2016년 제2호

사이버안보법정책논집

KOREAN JOUNAL OF CYBER SECURITY LAW

사단법인 한국사이버안보법정책학회

2016년 제2호

사이버안보법정책논집

KOREAN JOUNAL OF CYBER SECURITY LAW

사단법인 한국사이버안보법정책학회

목차

제2호 사이버안보법정책논집

발 간 사

오늘날 우리 모두는 현실공간에서 생활하고는 있지만 그 실질은 초연결사회를 기반한 것이라고 평가할 수 있다. 하루가 멀다 하고 발생하는 사이버 보안사고에 조바심을 내면서 현실공간의 삶을 유지하고 있는 것이다. 돌이켜 보건대, 2016년 한해만 하더라도 국내에서는 우리 군이 운영하는 내부망이 해킹되는 사상초유의 사태가 발생하였고, 국외에서는 2013년 8월을 전후하여 '야후'를 이용하는 10억 명의 데이터가 유출되었다는 사실이 각각 뒤늦게 밝혀져 사이버 보안사고의 사전예방 곤란성과 사고 발생의 실시간 인지곤란성을 다시 한 번 일깨워 주었다. 그밖에 2016년을 대표하는 악성코드인 랜섬웨어는 전세계의 모든 인터넷 이용자가 처리하는 모든 데이터를 볼모로 삼아 금융감시망을 피할 수 있는 '비트코인'을 요구하고 있음은 주지의 사실이다.

실정이 이러함에도 불구하고, 사이버 보안에 대한 우리의 경각심은 매우 우려할 수준이다. 단적으로 말하자면, 2017년의 사이버 보안을 위한 예산이 전년도 대비 8%가 줄어든 3,102억으로 삭감되었다는 점에서 우리 사회가 여전히 사이버 보안에 대한 불감증으로부터 벗어나지 못한 것이 아닌가 하는 의심을 갖게 한다. 이러한 예산삭감 조치는 이철우의원이 올해 초 대표발의한 「국가사이버안보에 관한 법률(안)」이나 최근 정부안으로 입법예고된 「국가사이버안보기본법(안)」 등 입법차원의 노력에도 역행하는 것이라고 할 것이다. 이러한 장면에 이르러 "뿌리 깊은 나무는 바람에 아니 흔들린다"는 용비어천가의 글귀를 되새기게 한다. 과연 우리가 초연결사회의 열매만 즐기려고 할 뿐, 초연결사회를 뿌리 없는 나무로 만들려는 것이 아닌지, 아직도 안전불감증에 사로잡혀 구태의연한 전시행정으로 일관하고 있는 것이 아닌지를 심각하게 의심해보아야 한다.

그럼에도 불구하고, 현재 진행되고 있는 초연결사회의 위험을 조금이라도 이해하고 있거나 이해하고자 하는 모든 이는 지혜를 모아 초연결사회가 가져올 위험을 최소화하고, 반석처럼 안전한 사이버를 기반으로 하는 초연결사회

의 열매를 맺을 수 있게 하는 수고로움을 아끼지 말아야 한다. 2014년에 이어 올해 다시 발간하게 되는 사이버안보법정책논집은 비록 학술 등재지는 아니지만, 사이버안보의 중요성을 일깨워주는 전문학술지로서 미래사회의 안전을 위한 조그만 밀알이 될 것임을 믿으면서 등재지가 아님에도 불구하고 옥고를 게재하여 주신 분에게 이 자리를 빌려 다시 한 번 감사의 말씀을 전하고자 한다. 우리 학회가 사이버 안보법제의 정당성과 필요성을 위해 노력하면 노력한 만큼 반드시 국가차원의 법제정비가 이루어지게 된다는 믿음과 자부심을 밝히면서, 이 논집이 발간되기까지 고생하신 우리 학회의 김재광 부회장님과 강주영 간사 그리고 관계자 여러분에게도 마음 깊은 감사의 말씀을 전하고자 합니다.

2016년 12월 26일

한국사이버안보법정책학회 회장 **정 준 현**

01

사이버안보법정책논집

권 두 언

초연결사회와 사이버안보에 관한 법적 과제

정 준 현*

현재 우리 사회는 어둠을 밝히는 촛불의 평온 속에서도 극심한 정치적 혼란을 겪고 있다. 소위, 최순실의 국정농단사건에 맞물린 경제계의 혼란과 대통령에 대한 탄핵심판으로 인한 정국의 혼란이 그것이다. 이와는 별도로 2017년 12월에는 미국의 대통령선거에 이은 우리의 대통령선거가 예정되어 있다. 현재의 세계는 미국의 대통령 당선인인 트럼프의 자국보호 우선주의로 인하여 요동치고 있다. 즉, 트럼프는 한편으로는 한국·일본·유럽과 미국 간에 체결된 집단안보조약의 중요성을 강조하면서도, 동맹국에 대해 보다 많은 미군 주둔비를 부담할 것을 강변하여, 미국에 대한 적대적 행위를 미국 영토 이외의 지역에서 제압함으로써 자국보호와 동맹국보호라는 '일석이조(一石二鳥)'의 전통적 신뢰관계를 와해시키고 있다. 다른 한편으로는, 자국의 경제보호를 위해 우리를 비롯한 전통적인 동맹국과 체결된 자유무역협정의 개정을 주장하는 파행을 거듭함으로써 '통화의 양적 완화' 내지 "마이너스 금리"로도 치유되지 아니한 세계경제를 더욱 어렵게 만들고 있는 것이다.

특히, 우리 한반도와 접하고 있는 중국에 대하여는 트럼프가 '하나의 중국'을 부인하는 대외정책방향을 제시함으로써, 미국의 '사드배치'를 허용한 우리의 정치적·경제적 운신을 더욱 어렵게 하고 있다. 미국과 러시아를 둘러싼 쿠바 사태에서 알 수 있듯이 중국은 전통적인 '이이제이'(以夷制夷)에 따라 미국과 동맹관계에 있는 대한민국을 제압하기 위해 북한의 도발을 방조하

* 단국대학교 법과대학 교수, 한국사이버안보법정책학회 회장

거나 묵인할 가능성은 더욱 높다.

사정이 이와 같다고 한다면, 북한의 도발형태는 군사력의 행사가 아닌 사이버공격에 방점을 둘 것으로 보인다. 그 이유는 다음과 같다. 첫째, 에스토니아 및 그루지아 사태에서 보듯이 사이버공격은 사전탐지가 어렵고 설사 탐지된다고 하더라도 도발의 주체가 누군지에 대한 증명이 어렵고, 국제법상으로도 사이버공격을 전쟁으로 보고 있지 않기 때문에 군사적 도발과 달리 사이버도발에 따른 책임으로부터 자유로울 수 있다. 두 번째로, 우리 사회는 이미 초연결사회로 진입하여 사이버공간에 대한 국민 의존도가 매우 높기 때문에 우리 사회에 대한 북한의 사이버공격은 핵무기의 사용에 버금가는 피해를 야기할 수도 있다. 이와 달리, 사이버 원시상태에 머물러 있는 북한에 대한 우리 측의 사이버 대응공격은 아무런 전략적 이익을 갖지 못한다. 즉, 남·북한간의 심각한 정보화 격차로 인하여 북한은 물리적 도발보다는 사이버도발에 전략적 우위를 둘 수밖에 없기 때문이다. 셋째로, 인터넷상 정보전달의 최소 단위인 패킷을 통해 전통적인 음성정보 이외에도 일반인을 선전·선동할 동영상이나 정보통신망 또는 자동화기기를 오·작동시킬 수 있는 각종 악성프로그램을 담아 불순분자에게 전송하거나 일반인을 대상으로 유포할 수도 있다. 그러나 김일성·김정일주의를 근간으로 모든 주민의 희생을 강요하는 북한과 달리 우리 대한민국은 자유·민주적 법치주의에 기초한다는 제도적 격차가 상존한다는 점이다. 즉, 북한의 사이버도발을 민·관·군이 힘을 모아 사전에 탐지하여 공동대응하려면 자유권적 기본권인 통신비밀권·사생활비밀권을 비롯하여 개인정보권 등에 대한 제한이 따를 수밖에 없어 법치국가 원칙상 반드시 법적인 근거가 필요함에도 불구하고 아직 입법적 뒷받침이 제대로 이루어지고 있지 않아 그 대응이 여의치 못하기 때문이다.

위와 같은 사정과 아울러 최근 한국인터넷진흥원은 2017년의 7대 사이버공격으로 '산업전반으로 번지는 한국 맞춤형 공격', '자산관리 등 공용 소프트웨어를 통한 표적 공격', '한국어 지원 등 다양한 형태의 랜섬웨어 대량유포', '사회기반시설 대상 사이버테러 발생', '멀버타이징(Malvertising : 온

라인 광고를 통해 악성코드를 유포하는 행위) 공격 등 대규모 악성코드 감염 기법의 지능화', '악성앱 등 모바일 금융서비스에 대한 위협증가' 그리고 '좀비화된 사물인터넷 기기의 무기화' 등이 제시되고 있는 점과 2009년을 기준으로 McKinsey의 보고서(Internet Matters, 2011.5.)에 의하면, 세계 GDP의 70%를 차지하는 13개국 중 한국의 인터넷 경제의 GDP 비중은 4.3%로 3위이며, GDP성장 기여율은 16%로 세계 6위를 차지하고 있는 점 등을 종합적으로 고려할 때, 우리 사회의 정치적 과도기를 악용하여 사회적·경제적 혼란을 야기하고자 하는 북한으로서는 사이버도발을 선택할 수밖에 없을 것이다.

그렇다면, 일당독재국가가 민주국가를 이기지 못한 역사적 진리를 바탕으로 지금부터라도 국민적 합의에 기초한 법제정비를 서둘러야 할 때이다. 과거의 사회가 그러한 것처럼 초연결사회 또한 안전을 바탕으로 하지 않고서는 국민의 복리를 약속할 수 없다. 초연결사회의 안전은 인터넷의 안전에 대한 보장이어야 하며, 이러한 안전은 국가 단독의 힘으로는 불가능하고 민간전문기관의 협치가 동반되어야 하며, 모든 국민 스스로가 자유권적 기본권에 대한 일부제한을 사회적 제약으로 받아들일 때 가능하다.

