

# 입법교착 요소로 분석한 사이버안보법 표류에 관한 연구

방 휴,<sup>1\*</sup> 권 현 영<sup>2\*</sup>  
<sup>1,2</sup>고려대학교 (대학원생, 교수)

## A Study on the Drift of Cybersecurity Law by Element Analysis of Political Gridlock

Hyu Bang,<sup>1\*</sup> Hun-Yeong Kwon<sup>2\*</sup>  
<sup>1,2</sup>Korea University (Graduate student, Professor)

### 요 약

4차 산업혁명의 진행으로 사회의 다양한 영역이 연결된 초-연결 사회로 진입하게 되었고 물리적 전쟁에 대한 정치, 사회적 비용이 급증하게 되었다. 이로 인해 국가 혹은 비국가적 행위자에 의한 사이버공격은 목표대상에게 가장 효과적인 수단으로 기능하게 되었다. 또한 전통적 격차가 북한과의 대립현실은 북한이 비대칭 전력인 사이버공격에 집중할 수밖에 없는 환경을 조성했으며 우리나라는 대부분의 기간시설을 정보통신기술을 이용하여 관리하는 정보통신기술분야의 선진국이기에 사이버공격이 한국에 가장 위협적인 요소가 되었다.

이러한 상황을 일찍부터 맞이했음에도 불구하고, 우리나라에서 사이버공격을 대응하는 방식은 항상 임기응변적이었다. 현재까지도 사이버안보 기본법이 표류되어 사이버안보 체계 구성에 한계를 가지고 있으며 보완에도 불구하고 사이버위협대응에 혼선이 발생해 지속적으로 사회의 문제점으로 제기되어 왔다.

이 연구는 우리나라 정도의 정보통신분야의 선진국에서 사이버안보 기본법이 꾸준히 발의되었음에도 불구하고 결과적으로 모두 임기만료 폐기되고 기존에는 대통령훈령의 형식으로 2021년이 되어서는 대통령령의 형식으로 제정된 원인을 입법교착의 요소인 거대양당이 제시하는 폐기안의 내용 및 이해관계의 차이, 제기된 시점과 주기를 포함하는 한국의 입법제도 등을 통해 분석하여 기존 사이버안보기본법이 왜 표류되었는지 분석한다.

### ABSTRACT

This study analyzes the political and legislative progress that although basic acts to establish an integrated system of cybersecurity are steadily being proposed, they have not been passed as legislative deadlocks under the two major parties. It shall be analyzed through Korea's legislative system, including differences in contents and interests of the disposal act, the timing and cycle of election ect. The study analyzes why the basic cybersecurity law was previously scrapped and faced political gridlock situation by analyzing the differences in the contents and interests of the two major parties, and the timing and cycle of the proposed legislation.

**Keywords:** Cybersecurity, National Cybersecurity, Governance, Legislation, Political Gridlock

## 1. 서 론

정보통신기술 및 사이버공간의 활용은 현대 사회의 핵심적 요소가 되었다. 국가기간시설들은 정보통신기술들을 이용하여 운용되어 사이버공간으로 편입되었다. 사이버공간 활용의 증가로 인하여 국가의 시스템 운용을 효율적 가능하게 하였으나 그러한 사용 증가에 비례해 위협성과 부작용 역시 커지고 있다.

신기술들을 이용하여 운용되어 사이버공간으로 편입되었다. 사이버공간 활용의 증가로 인하여 국가의 시스템 운용을 효율적 가능하게 하였으나 그러한 사용 증가에 비례해 위협성과 부작용 역시 커지고 있다.

예를들어 우리나라의 경우 2000년 초부터 다양한 사이버공격 및 사전사고가 발생하였고 2003년 1월을 시작으로 2013년 민간의 방송·금융 전산시스템이 대상으로 파괴되는 사이버공격, 2014년 한수원 원자력 제어시스템을 목표로 한 사이버공격이 시행되는 등 사이버공간에서의 위협은 단순히 정보획득의 범위를 넘어 국민의 안전과 직접적인 관련이 있는 사회기반 시설의 운영과 안전을 위협하고 있다.

이러한 사이버공간에서의 위협은 제2차 세계대전 당시의 전략적 폭격행위의 확장을 넘어섰다고 봐도 무방할 정도로 전장과 민간의 경계를 허물고 있으며 그러한 복잡성이 안보의 패러다임을 전환하고 있다. 사이버공격은 그 저비용성과 고효율성 무엇보다 그 행위가 초래하는 결과에 비해 물리적 위협 행위보다 행위에 대한 정치적으로 낮은 부담 및 위험성 및 시행에의 시간적 제한이 상대적으로 원활한 특징을 가지고 있기에 행위 자체의 빈도도 비약적으로 증가하고 있다. 그러한 행위는 또한 점점 지능적이고 고도화되고 있어, 사회경제와 국가안보를 저해하는 가장 심각한 위협 중의 하나가 되었다.

시간과 공간을 초월하고 공공, 군사, 민간 영역의 구분 없이 동시다발적으로 발생 가능한 사이버공격을 예방하고 신속하고 정확히 대응하기 위해서, 사이버 위협정보를 협력적으로 공유·분석하고 사이버위협을 조기에 탐지하고 대응책을 빠르게 전파할 수 있는 체계의 구축이 필요하다는 주장이 일어났다. 그 결과 유관 기본법들만이 지속적으로 의회에 제출되었으나, 각 정당간 입장의 충돌로 법률안이 회기내에서 계류되었다가 통과되지 못하고 임기만료 폐기되었다. 물론 큰 정책적 담보성을 필요로 하지 않는 민간부문에서의 정보공유는 어느 정도 이뤄져 왔지만, 상기 언급한 바와 같이 사이버공격의 경우 민간에서 정보공유만 제대로 이루어진다고 공공과 군사영역의 사이버안보까지 담보할 수는 없어 공공과 민간을 구분하지 않고 빠르게 사이버위협정보를 분석·공유할 수 있는 사이버안보체계의 보완과 컨트롤타워구축 등 명확한 제도와 법 입안의 필요성이 지속적으로 제기되어 왔다[1].

우리나라는 경제적 측면에서나 군사적 측면에서 북한보다 우위를 점하고 있다. 이 때문에 전통적 군사안보 경쟁에서 남한의 승리가 담보되어 있고, 북한은 비대칭적 전력을 적극적으로 활용하여 해당 상황을 극복하고자 한다. 그러한 갈등은 기존에는 핵전력으로 이제는 사이버공간에서 이어지고 있다[2].

우리나라는 세계적으로도 고도로 선진화되어 정보통신기술에 대한 의존도 역시 매우 높다. 거기에 특수한 외교·안보적 상황을 맞이하고 있어 사이버피해를 방어하기 위해 명확한 법·제도 구축 필요성이 제기되었다. 그러나 사이버안보 관련 기본법들이 경제를 비롯한 타 이슈의 법안들에 비해 중요성이 간과되어 간결하고 명확한 제도와 법체계를 구축하지 못했다. 2021년 1월 국가정보원법이 개정되고 사이버안보 업무규정이 대통령령으로 제정되어 국가 전체 영역을 포괄하는 사이버안보 관련 업무 체계와 공공부문의 사이버위협·공격에 대한 예방·대응 업무를 보완하였으나, 2020년 제시된 사이버안보 기본법안 역시 여전히 표류하고 있으며 기본법 형태로는 보완되지 못하고 있다.

정부와 입법부 및 학계를 비롯한 각종 사회에서 제기되었던 문제를 바탕으로 지속적으로 요구되던 사이버안보 관련 기본 법안들이 지속적으로 표류해 왔던 것은 입법 단계에서 각 정당들이 사이버안보에 대해 가지고 있는 인식이나 이해관계가 달라 발생한 입법교착의 결과이다[3].

이 연구는 II장에서 기존 한국의 사이버안보체계가 어떤 과정을 거쳐서 구성이 되었고 기존 사이버안보체계가 어떠한 문제점을 가지고 있다고 논의되었는지에 대해 제시한 뒤, III장에서는 그러한 문제점을 극복하기 위한 다양한 입법논의들이 10년이 넘는 기간 동안 입법교착 상황에 빠져 통과되지 못했던 상황을 입법교착의 요소를 통해 분석하여 원인을 분석한다.

## II. 이전 사이버안보 제도의 연혁과 쟁점

### 2.1 이전 사이버안보 제도 구축의 연혁

2003년 1월 25일 인터넷 대란의 발생으로 인터넷을 통한 전자상거래, 금융서비스 등이 전면 중지됐다. 워 바이러스에 의해 인터넷 기능이 마비됐기 때문이었다. 이러한 일련의 사건들로 인하여 노무현 대통령 시기부터 사이버공격에 대한 국가 차원의 체계적인 대응체계의 필요성을 절감해 취임 직후 국가정보원을 중심으로 국가사이버안전관리체계를 구축하도록 했다. 이에 국가정보원과 국가안전보장회의는 국방부·정보통신부 등과 협조해 기본계획을 세웠고 이 계획에 따라 범국가 차원의 사이버안전을 담당하는 국가사이버안전센터가 창설됐다[4].

