사이버 대응태세 구축을 위한 법·제도적 개선방안 연구

이 용 석*, 임 종 인**

요 약

사이버공간은 자유로운 활동이 보장되는 공간이다. 그러나 모든 개인과 국가가 평화로운 사이버공간을 위해 노력하고 있지 않고 이 공간을 통해 불의한 이익을 얻으려는 활동이 점차 증가하고 있는 것도 사실이다. 따라서 국가는 사이버공간을 안전하게 유지할 수 있도록 법과 제도를 정비해야 한다. 사이버공간에 대한 국가의 법철학을 담은「사이버기본법」을 제정하여 국민들이 사이버에 대한 국가의 법 규율방향을 인지하고 대응해 나갈 수 있어야 한다. IT의 급속한 발달에 따라「Digital Forensic 법」의 제정 또한 시급하다. 그러나 법률의 제정이 여러 가지 이유로 지연된다면 현행 법률의 일부를 상황에 부합되도록 개정하여 법 안정성을 높여야 한다. 이를 위해「정보통신기반보호법」,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「통합방위법」,「국방정보화 기반조성 및 국방정보자원관리에 관한 법」등의 개정이 필요하다.

A Study on the Legal and Institutional Improvement Plan for Cyber Correspondence

Yong Seok Lee*, Jong In Lim**

ABSTRACT

Cyber space is a place where free activities are guaranteed. However, it is also true that not all individuals and countries strive for peaceful cyberspace, and that there is a growing tendency to gain unfair advantage through this space. Therefore, the state should reform laws and institutions to keep cyberspace safe. By establishing the "Basic Law on Cyberspace" which includes the law of the state law on cyberspace, it is necessary to be able to recognize and respond to the direction of the national legal discipline on cyberspace. The development of digital forensics is an urgent task due to the rapid development of IT. However, if the law is delayed for various reasons, some of the existing laws should be amended to improve the stability of the law in accordance with the circumstances. To this end, it is necessary to revise the 「Information and Communication Infrastructure Protection Act」, 「Information and Communication Network Enhancement and Information Protection Act」, 「Integrated Defense Law」, 「Establishment of Defense Information Infrastructure Infrastructure and Defense Information Resource Management Act」.

Key words : Cyber Basic Law, Digital Forensic Law, Revision of Cyber Law

접수일(2019년 1월 9일), 수정일(1차: 2019년 3월 23일), 게재확정일(2019년 3월 28일)

* 고려대학교/정보보호학과(주저자)
** 고려대학교/정보보호학과(교신저자)

1. 서 론

지금까지 사이버전과 정보보호를 위한 이론들은 사이버공간의 인식에 대한 재검증을 요구받고 있다. 그 이유는 첫째, 사이버공간과 Offline이 '무한연결'되면서 사이버공간의 범위가 확장되고 있기 때문이다. 둘째, 과거 사이버안전과 정보보호의 범위가 '유통되는 정보'에 국한되어 있었으나 '네트워크'가 추가된 이후 그 범위가 수정, 확장되고 있다. 셋째, 해커와 비국가행위자가 등장하고 포털기업과 검색 엔진을 운영하는 기업 등 다양한 다국적 플랫폼기업들이 등장하면서 사이버에 관계되는 수많은 '안보 중심축'이 다차원적으로 변화하고 있다. 넷째, 사이버안전과 정보보호를 위협하는 사이버공격 방법과 기술의 진보가 정부 등 국가행위자의 통제범위를 벗어나고 있다. 다섯째, 사이버안전, 프라이버시, 정보자기결정권[1] 등이 '보호받아야 할 가치'들로 자리 잡게 되면서 제 가치들의 보호와 적법요건 간의 조화가 더욱 중요해지고 있다. 여섯째, 프라이버시와 기본권 보호수준이 국제적인 기준으로 상향되고 있다.[2] 나아가서 이러한 상황과 여건들은 모두 법률을 통한 국가행위를 규율하는 방법으로 확립되고 있다.