이러한 점에서 인터넷에 기반을 둔 사이버위협의 특성에 대한 국민적 홍보와 이해를 바탕으로 다음과 같은 법률의 제·개정을 위한 노력이 이어져야 할 것이다. 첫째, 국가와 사회 및 개인이 상호연동하는 초연결사회의 국가안전보장의 개념은 '국민·주권·영토(사이버영토 포함) 등 국가의 성립요건 전체에 대한 위험의 부존재상태'로 법적 개념을 정립하여야 한다. 둘째로, 초연결사회의 패러다임에 합당한 국가안전보장의 새로운 법적 개념에 입각하여 '국가사이버안보에 관한 법률'을 국민적 합의를 바탕으로 신속하게 제정하여 이러한 위험의 부존재상태를 제도적으로 보장하여야 한다. 셋째로, 북한을 비롯한 적대세력의 사이버도발로부터 국가 전체에 대한 사이버위험을 민·관·군의 협치(Governance)로 예방·방어할 수 있도록 해야 한다. 그러기 위해서는 국가기관이 보유하거나 보유하게 될 위협정보에 대한 비밀분

류의 기준과 비밀분류된 위협정보를 공유·분석할 수 있는 민간전문기관의 비밀취급인가자격 등을 규정한 '비밀분류법'이 조속히 제정되어야 한다. 끝으로, 패킷데이터로 전송되는 정보로는 반국가활동 혐의자의 대화내용으로서의 통신정보뿐만 아니라 국가기반시설을 마비시킬 수 있는 악성프로그램 등 반국가활동을 실현시킬 수 있는 사이버도구로서의 통신정보도 포함된다는 점에서 '통신비밀보호법' 제7조의 통신제한조치의 대상에 대한 새로운 국민적 인식을 확산하는 노력과 함께 통신제한조치의 기술적 속성상 불가피한 혐의자 이외의 제3자에 대해 일시적으로 이루어지게 되는 감청사실을 혐의자뿐만 아니라 제3자도 일정한 시점에서 알 수 있도록 통신제한조치의 집행에 관한 통지를 정한 법 제9조의2도 일부 수정할 필요가 있다.

'종이와 대나무와 서로 어우러진 부채가 맑은 바람을 일으키듯'(竹紙相合生起淸風), 국가기관과 국민이 화합하고, 법치주의와 자유주의가 서로 화합할 때, 초연결사회의 대한민국은 안전 위에 맑은 기운만 가득한 복지사회로 변모할 것이다.

02

사이버안보법정책논집

정부 3.0시대의 사이버안보

정부3.0 성공을 위한 사이버보안의 역할

이 창 범*

목 차

Ⅰ 정부3.0과 사이버보안

정부3.0은 공공정보를 적극 개방·공유하며 부처간 칸막이를 없애 소통하고 협력함으로써 국민에게 맞춤형 서비스를 제공함과 동시에 일자리 창출과 창조경제를 지원하는 새로운 정부운영의 패러다임이다.[1] 특히 정부3.0은 공공정보의 적극 공개, 공공데이터의 민간 활용 활성화, 빅데이터를 활용한 과학적 행정 구현 등 10대 중점 추진과제를 발굴·시행함으로써, 투명한 정부, 유능한 정부, 국민중심의 서비스 정부를 구현한다는 것이 목표이다. 그리고 정부운영의 새로운 패러다임으로써 정부3.0을 떠받치고 있는 핵심가치는 개방, 공유, 소통, 협력이다.

* 경희대학교 법무대학원 겸임교수
1) 관계부처 합동, 『정부3.0』 추진 기본계획, 2013.6.19, 3쪽

한편, 2013년의 '정부3.0 추진 기본계획'을 한단계 업그레이드한 2014년의 '정부3.0 발전계획'[2]은 정부3.0의 목표를 서비스 정부, 유능한 정부, 투명한 정부로 수정하고, 이를 실현하기 위한 핵심과제로 개인 맞춤형 통합 서비스 제공, 클라우드 기반의 지능정부 구현, 빅데이터를 활용한 과학적 행정 구현, 정보공개제도의 전면 재정비, 공공데이터의 민간활용 기반 혁신 등 8대 과제를 제시하고 있으며, 특별히 민관 협치의 개방형 생태계를 강조하고 있다. 2014년 정부3.0 발전계획은 2013년 정부3.0 기본계획에 비하여 클라우드와 민간자원 활용을 강조하고 있다는 점이 특색이다.

그러나 공공정보의 공개 및 공유의 활성화나 클라우드 기반의 지능형 정부 구현은 개인정보 누출, 국가기밀 유출, 영업비밀 및 산업기술 공개, 공공정보통신망 해킹・장애 등 그 자체로 다양한 형태의 보안상 문제점을 본질적・태생적으로 안고 있다. 예컨대 이미 국내에서는 일반화된 영농법이라고 해도 다양한 영농기술이 집합적으로 공개할 경우 새로운 영농법의 개발에 기여하겠지만, 다른 한편으로는 공개된 대량의 농업기술정보가 경쟁국으로 넘어가 식량안보 문제를 초래할 수 있고, 과학기술정보를 공개 또는 개방할 경우 기술유출, 품질경쟁력 저하 등의 부작용을 초래할 수 있다. 공개・개방된 정보는 언제든지 국경을 넘어 다른 나라로 흘러갈 수 있고, 다른 나라 기업들도 이용이 가능하기 때문이다. 또한 정부의 전산시스템을 클라우드컴퓨팅 환경으로 전환할 경우에는 과학적이고 능률적이며 민첩한 정책 수행이 가능하겠지만, 클라우드컴퓨팅 시스템에서 처리되거나 저장된 빅데이터가 순간의 실수나 사고로 공개될 경우 국가안보에 심각한 위험을 초래할 수 있다는 문제점이 있다.

따라서 국민과 기업의 자발적 참여를 유도함으로써 민관협치의 토대 위에서 정부3.0이 성공하기 위해서는 사이버보안에 대한 국민과 기업의 우려를 불식시켜야 하며 현실적으로 존재하거나 잠재되어 있는 다양한 사이버보안

2) 정부3.0 추진위원회, 정부3.0 발전계획, 2014.9.17.

문제를 극복하지 않으면 안 된다. 이를 위해서는 공공정보든 민간정보든 획일적·일률적으로 정보를 공개할지 말지를 결정하기 보다는 국가안보 및 사이버보안 관점에서 정보마다 정보의 보호 필요성과 활용 필요성을 비교·분석하여 어떤 정보를 공개하고 개방할 것인지, 어떤 방식으로 공개 또는 개방할 것인지에 대하여 체계적으로 필터링하고 검증·평가하는 체계가 필요하며, 민간과 정부가 상호 교류하고 교호하는 클라우드기반의 개방형 전자정부 시스템을 어떻게 안전하게 관리하고 보호할지에 대하여도 전환기적인 보안대책이 필요하다.

Ⅱ 정부3.0의 비전과 과제

1. 정부3.0의 추진배경

정부는 정부3.0의 추진 배경으로 저성장 구조 속에서 경제부흥의 새로운 모멘텀이 필요하고, 기존의 방식으로는 풀기 어려운 복잡다기한 사회문제가 대두되었으며, 지식정보사회로의 전환에 따른 정부-국민 간 관계가 변화하고, 지식과 기술의 융복합 혁명이 새로운 기회의 요인으로 등장하였음을 들고 있다. 아울러 이 같은 추진 배경을 이끄는 기술적·환경적 요인으로 모바일·SNS 등의 확산에 따라 국민의 정책 참여 욕구가 증대하고 정부의 정책결정에 대한 투명성 요구가 증대하였으며, 다양한 정책문제 해결 및 맞춤형 서비스 제공 수단으로 ICT 기술의 활용 필요성이 제기되었음을 강조하고 있다.[3)]

이처럼 정부3.0의 등장 배경에는 오늘날 세계적으로 열풍을 일고 있는 빅데이터와 클라우드컴퓨팅 기술이 깊이 자리를 잡고 있으며, 정부3.0이라는 명칭도 웹1.0, 웹2.0, 웹3.0으로 발전해 온 인터넷의 진화에 대응하는 공공부문의 변화를 상징적으로 지칭한 것이다. 정부3.0은 이러한 정보통신기술

3) 관계부처 합동, 앞의 보고서, 1쪽

을 활용하여 정부의 일하는 방식과 서비스 전달 체계를 업그레이드함으로써 신뢰받는 정부를 건설하고, 궁극적으로 국민 개개인이 존중받고 행복한 국가 건설 추구하려는 것이 핵심이라 할 수 있다.[4)]

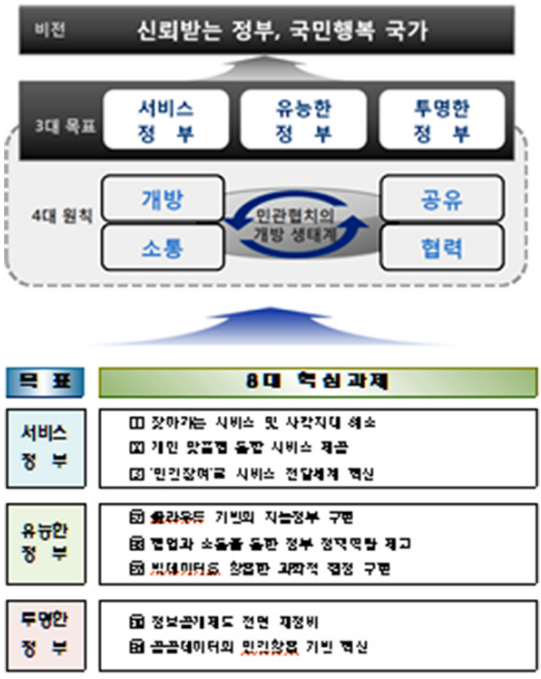
2. 정부3.0의 주요과제

아래 그림에서 보는 바이와 같이 정부3.0은 1)서비스 정부, 2)유능한 정부, 3)투명한 정부를 3대 전략 목표로 설정하고, 이들 목표를 달성하기 위한 과제로 ① 찾아가는 서비스 및 사각지대 해소, ② 개인 맞춤형 통합 서비스 제공, ③ '민간참여'로 서비스 전달체계 혁신, ④ 클라우드 기반의 지능정부 구현, ⑤ 협업과 소통을 통한 정부 정책역량 제고, ⑥ 빅데이터를 활용한 과학적 행정 구현, ⑦ 정보공개제도 전면 재정비, ⑧ 공공데이터의 민간활용 기반 혁신을 8대 핵심과제로 선정하고 있다. 정부3.0의 핵심 정책과 과제가 정보의 공개 및 공유를 통한 투명하고, 유능하며, 서비스 정신을 발휘하는 정부가 되는 것이고, 이를 달성하기 위한 전략과 기술이 곧 빅데이터, 클라우드, 시맨틱 웹, SNS 등의 정보통신기술과 서비스임을 한눈에 알 수 있다. 이는 기존에 구축된 칸막이식 전자정부의 단순 확대나 연장과는 전혀 다른 것으로, 정부의 체질 자체를 공개, 공유, 협력, 소통이 가능한 개방형의 클라우드 정부 내지 빅데이터정부로 질적 변화를 추구하는 것이라고 할 수 있다.