이후 2005년 국가정보통신망을 사이버공격으로부

터 보호하기 위해 사이버안전에 관한 조직, 운영사항을 체계적으로 정립하려 했다. 이 결과 사이버공격에 대한 종합적, 체계적인 국가적 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터를 설치해 국가사이버안전정책의 수립, 사이버위협 관련 정보의 수집·분석 등의 업무를 수행하도록 했다. 또한 공공부분의 국가정보통신망에 대한 사이버공격, 사이버위협 정보를 즉각적으로 국가정보원장에게 통보하도록 하고 국가정보원장은 사이버공격에 인한 사고의 발생 또는 징후를 발견하거나 관계 중앙행정기관의 장으로부터 사고의 발생사실 등에 대하여 통보를 받은 때에는 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 하게 하는 내용을 담은 '국가사이버안전규정'이 대통령령으로 제정되었다[5].

2009년 7.7 디도스 대란으로 일컬어지는 사이버테러가 발생하면서 청와대, 국방부, 등 공공기관의 웹사이트와 농협과 시중은행의 웹사이트 등 많은 웹사이트가 공격을 받고 그러한 사건들에 대한 대응체계가 잘 작동하지 않아 국민들의 불편이 초래되고 안보위협의 우려가 나타났다. 게다가 2011년에도 디도스 공격이 발생하여 기존보다 더 큰 사이버피해가 사회적으로 확산되게 되고 농협전산망이 당해 4월 해킹되었다. 그 결과 범정부 차원의 국가사이버위기종합대책 이행을 위해 중앙행정기관의 장 등은 보안관계센터를 설치·운영하도록 하고, 국가정보원장은 주의 수준 이상의 경보 발령 시 사이버위기대책본부를 구성할 수 있도록 하는 한편, 그 밖에 기존 제도를 개선·보완하기 위해[6] '국가사이버안전규정'이 개정되었다.

2012년에도 지속적으로 국가기관 홈페이지에 대한 디도스 공격이 발생하여 사회·경제적 혼란이 발생하자 국정원장의 지휘하에 사이버안전 정책을 효율적·체계적으로 수행하기 위하여 사이버안전기본계획을 수립·시행하도록 하고, 사이버위협에 대한 국가차원의 상황관제, 위협분석, 합동조사 등을 하기 위하여 사이버안전센터에 민·관·군 합동대응반을 설치하고, 공공기관의 사이버공격 대응훈련을 강화하는 등[7] 기존 제도의 한계를 보완하기 위해 '국가사이버안전규정'이 또 개정되었다.

또한 '2013년 국가사이버안보종합대책'에 따라 국가안전에 대한 대응을 위해 대통령령으로 국가안보실을 신설하여 대통령을 보좌하기 위해 청와대 직속 산하로 둔 뒤 정보융합비서관을 신설하여 사이버공간을

포함하는 안전보장의 컨트롤타워로 세우고 실무총괄은 상기 언급한 바와 같이 국가정보원이 하도록 하였다[8]. 하지만 과학기술정보통신부, 국방부 등 유관 행정기관에게는 담당 대응체계를 구축하여 발표하도록 하여 민간 영역의 사이버보안은 분야별로 다양한 기관에서 컨트롤타워 역할을 수행하게 하였다.

이에 따라 사이버공격에 체계적으로 대응하기 위해 국가안보실의 역할을 강화하여 신속한 위기상황 전파체계를 구축하는 등 기존 제도의 운영상 나타난 한계들을 개선·보완하기 위해 사이버공격에 관한 정보를 입수하거나 사이버공격으로 인한 사고가 발생한 경우 중앙행정기관의 장이 국가정보원장뿐만 아니라 국가안보실장에게도 같이 통보하도록 하였으며 군사부분의 경우 국방부장관이 국방분야 사이버공격 경보를 발령하기 전에 국가정보원장 및 미래창조과학부장관과 경보 관련 정보를 교환하도록 하여 국방분야 사이버위기에 체계적으로 대응하도록 하고 국가안보실장이 상기한 상황을 종합하여 대통령에게 보고하도록[9] '국가사이버안전규정'을 개정하였다.

2014년 한국수력원자력의 원전 설계도면이 해킹되는 등 다양한 사이버안보에 위협이 되는 사건이 발생하여 2015년 4월 '국가사이버안보대체 역량 강화 종합대책'을 수립하고, 대규모 사이버공격 발생시 민·관·군 간 정보공유로 신속한 상황 파악·공동대응을 통한 피해확산 방지를 위하여 '국가사이버위협 정보공유시스템'을 구축하였고 사이버안보 수행체계를 국가안보실 중심으로 일원화하기 위해 대통령령으로 국가안보실직제가 개정되어 사이버안보비서관이 신설되었다[10]. 이를 통해 사이버안보 수행체계를 일원화하고자 노력하였고 대통령의 유관 직무를 효율적으로 보좌하고자 하였다. 다만 국가안보실은 국가안보에 관한 대통령의 직무를 보좌하기 위한 청와대 소속 보좌기관이기에 대통령을 도와 국가안보에 관한 기능을 원활히 수행할 수 있도록 보조하는 기관으로 정책결정권은 없고, 오직 대통령에 대하여만 책임을 부담했기에 실질적으로 컨트롤타워가 일원화되었다고 평가받지는 않았다[11].

## 2.2 이전 사이버안보 제도의 쟁점

사이버 공격 및 테러에 대한 신속한 대응과 피해 확산 방지를 위해 국가적 차원에서 사이버위협정보 공유체계를 구축하여 실시간으로 사이버위협 정보를 공유하고 협력적인 대응책을 구축할 필요가 지속적으로

로 제기되어 왔기에 그 중심축의 역할을 담당할 컨트롤타워 및 사이버안보의 통합적이며 협력적인 체계의 필요성이 지속적으로 논의되어 상기 언급한 바와 같이 2005년에 제정된 '국가사이버안전관리규정'에 따라 사이버공격으로부터 국가정보통신망을 보호하기 위한 국가사이버안전관리체계가 구축되었고, 2015년 국가사이버안보 강화 및 국가안보실직제의 제정으로 사이버안보 수행체계의 정비 및 국가정보원 산하에 국가사이버위협정보공유시스템이 구축되었다[12].

우리나라는 행정부처의 기능별로 대응체계가 구축되어 있어 국가안보실을 중심으로 국가정보원과 협의하여 컨트롤타워가 성립되어 역할을 수행했고 국가정보원은 공공기관, 과학기술정보통신부는 민간분야의 정보보호 역할을 수행했다[13]. 그 결과 각종 사이버위협사고가 발생할 때마다 사이버안보 추진체계의 및 컨트롤타워 정비의 필요성이 항상 제기되었고, 어느 기관에서 컨트롤타워를 맡을 것인지에 대해 논의가 오갔던 것이다[14].

기존 사이버안보의 실무부처 및 컨트롤타워의 역할은 국가정보원장이 국가안보실장과 협의하여 담당하고 있었는데, 하위 훈령에 근거하여 사이버안보 직무를 수행하는 국가정보원이 컨트롤타워 기능을 수행하고 법령에 근거하여 업무를 수행하는 중앙 및 지방행정기관이 실무를 맡는 문제가 제기되었다. 이에 따라 정부 각 부처에 분산된 정보보안 대응조직의 협력과 지원을 얻어내기 어려우며 정보공유에 한계가 지적된 것이다[15]. 특히 사이버안보 분야의 경우 꾸준히 민·관·군의 협력이 강조되었으나, 정보통신기반은 정부 이외에도 민·관이 함께 운영하고 있기에 이들의 협조를 얻는 것에 있어 다양한 외부기관과의 긴밀한 협력체계를 구축하기 어려운 점이 지적되었다[16].

여기에 추진체계가 국가정보원, 행정안전부, 과학기술정보통신부, 국방부 등으로 분산되어 있었는데 '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '정보통신기반보호법', '국가사이버안전규정' 등 다수의 법률을 기반으로 여러 정부조직이 동시에 정보보안 기능을 수행했었기에 부처 간 업무혼선 및 기능상 중복을 자일 수 있고 그에 따른 신속한 대응의 문제 발생 가능성 역시 제기되었다[17].

또한 사이버안보와 관련된 법체계의 조정 필요성도 제기되었다[18]. 우선 사이버안보 부분에 있어 체계적인 분석과 정책적 고민 없이 필요 혹은 사건 발생 시마다 임기응변식으로 관련 법률을 제·개정해

왔기에[19] 전통적안보와 사이버안보 분야 간의 역할 구분이 불분명했고 사이버안보의 개념과 범위가 불분명하게 확정되어 일반법적 정보보안활동과 혼용되어 정보보안과의 개념적 혼동을 가져왔다[20].