이러한 상황임에도 불구하고 우리나라는 국가 사이버안보와 관련된 기본법체계가 다양한 법률에 분산되어 기술됨으로써 국가 법철학적 공통성에 따른 일관성이 매우 결여되어 있는 실정이다. 이런 와중에 2017년 1월 3일에 정부에 의해서 국회에 제출된 「국가사이버안보법안」은 국회에서 제대로 다루어지기도 전에 시민단체에 의해서 법안이 거부되고 있다.

본 논문은 이와 같은 현상 진단 하에 사이버기본법 제정의 필요성을 다시 한 번 살펴보고, 사이버기본법 제정 전이라도 현행 법체계의 개정을 통한 국가 사이버상황 규율의 방법을 모색하여 국민이 사이버환경에서 법안정성을 확립하고 사이버공간에 대한 행위규범의 예축 가능성을 높이고자 한다.

2. 주요국의 사이버기본법 제정사례

2.1 미국의 사이버기본법

세계는 사이버안보 문제를 사이버공간에 국한된 논의가 아니라 국가존립과 연결된 심각한 안보문제라는 인식을 공유하고 있다.[3] 미국은 911테러 이후 2001년에 「애국법」을 제정하여 모든 전자통신을 감시, 추적할 수 있도록 하였고, 이 법의 몇 가지 문제를 해결하기 위해 2002년에 「사이버보안강화법」을 제정하였으며, 이 두 법을 통합하여 2002년 12월 「국토안보법」을 제정하였다. 총 17편으로 구성된 이 법은 사이버테러를 포함한 모든 테러로부터 미국을 보호하고, 공공과 민간에 대해 사이버 및 물리적 위협을 막론한 보호조치를 총괄적으로 집행하는 근거가 되고 있다. 이후에도 사이버법률의 미흡한 부분을 보충하기 위해 2009년 「사이버보안 교육증진법」, 2010년 「사이버안보증진법」, 2014년 「국가 사이버안보 강화법」, 2015년 「사이버보안법」을 제정하여 사이버공간에 대한 안전을 확보하고 국민들에게 사이버공간에서의 행위규범에 대한 예축가능성을 높이기 위한 다각적인 노력을 하고 있다.

2.2 일본의 사이버기본법

일본은 법치국가의 원리를 사이버보안분야에서도 준수하기 위해 국가의 기본이념에 바탕을 둔 범국가적 사이버보안을 추진하는 법적근거를 마련하였으며, 국가 사이버보안 총괄기구를 법제화하여 위상을 보장하였다. 일본은 1997년 「산업설비 네트워크 보안대책위원회」 활동을 통해 타국가의 사이버 대응체계에 대한 사례를 연구하였고, 1999년 「정보보안 관계 성·청 국장회의」, 2000년 「정보보안부회」와 「고도 정보통신 네트워크사회 형성 기본법」 제정을 거쳐 2014년에 「사이버보안기본법」을 제정하였다. 필두로사이버보안 강화활동의 투명성 확보와 국민 참여의 보장을 통해 국제협력에도 적극 나서겠다는 취지로 「사이버보안기본법」을 2014년에 제정하였다. 이

법을 통해 일본의 국가적 사이버보안활동이 하나의 기본법에 의해 체계적으로 규율되게 되었다.

2.3 독일의 사이버기본법

독일은 과거 사이버 관련법의 분산 입법으로 법률적인 난맥상을 겪던 중「독일연방기본법」에 '전자정부조항'을 입법하면서 연방 수준의 일반법인「전자정부법」을 갖추게 되었다. 이를 근거로 '연방정보기술보안청(BSI)'을 설치하였으며, 정보기술을 수단으로 사이버안보에 대한 다양한 역할을 수행하게 되었다. 나아가서 독일은 EU의 '네트워크 및 정보시스템 보안지침'인 NIS 지침을 이행하기 위한 법률(Gesetzes zur Umsetzung der Richtlinie (EU)2016/1148 des Europaischen Parlaments und des Rates vom 6. Juli 2016 uber Maßnahmen zur Gewahrleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz-und Informationssystemen in der Union,)을 2017년 6월부터 시행하였다.[4] 이를 기반으로 기술적 기준과 규제에 대한 정보규범의 절차와 2012년에 개정된「유럽공동체 규정」을 준수할 수 있게 되었다.