이와 같이 정부3.0이 지향하는 궁극적인 목표가 클라우드정부 내지 빅데이터정부로 전환·변신하는 것임에도 불구하고 정부3.0 기본계획, 발전계획, 시행계획 등 어디에서도 사이버보안 문제는 심각하게 다루어지지 않고 있으며, 정부3.0 추진위원회에도 다양한 전문분과위원회가 구성되어 있지만 사이버보안분과는 없다. 이들 보고서는 대부분 국가적인 사이버보안 및 사이버안보 문제를 단순히 시스템, 조직, 기업, 개인, 파일, 문서 단위의 정보보호 및 개인정보보호 차원에서 다루고 있다. 정부의 체질이 행정 내부의 전자 결

4) 한국정책학회, 정부3.0의 이론적 배경 및 변화관리에 관한 연구, 2013.12, 2쪽

재화 및 대국민 원스톱서비스 제공에 초점을 둔 전자정부에서 전자결재한 원문까지 자동으로 공개하고 공유하는 오픈 정부(open government)로 변신하겠다면 그에 걸맞는 범정부 차원의 보안대책이 필요할 것이다.



반면, 우리가 그동안 정보보호 특히 사이버보안이나 사이버안보에 관한 한 별로 배울 것이 없다고 생각해 온 일본이지만, 정부3.0에서만큼은 그렇지 않은 것으로 보인다. 일본은 우리나라의 정부3.0에 대응하는 정보화 정책으로 2010년 총리실 산하 '고도정보통신 네트워크사회 추진전략본부'가 발표한 '신정보통신기술전략'을 비롯하여 2012년 발표한 '전자정부 오픈 데이터 전략'과 '액티브 재팬 ICT(Active JapanICT)' 전략이 있고, 2013년에 발표된 '세계 최첨단 IT 국가 창조선언'이 있다.[5] 이들 보고서는 모두 개방, 참

5) 한국정책학회, 앞의 연구 보고서, 61쪽

여, 협력, 협업 등을 통한 국민 중심의 행정서비스의 실현과 데이터의 활용 촉진을 통한 새로운 시장 창출을 강조하고 있다. 특히 IT 국가 창조선언은 정보 자원을 새로운 경영 자원으로 인식하고, 오픈 데이터 및 빅 데이터 활용을 통해 경제 성장을 도모하겠다는 의지를 명백히 하고 있다. 그러나 동시에 '액티브 재팬 ICT 전략'은 안심・안전・신뢰도 높은 ICT 전략을 '액티브 재팬 ICT 전략'의 5대 중점 추진 전략의 하나로 선정하고, 새로운 기술・서비스에 적응하고 사이버 공격 등의 영향을 받지 않는 세계 최고 수준의 사이버 보안 환경을 구현하겠다는 의지를 담고 있다. 이를 구체화시킨 것이 2014년 1월 12일 제정한 '사이버시큐리티기본법'이라고 할 수 있다. 이 법은 범정부 차원에서 사이버보안에 관한 시책을 종합적이고 효과적으로 추진하기 위한 사이버보안전략의 수립・시행과 사이버보안전략본부의 설치를 주요 내용으로 하고 있다.

Ⅲ 정부3.0과 정보 공개 및 공유

공공정보의 공개 및 공유 정책은 정부3.0에서 다양한 목적과 다양한 방법으로 투영되어 있다. 정보의 공개 및 공유를 통한 국민과 정부 간 및 행정기관 상호간 소통・협치의 활성화와 더불어, 빅데이터의 활용을 통한 과학적 행정 구현, 공공데이터 민간활용 활성화를 통한 신성장동력 창출 등이 그것이다.

1. 빅데이터를 활용한 과학적 행정 구현

첫째, 다양한 형태로 존재하는 공공정보와 민간정보를 통합적으로 분석할 수 있는 빅데이터 기반의 정책 개발・수립 시스템을 구축・운영함으로써 빅데이터를 이용한 과학적 행정을 구현한다.

둘째, SNS 등 다양한 정보통신수단을 활용해 국민 참여 및 소통 채널을 다양화 하고, 온라인 민・관 협업 공간을 구축해 주요 국정과제 등 정책의

전 과정에 집단지성을 활용하고 민·관 협치를 강화한다.

셋째, 정부 정책 수립의 기초가 되는 원천정보 및 데이터를 공개하여 민간이 정책의 타당성, 효과성, 적법성 등을 검증할 수 있도록 한다.

넷째, '국민에게 믿음을 주는 투명한 정부' 구현을 위해 결재문서, 회의록 등 결과중심 정보공개를 정책결정 과정을 국민이 알 수 있도록 과정중심 공개로 전환한다.

이상의 목표를 실현하기 위해 아래의 핵심 추진과제를 선정해 연차적으로 추진하는 것으로 하고 있다.

핵심 추진과제

과제명	'14	'15	'16	'17	'18
1. 데이터 기반 국가미래전략과 과학적 정책결정 도입					
1) 정책영역별 데이터기반 미래전략센터 구축	■	■	■	■	
2) 정책 수립에 빅데이터 적용을 위한 기술 및 관련 산업 육성	■	■	■	■	■
3) 빅데이터로 주요 정책지표 및 예측자료의 정책 활용성 제고	■	■	■	■	
2. 증거기반 정책 수립의 법제화					
1) 정책 수립시 객관적 데이터 확보 및 분석을 의무화	■	■	■		
2) 근거기반 정책수립을 확대하기 위한 지원사업 실시		■	■	■	■
3) 정부업무평가를 데이터 분석기반의 객관적 평가방식으로 전환	■	■	■	■	
3. 국가안전 진단 등 ICT를 활용한 재난안전 대응능력 강화					
1) '대한민국 안전大진단'을 위한 ICT 및 빅데이터 기반 마련	■	■	■		
2) 범정부 재난안전 통합관리시스템을 클라우드 방식으로 구축		■	■	■	
3) 사회·환경 위험요인 시뮬레이션 모델 개발		■	■	■	■
4) 국가재난예측 심층연구 및 대응역량 강화 교육 실시	■	■	■	■	■

2. 공공데이터 민간활용 기반 혁신

첫째, 민간의 개방 수요가 많고 개방의 파급 효과가 큰 공공데이터를 대폭 개방해 공공데이터의 민간 활용을 활성화하고, 공공데이터 개방·활용 인프라 구축 등을 통해 신성장동력을 창출한다.

둘째, 빅데이터 분석을 통한 복지 및 생활 서비스 분야의 사각지대를 발굴해 선제적인 행정서비스를 제공한다.

셋째, 전자결재시스템에서 생산되는 원문정보를 정보공개시스템에서 실시간으로 조회가 가능하도록 시스템을 연계하고, 정보공개법에 따른 정보공개의 대상정보와 대상기관을 대폭 확대하는 등 공급자 위주에서 국민 중심의 정보공개로 패러다임으로 전환한다.

넷째, 정부 부처가 보유하고 있는 각종 개인정보를 분석·이용하여 생애주기별 또는 수혜자 유형별로 맞춤형 행정서비스를 제공한다.

마지막으로, 전자태그, 위치정보, 모바일기술 등 최신 정보기술(IT) 기반의 지능형 서비스의 발굴 및 확산을 통해 생활밀착형 행정서비스를 제공함으로써 국민 중심의 행정서비스를 구현한다는 계획이다.

이상의 목표를 실현하기 위해 아래의 핵심 추진과제를 선정해 연차적으로 추진하는 것으로 하고 있다.

핵심 추진과제

핵심 추진과제	'14	'15	'16	'17	'18
1. 국민 기업이 원하는 고가치, 고수요 데이터 우선 개방					
1) 민간활용 및 파급효과 높은 대용량 데이터 선별 및 범정부적인 조기 개방	■	■			
2) 국민의 데이터 제공요청에 대한 투명한 처리 절차 마련	■	■			
2. 공공데이터 품질 보장 강화					
1) 공공데이터 품질관리를 선진국 수준으로 개선	■	■	■	■	

핵심 추진과제	'14	'15	'16	'17	'18
2) 데이터 품질인증제도 마련 및 부처별 기술・컨설팅 지원 강화	■	■	■		
3. 민간–공공 상생의 데이터 생태계 조성					
1) 민간 데이터 플랫폼이 등장 할 수 있는 여건 조성	■	■			
2) 유망기업에 대한 지원 강화 및 데이터 활용 대기업과 중소기업 간 협력・지원을 활성화	■	■			
3) 공공데이터 이용실태를 조사 및 시장의 데이터 활용도를 평가할 수 있는 모델 개발	■	■			
4. 오픈플랫폼 방식의 공공데이터 개방					
1) 민간 데이터 플랫폼이 등장할 수 있는 여건 조성	■	■			
2) 공공기관의 데이터 개방전략 및 데이터 활용역량 강화	■	■			

Ⅳ 정부3.0과 클라우드 컴퓨팅

정부3.0은 빅데이터 활용 및 공개와 더불어, 클라우드 기반의 지능형 정부 구현과 지식정부 구현을 정부3.0의 가장 중요한 핵심과제로 추진하고 있다. 이는 정부가 그동안 폐쇄적으로 관리・운영되어온 전자정부시스템을 참여・공유・협업・협치가 가능한 개방형 클라우드정부로 전환하겠다는 의지로 해석된다.

1. 클라우드 기반 지식정부 구현

첫째, 지식관리시스템 기반의 제한적 정보공유에서 웹 기반 및 개방형 클라우드로 전환해 무제한의 정보 공유와 지능형 정보검색이 가능하도록 하고 폐쇄형 온나라시스템을 개방형 클라우드로 전환하여 정책자료와 정부기록물을 범정부적으로 공유 가능하도록 하여 차세대 지식경영체계를 구축한다.

둘째, 공무원 개인 PC에 저장된 자료를 클라우드 저장소로 이관하고 무제한 공유가 가능한 개방형 문서표준으로 전환하며, 클라우드 기술을 활용하여 정부부처의 웹사이트를 통합하고, 클라우드 기반의 원격 보안 환경을 구축해 미래형 클라우드 정부를 구현한다.

셋째, 정부내 및 정부-민간 사이의 원활한 데이터 공유와 서비스 위탁을 위하여 보안등급기준을 개발하고, 보안등급별 보안요건을 국제표준과 개방형 체계에 맞게 개발하며, 민간 클라우드 시설에 대한 보안인증제를 도입해 클라우드 환경에 맞게 정보보안체계를 혁신하며, 공무원 개인의 모바일 기기를 편리하게 업무에 활용할 수 있도록 모바일 행정을 뒷받침하기 위한 획기적인 보안기반을 강구한다.