'정보통신망 이용촉진 및 정보보호 등에 관한 법률', '정보통신기반보호법', '국가사이버안전규정' 등 다수의 법령 및 훈령에 따라 체계를 구성해 왔었기에 법제도 및 각 기관의 기능과 책임에 있어 사이버안보 법체계에 있어 법률 간 공백 및 중복되어 특정한 문제가 발생할 경우 이를 처리할 수 있는 조항이 없거나, 또는 특정한 보안사고가 발생할 경우 혼선의 여지가 생겼던 것이다[21].

예를들어 '국가사이버안전관리규정'과 '정보통신기반보호법'의 경우 물론 '정보통신기반보호법'이 상위기본법인긴 하나 주요정보통신망을 동시에 규제했기에 사이버사고 발생 시 부처 간 역할 및 책임이 불분명했다[22].

### 2.3 이전 사이버안보 기본법의 입법과정

상기 언급한 한국의 사이버안보 제도의 변화에 따른 쟁점의 발생으로, 국회에서 사이버안보와 사이버안보체계를 명확하게 하기위한 관련 기본법률 제정 및 개정을 위한 움직임이 꾸준히 있어왔다. 2008년 공성진 의원이 대표로 '국가사이버위기관리법안'이 최초로 발의되었고, 사이버안보에 있어 위협이 되는 사건들이 발생한 이후로 이전에 비해 지속적으로 법안이 발의되었으나 모두 임기만료로 폐기되었다.

18대 국회(2008.04 ~ 2012.04)시기 여당인 한나라당 공성진 의원이 대표로 2008년 10월 '국가사이버위기관리법안'을 대표로 발의했다. 내용을 살펴보면 국가규모의 정보통신망 마비사태와 조직적인 사이버공격에 대해 민간과 공공 단독으로의 차단에 대한 한계를 지적하고, 민간과 공공이 포함되는 종합적인 대응체계 구축을 통한 국가안전보장을 목표로 하고 있으며 이 법안은 국가정보원장 산하로 국가사이버안전센터 설치 및 민·관 협의체 구성을 제안하였고 사이버공격 혹은 사고 발생시 그 조사 결과를 국가정보원장 및 중앙행정기관장에게 통보하도록 규정하였고, 국가정보원장의 경우 필요하다는 판단이 있으면 직접적인 조사를 실시하도록 제안하였으나[23] 2012년 임기만료로 폐기되었다.

19대 국회(2012.04 ~ 2016.04)시기 '농협전산망 해킹'사건이나 '3.20 대란' 및 개인정보 대량유출

사건과 같은 사이버안보체계의 보완과 그에 따른 법제화의 필요성을 체감할 수 있는 사건들이 다양하게 발생하여 많은 법안들이 발의되었다.

2013년 3월에 여당인 새누리당 하태경 의원이 대표로 발의한 '국가 사이버안전관리에 관한 법률안'을 살펴보면 북한에 의한 디도스 공격, '농협전산망 해킹' 등을 언급하며 당시 사이버위협을 관리하는 제도가 정립되지 아니하였으므로 국가 차원의 기본계획을 수립을 통한 사이버안전을 확보를 주장하였다. 이 법안은 전 회기 공성진 의원안과 마찬가지로 국가정보원장 휘하에 국가사이버안전센터를 설치하고 정보통신망에 발생한 사고에 대하여 공공의 경우 국가정보원장에게 보고하고 국가정보원장이 조사할 권한을 부여하게 되어 있었으나[24], 국무총리산하로 국가사이버안전전략회의를 설치하는 점 및 민간분야에 대해서는 방송통신위원회 위원장이 사이버경보를 발령하는 점에서 같은 당에서 제시되었던 법안과 차별성을 가지고 있었으며, 역시 회기내 가결되지 못하고 임기만으로 폐기되었다.

당해 4월 여당인 새누리당 서상기 의원이 대표로 발의한 '국가 사이버테러 방지에 관한 법률안'을 살펴보면 사이버공격으로부터 정보통신망 마비사태, 첨단 기술의 유출 등의 위기 발생시 대응하고 사이버공격을 민간과 정부가 단독적으로 차단하기엔 그 공간의 특수성으로 인한 한계가 있기에 민·관의 종합적인 대응체계 구축을 제안하였다[25]. 기존 보수정당 의원법안들과 다르게 사이버안보 분야의 통합적 거버넌스 구축을 위한 민·관 협력을 명시했고 직전 하태경 의원안과 달리 국무총리가 아닌 국가정보원장 소속의 국가사이버안전전략회의의 설치를 제시해 국가정보원 중심의 대응체계 구축을 제안했다. 이 법안 역시 회기내 가결되지 못하고 임기만으로 폐기되었다.

당해 7월 야당인 민주통합당 정청래 의원은 '정보통신기반 보호법 일부개정법률안'을 대표로 발의하면서 기존 '정보통신기반 보호법'의 개정을 통한 사이버공격대응책을 제시했다. 이 개정안은 사이버공격 발생시 공공은 국가정보원이 담당하고 민간은 미래창조과학부가 담당하는 이원화된 체계로 인해 대응에 한계가 있다는 점을 보수정당의 안과 마찬가지로 지적했으나 사찰의 위험이 있고 국회의 통제가 이뤄지기 힘든 국가정보원이 아닌 미래창조과학부 중심의 '정보통신기반시설 보호센터' 설치와 침해사고 대응훈련, 침해사고에 대한 경보발령과 사고조사 실시 및 국방분야의 경우 국방부장관을 중심으로 하는 체계를

제안했다[26]. 이 개정안은 기존 '국가사이버안전규정'에서 정해진 국가정보원의 권한인 침해사고 대응 계획 수립 및 대응훈련과 경보발동 및 사건에 대한 조사 등을 미래창조과학부 장관에게 이관하도록 명시하며 국가정보원 중심의 체계를 제안한 보수정당 의원들의 제안 법안과 대비되는 안을 제안하였다.

2014년 1월 야당인 민주통합당 변재일 의원이 '정보통신기반 보호법 일부개정법률안'을 대표로 발의하였다. 이 법률안 역시 직전 정청래 의원이 발의한 법률안 및 보수정당의 안들과 동일하게 공공과 민간을 분리해 사이버안전을 도모하는 체계가 효과적이지 않다는 점을 지적하였다. 이 법률안 역시 같은 당 정청래 의원이 대표발의한 개정안처럼 미래창조과학부 중심의 대응체계 구축을 언급했다. 다만 보다 좀 더 통합적으로 민·관·군을 관리하는 '국가정보통신기반안전센터'의 설치를 제안했다[27]. 두 개의 야당에서 제시한 개정안 역시 회기내 가결되지 못하고 임기만으로 폐기되었다.

19대 회기 후반 2015년 5월 여당인 보수정당 새누리당 이철우 의원이 '사이버위협정보 공유에 관한 법률안'을 대표로 발의하였다. 당시 미국의 오바마 정부의 사이버 정보공유 및 보호법(Cyber intelligence Sharing and Protection Act)이 한창 논의되고 있는 시점[28]이었다. 비슷하게 사이버위협정보공유에 초점을 맞추고 있는 법안이었다. 이 법안은 국가정보원장 산하에 '사이버위협정보 공유센터'를 설치하고 국가안보실장, 미래창조과학부장관 등과 협의를 통한 사이버위협정보 공유체계 구축을 제안했다[29]. 기존에 제시되었던 법률안들이 사이버공격에 대응하는 전체적 체계 구축과 전반 내용을 담고있는 반면 이 법률안의 경우 사이버위협정보의 분석, 제공, 공유와 그 체계에 한정된 법안이었다.

당해 6월 여당 소속의 이노근 의원은 '사이버테러 방지 및 대응에 관한 법률안'을 대표로 발의했다. 이 법안은 이전의 법률안들과 마찬가지로 국가적 차원에서 체계적인 사이버테러 방지와 대응제도가 수립되지 못한 한계를 지적하고 민·관이 협력적으로 대응할 수 있는 체계를 제안했다. 2013년 4월 같은 정당의 서상기 의원이 대표발의한 법률안과 비슷한 내용을 담았는데 국가정보원장을 소속으로 사이버안전센터를 두며 민·관협의체를 구성하고 운영할 수 있는 권한을 부여하고자 하였으며 국가정보원장에게 사이버테러의 방지 및 대응 기본·시행계획 수립 및 배포와 경보발령 권한 사고조사권한 등을 부여해 국가정보원

중심의 체계를 제안하였고 행정부 주도로 기술개발, 산업육성, 인력교육, 국제협력 등에 대한 지원시책을 제공하는 법안을 제안했다[30]. 해당 법률안의 경우 테러방지에 집중되어 있기에 국방 분야의 대응에 관한 규정이 포함되지 않았고 국회·법원·헌법재판소·중앙선거관리위원회에 대한 사이버테러 방지 대응 실태를 점검·평가하는 행위는 국회·법원·헌법재판소·중앙선거관리위원회가 요청한 경우로 제한해 타당의 정청래 의원이 대표발의한 개정안에서 제기된 국가정보원

의 사찰의 위험과 국회통제의 문제를 다른 방향으로 반영한 안으로 평가받았다.