2.4 사이버기본법 제정의 필요성

이처럼 세계 각 국이 사이버기본법을 제정하는 이유는 첫째, 국가의 각 행정 분야를 관장하는 개별기관의 전문성에 국가차원의 법철학을 더하여 행정기관들이 상호 견제와 균형을 유지하면서도 국가차원에서의 개별 법률 간 충돌요소를 제거하고 일관되고 통합적인 법 집행이 가능하게 하기 위한 것이다. 둘째, 4차 산업혁명 시기를 맞이하여사이버기술의 발달이 급속히 진행되고 있음에 따라 일일이 대응하는 개별법의 제·개정이 어려운 만큼 '사이버기본법'에 사이버분야에 대한 국가 차원의 지향방향과 법철학을 설정해 놓고 법의 해석과 적용에 일관성을 확립하기 위한 것이다. 그래야 국민들의 법 안정성이 높아지고 향후 행동에 대하여 예측이 가능하게 되기 때문이다.[5]

3. 사이버 관련법 개정 소요

3.1 우리나라의 사이버 관련법 발전 과정

우리나라 사이버 관련법은 어떤 발전을 거쳐 왔을까? 이 질문에 대하여 2018년 발간된 국가정보보호백서[6]는 다음과 같은 답을 주고 있다. 1단계는 정보사회 초기 단계로 1986~1999까지이다. 이 기간에 우리나라는「전산망보급확장과이용촉진에관한법률」,「정보화촉진기본법」,「전자서명법」을 제정하여 정보보호의 법률적 기초를 마련하였다. 2단계는 2000~2007년까지로「정보통신기반보호법」,「국가사이버안전관리규정」을 신설하고「형법」에 컴퓨터 범죄를 포함하여 사이버범죄에 대응하기 시작하였다. 3단계는 2008~2015년까지 지식정보사회 구현단계로「국방정보화기반조성및국방정보자원관리에관한법률」,「개인정보보호법」,「지식재산기본법」,「정보보호산업의진흥에관한법률」을 제정하여 개별 정보보호 활동에 관한 국가적인 규율이 가능해졌다. 4단계는 2016년 이후로 4차 산업혁명 태동단계라고 하며「4차산업혁명위원회의설치및운영에관한규정」을 제정하여 급변하는 사이버환경 변화에 대응하기 시작하였다.

3.2 「사이버기본법」제정

이처럼 우리나라는 사이버법률에 대한 관심과 공공규율을 위한 노력을 지속하고 있다. 그러나 헌법의 일관성 있는 구현과 국가 법철학적 관점에서 국민의 사이버생활을 통일성 있게 규율하고 법적 안정성을 추구하는 측면에서는 미흡하다고 할 것이다. 따라서 이를 보완하기 위해서는 전술한 바와 같이 반드시 '사이버기본법'이 속히 제정되어야 한다. 사이버기본법을 통해 국민들은 예측 가능한 법 생활이 가능해 질 것이다. 그러나 여러 가지 이유로 '사이버기본법' 제정이 곤란하다면 동법 제정 전까지는 현행법을 일부 개정하여 국가 사이버분야를 안정적으로 규율할 수 있는 방안을 모색하는 것이 필요하다. 따라서 급변하는 IT 환경에 맞춘 제정이 필요한 법률과 개정이 필요한 법률을 살펴보기로 한다.

3.3 「Digital Forensic법」 제정

우리나라에서 2000년 이후 사이버위기가 발령된 10건의 사건은 모두 범인 검거에 실패하였었다. 그 이유 중 하나는 사건 관련 증거수집과 범죄자 검거를 위해서 Digital Forensic 수사절차를 정한 법률체계가 미비하였기 때문이다. Digital Forensic이란 범죄현장에서 확보한 개인PC, 서버 등의 System이나 전자장비에 저장된 디지털증거물에 대해 식별, 수집, 보존, 분석, 기록, 재현 등 과학적으로 도출되고 증명 가능한 방법으로 법정에 제출하는 것을 말한다.

