부정경쟁방지 및 영업비밀보호에 관한 법률」(법률 제14839호)
「산업기술의 유출방지 및 보호에 관한 법률」(법률 제14591호)
「전기통신사업법」(법률 제14839호)
「전자금융거래법」(법률 제14828호)
「전자문서 및 전자거래 기본법」(법률 제13768호)
「전자서명법」(법률 제14839호)
「전자정부법」(법률 제14914호)
「정보보호산업의 진흥에 관한 법률」(법률 제14839호)
「정보통신기반 보호법」(법률 제14839호)
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(법률 제14839호)
「형법」(법률 제13719호)

【Abstract】

A Study on the Necessity of Establishing the National Cyber Security Act through a Comparative Legal Analysis

Kim, Sung-Hyun · Lee, Chang-Moo

During the recent years, cyber attacks have been increasing both in the private sector and the government. Those include the DDOS cases in 2009, the Blue House cyber attack, bank hackings etc. Cyber threats are becoming increasingly serious. However, there is no basic law related to cyber security at present, and regulations related to cyber security are scattered in various domestic laws. This can lead to confusion in the application of the law and difficult to grasp the regulations related to cyber security. In order to overcome this situation, the bill on the prevention and countermeasures against cyber crisis was initiated in 2006, but it has been abrogated. Since then, it has been repeatedly proposed, but it has been abrogated repeatedly due to the overlapping of existing laws and concerns about infringement of personal information. The most recent initiative was the National Cyber Security Act, which was initiated by the government in January 2017. The act focuses on resolving the absence of a basic law related to cyber security, strengthening its responsiveness in the event of a cyber security crisis, and fostering security strength. Therefore, this study seeks to contribute to the establishment of National Cyber Security legislation as a basic law of cyber security by examining the necessity of National Cyber Security legislation through comparative legal analysis with existing domestic laws related to cyber security and suggesting policy implications.

Keywords: Cyber Security, Cyber Security Law, Cyber Attack, Cyber Terror, National Cyber Security Act