19대 국회 회기가 거의 종료되는 시점인 2016년 2월 여당 소속 서상기 의원은 ‘국가 사이버테러 방지 등에 관한 법률안’을 대표로 발의하였다. 이 법안은 기존에 제안된 이노근 의원의 법안 및 2013년 4월 제안했던 법안과 유사한 법안이었다. 이 법안 역시 사이버공간의 특수성과 강한 연계성 및 복잡성으로 인해 국가차원의 체계적인 제도와 절차의 필요성을

Table 1. Progress of Cybersecurity legislation

Legislator	Sung-Jin Gong	Tae-Kyung Ha	Sang-Ki Suh	Chung-Rae Jung	Jae-Il Byun
Affiliated Party	Conservative	Conservative	Conservative	Democrats	Democrats
Government	Trifecta	Trifecta	Trifecta	Trifecta	Trifecta
Assembly No.	18th	19th	19th	19th	19th
Date.	Oct. 2008	Mar. 2013	Apr. 2013	Jul. 2013	Jan. 2014
Result	Disposal by term expiration	Disposal by term expiration	Disposal by term expiration	Disposal by term expiration	Disposal by term expiration
Name of bill	National Cyber Crisis Management Act	National Cyber Safety Management Act	National Cyber Terrorism Prevention Act	Amendment of Information and Communication Infrastructure Protection Act.	Amendment of Information and Communication Infrastructure Protection Act.
Main Authority	National Cyber Safety Strategy Conference, Prime Minister, NIS	National Cyber Safety Strategy Conference, Prime Minister, NIS	National Cyber Safety Strategy Conference, NIS	National Information and Communication Infrastructure Protection Center, MSIP	National Information and Communication Infrastructure Protection Center, MSIP
Legislator	Chul-Woo Lee	Noh-Geun Lee	Sang-Ki Suh	Chul-Woo Lee	Executive
Affiliated Party	Conservative	Conservative	Conservative	Conservative	Executive (Conservative)
Government	Trifecta	Trifecta	Trifecta	Divided	Divided
Assembly No.	19th	19th	19th	20th	20th
Date.	May. 2015	Jun. 2015	Feb. 2016	May. 2016	Jan. 2017
Result	Disposal by term expiration	Disposal by term expiration	Disposal by term expiration	Disposal by term expiration	Disposal by term expiration
Name of bill	Cyber Threat Information Sharing Act	Cyber Terrorism Prevention and Response Act	National Cyber Terrorism Prevention Act	National Cyber Security Act	National Cyber Security Act
Main Authority	Cyber Threat Information Sharing Center, ONS, NIS	Cyber Safety Strategy Conference, NIS	National Cyber Security Center, NIS	National Cyber Security Policy Coordination Conference, National Cyber Security Center, NIS	National Cyber Security Council, ONS, NIS

역설했다. 이 법안은 국가정보원 소속으로 국가사이버안전센터를 설치해 이노근 의원안과 마찬가지로 제안했으나 기본계획의 경우 행정부에서 수립하도록 하고 사이버테러에 및 사고 조사시 그 결과를 미래창조과학부 장관에게도 통보해야 하는 절차를 포함하고 역시 국회·법원·헌법재판소·중앙선거관리위원회에 대한 사이버테러 지침의 시행과 대응 실태 점검 등의 행위를 요청한 경우로 제안하여 민주통합당에서 제안한 국가정보원의 사찰의 위험과 국회통제의 문제들을 분산화와 보고의 다양화를 통해 반영하려고 했다 [31]. 하지만 2015년도부터 2016년까지 19대 국회 회기 후기에 여당으로부터 제안된 법률안 모두 역시 임기만료로 폐기되었다.

20대 국회(2016.04 ~ 2020.04) 회기 초 2016년 5월 여당인 새누리당 이철우 의원이 '국가 사이버안보에 관한 법률안'을 대표로 발의하였다. 이 법안 역시 사이버공격에 대한 대응을 사이버안보의 영역으로 간주하며 공공과 민간이 분리되어 운영되고 있어 대처가 효율적이지 못한 부분이 있음을 지적했다. 특히 '국가사이버안전관리규정'의 한계를 지적하면서 민간 부분에 대한 사이버공격의 예방과 대응에 있어 기본법 입법을 통해 국가차원의 일원화된 체계 구축을 목적으로 하고 있다고 명시했다. 해당 법률안의 경우 대통령 소속으로 국가사이버안보정책조정회의를 두고 국가정보원장 산하 국가사이버안보센터를 설치해 체계적이며 종합적인 사이버안보 업무 수행을 도모하며 여기에 더해 국가정보원장은 사이버위협정보의 국가차원에서의 효율적인 관리 및 공유를 위하여 국가사이버위협정보공유센터를 구축해 운영하는 내용을 포함했다[32].

이후 박근혜 정부에서는 정부입법의 형태로 2017년 1월 '국가사이버안보법안'을 발의하였다. 해당 법안 역시 사이버공격의 민간과 공공을 가리지않는 성격에 대해 제시하고 사이버공간을 책임기관에게 보호할 권한을 부여해 사이버위협에 관한 정보의 공유와 공격의 예방과 대응을 위한 체계 정립을 목적으로 하였다. 내용을 보면 대통령 소속으로 국가사이버안보위원회를 신설해 국가안보실장을 위원장으로 하여 사이버안보 전문가들을 임명하도록 하였다. 국가정보원장의 경우 사이버안보 계획을 수립·시행하고 공공의 영역에 있어 예방과 대응에 관한 실태를 평가할수 있도록 하며 사이버공격으로 인한 사고 발생시 국가정보원장에게 조사할수 있는 권한 및 경보를 발령하고 책임기관에 대한 지정 권한을 부여하였다. 사이버위협

정보공유의 경우 국무총리 휘하 사이버위협정보공유센터를 설치하는 내용을 담았으며 중앙행정기관장 등은 경보발령 및 공격발생시 사이버위기대책본부를 구성해 운영할 수 있다는 내용도 포함했다[33]. 새로운 사이버안보 컨트롤타워로 국가사이버안보위원회를 구축하고, 대통령, 국무총리, 국가안보실장, 국가정보원장 등의 협력체계를 구성하려는 법률안이었으나 제안되었을 당시 박근혜 대통령이 국정농단사태로 인한 직무정지 중이었고 당시 야당인 더불어민주당은 비록 분산화되어 있다 하더라도 사찰의 위험이 있는 국정원의 권한이 여전히 강하다는 이유로 반발했으며 20대 국회에서 제안되었던 사이버안보 기본법률안 역시 모두 임기만료로 폐기되었다.

2021년 국가정보원법 개정과 '사이버안보 업무규정' 제정 전 사이버안보 관련 법안 혹은 개정안들이 입안되고 폐기되는 과정은 Table 1.과 같다.

### III. 사이버안보 기본법안의 입법교착 현상에 대한 검토

#### 3.1 입법교착

앞에서 본 바와 같이 사이버안보는 한국의 주요한 안보로 간주되어 사이버안보체계 정비 및 기본법 제정의 문제가 꾸준히 제기되어 왔다. 그러나 입법부에서 논의된 사이버안보체계 보완 및 관련 기본법안들은 논의만 진행되고 실질적인 가결의 결과를 도출해 내지 못했다. 21대 회기 조태용의원이 대표로 발의한 '사이버안보 기본법안' 역시 가결의 흐름을 이어가지 못하고 자연스럽게 논의의 대상에서 제외되고 있다. 다만 2021년 국가정보원법의 개정안이 의회제도를 이용하여 통과되고 동시에 '사이버안보 업무규정'이 기본법이 아닌 대통령령으로 제정되는 변동은 있었다.

한국의 사이버안보 관련 법은 없는 것이 아니라 다양한 법령·훈령에 흩어져 있는데, 사이버위협이나 공격이 발생했을 때 법적 대응체계가 분산되어 개인 정보, 행정정보, 국가기밀 등 정보보호의 대상이 되는 정보별 유관 부처와 지원·전문기관도 다른 상황에서의 사고처리와 수습과정의 혼선이 있었다. 정보화 사회에서는 사이버안보 거버넌스의 융통적 통합을 요구하며 협력적 체계로의 운영을 필요로 하는데, 헌법과 정부조직법에 근거하는 전통적 체계에 더하여 정보보안에 유관한 각종 조직·작용법을 운용하기 위한

기본법 입법 혹은 관련 기본법 개정의 조치의 필요성이 꾸준히 제기되었다[34].