Digital Forensic을 위한 기본원칙이 현재는「형사소송법」에 포함된 일반적인 원칙을 준용한 것이기 때문에 급변하는 사이버공간을 모두 규율할 수 없다. 따라서 Digital Forensic법을 제정하여 수사기관과 민사소송을 위한 Digital Forensic활동의 적법한 보장을 통해 Digital Forensic 관련 산업을 보호육성하고 국민의 안전을 보장해야 한다. 또한 법률체계는 증거수집, 분석, 제출, 평가라는 수사의 시간적 흐름에 따른 법률적 근거를 마련해야 한다.[7] 더구나 Digital 증거는 조작이 가능하기 때문에 Digital Forensic을 통한 검증이 꼭 필요하다. Digital Forensic은 기업 기밀유출 사건이나 해킹 조사에 주로 활용돼 왔지만 최근에는 성범죄 사건을 비롯한 민・형사사건으로도 그 활용 영역을 넓혀가고 있기 때문에 국민의 법 안정성을 보장하기 위해서라도 시급히 제정되어야 할 법률이다.

3.4 「정보통신기반보호법」 개정

「정보통신기반보호법」은 사이버위험 방지와 최소화 정책의 구현을 위해 주요 정보통신기반시설에 대한 사이버위험의 분배를 법률적으로 강제하여 입법적으로 구현한 것이다. 따라서「정보통신기반보호법」은 사이버위협 탐지, 취약성 분석・평가, 관리체계 구축, 주요 정보통신 기반시설에 대한 보안체계 강화, 악의적 결과 발생의 방지나 예방을 통해 사이버위험을 방지 또는 최소화시킬 수 있다.

위험분배와 대응능력의 확보 측면에서 국민의 안전에 대하여 무한책임을 가지는 정부는 민간부문보다 많은 위험분배를 받고 민간기관은 영업활동 수준에서 위험분배를 받도록 하는 것은 타당하다고 할 것이다. 특히 네트워크화 된 사이버공간에서의 보안은 '공공재(public goods)'적인 성격이 강하고 시장 실패적인 요소가 내재되어 있기 때문에 사이버보안 강화를 위해 국가가 적극 개입하여 국가와 국민의 안전을 보장하기 위해 발생하거나 내재되어 있는 사이버위험에 대하여 이해관계자와 관계기관이 비용을 부담하도록「정보통신기반보호법」을 개정해야 한다.

3.5 「정보통신망법」 개정

「정보통신망이용촉진및정보보호등에관한법률(약칭 : 망법)」은 정보통신망의 안전성, 건전성, 개인정보와 유해정보의 차단을 포괄하고 있다. 그러나 규제측면에서 행정기관의 과도한 규제가 자칫 민간의 창의적인 사이버활동과 민・관・군 협력의 자율적인 참여까지를 거부하게 하는 결과를 가져올 수도 있다, 따라서 이 법도 규제의 주체를 행정기관의 '고권적 규제'에서 민간의 '자율규제'에 대한 비율을 늘려 행정작용이 민간의 자율성 영역에 다양하게 미칠 수 있도록 하고 국가 사이버공간에 대한 침해사고 발생 시 애국적인 사이버전사들이 자발적으로 활동할 수 있는 토대를 마련해야 한다.

3.6 「통합방위법」 개정

「통합방위법」은 적의 침투・도발・위협에 대응하기 위하여 국가 총력전을 바탕으로 국가방위요소를 통합・운용하는 통합방위 대책을 수립・시행하고 필요한 사항을 규정함을 목적으로 하고 있다.[8] 즉 우리나라의 국가 방위를 위한 법령체계는 평시「통합방위법」, 전시「전쟁법」에 의해 대비하는 것이다. 여기서 '통합방위'[9]란 '적의 침투・도발・위협에 대응하는 각종 국가방위요소를 통합하고 지휘체계를 일원화하여 국가를 방위'하는 것을 말한다. 이를 위해 발생하는 사태의 규모에 따라

'갑·을·병종 사태'로 구분하고, 다양한 통합방위 용어의 정의를 통해 군·민이 국가안보와 국민생활에 심각한 영향을 주는 상황에 대한 이해의 통일을 추구하고 있다.