넷째, 클라우드 컴퓨팅 기반 위에서 기존에 정부만이 제공하던 서비스를 민간협업 또는 민간제공으로 다양화하고 정부 서비스 사이트의 API를 민간에 공개하여 정부 서비스를 네이버, 다음 등의 민간 포털에서도 직접 제공할 수 있도록 해 정부-민간 연계형 서비스를 확대함으로써 정부의 서비스 전달 체계를 혁신한다.

다섯째, 공문서 외에 각종 정책자료를 개인보관 방식에서 클라우드 기반 보관 방식으로 전환하고, 정부 기록을 누구나 확인할 수 있도록 표준형으로 전환한다.

이상의 목표를 실현하기 위해 아래의 핵심 추진과제를 선정해 연차적으로 추진하는 것으로 하고 있다.

핵심 추진과제

과제명	'14	'15	'16	'17	'18
1. 차세대 지식경영 체계 구축					
1) 정부 공문서의 범정부 공유환경 조성(온나라 고도화)	■	■			
2) 웹 기반의 무제한 정보공유로 고도화		■	■	■	

과제명	'14	'15	'16	'17	'18
3) 부처 경계를 넘어 지식정보를 공유・활용하는 근거 마련					
2. 미래형 클라우드 정부 구현					
1) 공무원 개인 PC시대로 마감하고 클라우드 환경으로 전환					
2) 웹사이트 통합・정비 플랫폼 마련 및 IT자원의 공동 활용 추진					
3) 정부와 민간의 서비스 융합 촉진					
4) 정부통합전산센터의 관리체계 개선					
3. 클라우드 및 모바일 환경에 맞는 정보보안 체계 혁신					
1) 정부 데이터 및 서비스에 대한 보안등급제 도입					
2) 모바일 행정을 뒷받침하기 위한 획기적 보안기반 강구					

2. 협업과 소통을 통한 정부 정책역량 제고

첫째, 소속부처와 상관없이 전 공무원이 SNS, 메일, 전화, 모바일, 영상회의 등의 다채널로 의사소통이 가능하고 온라인 협업이 가능한 '정부통합의사소통시스템'을 구축해 부처간 협업을 지원하는 기반시스템을 마련한다.

둘째, 클라우드 기반의 영상회의 시스템 및 스마트워크센터 확대를 통해 원격근무의 비효율을 극복할 수 있는 디지털 협업 시스템을 구축・운영한다.

셋째, 정부통합전산센터를 클라우드 컴퓨팅 센터로 전환하여 지식・정보 공유 기반을 마련한다.

마지막으로, 부처간 시스템 연계 또는 통합이 필요한 과제에 대해서는 관련 시스템의 연계・통합을 적극 지원하고 공동이용 정보 및 공동이용 기관의 확대를 통해 부처 간 협업을 추진하는 등 정부 내 칸막이를 제거한다.

이상의 목표를 실현하기 위해 아래의 핵심 추진과제를 선정해 연차적으로

추진하는 것으로 하고 있다.

핵심 추진과제

과제명	'14	'15	'16	'17	'18
1. 협업을 우선시 하는 융합행정 실현					
1) 부처간 협업지도를 구축하여 시기별, 쟁점별 협업수요 파악		■			
2) 협업 프로세스 개선 시범사업 실시		■	■		
3) 부처별, 조직별 협업 포인트 제도 도입		■			
2. SNS 기반 범정부 통합소통체계 실현					
1) 정부내 소통 미디어를 SNS 기반의 항시적 소통방식으로 전환	■	■	■	■	
2) 정부내 모든 소통수단을 상호연계한 통합소통시스템 고도화	■	■	■	■	
3) 영상회의 활성화를 통한 원거리기관 간 효율적 협업 추진		■	■		
3. 정부업무 다이어트 등으로 공무원 업무생산성 제고					
1) 업무감축목표제 시행으로 정부내 불필요한 업무 제거	■	■	■	■	
2) 야근, 출장을 과학적 분석을 기반으로 감축		■	■		
3) 모바일 행정과 스마트 워크 조기 분격화		■	■	■	
4. 민관협치, 과학자급 공무원 양성 등 정부 전문성 강화프로그램 운영					
1) 민간의 정책참여 방식을 다양화하여 집단지성적 정책적용	■	■	■		
2) 국내외 민간전문가 영입 확대와 과학자급 전문공무원 양성	■	■	■	■	

V 정부3.0 성공을 위한 사이버보안 대책

1. 정보개방에 따른 정보보호대책

정부3.0은 정보 개방 및 공유에 따른 보안 위협 및 개인정보보호 문제를 해결하기 위하여 몇 가지 중요한 대책을 마련하고 있다.

첫째, 전자정부서비스(대민서비스)의 중요도에 따른 보안등급제 도입, 정부전산백업센터 구축, 전자정부 정보시스템 소프트웨어(SW) 개발보안 강화, 민·관·군 사이버위협 정보 공유 등 사이버위협 협조체계 및 합동대응체계 강화 등을 통해 정보시스템의 보안을 강화한다.

둘째, 암호화, 익명화, 비식별화 등 공공정보 개방·공유 등의 처리단계별로 개인정보보호지침을 개발·보급하고, 개인정보 보호법익을 고려한 정보개방·공유의 범위·수준·방법 등을 제시하며, 개인정보 보호·개방 지원센터를 설립·운영하는 등의 안전한 정보 활용 기반을 마련한다.

셋째, 민감정보 다량 보유기관 대상 유·노출 정기 모니터링 및 삭제조치 강화, 공공기관의 안전성 확보조치 이행 여부 정기점검, 공공기관 개인정보 실태개선 및 수준제고 등을 통해 개인정보 보호조치를 강화한다.

이상의 조치들을 강구함으로써 정보를 안전하게 이용·제공할 수 있는 환경을 조성하겠다는 것이다. 그러나 빅데이터와 클라우드를 기반으로 한 정부3.0은 기존의 정보공개제도 및 전자정부시스템에서와는 질적으로 다른 침해사고 위협과 정보유출 위험이 내재되어 있다. 현재도 공공기관이 보유·관리하는 정보는 원칙적으로 공개 대상이지만, 「공공기관의 정보공개에 관한 법률」에 따라 공개하지 않아도 되는 비공개 대상정보가 실무적으로 광범위하게 인정되고 있어[6] 정보 공개에 따른 현실적인 리스크는 크지 않았다고 할 수 있다. 그러나 정부3.0 기본계획 및 발전계획의 시행과 이를 뒷받침하기 위한 「공공데이터의 제공 및 이용 활성화에 관한 법률」의 제정·시행으로 인

6) 「공공기관의 정보공개에 관한 법률」 제9조 제1항 참조

해 그동안 공공기관들이 보여 온 소극적인 정보공개 행태는 더 이상 유지하기 어렵게 되었고 보다 적극적이고 선제적인 정보 공개와 개방이 요구되고 있다.

또한 기존의 전자정부시스템이나 정부통합전산센터는 데이터의 수집・이용 및 관리가 부처별로 이루어지고, 정부와 민간 사이는 물론 정부 내에서도 정보의 공유 및 교류가 제한적이어서 해킹 위협이나 오남용 위험이 그만큼 제한적이었다고 할 수 있다. 따라서 전자정부법, 정보통신기반보호법, 국가사이버안전관리규정 등만으로도 유・노출 위협에 대한 대응이 어느 정도 가능하였다. 그러나 공개와 공유를 기반으로 하는 클라우드정부 시스템에서는 다양한 유형의 정보들이 정부기관을 넘어 정부와 민간 사이에서까지 광범위하게 공유 및 교류되므로, 범정부 차원의 보다 다층적이고 체계화된 정보보안 활동이 요구된다.

2. 빅데이터 가이드라인과 개인정보보호

정부3.0에서는 빅데이터를 위한 개인정보의 안전한 처리방법으로 비식별화를 제시하고 있다.[7] 비식별화는 빅데이터의 핵심 기술로 개인정보의 안전한 이용과 정보주체의 권리 보호를 위해 매우 중요한 기술적 방법이나 우리나라에서는 적법성 여부를 둘러싸고 많은 혼란을 겪고 있다. 즉 개인정보를 비식별화 하더라도 재식별화가 가능하다면 여전히 식별성이 존재하는 것이니 정보주체의 동의 없이는 수집・이용 및 제공할 수 없다는 것이고, 개인정보의 비식별화 조치도 개인정보의 처리에 해당하는 행위이므로 정보주체의 동의 없이는 비식별화를 할 수 없다는 주장이 있다.[8]

먼저 개인정보의 정의와 관련하여 비식별화된 정보가 개인정보에 해당하는

7) 방송통신위원회, 「빅데이터 개인정보보호 가이드라인」, 2014.12. ; 미래부/NIS, 빅데이터 활용을 위한 개인정보 비식별화 기술 활용 안내서(Ver 1.0) ; 행정자치부/NIS, 개인정보 비식별화에 대한 적정성 자율평가 안내서, 2014.12

8) 경실련 소비자정의센터/진보네트워크센터, 빅데이터 및 비식별화 관련 법안에 대한 반대 의견 발표(보도자료), 2015. 6. 8.

지 여부를 살펴본다. 각국의 법률은 개인정보의 정의를 각기 달리 표현하고 있으나, 그럼에도 불구하고 그 정의에 대한 해석은 유사하다. 어느 나라에서든 개인정보성 여부를 판단하는 핵심적 기준은 식별 가능성이다. 이 때 식별 가능성을 판단함에 있어서 우리나라 개인정보 보호법은 '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다'라고 되어 있다. 이에 비해 2014년 EU Regulation은 '합리적으로(reasonably)'으로 라는 단어를 사용하고 있고, 1995년 EU Directive에서는 명시적으로 'reasonably'라는 단어를 사용하고 있지는 않았으나 직·간접적이라는 표현을 사용하고 있으며 그 해설서에서는 'reasonably'라는 단어를 사용하고 있다.

이 경우 결합 가능성은 다른 정보의 입수 가능성을 전제로 한 것이며 입수 가능성이 없다면 결합 가능성도 없는 것이다. 과도한 비용과 노력을 들이지 않고(즉 쉽게 또는 합리적으로) 입수 가능한 정보들을 결합해서 특정인을 식별할 수 있는 정보가 곧 개인정보인 것이다.[9] 그러나 일부에서 '쉽게 결합하여'의 의미를 입수 가능성을 배제한 채 과학적·기술적 결합 가능성을 의미하는 것으로 해석하여 개인정보의 개념을 무한정 확장하고 있다.[10] 그러나 기술적·관리적으로 정보를 통제할 수 있는 합리적인 안전조치가 마련되어 있고, 해당 정보를 취급하는 자에게 법률적으로 또는 계약상으로 안전한 보호의무가 부여되어 있다면 쉽게 결합 가능한 것으로 보아서는 안 될 것이다.