그러한 사이버안보 관련 기본법안들은 10년 넘게 대부분 입법부에서의 가결에 실패해왔다. 해당 법안들이 항상 입법교착 상황을 직면했기 때문이다. 입법교착은 쟁점 사안에 대해 의회가 의결하지 못하는 상황을 지칭하는데[35], 대의민주주의하에서 이렇게 발의된 법안들이 통과되지 못하는 상황은 모든 공간이 사이버공간으로 연결되어 초연결사회에 진입한 한국에서 평시 시민들의 기본권 보호나 침해 등이 발생할 수 있어 다양한 논의가 필요한 사이버안보체계 구축과정에 대해 국민을 대표하는 입법부를 통해서서는 효과적으로 대응하지 못하는 것을 의미하는 것이다. 따라서 사이버안보에 대한 효과적인 대응을 위해 이러한 갈등을 극복하려는 노력이 요구된다.

입법교착은 의원내각제 국가보다는 한국과 같이 대통령과 의회가 각각 이원적 정통성을 갖는 대통령제 국가에서 더 많이 발생되고 있다[36]. 입법교착 크게 두 가지로 정의된다. 하나는 “의회가 국가적 문제를 해결하지 못하는 상태”로 입법교착을 정의하는 것으로 의회가 쟁점이슈를 제도하에서 처리하지 못하고, 교착상태에 빠진 상태를 입법교착으로 정의하는 것이다[37]. 두 번째는 의회의 다수당이 정책의 변화를 원하는데도 불구하고 “의회의 제도로 현 정책의 변화를 이끌어내지 못하는 상태”를 의미하는데 이러한 상황에서는 정책이 안정화되어 크게 개정할 수 없는 상태를 말한다. 물론 이러한 상황에서는 의원 개인간 합의가 이뤄지지 않는 미시적 갈등상황으로 볼 수도 있고, 특정 정책에 대해 개별 의원들이 법안을 통과시키거나 개정안을 통과시키기 위해 경쟁하는 상황으로 볼 수도 있다[38].

이러한 의회의 입법교착을 설명하는 대표적인 가설은 분점정부 상황이다. 분점정부 상황은 속칭 ‘여소야대’로 불리는 상황으로 대통령이 속하는 여당이 의회에서 과반수를 확보하지 못할 때 입법교착을 맞이하기가 더 쉽다는 것이다. 1980년대 미국에서 분점정부 상황이 자주 발생하면서, 학자들은 분점정부를 입법교착의 주요 원인으로 파악하기 시작했다. 분점정부 상황에서는 여당의 입장을 반영하는 경우가 많은 행정부와 야당의 목소리가 강한 입법부 사이에 당파적 갈등의 동기가 생긴다. 즉 분점정부 상황에서는 의회 다수당인 야당이 대통령이 주도하는 입법안을 수용하게 되면 대통령 및 여당의 능력을 인정하는 것이 되고, 이러한 상황이 자기들의 선거에 방해가

될 수 있기에 대통령과 여당의 의제를 강하게 거부할 동기를 가진다는 것이다. 따라서 분점정부 상황의 의회에서는 입법지연과 비효율적인 입법 결과가 나타나기 쉽다는 것이다[39].

그 이후 연구들은 분점정부와 입법교착의 인과성에 의문을 제기했다. 대표적으로 메이휴(Mayhew)는 20세기 중후반 미국 의회입법을 검토한 결과 꼭 분점정부 상황만이 중요법안의 입법을 감소시키지 않는다는 것을 발견했다[40]. 이러한 연구들이 진척됨에 따라 정당양극화의 수준으로 입법교착의 원인을 분석하는 즉 의석분포와 의원성향을 입법교착에 영향을 미치는 요인으로 주목했다[41]. 정당간의 이념적 대립과 양극화 수준이 낮으면, 양당 소속 의원 사이에 교차투표 가능성이 높아지기 때문에 정당 사이의 대립만으로 입법교착이 발생할 가능성이 낮아지는 것이다.

또한 다수당이 필리버스터와 같은 이슈화되기 좋은 입법지연 행위 및 행정부의 거부권 등을 막을 수 있는 의석수를 확보하면 입법교착이 발생할 가능성이 낮아진다. 연구자들은 경험적 분석을 통해서 분점정부상황 그 자체가 입법교착의 원인으로 설명되는 것이 아니라 정당양극화의 수준이 높고 입법지연 행위 및 행정부의 거부권 등을 막을 수 있는 초·다수 정당이 없는 경우 대통령이 속한 여당이 입법부 내에서도 다수인 단점정부 상황에서도 분점정부 상황에 버금하도록 입법교착이 발생할 가능성이 높아지며 초다수제를 포함한 의회 의사결정 제도를 포함하여 입법교착의 원인을 설명하였다.

그 외에도 법안의 정책적 특성이나 그 특성에 따른 선거와 재선상황 등 그 정책의 민감성 혹은 차이의 크기 등의 특성으로 인해서 입법교착이 발생할 수도 있다. 법안의 유형에 따라서, 입법과정 역시 유형에 따라 다른 양상으로 전개된다. 특히 여당과 야당이 첨예한 차이를 보이는 법안이나, 각 정당의 이념적으로 중시하는 분야를 규정하는 법안의 경우 입법교착 현상이 발생할 가능성이 크다. 예를 들어 한국에서 대북지원 관련법안과 국가보안법 및 그리고 기업규제 법안과 같은 법안들의 경우 다른 공감할 수 있는 요소들이 더 많은 법안들에 비해 입법교착이 발생할 가능성이 크며 선거기간이 가까워 오는 경우에 제기되는 법안과 같은 경우 입법교착의 가능성이 커진다[42].

이러한 입법교착 현상이 기존 연구들에서 한국의 의회에서 적용되는 상황을 살펴보면 첫째, 국회의사결



정 입법의 시간에 관련한 입법교착으로 원구성 특히 위원회에 의한 입법성공률이 높은 한국에서는 위원회 원구성이 회기의 후기로 갈수록 갈등관계가 심화되면서 유의미한 차이를 보이며 지연되는데 이를 포함하여 회기 후기 즉 선거기간에 가까울수록 입법교착의 가능성이 높아지게 된다[43].

둘째, 국회 의사결정과 관련된 제도에서 나타나는 입법교착으로 예를 들어, 2012년 5월 통과된 국회선진화법 이후에는 야당의 무제한 토론을 허용하고 국회의장 직권상정요건을 높여 모든 법안에 대한 실질적으로 초·다수결을 제도화했다는 점이 입법교착의 원인으로 지목되기도 한다[44].

셋째 입법의 주요 행위자들을 규율하는 조직, 정당에 의한 입법교착의 설명으로 대통령제 하에서 국회 내 의석확보 즉 분점정부 상황과 단점정부 상황에 근거한 설명이다. 한국에서는 입법부가 행정부와 그 수반인 대통령을 견제하는 경우는 적고 대통령에 저항하는 야당과 대통령을 지지하는 여당으로 갈등의 구도가 형성되었다[45].

넷째 한국의 의회정치에서 입법교착의 당파적 요인인 정당양극화로 의결에 있어 주요 정당 사이의 입장이 크게 다를수록, 입법교착에 빠질 확률이 높다. 한국에서 제16대 국회부터 제19대 국회까지 거대 양당의 정치·경제·사회 정책에 있어서 이념을 비교한 결과[46], 거대 양당 내부에서의 이념적 통일성은 강화되고 정당간의 이념적 이질감은 지속적으로 증가하면서 변화했다[47].

다섯째, 입법안의 성격이 쟁점적인 경우 입법교착 현상이 나타난다. 정책 여러 영역에서 여야 입장이 극단적으로 갈릴 수밖에 없는 조항을 많이 포함하고 있을 때, 입법교착이 발생한다고 설명되고 있다[48].

### 3.2 기존 사이버안보법 표류에 적용된 입법교착 요소

입법교착의 요소들을 사이버안보 관련 법안에 적용해보면 먼저 선거기간에 가까게 즉 회기 후반에 제기되는 법안일수록 입법교착이 진행된다는 요소는 사이버안보 관련 법안의 입법교착을 설명하는데 부족하다. 2008년 공성진 의원의 안이나 2016년 이철우 의원의 안의 경우 선거 직후 회기가 시작될 때 법안이 제기되었고 2015년부터 제시된 새누리당 의원들의 안의 경우 상대적으로 회기 후반에 제시되었으나 모두 결과적으로는 임기만료로 폐기되었기 때문이다.