「통합방위법」이 규정한 정의를 종합해서 사이버상황에 적용한다면 '적이 사이버기술을 이용하여 대량공격을 통해 국가중요시설이 파괴되거나 기능이 마비될 경우 국가 총력전 개념으로 국가방위 요소를 통합·운용하여 지휘체계를 일원화함으로써 사태별 조치를 통해 국가를 방위하는 것'이라고 할 수 있다. 그러나 이것은 국가 위기상황을 타개하기 위하여 법 규정을 준용 또는 원용한 것이다.

따라서「통합방위법」에 사이버와 관련된 '용어의 정의'를 우선 보완하여 사이버공간[10], 사이버정보수집, 사이버공격, 사이버방호, 등급별 사이버사태를 포함하고 국가 총력전을 수행하기 위하여 사이버사태 대응조직을 구성할 수 있도록 해야 한다. 나아가 사이버공간에 대한 평시 준비태세를 갖추기 위하여 민·관·군 통합 사이버대응체계 연구개발, 인력확보 및 유지, 통합된 교육훈련 등의 평시활동에 대해서도 규율하여야 한다.

3.7 「국방 정보화법」 개정

「국방정보화기반조성및국방정보자원관리에관한법률(약칭 : 국방정보화법)」[11]에는 '국방 정보보호'를 국방 정보통신망에 대한 전자적 침해행위의 거부·정지·제한·예방·확인·점검·역추적 및 봉쇄 등 군의 작전능력을 제고하기 위한 모든 활동을 말한다고 정의하고 있다. 이 법은 국방 정보화 및 국방 정보자원관리에 관한 사항을 규정함으로써 미래 정보사회에 걸맞은 선진 정예강군 육성과 국방 정보기술의 선진화에 이바지하기 위한 목적으로 제정되었다. 따라서 국방 정보침해에 대한 보다 능동적인 대응체계를 구축하기 위해 사이버대응태세 구축을 위한 관련 연구개발 조항을 추가할 필요가 있다. 동법 시행령[12] 제16조(국방사이버안전 전담기관)에도 사이버전 기술 연구개발·시험평가 및 관리가 포함되어 있으니 모법에서 추가가 가능할 것으로 판단된다. 이상을 종합하여 <표 1>과 같이 사이버대응태세 구축을 위한 법령의 제·개정 소요를 표로 작성하였다.

<표 1> 사이버대응태세 구축을 위한 법령의 제·개정 소요 현황

법 안	주요 내용	형식
사이버기본법	• 국가 사이버보안 분야에 대한 기본법 지위	제정
Digital Forensic법	• 적법한 Digital Forensic 활동과 관련 산업보호 육성	제정
정보통신기반보호법	• 사이버위험에 대하여 이해관계자와 관계기관이 비용을 부담	개정
정보통신망 이용촉진 및 정보보호 등에 관한 법률	• 규제의 주체/비율 조정 : 행정기관→민간	개정
통합방위법	• 사이버공간 침해 상황을 구체화 명시, 대비	개정
국방정보화 기반조성 및 국방정보자원 관리에 관한 법	• 사이버대비 태세구축을 위한 관련 연구개발 조항 포함	개정

4. 결 론

우리나라 헌법 제23조는 국가는 모든 역량을 동원하여 국민의 생명과 재산을 지키라고 명령하고 있다. 그것은 국가의 주권이 미치는 모든 공간에서 유효하며 새롭게 대두되고 있는 사이버공간에서도 이 언명은 적용된다. 법치국가는 모든 국가행동을 법률에 근거하여 집행한다. 법률에 의하지 아니한 통제는 있을 수 없다. 따라서 사이버공간에 대한 국가의 대비와 규율은 모두 법률에 의하여 수행되어야 한다.