한편 결합 가능성을 판단함에 있어서 개인정보처리자가 현재 보유하고 있는 정보만을 대상으로 해서 판단해야 하는지, 현재 또는 장래에 새로 입수 가능한 정보들까지 포함해서 판단해야 하는지에 대해서도 주장이 갈린다. 입수 가능성을 배제하고 현재 보유하고 있는 정보만을 대상으로 해서 결합 가능성을 판단해야 한다면 개인정보 보호법에 의해서 보호받을 수 있는 정보의

9) 졸저, 개인정보 보호법, 2012, 법문사, 18~20쪽
10) 이른바 증권통 판례(서울중앙지법 2011.2.23. 선고 2010 고단 5343) 등

범위는 크게 줄어들게 된다. 이 같은 주장은 개인정보의 개념을 지나치게 축소하여 권리보호의 사각지대를 양산할 우려가 있을 뿐만 아니라 개인정보보호법이나 정보통신망법의 문리적 해석에도 맞지 않다. 개인정보 처리자 자신의 수중에 있든 제3자의 수중에 있든 쉽게 입수할 수 있고 쉽게 결합이 가능하다면 모든 정보를 개인정보로 보아야 한다.

이 같은 이슈를 보다 명확히 해결하기 위해 2014년 EU Regulation은 'can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person'이라는 표현을 사용하고 있다. 즉 다른 사람으로부터의 입수 가능성을 법률에서 명시하고 있다. 또한 개인을 식별할 수 있는 정보에는 identification number, location data, online identifier 외에, physical, physiological, genetic, mental, economic, cultural or social identity가 포함된다. 우리나라에서는 아직도 논란의 대상이 되고 있는 online identifier도 개인식별정보로 보고 있다.

다만, 미국의 연방 Privacy Act는 우리나라 신용정보법이 그런 것처럼 name, identifying number, symbol, finger print, voice print, photograph 등과 같은 identifying particular가 포함된 정보만을 개인정보로 보고 있다. 하지만 미국은 EU와 대척점에서 개인정보보호제도를 운영하고 있는 국가로, 미국의 제도를 채택하고 있는 국가는 그리 많지 않다. 글로벌 네트워크 경제 사회에서 우리나라와 같은 작은 나라가 다른 나라와 상이한 개인정보 정의 규정을 운영한다면 국제적 외톨이가 될 우려가 크다.

1995년 EU Directive	2014년 EU Regulation	미국 연방 Privacy Act
"personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one	"personal data" means any information relating to a data subject. "data subject" means an identified natural person or a natural person	"record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not

1995년 EU Directive	2014년 EU Regulation	미국 연방 Privacy Act
who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity	who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.	limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

둘째, 비식별화와 익명화의 구별 문제이다. 빅데이터의 동의 없는 활용을 반대하는 측에서는 개인정보를 비식별화하면 정보주체의 동의 없이도 처리가 가능하다는 정부의 빅데이터 가이드라인[11]을 월권적 해석이라고 주장한다. 그러나 비식별화된 정보는 원칙적으로 개인정보가 아니므로 정보주체의 동의 없이도 수집·이용 및 제공이 가능하다고 보아야 할 것이다. 일반적으로 개인정보보호법 상 비식별정보(anonymised data or anonymous data)와 익명정보(pseudonymised data)는 엄연히 구분된다. 비식별화(anonymisation)는 누구든지(개인정보처리자는 물론 제3자도) 상당한 노력을 들이지 않고는 다시는 개인 식별을 하지 못하게(irreversible de-identification) 개인정보의 식별성을 제거해버리는 것이므로 비식별화된 정보(anonymised data)는 개인정보가 아니고 개인정보법의 적용도 받지 않는다. 반면, 익명화(Pseudonymisation)은 특정인의 정체(identities)을 숨기거나 위장하는 것에 불과하므로 익명화된 정보(Pseudonymised data)는 여전히 개인정보이다.[12] 비식별화가 식별성을 제거하는 것이라면, 익명화는 식별성을 숨기는

11) 방송통신위원회, 「빅데이터 개인정보보호 가이드라인」, 2014.12.

것에 불과한 것이다. 따라서 비식별화된 정보는 식별성이 상실되지만(구분성은 존재할 수도 있음), 익명화된 정보는 식별성이 존재하게 된다. 전자의 예로는 일방향 암호화가 이에 해당하고, 후자의 예로는 양방향 암호화, 키코드화(Key-Coded) 등이 있다.[13]

그러나 우리나라에서는 한 때 이 두 개의 차이를 구분하지 못하고 전문가들조차도 모두 "익명화"라는 동일어로 번역해서 사용해 왔다. 또 최근에는 de-identification을 anonymisation과 동의어로 사용하는 등 계속 혼란을 겪고 있다. 비식별정보(anonymised data)와 익명정보(pseudonymised data)가 다르듯이 de-identification와 anonymisation도 다르다. de-identified data 중에는 식별성이 완전히 제거되어 비식별정보에 이르는 정보가 있는가 하면, 아직 식별성이 남아 있어 익명정보 수준에 남아 있는 정보도 있다. 식별성이 완전히 제거된 것인지 여부는 개인정보 정의에서 사용된 합리성 원칙이 적용되어야 한다. 즉 기술적으로 식별이 불가능해야 하는 것이 아니라 합리적으로 식별이 불가능하면 de-identified data는 비식별 정보(anonymised data)가 된다.

한편, 개인정보의 비식별화를 위해서는 그 전제로써 개인정보의 수집과 저장이 필수적이다. 또한 개인정보의 비식별화 과정이 개인정보보호법 상 개인정보의 "처리" 행위에 해당하는지도 논란이다.[14] 즉 비식별화 행위 자체의 적법성이 문제된다. 그러나 비식별화는 암호화 등과 마찬가지로 개인정보의 안전성 확보 조치 방법의 하나에 불과하고 이를 개인정보 처리행위로 보는 것은 무리이다. 유럽연합도 비식별화를 위한 개인정보의 수집.저장은 이를 적법한 것으로 보고 있다. 다만, 개인정보의 비식별화 과정이 적법하려면 수집과 동시에(가능한 빨리) 비식별화가 이루어져야 한다.[15]

12) 졸저, 개인정보 보호법, 2012, 법문사, 2012, 18~20쪽
13) ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 4/2007 on the concept of personal data (Adopted on 20th June)
14) ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques (Adopted on 10 April 2014)

EU에서는 개인정보를 동의없이 이용 또는 제공할 수 있는 사유로 개인정보의 비식별화(anonymisation) 외에, 역사, 통계, 과학적 목적의 개인정보 이용, 제공 및 저장을 들고 있다. 즉, 역사, 통계, 과학적 목적으로 개인정보를 이용, 제공 및 저장할 때에는 목적 외로 처리하더라도 목적 범위 내의 처리로 본다. 다만, 이 경우 회원국은 역사, 통계, 과학적 목적의 이용, 제공 및 저장을 위한 안전기준(appropriate safeguards)을 제정하여야 한다. 이와 같은 안전기준의 대표적인 방법이 de-identification이라고 할 수 있다. 이와 같은 목적의 개인정보처리에 대해서는 반드시 비식별화(anonymisation)가 요구되는 것은 아니며 익명화(Pseudonymisation) 조치도 가능하다.

이상과 같이 빅데이터 활용 과정에서 발생할 수 있는 개인정보 및 사생활 침해 가능성 문제는 비식별화 조치에 의해서 어느 정도 예방 및 방지가 가능하게 되었다고 볼 수 있으나, 이에 대한 명확한 법적 근거가 마련되어 있지 아니하므로 정보통신망법 또는 개인정보보호법 등의 개정을 통해 비식별화 관련 문제를 명확히 할 필요가 있다.

3. 클라우드발전법과 사이버보안

「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 "클라우드발전법"이라 한다)은 주로 민간 클라우드사업자가 제공하는 상용의 클라우드서비스에 적용되지만, 공공기관이 상용의 클라우드서비스를 이용하는 경우에도 적용된다. 클라우드발전법에 따라 국가기관등은 클라우드컴퓨팅을 도입하도록 노력하여야 하고(제12조제1항), 특히 정부는 클라우드컴퓨팅서비스 제공자가 제공하는 클라우드컴퓨팅서비스를 이용할 수 있도록 노력하여야 한다(제20조). 또한 정부가 「국가정보화 기본법」에 따른 국가정보화 정책이

15) 정보통신망법 제22조는 '정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는……이용자에게 알리고 동의를 받아야 한다'라고 규정함으로써, 해당 개인정보를 이용할 의사가 없이 오로지 비식별화를 목적으로 수집해서 곧장 비식별화 한다면 정보주체의 동의가 필요하지 않다는 해석도 가능하다.

나 사업 추진에 필요한 예산을 편성할 때에는 클라우드컴퓨팅 도입을 우선적으로 고려하여야 하며(제12조), 클라우드컴퓨팅 사업의 수요 예보에 따라 국가기관등의 장은 연 1회 이상 소관 기관의 클라우드컴퓨팅 사업의 수요정보를 미래창조과학부장관에게 제출하고 미래창조과학부장관은 제출받은 클라우드컴퓨팅 수요정보를 취합해 연 1회 이상 클라우드컴퓨팅서비스 제공자에게 공개하여야 한다(제13조).

클라우드발전법은 이상과 같이 원래 클라우드 컴퓨팅의 발전과 이용 촉진을 목적으로 제정된 법이므로 정보보호나 정보보안에 대해서는 그다지 큰 관심을 두고 있지 않다. 개인정보보호와 정보보안 문제는 정보통신망법, 정보통신기반보호법, 전자정부법, 개인정보보호법 등에 맡긴다는 입장이다. 따라서 클라우드발전법은 최소한의 정보보호 규정만을 두고 있다. 클라우드발전법은 클라우드컴퓨팅서비스 제공자에게 클라우드컴퓨팅서비스의 품질·성능 및 정보보호 수준을 향상시키기 위해 노력할 의무를 부여하는 한편, 미래창조과학부장관은 클라우드컴퓨팅서비스의 품질·성능에 관한 기준 및 정보보호에 관한 기준을 정하여 고시하고 클라우드컴퓨팅서비스 제공자에게 그 기준을 지킬 것을 권고할 수 있도록 규정하고 있지만(제23조), 이를 따르지 아니한 자에 대한 처벌규정을 준비하고는 있지 않다.

따라서 클라우드컴퓨팅 도입에 따른 개인정보보호 및 정보보호문제는 원칙적으로 정보통신망법, 개인정보보호법, 전자정부법, 국가사이버안전관리규정 등의 개별법에 맡겨져 있다고 보아야 할 것이다. 클라우드 도입에 따른 사이버보안 문제는 아래 절에서 별도로 논하기로 한다.