의회자체의 제도 및 분점정부, 단점정부 상황과 관련한 설명도 사이버안보 관련 법안의 입법교착 현상을 설명하지 못한다. 2008년 공성진 의원이 “국가 사이버위기 관리법안”이 발의했을 때 공성진 의원은 국회의 과반이 넘는 한나라당 소속의 의원이었다. 즉, 단점정부 상황이었으나 “국가 사이버위기 관리법안”은 통과되지 않았고 임기만료로 폐기되었다. 이는 다음 회기 및 다다음 회기에도 여당인 새누리당이 국회 다수당이 되었으나 박근혜 대통령이 당선된 시기의 새누리당 의원의 발의 역시 모두 단점정부 상황임에도 여당의원들에 의해 발의된 관련 법안들이 전부 임기만료로 폐기된 것으로 알 수 있다.

초다수제와 같은 다양한 제도적 특성 역시 사이버안보 관련 법안의 입법교착을 설명하는데 부족하다고 할 수 있다. 2012년 5월 통과된 국회선진화법 이후에는 야당의 무제한 토론을 허용하고 국회의장 직권상정요건을 높여 입법교착이 증대되었다고 하나 사이버안보법은 그 전후를 가리지않고 제의되었다 폐기되었다. 이후 사이버테러방지법의 경우는 당시 국회의장이 정부여당의 직권상정을 거부하는 등 어느정도 제도에 의한 교착상황이 발생했으나 그 이외의 법안들은 크게 제도를 이용하여 방해받지 않았다. 주체의 측면에 있어서도 여당과 야당이 제시한 안 심지어는 정부에서 제안한 법률안 모두 임기만료로 폐기되었고 2016년 이철우 의원의 안의 경우 122명이 넘는 의원을 통해서 제안했음에도 모두 계류되어 해당 요소들이 폐기법안마다 다르게 적용되어 폐기의 근거로 사용됨에 있어 부족함을 알 수 있다.

사이버안보 관련 법안들의 정책적 특성이 모든 측면에서 쟁점적이고 정당양극화가 단기에 급속도로 심화되어 입법교착 현상이 나타났다고 보기는 어렵다. 그래서 민주화 이후 한국의 경우 이념적 특징을 강하게 드러내는 노동정책, 조세정책, 개발정책 등에서의 입법교착이 많았다[49]. 그러나 사이버안보 분야의 경우, 일부분 차이가 일정하게 존재하지만 사이버안보의 기존 체계를 보완하고 통합적인 추진체계를 갖춰야 한다는 조항들이 모든 경우 비슷하게 제시되었기에 그 이념적 특성이 특정 정당이나 정권의 목적에만 부합하는 법안이라고 보기 어렵다.

게다가 사이버안보 관련 법안은 시민들에 의한 체감도가 낮아 선거에 영향을 줄만한 의제는 아니다. 그래서 제출되었던 법안의 세부 내용을 비교해 보면 현행 사이버안보 법안을 보완하는 것 자체에 대한 찬반이 아닌 사이버안보를 담당하는 주체의 권한을 어

Table 2. Elements of Political gridlock applied to enacting Parliamentary Cybersecurity legislation

Element of Political gridlock	National Cyber Crisis Management Act (Sung-Jin Gong)	National Cyber Safety Management Act (Tae-Kyung Ha)	National Cyber Terrorism Prevention Act (Sang-Ki Suh)	Amendment of Information and Communication Infrastructure Protection Act. (Chung-Rae Jung)	Amendment of Information and Communication Infrastructure Protection Act. (Jae-Il Byun)
Legislate Time	×	×	×	×	×
Parliamentary system	×	×	×	×	×
Divided government	×	×	×	×	×
Political polarization	×	×	×	×	×
Contentious Law	○	○	○	○	○
Element of Political gridlock	Cyber Threat Information Sharing Act (Chul-Woo Lee)	Cyber Terrorism Prevention and Response Act (Noh-Geun Lee)	National Cyber Terrorism Prevention Act (Sang-Ki Suh)	National Cyber Security Act (Chul-Woo Lee)	National Cyber Security Act (Executive)
Legislate Time	○	○	○	○	○
Parliamentary system	×	×	○	×	×
Divided government	×	×	×	○	○
Political polarization	×	×	×	×	×
Contentious Law	○	○	○	○	○

이에 둘 것인가에 대한 차이만을 보인다.

2011년 제정된 개인정보보호법의 경우 감독기구의 독립성을 둘러싸고 첨예한 대립이 없었던 노무현 정부시기에는 임기만료로 폐기되었고 대립이 강화되었던 이명박 정부시기에 오히려 법제화되었는데 [50], 사이버안보 관련 법안의 임기만료폐기 과정에선 이러한 과정을 찾아볼 수 없이 계류되어 임기만료 폐기되는 현상이 반복되었다. 즉 그 필요성에 대한 공감대는 형성되어 왔기에 지속적으로 법안은 발의되었나, 실제 입법을 위한 노력이 상대적으로 떨어졌던 문제가 발생한 것이기도 하다[51].

한국의 사이버안보 관련 법안은 쟁점화의 수준이 전통 안보문제들에 비해서는 낮지만, 안보 의제의 종류로 간주되어 입법교착이 나타났을 수는 있다[52]. 사이버안보 관련 법안이 정당 입법을 통해 지속적인

로 발의되어도 기간만료로 폐기되거나 계류하는 상황은 사이버안보 의제에 대한 서로의 인식이 미흡한 것이 아니라 심화된 정당 간 이념적 경쟁 속에서 특정 요소로 인한 갈등이 교착으로 이어진 것이라 해석될 수도 있다[53].

제안된 요소중 차이를 구체적으로 살펴보면 2008년 이후 보수정당(한나라당, 새누리당, 현 국민의힘)이 발의한 안들의 경우 모두 법안의 실무주체에 국가정보원장이 기재되어 있다. 반면에 주요 양당 중 진보정당(민주통합당, 현 더불어민주당) 발의한 안들의 경우 실무주체가 미래창조과학부(현 과학기술정보통신부) 장관으로 기재되어 있다. 두 정당의 사이버안보에 있어서 주무 기관에 관한 입장의 차이와 각자의 주장을 관철하고자 하는 갈등이 사이버안보 관련 법안의 입법교착으로 이어졌다고 할 수 있는 것이다.

정리하면, 사이버위협을 우리나라의 주요한 사회적 위협으로 받아들이며, 국가주도로 사이버안보를 효과적으로 구축하기 위하여 대응체계를 일원화하고 보완하는 노력이 필요하다는 것에는 양 거대 정당에 공감대가 형성되었으나, 입법교착의 핵심은 바로 국가안보로서의 중요도를 가진 사이버안보의 관할 권한을 어느 기관에 둘 것인가의 문제이다. 구체적으로는 사이버안보 영역에서 국가정보원에 권한을 부여할 지 갈등이 있어왔던 것이다[54].

입법부를 통해서 사이버안보와 관련한 법안 제정 및 개정안이 제정되는 것에 있어서 각 법안들에게 적용되는 입법교착 요소를 보면 Table.2에서 확인할 수 있는데, 각 법안들에 적용된 요소를 보면 비슷한 성격 및 조항을 가지고 있는 법률안들임에도 불구하고 입법시기에 따른 입법교착, 의회제도에 따른 입법교착, 분점정부 구성에 따른 입법교착, 정당양극화에 따른 입법교착 요소들은 공통적으로 적용되지 않았고, 특정 기관에 대한 입장 차이 즉 해당 쟁점조항으로 인하여 입법교착이 공통적으로 발생해왔음을 알 수 있다.

특히 거대양당중 진보정당의 경우 국정원의 권한 강화에 대해 반대입장을 꾸준히 견지하고 있었다. 이러한 입장이 사이버안보 관련 법안에서도 드러난 것으로 볼 수 있다. 2013년 장외투쟁 등을 통해 국정원개혁을 강하게 주장했고 이는 곧 19대 대선 이후 국가정보원법 개정 및 기무사령부 해체로 이어지기도 했다. 2016년 3월 국정원의 권한 강화에 대한 반발로 테러방지법에 대한 필리버스터를 192시간 동안 진행하기도 했다. 거기에 2020년 국가정보원법에서 대공수사권 제외를 포함한 개정안을 초-다수 의석을 통해 강행하였다. 진보정당은 여러 이슈에서 국가정보원 권한 강화에 반대하는 모습을 보여왔고 이러한 입장이 보수정당의 입장과 충돌을 일으켰던 것으로 판단된다.

#### IV. 결 론

2020년 12월 15일 야당의 반대에도 불구하고 현 21대 국회 회기에서 여당이 3/5이상의 의석을 점유하며 필리버스터제도까지 무력화하며 기존 국가정보원법을 전면 개정하였다.

주요 골자로는 먼저 대공수사권을 경찰에 3년 유예하여 이관하고 두 번째로는 국정원의 국내 정보 수집을 금지하기 위해 국정원 직무 범위에서 국내보안

정보, 대공, 대정부전복 등 불명확한 개념을 삭제하였으며 세 번째로는 정보위원회 재직 의원 2/3 이상의 찬성으로 특정사안에 대하여 보고를 요구할 경우 관련정보를 공개 하도록 하였다.