세계 각국은 '사이버기본법'을 제정하여 헌법정신과 국가 법철학의 일관된 구현을 보장한다. 그러나 발전 속도가 빠른 사이버공간을 법률적으로 규율하기 위하여 그때마다 법률을 개정한다면 법 안정성을 해치고 국민의 법 적용을 혼란스럽게 할 우려가 있다. 따라서 해당 분야에 대한 기본법을 제정

하는 것은 국민들이 해당분야에 대한 국가의 지향점과 법철학에 대하여 이해하게 되고 예측 가능성을 높여주는 것이다.

그러나 '사이버기본법'이 제정되지 않는다고 하여 사이버공간에 대한 국가의 규율을 포기할 수는 없다. 그래서 '사이버기본법'이 제정되기 전까지는 현행 법률의 일부 조항을 개정하여 사이버공간에 대한 국가기관과 국민들의 일관된 법 적용성을 확보해야 한다. 이를 위해 본 논문은 「사이버기본법」과「Digital Forensic법」의 제정 필요성을 제기하였으며,「정보통신기반보호법」등 4개 법률의 개정을 제안하였다.

참고문헌

[1] Seong, Bong-geun, "Germany's Legislative Trends and Implications for Cyber Security and Protection," Law and Policy Studies, 17 (1) p 112, 2017

[2] Sung, Bong-geun, "German Legislative Trends and Implications for Cyber Security and Protection", Law and Policy Studies, 17 (1), pp. 97 ~ 98, 2017

[3] Cho Won-sun, "National Cyber Security Discourse and Security Theory: Focusing on the Analysis of Cyber Security Situation in Korea", Defense Policy Research, Vol. 33, No. 2, pp. 148 ~ 174, 2017

[4] Sang-Don Park, "A Study on the Role of the Federal Information Security Authority of Germany (BSI) in 2017", Security Engineering Research, Vol.15, No.2, pp 69 ~ 80, 2018

[5] Sung Bong-geun, "Germany's Legislative Trends and Implications for Cyber Security and Protection," Law and Policy Studies, 17 (1), 2017

[6] NIS, etc., "White Paper on the Protection of National Information Security 2018", Aug. 2018

[7] Kwak, Byung-Sun Kwon, "A Strategy for Building a Cyber Forensic Legal System", Wonkwang Laws, Vol. 28 (2), 2012

[8] Law No. 14184 (Revised on November 30, 2016), Unified Defense Law, Article 1 (Purpose)

[9] Yu Hyeon-seok, "Military and Human Security: Theory, Case, and Korean Implications," Korean Political Science Review, Vol. 45 (5), pp. 221 ~ 241, 2008

[10] "Cyber space (cyberspace)" in the Attachment 1 (Definition of Terms) of the Defense Cyber Security Order of the Ministry of National Defense No. 2110 (Dec. 28, 2017) includes information, communication systems, Devices, and devices connected to each other, to create, store, distribute and utilize information.

[11] Law No. 12553 (revised part of May 9, 2014)

[12] Presidential Decree No. 25906 (Amended part of Dec. 30, 2014)

〔저자소개〕

이 용 석(Lee Yongseok)
2003년: 연세대학교 정치학석사
2019년: 고려대학교 공학박사
관심분야: 사이버국방/안보, 사이버무기체계, 사이버보안, 정보보호, 암호체계 개발
lyskms@korea.ac.kr

임 종 인(Jong In Lim)
1980년: 고려대학교 수학과 학사
1982년: 고려대학교 수학과 석사
1986년: 고려대학교 수학과 박사
현재 : 고려대학교 정보보호대학원 / 사이버국방학과 교수, 대검찰청 디지털수사자문위원장, 한국CISO협회장, 합참 정책자문위원 등
관심분야 : 사이버 국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안
jilim@korea,ac,kr