4. 정부3.0 성공을 위한 사이버보안 대책

정부3.0은 빅데이터와 클라우드에 기반을 두고 있기 때문에 정보보호가 가장 큰 걸림돌 내지 취약점이 되고 있다. 따라서 정부3.0이 성공을 거두기 위해서는 정보보호에 대한 국민과 기업 그리고 공무원들의 신뢰를 확보하지 않으면 안 된다. 특히 정부3.0에서는 정부와 민간의 경계가 더욱 불분명해지

고, 행정부처 간에도 데이터 및 시스템의 공유가 확대되어 행정기관 내에서도 책임영역이 불분명해진다. 그 결과, 현재와 같이 폐쇄적이고 분절된 정보보호법제와 행정체계로는 정보보호의 중복지대와 사각지대가 다수 발생할 것으로 예상된다.

즉 정부3.0에서는 정부와 민간이 상호 정보를 활발하게 교류 및 공유하게 되고, 정부는 정부 사이트의 API를 민간에 공개하여 민간 포털들이 국민에게 정부 서비스를 직접 제공할 수 있게 하는 한편, 국민들도 민간 포털에서 직접 공공정보를 검색하고 공공서비스를 이용할 수 있게 된다. 또한 정부와 민간의 서비스 융합 촉진을 위해 다음, 네이버 등의 민간 플랫폼 서비스를 정부 앱 개발에 손쉽게 적용할 수 있는 G-PaaS 서비스 및 인터페이스를 개발·보급한다는 계획이다. 그렇게 되면 불가피하게 공공부문과 민간부문이 중복되는 영역에서 정보보호의 회색지대가 발생할 가능성이 높아질 것이다.

따라서 사이버보안에 관한 사항을 종합적이고 효과적으로 추진하기 위하여 현재의 개별법 체계를 보완하거나 대체할 사이버보안기본법의 제정이 시급하며, 사이버보안에 관한 시책을 종합적이고 효과적으로 추진하기 위한 범정부 차원의 사이버보안 전담기관을 지정하거나 신설하여야 할 것이다. 현재 국회에는 2013년에 하태경의원등 11인이 발의한 「국가 사이버안전 관리에 관한 법률안」과 서상기의원등 13인이 발의한 「국가 사이버테러 방지에 관한 법률안」이 발의되었으며, 2015년 5월에는 최근 발생한 청와대 홈페이지 변조 사건(2013), 방송사·금융사 전산시스템 대량 마비 사건(2013), 한국수력원자력의 대량 메일 해킹 사건(2014) 등을 계기로 이철우의원 등 22인이 발의한 「사이버위협정보 공유에 관한 법률안」이 있다.

빅데이터나 클라우드에서의 정보 유출 사건 또는 서비스 장애(중단) 사건은 단순한 해킹사고를 넘어 국민생활과 직결되어 있는 클라우드정부 시스템 자체의 안전에까지 위협을 가함으로써 우리의 경제와 국가안보를 저해하는 심각한 위협이 될 수 있다는 점에서 정부3.0 자체의 존립을 위협할 수 있다는 점에 유의할 필요가 있을 것이다.

Ⅵ 일본 사이버시큐리티기본법의 주요내용과 정부3.0에의 함의

1. 사이버시큐리티기본법의 제정 목적

정부3.0 정책이 본격적으로 추진되고 있는 현실에서 2014년 11월 제정된 일본의 「사이버시큐리티기본법」은 우리에게 시사하는 바가 크다. 우리나라는 그동안 여러 차례 정보보호법제 및 행정체계를 정비하기 위한 정보보호기본법의 제정 필요성이 제기되었으나 아직껏 입법화가 이루어지지는 않고 있다.

이 법률은 법의 제정 목적을 '인터넷 및 기타 고도정보통신 네트워크의 정비 및 정보통신기술 활용의 촉진에 따라 세계적 규모에서 발생하고 있는 사이버보안에 대한 심각한 위협과 기타 내외의 제반 정세변화에 따라 정보의 자유로운 유통을 확보하면서 사이버보안의 확보를 도모하는 것이 중요한 과제가 되어 있는 상황을 고려하여 일본의 사이버보안에 관한 시책의 기본이념을 정하고 국가 및 지방공공단체의 책무 등을 분명히 하며, 사이버보안전략의 책정 및 기타 사이버보안에 관한 시책의 기본이 되는 사항을 정하는 동시에, 사이버보안전략본부를 설치하는 것 등에 의하여 「고도의 정보통신 네트워크 사회 형성기본법」(2000년 법률 제144호)과 함께 사이버보안에 관한 시책을 종합적이고 효과적으로 추진함으로써 경제사회의 활력 향상 및 지속적 발전과 국민이 안전하게 안심하면서 생활할 수 있는 사회의 실현을 도모하는 동시에 국제사회의 평화 및 안전의 확보, 일본의 안전보장에 기여하는 것을 목적으로 한다'(제1조)라고 규정하고 있다.

또한 동법은 사이버보안의 6대 기본이념을 제시하고 있는데, 첫째, 사이버보안 시책의 추진은 인터넷 기타 고도정보통신 네트워크의 정비 및 정보통신기술의 활용에 의한 정보의 자유로운 유통의 확보가 이를 통한 표현의 자유의 향유, 이노베이션의 창출, 경제사회의 활력 향상 등에 있어서 중요함에 비추어 사이버보안에 대한 위협에 대하여 국가, 지방공공단체, 중요사회기반사

업자(국민생활 및 경제활동의 기반으로서, 그 기능이 정지 또는 저하된 경우에 국민생활 또는 경제활동에 지대한 영향을 미칠 우려가 발생하는 것에 관한 사업을 하는 자를 말한다) 등 다양한 주체의 연계에 의하여 적극적으로 대응하는 것을 취지로 실시하여야 하고, 둘째, 국민 한 사람 한 사람의 사이버보안에 관한 인식을 높이고 자발적으로 대응하는 것을 촉진하는 동시에 사이버보안에 대한 위협에 의한 피해를 방지하고 피해를 신속하게 복구할 수 있는 강인한 체제를 구축하기 위한 대처를 적극적으로 추진하는 것을 취지로 실시하여야 하며, 셋째, 인터넷 및 기타 고도정보통신 네트워크의 정비 및 정보통신기술의 활용에 의한 활력있는 경제사회를 구축하기 위한 대처를 적극적으로 추진하는 것을 취지로 실시하여야 하고, 넷째, 사이버보안에 대한 위협에의 대응이 국제사회에 있어서 공통의 과제이고 일본의 경제사회가 국제적인 밀접한 상호의존관계 속에서 영위되고 있음에 비추어 사이버보안에 관한 국제적인 질서의 형성 및 발전을 위하여 선도적인 역할을 담당하는 것을 취지로서 국제적 협조 하에 실시하여야 하며, 다섯째, 「고도의 정보통신 네트워크 사회 형성 기본법」의 기본이념을 배려하여 실시하여야 하고, 여섯째, 국민의 권리를 부당하게 침해하지 않도록 유의하여야 한다고 규정하고 있다(제3조).

2. 사이버시큐리티의 정의

이 법에서 사용되고 되고 있는 "사이버시큐리티"란 전자적 방식, 자기적 방식 및 기타 사람의 지각으로는 인식할 수 없는 방식(이하 "전자적 방식"이라 한다)으로 기록되거나 발신, 전송 또는 수신되는 정보의 누설, 멸실 또는 훼손 방지 및 기타 정보의 안전관리를 위하여 필요한 조치와 정보시스템 및 정보통신 네트워크의 안전성 및 신뢰성의 확보를 위하여 필요한 조치가 강구되고 그 상태가 적절하게 유지・관리되고 있는 것을 말한다(제2조)라고 정의하고 있다. 물론 이 같은 조치에는 정보통신 네트워크 또는 전자적 방식으로 작성된 기록과 관련된 기록매체를 통한 전자계산기에 대한 부정한 활동에 의

한 피해의 방지를 위하여 필요한 조치를 포함한다. 우리나라는 아직 사이버보안에 대해서는 물론 정보보안에 대해서도 명확한 법률상 정의가 없으며, 국가정보화 기본법에서 “정보보호”란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것이라고 규정하고 있을 뿐이다(제3조 제6호).

3. 법률의 주요 내용

(1) 사이버보안의 주체별 책무

법률은 국가, 지방공공단체, 중요사회기반사업자, 사이버 관련 사업자 및 기타 사업자, 교육연구기관, 국민 등으로 나누어 사이버보안을 위한 각각의 책임과 역할을 구체적으로 규정하고 있다. 또한 사이버보안 시책을 실시하기 위하여 필요한 법제상, 재정상 또는 세제상의 조치 및 기타 조치를 강구하여야 할 정부의 법제상의 조치 의무와 사이버보안 시책을 강구하기 위하여 행정조직을 정비하고 행정운영을 개선하기 위해 노력해야 할 국가의 행정조직 정비 의무도 규정하고 있다.

(2) 사이버보안전략의 수립 및 시행

정부는 사이버보안 시책을 종합적이고 효과적으로 추진하기 위하여 사이버보안에 관한 기본적인 계획(사이버보안전략)을 정하여야 하며, 사이버보안전략에는 다음에 정하는 사항이 포함되어야 한다.

1. 사이버보안 시책에 대한 기본적인 방침
2. 국가 행정기관 등에서의 사이버보안의 확보에 관한 사항
3. 중요사회기반사업자 및 그 조직단체와 지방공공단체에서의 사이버보안의 확보의 촉진에 관한 사항
4. 기타 사이버보안에 관한 시책을 종합적이고 효과적으로 추진하기 위하여 필요한 사항

내각총리대신은 각의에 사이버보안전략안에 관하여 결정을 요구하여야 하고, 정부는 사이버보안전략을 책정한 때에는 지체없이 이를 국회에 보고하는 동시에 인터넷의 활용 및 기타 적절한 방법으로 공표하여야 한다.

(3) 사이버보안을 위한 기본시책

이 법률은 적용범위가 민간과 공공을 아우르고 일반정보통신시설과 주요 정보통신기반시설을 함께 규율하고 있다는 점에서 우리나라의 정보통신망법과 정보통신기반보호법, 산업기술유출방지법 그리고 국가사이버안전관리규정을 합해 놓은 것과 유사하다. 주목할 것은 이 법이 행정기관, 독립행정법인, 특수법인, 중요사회기반사업자뿐만 아니라, 중소기업자, 민간사업자, 대학 및 교육·연구기관까지도 시책추진의 주체 및 대상에 포함하고 있고, 더 나아가 일반 국민까지 포함하고 있다는 점이며, 그런 점에서 동법은 우리나라 제18대 국회에 발의된 「악성프로그램의 확산방지 등에 관한 법률안」과도 유사하다.