사이버안보와 관련하여 제4조에 따라 국가정보원의 직무 범위를 국외 및 북한에 관한 정보, 방첩, 대테러, 국제범죄조직에 관한 정보, 사이버안보 및 위성자산 정보 등의 수집·작성·배포, 보안 업무, 직무수행 관련 대응조치, 사이버 공격 및 위협에 대한 예방 및 대응, 정보 및 보안 업무의 기획·조정 등 조직의 업무 범위를 명확히 하였다[55].

이는 국가정보원이 국가안전보장에 관한 사무의 일환으로 오랫동안 담당했던 국가 전체 영역을 포괄하는 사이버안보 관련 정보 업무 체계와 공공부문의 사이버공격·위협에 대한 예방·대응 업무를 기존 훈령에 의해 규정되던 체계보다 법체계적으로보다 공고히 하였다고 평가될 수 있다[56].

국가정보원법이 개정됨에 따라, 정부는 국가정보원의 주요업무로 명시된 사이버안보 업무의 수행과 관련하여 법률에서 위임된 사항과 그 시행에 필요한 사항을 정하기 위하여 대통령령으로 사이버안보 업무 규정 역시 2020년 12월 31일 제정하고 명일 시행하였다.

주요 내용을 살펴보면 첫째 기존 국가사이버안전센터를 사이버안보 업무를 효율적으로 수행하기 위하여 산하 국가사이버안보센터로 변동하였다. 둘째 사이버안보 관련 업무의 수행을 위하여 중앙행정기관 등 및 외국 정보기관과 정보협력체계를 구축할 권한을 부여하였다. 세 번째 중앙행정기관 등에 배포·공유하기 위하여 정보공유시스템을 구축·운영할 수 있게 하였다. 네 번째 중앙행정기관 등에 대한 사이버안보 기본대책을 수립·시행 권한도 부여하였다. 거기에 보안성검토, 보안관리 컨설팅, 훈련과 실태평가, 공공보안관제, 경보발령, 피해 조사 등의 권한 역시 부여하고 기술연구 개발과 전문기관 지정 권한 역시 부여하였다[57].

국가정보원법의 개정 및 대통령령으로 사이버안보 업무규정을 제정함에 따라 기존 사이버안보체계에 대한 많은 쟁점들이 일정부분 해소된 것으로 보인다. 개념이 분산화되어 한계가 지적된 초연결사회에서의 사이버공간 관리를 국가안보로 격상하는 사이버안보 개념의 법률로 지정함에 따라 사이버안보의 범위 및 법체계와 거버넌스가 정비되고 상대적으로 유관 기관들의 권한이 명확해 졌으며 국외정보기관과의 협력

주체 역시 상대적으로 명확해 졌다.

이러한 의의에도 불구하고 기존 정당들에 의해 제 기되어 왔던 각종 사이버안보 기본법 조항 중 누설 등을 포함하는 벌칙조항이 빠졌고 여전히 정보통신망법을 비롯한 타법과의 혼선가능성이 완전히 해소되었다고는 할 수 없다. 또한 사이버공간의 사회연결성 및 활용성이 지속적으로 증가되고 있는 특성과 빠른 기술의 발전이 도모되고 있는 상황, 사이버안보의 업무상 국민의 기본권과의 충돌가능성 문제, 대의민주주의하 정당성 확보의 문제 등을 고려하면 입법부에 의한 사이버안보 기본법의 제정 혹은 사이버안보 업무규정의 보완은 지속적으로 이뤄져야 할 것이다.

상기 조사한 바와 같이 기존 사회에서 꾸준히 한계점으로 지적되어왔던 사이버안보체계 완결성 부족을 보완하기 위한 사이버안보기본법의 제정이 입법부에서 꾸준히 임기만료로 폐기되어 버린 이유는 입법교착의 요소중 정책 쟁점이 적용된 사항으로, 양 거대 정당들은 사이버안보 확립의 필요성과 해당분야의 중요성에 대해서는 지속적으로 거대 정당사이에서 동의했으나 국가정보원의 역할에 대한 견해 차이로 인해 해당 법안들이 지속적으로 표류한 것이다. 특히 진보정당에서 기존 한국사회가 가지고 있는 역사적 경험 등을 바탕으로 국가정보원의 권한 강화에 대해 강하게 반발하였고 그에 대한 합의가 양 정당간 이뤄지지 않아 문제제기가 꾸준히 있었음에도 불구하고 10여년이 넘는 기간동안 임기응변적 체계만을 구축해왔던 것이다

그런 면에서 이번 국가정보원법이 진보여당 주도로 개정되어 기존에 적용된 입법교착 원인을 완화시켰다고 볼 수 있으며 추후 사이버안보 업무규정으로 구축한 사이버안보체계와 법제에 한계점이 지적되고 문제가 발생하여 정책의 창이 열렸을 때 입법부에 의한 기본법 제정을 원활하게 할 것으로 예측된다.

## References

- [1] Oh-Kook Kwon and Jae-Wang Seok, "A study of the major countries cyber terrorism Response System and Implications - Focusing on Analyzing the U.S., U.K. and Germany Cases," Korean security science review, 0(49), pp.100-103, Dec. 2016.
- [2] Nye, Jr. Joseph S, "Nuclear Lessons for Cyber Security", Strategic Studies Quarterly Vol. 5 No. 4, pp.18-38, Jan. 2011.
- [3] Jaeyoung Hur, "A Study on the Legislation of Cybersecurity Acts in South Korea", Journal of Korea Party Studies, 18(3), pp. 71-102, Sep. 2019.
- [4] Republic of Korea Policy Briefing (2005.03.24.), "[National Cyber Safety Center] Cyber Attacks Frontline Catcher". <https://m.korea.kr/news/policyBriefingView.do?newsId=70085558#policyBriefing>
- [5] National Cyber Safety Regulations (2005.01.31.), Enactment and Amendment.
- [6] National Cyber Safety Regulations (2010.04.16.), Enactment and Amendment.
- [7] National Cyber Safety Regulations (2012.01.02.), Enactment and Amendment.
- [8] Presidential Decree of Office of National Security Establishment (2013.03.23.), Enactment and Amendment.
- [9] National Cyber Safety Regulations (2013.09.02.), Enactment and Amendment.
- [10] Presidential Decree of Office of National Security Establishment (2015.04.03.), Enactment and Amendment.
- [11] Jun-Ho Hong, "Research on the Necessity of Cyber Security Control Tower", Law Review, 19(1), pp. 235-254, Mar. 2019.
- [12] Jongho Kim, "Asymmetric Threats and State Takedown focusing on the Contents of Annual Strategic Conference in U.S. Army War College", National Intelligence Research, 8(2), pp.99-147, Aug. 2015.
- [13] Kwang-Seok Yoon, Geon Lee, "The

- Problems and Alternatives of Information Security in the Korean Public Sector”, *Journal of Korea Society of Public Management* 8(2), pp. 99-147, Apr. 2017.
- [14] Jun-Ho Hong, “Research on the Necessity of Cyber Security Control Tower”, *Law Review* 19(1), pp. 235-254, Mar. 2019.
- [15] Il-Suk Oh, “A Legal Study on Enhancing Security Authority’s Cyber Security Activities”, *Research on Science and Technology Law* 20(3), pp. 41-90, Oct. 2014.
- [16] Yu-Sung Ahn, “A Research on ways to strengthen cyber security response capabilities”, *Review of KIISC*, 24(6), pp. 60-68, Dec. 2014.
- [17] Kwan-Hoon Kwak, “The Study on the Improvement of Acts to protect Information and Communications Network Utilization”, *IT & Law Review*, 0(6), pp. 147-175, Feb. 2012.
- [18] Kwang-Seok Yoon, Geon Lee, “The Problems and Alternatives of Information Security in the Korean Public Sector”, *Journal of Korea Society of Public Management*, 8(2), pp. 99-147, Apr. 2017.
- [19] Moon-ho Joo, Hun-Yeong Kwon, Jong-in Lim, “Cyber Security Governance Analysis in Major Countries and Policy Implications”, *Journal of the Korea Institute of Information Security & Cryptology* 28(5), pp. 1259-1277, Oct. 2018.
- [20] Hun-Yeong Kwon, “Information and Communication Security legal system’s problems and improvement plan”, *Journal of the Korea Institute of Information Security & Cryptology*, 25(5), pp. 1269-1279, Oct. 2015.
- [21] Hae-Sung Yoon, Min-Woo Yoon, Joshua Freilich, Steven Chermak, Robert G. Morris and Il-Soo Kim, “Cyberterrorism : Trends and Reponses”, *General Research book of Korean Institute of Criminology*, pp. 4-334, Dec. 2012.
- [22] Kunwoo Kim, Jungduk Kim, “An Analysis of Research Trends in Information Security Education”, *Journal of the Korea Institute of Information Security & Cryptology*, 26(2), pp. 489-499, Apr. 2016.
- [23] The National Assembly of the Republic of Korea, [1801619], “National Cyber Crisis Management Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_I0S8T1G0H2K8E1L7D5H8O4U9D4W8S5](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_I0S8T1G0H2K8E1L7D5H8O4U9D4W8S5)
- [24] The National Assembly of the Republic of Korea, [1904286], “National Cyber Safety Management Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_P1D3O0N3T2Y6A1K7D5A5E5J8Q2M5Q3](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_P1D3O0N3T2Y6A1K7D5A5E5J8Q2M5Q3)
- [25] The National Assembly of the Republic of Korea, [1904459], “National Cyber Terrorism Prevention Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_N1Q3G0N4A0A9R1X7S3M6L0L6N4M0U2](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_N1Q3G0N4A0A9R1X7S3M6L0L6N4M0U2)
- [26] The National Assembly of the Republic of Korea, [1905884], “Amendment of Information and Communication Infrastructure Protection Act.”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_O1A3C0P7U0S4U1Q3P3X3L3Q0U9L1D0](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_O1A3C0P7U0S4U1Q3P3X3L3Q0U9L1D0)
- [27] The National Assembly of the Republic of Korea, [1909028], “Amendment of Information and Communication Infrastructure Protection Act.”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_U1I4N0S1C0D9E1C8J5H5H4J8O5M1W0](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_U1I4N0S1C0D9E1C8J5H5H4J8O5M1W0)
- [28] Geunhye Kim, “A Study on the