기본시책 분야에서 특별히 눈에 띄는 것은 사이버보안 관련 연습 및 훈련과 국내외 관련기관과의 연계 및 연락조정에 의한 사이버보안에 대한 위협에의 대응, 사이버보안에 관한 정보의 공유이다. 정보 공유는 국가 행정기관, 독립행정법인 및 특수법인 사이에만 적용되는 것이 아니라 중요사회기반사업자에게도 적용된다.

또한 국가는 관계부성 상호간의 연계를 강화하는 동시에 국가, 지방공공단체, 중요사회기반사업자, 사이버 관련사업자 등의 다양한 주체가 상호연계하여 사이버보안에 관한 시책에 대처할 수 있도록 필요한 시책을 강구해야 하며, 일본의 안전에 중대한 영향을 미칠 우려가 있는 것에 대한 대응에 관하여 관계기관에서의 체제의 충실강화와 관계기관 상호의 연계강화 및 역할분담의 명확화를 도모하기 위하여 필요한 시책을 강구하도록 규정하고 있다.

그밖에 사이버보안을 위한 국가의 기본시책으로 사이버보안 관련 산업의 진흥(고용기회 창출 등 신성장 산업화), 국제경쟁력 강화(첨단연구개발 추진

등), 인재의 육성 및 확보, 사이버보안 관련 기술의 자립화, 연구개발 및 기술의 실증 추진, 연구개발을 위한 산・학・연 연계 강화, 사이버보안 관련 종사자의 처우개선 및 직장환경 개선, 청년기술자의 양성, 대국민 사이버보안 교육 및 학습의 진흥 및 지식의 보급・계발, 사이버보안에 관한 국제적인 규범 책정에 대한 주체적 참여, 개발도상국가의 사이버보안 관련 대응능력 구축의 적극적 지원 등을 규정하고 있다.

(4) 사이버보안 전략본부의 설치

동법은 사이버보안 시책을 종합적이고 효과적으로 추진하기 위해 내각에 사이버보안 전략본부를 두도록 규정하고 있다. 본부장은 관방장관이 되고, 국가공안위원회 위원장, 총무대신, 외무대신, 경제산업대신, 방위대신, 국무대신 또는 사이버보안에 관하여 뛰어난 식견을 가진 자 중 내각총리대신이 지정하는 자가 본부원이 되며, 본부에는 직원을 둔다.

전략본부는 사이버보안전략안의 작성 및 추진, 사이버보안대책 기준 작성 및 시책 평가(감사 포함), 사이버보안 관련 중대현상에 대한 시책 평가 및 원인규명, 그밖에 사이버보안 관련 중요 시책에 대한 예산책정, 종합조정, 시책 추진평가 등의 사무를 담당하게 된다. 전략본부가 사이버보안전략안을 작성할 때에는 사전에 고도정보통신네트워크사회추진전략본부 및 국가안전보장회의의 의견을 들어야 하고, 고도정보통신네트워크사회 추진전략본부와 긴밀한 연계를 도모해야 하며, 일본의 안전보장과 관련된 사이버보안에 관한 중요사항에 대하여는 국가안전보장회의와도 긴밀한 연계를 도모해야 한다.

이상과 같은 사무의 원활한 수행을 위하여 전략본부는 필요하다고 인정하는 때에는 관계행정기관, 지방공공단체, 독립행정법인, 국립대학법인, 대학공동이용기관법인, 일본사법지원센터, 특수법인 및 인가법인, 사이버보안 관련 현상이 발생한 국내외의 관계자와 연락조정업무를 담당하는 관계기관에 대하여 자료제출, 의견개진, 설명 및 기타 필요한 협력을 요구할 수 있고 그 밖의 필요한 자에 대하여는 협력을 의뢰할 수 있다.

Ⅶ 맺음말

정부3.0은 빅데이터와 클라우드 그리고 모바일, SNS, 웹3.0 등 새로운 정보통신기술을 기반으로 한 지능성 정부이다. 기존의 전자정부의 개념을 완전히 뛰어넘는 새로운 개념의 "클라우드정부"라고 할 수 있다. 따라서 정부3.0의 성공은 곧 사이버보안에서부터 시작된다고 해도 과언이 아닐 것이다. 그러나 우리나라의 사이버보안법제와 행정체계는 클라우드 환경에는 적합하지 않다. 기존에도 우리나라의 사이버보안법제와 행정체계는 행정주체별로 책임영역이 단절되어 있고 역할이 분산되어 있어 위기에 대응하기 어렵다는 지적을 받아 왔으나 아직까지 해법을 찾고 있지 못한 상태이다.

따라서 이번에 정부3.0을 계기로 하여 우리나라의 사이버보안 또는 사이버안보의 틀을 완전히 전환할 필요가 있다. 즉 기존에 익숙해온 좁은 의미의 정보보호의 개념에서 벗어나 사이버보안이라고 하는 안보적 관점에서 접근할 필요가 있다. 굳이 전쟁이 아니더라도 세월호나 메르스와 같은 사고가 국가적 위기를 가져올 수 있고, 정보통신망에 대한 공격이나 침입이 아니더라도 정보를 제대로 수집·이용 및 관리하지 못해 생긴 위기도 빈번하다. 정보법의 관점에서 보면 세월호나 메르스는 관련 정보만 제때에 정확히 수집해서 분석했더라면 충분히 예측하거나 막을 수 있는 사건이라고 할 수 있다. 이와 같은 정보들의 원활한 수집과 안전한 이용을 보장하는 장치가 곧 사이버보안이다. 따라서 정부3.0과 사이버보안은 동전의 앞뒷면과 같다.

안보적인 관점에서, 통합적인 접근 방법에 기초한 사이버시큐리티기본법이 필요하다고 해도 기존의 법률을 모두 폐지하거나 개정해야 할 필요는 전혀 없다. 기존의 법질서 내에서 안보적 개념이 추가된 사이버시큐리티기본법을 제정하여 위기상황을 상시 관리하고 즉시 대응할 수 있는 범정부적 시스템을 구축하면 된다. 각 부처가 사이버보안과 관련한 시책을 잘 수립해서 열심히 시행하는 것도 중요하지만, 이를 국가안보라는 관점에서 보안적 감수성이 강한 전문기관으로부터 종합적으로 평가받고 검증받은 관리·감독

시스템이 무엇보다 중요하며, 각 주체들 간에 사이버보안 관련 정보를 공유하고 상호 협력할 수 있는 협력시스템을 구축하는 것이 급선무라고 할 수 있다.

미국의 공공정보 개방과 사이버보안 정책의 패러다임 전환*

손 승 우**

목 차

Ⅰ 미국의 공공정보 개방 정책

1. 정책 추이

2009년 오바마 정부는 일반 국민이 공공자원을 자유롭게 사용하고 기업

* 이 자료는 저자가 2015.6.25. 한국사이버안보법정책학회 2015년 상반기 정기 학술대회('정부 3.0시대의 사이버안보')에서 동일한 주제로 발제한 PPT 자료를 한글 파일 형식으로 전환하고 일부 내용을 보완한 것임을 밝힙니다.

** 단국대학교 법과대학 교수, 법학박사(S.J.D.).

의 업무 효율화 및 신규 비즈니스 창출을 도모하기 위해 공공데이터를 민간에 개방하는 '오픈 데이터 정책(Open data policy)'을 시행하기로 하였다. 2009년 백악관은 열린정부계획(Open Government Initiative: OGI)의 추진을 통해 정부가 보유한 공공데이터 개방 원칙을 천명하였다. 그리고 2012년 오픈데이터 계획(Open Data Initiative)을 추진하여 데이터를 기반으로 하는 새로운 서비스 창출을 지원하는 한편 벤처기업을 육성하였다.

미국은 이미 1996년 전자정보공개법(Electronic Freedom of Information Act)을 제정하여 공공정보를 민간이 자유롭게 활용할 수 있도록 하였는데, 동법은 정부기록의 전자화에 따라 정보 공개 청구 대상에 전자 기록도 포함시키도록 규정하였다. 2000년대 후반 미국의 공공정보 개방 정책은 영국, 일본, 우리나라 등에 상당한 영향을 미친 것으로 평가된다.

2009년 1월 21일, 오바마 행정부는 "투명성과 열린정부(Transparency and Open Government)"국정계획을 추진하기 위해 3월에는 백악관 데이터 저장소 구축 계획안을 발표하고, 5월에는 조달청(General Service Administration)과 행정관리예산국(Office of Management and Budget: OMB)의 지원과 내무부(Department of the Interior)와 환경보호국(Environmental Protection Agency)의 주도로 오픈 플랫폼인 'Data.gov' 포털을 설치하여 공공정보를 일반시민이 자유롭게 활용하도록 하였다. 또한 연방공공기관, 주 및 지방정부, 공기업의 공공정보 및 서비스를 분야별, 기관별로 제공하였다. 12월 8일에는 관리예산국(Office of Management and Budget)이 "Open Government Directive(OGD)" 발표하였다.

2. 특징

미국의 공공정보 개방 정책(Open Data Policy)의 특징은 우선 하향스트림 정보 처리와 배포(이용)가 가능한 형태로 정보를 수집하고 생성하였다. 아래에서 상술하는 바와 같이, 일반 국민과 기업들이 공공정보를 효율적이고 실질적으로 이용할 수 있도록 수집 및 생성에 있어서 이용 가능한 형태를 취

하도록 한 것이다. 또한 개방정책은 상호운용성과 정보 접근성(API 개방)을 지원하는 정보 시스템을 구축하고, 데이터 관리 및 배포 기준을 강화하였다.