- Analysis of Trump Administration Cybersecurity Policy : Focusing on Critical Infrastructure”, Journal of the Korea Institute of Information Security & Cryptology, 29(4), pp. 907-918, Aug. 2019.
- [29] The National Assembly of the Republic of Korea, [1915185], “Cyber Threat Information Sharing Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_V1F5Z0J5U1L9T1X3E4S1B4T2L1F7W7](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_V1F5Z0J5U1L9T1X3E4S1B4T2L1F7W7)
- [30] The National Assembly of the Republic of Korea, [1915777], “Cyber Terrorism Prevention and Response Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_C1Z5Z0N6B2A4T1L6C5S3G1N7X4S8U6](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_C1Z5Z0N6B2A4T1L6C5S3G1N7X4S8U6)
- [31] The National Assembly of the Republic of Korea, [1918583], “National Cyber Terrorism Prevention Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_W1J6T0P2L2F2G2Y2E5Y0K5P4U9O3C8](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_W1J6T0P2L2F2G2Y2E5Y0K5P4U9O3C8)
- [32] The National Assembly of the Republic of Korea, [2000032], “National Cyber Security Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC\\_L1Z6M0L5M3W0U1W4T2M8K4L3S5I0Y2](https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_L1Z6M0L5M3W0U1W4T2M8K4L3S5I0Y2)
- [33] The National Assembly of the Republic of Korea, [2004955], “National Cyber Security Act”. [https://likms.assembly.go.kr/bill/billDetail.do?billId=ARC\\_C1J7Y0Z1J0B3I1K6D4K6M4X8X9W8W1](https://likms.assembly.go.kr/bill/billDetail.do?billId=ARC_C1J7Y0Z1J0B3I1K6D4K6M4X8X9W8W1)
- [34] Hun-Yeong Kwon, “Information and Communication Security legal system’s problems and improvement plan”, Journal of the Korea Institute of Information Security & Cryptology, 25(5), pp. 1269-1279, Oct. 2015.
- [35] Yong-soo Park, “A Study on the Characteristics and Causes of Legislative Gridlock in Korean National Assembly”, A Comparative Democracy Study, 16(6), pp. 57-90, Dec. 2020.
- [36] Juan Ortner, “A Theory of political gridlock”, Theoretical Economics, Vol. 12, no. 2, pp. 555-586, May. 2017.
- [37] Bond Jon R, Richard Fleisher, “Polarized Politics: Congress and the President in a Partisan Era”, CQ Press, Washington, D.C, pp. 174-185, 2000.
- [38] Krehbiel Keith, “Pivotal Politics. A Theory of U.S. Lawmaking”, University of Chicago Press, Chicago, pp. 51-75, 1998.
- [39] Sundquist James L, “Constitutional Reform and Effective Government”, The Brookings Institution, Washington D.C, pp. 230-277, 1986.
- [40] Mayhew David R, “Divided We Govern”, Yale Univ. Press, New Haven, 1991.
- [41] Jones, David R, “Party Polarization and Legislative Gridlock”, Political Research Quarterly, Vol. 54, No. 4, pp. 125-141, Mar. 2001.
- [42] Juan Ortner, “A Theory of political gridlock”, Theoretical Economics, Vol. 12, no. 2, pp. 555-586, May. 2017.
- [43] Yong-soo Park, “A Study on the Characteristics and Causes of Legislative Gridlock in Korean National Assembly”, A Comparative Democracy Study, 16(6), pp. 57-90, Dec. 2020.
- [44] Sang-Sin Lee, “The Revisions of National Assembly Act in 2012 and Gridlock in South Korea”, Journal of Future Politics, 5(1), pp. 69-86, Feb. 2015.
- [45] National Assembly Research Service, “Political party models to overcome the governance crisis: Based on the party, executive, and government relations”, 2015.

- [46] Sangjoon Ka, "Policy Attitude of Legislators and Polarization of the National Assembly", *Oughtopia*, 31(1), pp. 327-354, May. 2016.
- [47] Sangwoo Lee, "Studying Causes of Legislative Gridlock in the Korean National Assembly: Focusing on the National Assembly Advancement Bill", *Korean Journal of Political Science*, 23(2), pp. 47-75, May. 2015.
- [48] Jinyoung Jeon, In-Kyun Kim, Young-kwan Yoon, "Politics of Time: What factors influence legislation speed?", *Korean Journal of Legislative Studies*, 17(2), pp. 171-196, Aug. 2011.
- [49] Jinyoung Jeon, "The Causes of Legislative Gridlock in Korean National Assembly", *Journal of Korea Party Studies*, 18(4), pp. 201-228, Dec. 2019.
- [50] WookJoon Sung, "A Study on Lawmaking Process of Personal Information Protection: Focusing on Policy Streams Model", *Journal of Korean Policy Studies*, 22(2), pp. 151-179, Jun. 2013.
- [51] Jaeyoung Hur, "A Study on the Legislation of Cybersecurity Acts in South Korea", *Journal of Korea Party Studies*, 18(3), pp. 71-102, Sep. 2019.
- [52] One-Sun Cho, "Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues", *The Quarterly Journal of Defense Policy Studies*, 33(2), pp. 145-177, Jul. 2017.
- [53] Jeong Hun Han, "Legislation Conflicts in the Korean National Assembly: Focusing on the Health and Welfare Policies", *Korean Political Research*, 22(3), pp. 35-62, Oct. 2013.
- [54] Jaeyoung Hur, "A Study on the Legislation of Cybersecurity Acts in South Korea", *Journal of Korea Party Studies*, 18(3), pp. 71-102, Sep. 2019.
- [55] National Intelligence Service Act (2020.12.15.), Enactment and Amendment.
- [56] National Intelligence Service, "2021 National Information Protection White Paper", 2021.
- [57] Operational rules Cybersecurity (2021.01.01.).

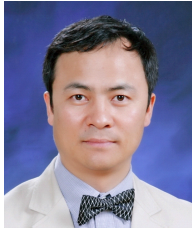
---

 <저자소개>
 

---



방 휴 (Hyu Bang) 학생회원  
 2018년 2월: 고려대학교 행정학과 졸업  
 2021년 8월: 고려대학교 정보보호대학원 석사과정 재학  
 <관심분야> 사이버안보, 사이버국방, 사이버법률, 정보보호정책



권 헌 영 (Hun-Yeong Kwon) 종신회원  
 1998년 2월: 연세대학교 법학과 석사  
 2005년 2월: 연세대학교 법학과 박사  
 2008년~2015년: 광운대학교 법학과 교수  
 2015년 9월~현재: 고려대학교 정보보호대학원 교수  
 現, 한국정보보호학회 법률지원단장 및 개인정보보호연구회장, 한국공법학회 ICT와 공법  
 연구포럼 의장, 대통령직속 제4차산업혁명위원회 데이터특별위원회 총괄분과위원장, 한국  
 행정학회 인공지능데이터행정특별위원회 위원장, 사이버안전포럼 운영위원장  
 전, 광운대학교 법과대학 교수, 한국인터넷윤리학회장, 사이버커뮤니케이션학회장, 정부  
 3.0위원회 법제도특별위원회 위원장  
 <관심분야> 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부