그리고 공공정보 개방에 있어서 데이터의 안전과 프라이버시 및 기밀 보호 대책을 강화하였다. 이를 위해 상호운용성 및 개방성 요건을 기관의 핵심 절차에 포함하도록 주요 정책으로 정하였다. 여기서의 공공정보는 연방, 주, 지방 정부나 공공기관이 생산, 보유, 관리하는 모든 데이터를 의미한다. 그리고 미국의 경우에는 정부 저작물에 대해서는 저작권 보호를 하지 않도록 규정하고 있다.[1)]

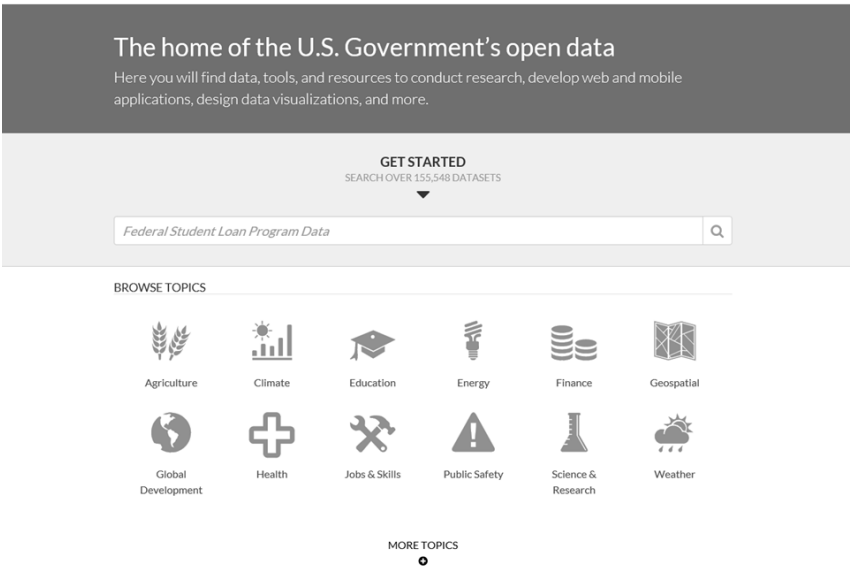
3. 공공데이터 포털

미국의 공공데이터 포털(http://data.gov)의 특징을 살펴보면, 공공정보에 대한 민간 접근성을 향상시키고, 정부의 연구 및 분석 자료 등 정보 활용을 확대하는 역할을 한다. 그리고 정부 정책과정에 시민이 참여할 수 있도록 유도하여 민관협업의 창구로서 역할을 하기 위해 시민의 제안 및 의견을 수렴하고 있다. 동 포털의 현황을 살펴보면, 2014년 9월 기준으로 정부조직(229개), 출판사(333개), 그 밖의 공공기관(90개) 참여하여 약 7억 개 상당의 데이터를 제공하고, Dataset[2)] Management System를 통해 공공정보를 등록하도록 하고 있다.

또한 해외에서도 접근이 가능한 개방형 플랫폼으로 클라우드 컴퓨팅을 활용하여 데이터 공개 절차 및 예산을 절감하고, 이용자의 접근성을 극대화하는 동시에 관리를 용이하게 하고 있다. 또한 플랫폼을 오픈소스로 개방하여 다른 플랫폼과 연동을 증진할 수 있다. 동 포털을 통해 데이터를 카테고리별로 분류하여 제목, 기관, 키워드 검색이 가능하도록 하고, Datasets 108,719건, 애플리케이션 349개, 모바일 앱 140개, 정부 API 409개 등이

1) 미국 백악관 홈페이지 https://www.whitehouse.gov
2) 공공데이터를 각 분야별로 구분하여 집합해 놓은 것을 '데이터셋(dataset)'이라고 한다.

제공되고 있다.[3)]



동 포털은 데이터를 RDF(Resource Description Framework) 형식으로 변환하여 제공하되 정보 활용이 가능하도록 CVS, XLS, Text, KML 등 다양한 데이터 형식으로 제공하고 다른 데이터 셋과 결합이 용이하도록 한다. 그리고 연방 최고정보책임자 협의회(Federal Chief Information Officer Council)와 연방 조달청(General Service Administration)이 공동으로 운용한다. 이를 위해 조달청은 "Data.gov Next Generation" 및 "Data.gov in a box" project를 추진하였다. 또한 동 포털에서는 공공정보 외에 정보활용 교육 및 커뮤니티를 제공하는데, 예를 들면 미세먼지 정보 위젯, 병원 추천 서비스(iTriage), 종합날씨 보험서비스 등을 들 수 있다.

3) 지리, 교통, 출생/사망/결혼/이혼, 인구, 국가안전 및 재향군인, 에너지, 농업, 정보통신, 정부재정 및 고용 등으로 분류

※ 이혜진, 현미환, 김혜선, KiSTi 지식리포트[No.43], 2014.12.

Ⅱ 미국의 공공정보 개방과 사이버 보안 정책

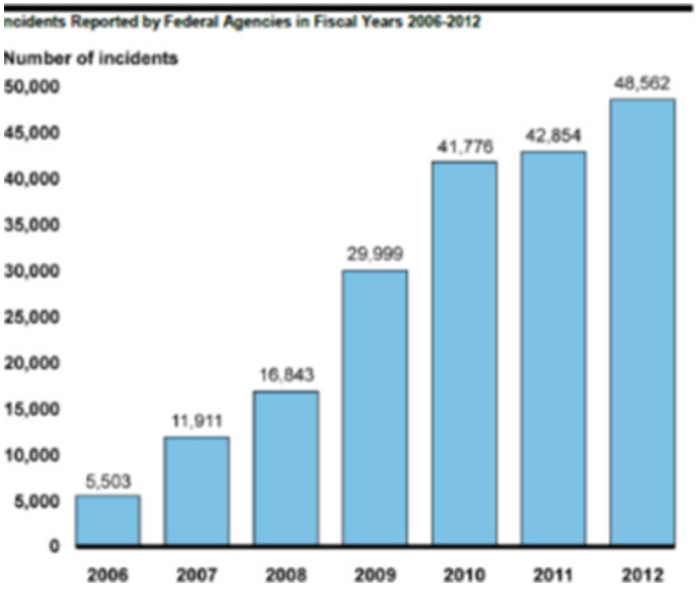
1. 서설공공정보 개방에 있어서 사이버 보안

미국은 공공정보 개방에 있어서 정보 공개로 인한 사이버침해 발생을 방지하기 위한 사이버 보안의 중요성도 인식하고 있으며 상충되는 두 개념 간의 조화를 통해 공공의 이익과 개인의 권리 간의 균형을 이루고자 한다. 이를 위해 공공데이터 개방 정책은 공공정보제공뿐만 아니라 보안, 데이터안전 관리, 프라이버시 보장 등 지속적인 관리 노력을 규정하고 있다.

그러나 공개될 정보와 민감한 정보의 구분 및 공공과 민간의 구분 등이 모호하다는 것이 문제로 지적된다. 즉 개인정보 등 민감한 정보를 포함하고 있는 공공데이터의 제공 범위가 명확하지 않고 공공데이터포털의 API 민간 제공 및 민-관 상호 정보 교류 및 공유로 인해 발생하는 책임의 경계가 모호하다. 그럼에도 불구하고 공공기관이 보유한 민감한 정보에 대한 사이버 보안이 요구되므로 미국 공공데이터 포털의 경우 특수목적의 분리된 네트워크를 사용하고 민감한 정보는 게시하지 않도록 사전 필터링을 작동하고 있다.

2. 사이버 침해 사례와 현황

미국에서는 2015년 4월, 러시아 해커가 오바마 미국 대통령의 이메일을 해킹하는 사건이 발생하고, 6월 4일에는 미국 연방인사관리처(OPM) 전산시스템이 해킹되어 “4월말부터 미국의 연방공무원 전산시스템이 해킹돼 300만명의 전현직 연방공무원 정보가 유출”되었다고 국토안보부는 발표하였다. 또한 소니사 종업원의 사회보장번호, 금융정보, 병원 기록 등이 유출되는 해킹 사건도 발생하였는데, 민간뿐만 아니라 공공기관에 대한 해킹도 급증하고 있는 추세이다. 이러한 추세는 공공정보의 개방이 확대될수록 보안의 위험이 높아지고 있음을 보여준다. 아래 GAO 분석 보고서에 따르면 2006년 - 2012년 사이 연방정부기관에 대한 사이버위협 789% 증가하였고, 연간 사이버범죄에 따른 비용은 $4,000억로 추산되고 있다.



※ GAO analysis(2013.2) of US-CERT data for fiscal years 2006-2012

3. 공공정보에 대한 사이버 보안 법제

공공정보는 디지털형태로 존재하고 인터넷을 통해 공개, 제공되므로 사이

버 보안의 적용이 요구된다. 특히 공공데이터 포털 뿐만 아니라 개별 공공기관이 클라우드 기반 또는 해당 웹사이트에서 공공정보를 개방, 제공하기도 하므로 데이터 보안이 중요한 요소로서 미국은 공공정보 개방관련 사이버보안 문제를 연방프라이버시법(Privacy Act), 전자정부법(E-Government Act), 연방정보보안관리법(Federal Information Security Management Act) 등으로 규율하고 있다.

또한 2010년 Government Performance and Results Modernization Act에 따라 연방정부기관은 개별적으로 사이버보안 전략계획을 수립해야 한다. 연방부처는 개별적으로 보안 수립계획을 수립하므로 부처에 따라 보안 수준에 편차가 크다. 예를 들면, 보건복지부(Department of Health and Human Services)의 계획은 구체적으로 수립되어 있는 반면 에너지부(Department of Energy)의 경우에는 상대적으로 구체적 계획을 수립하고 있지 않다.

미국은 최근 범국가 차원의 사이버보안 민관 협력 강화를 추진하고 있다. 2014년7월 15일 주지사위원회(Council of Governors)는 국방부, 국토안보부와 함께 "사이버보안 위협에 대응하기 위한 연방과 주의 공동 계획(Joint Action Plan for State-Federal Unity of Effort on Cybersecurity)"을 발표하고, 201년 2월 13일 "민·관 사이버보안 정보공유 촉진 행정명령(Promoting Private Sector Cybersecurity Information Sharing EXECUTIVE ORDER 13691)"을 발표하였다. 민-관 간 사이버 위협 정보 공유는 기존의 민-민 간 정보 공유를 넘어 범국가적 사이버 보안 거버넌스를 형성하는 것으로 연방거래위원회(FTC)와 법무부(DOJ)는 민간 기업간 사이버 위협 관련 정보를 공유하는 것은 반독점적 행위에 해당하지 않는다고 밝혔으나, 사이버 위협 관련 정보를 공유하는 과정에서 개인정보 유출, 오남용, 프라이버시 침해 등의 우려가 존재한다.[4)]

4) FTC, "Antitrust Policy Statement on Sharing of Cybersecurity Information", 2014.4.10.

미국은 50여 개 법률에서 사이버보안을 직·간접적으로 규율하고 있다. 예를 들면, 위장접근수단 및 컴퓨터사기·남용방지법(Computer Access Device and Computer Fraud and Abuse Act of 1984)에서 연방정부와 은행이 사용하는 컴퓨터시스템, 주간거래 및 해외거래에 이용되는 컴퓨터시스템에 대한 공격을 금지하고 있다. 전자통신 프라이버시법(Electronic Communications Privacy Act of 1986)에서 승인받지 않은 전자적 도청을 금지하고 있다. 국토안보법(Homeland Security Act of 2002)에서 국토안보부에 사이버테러를 포함한 국가적 위기 및 재해로부터 미국의 안전을 지키는 컨트롤타워 기능 및 권한을 부여하도록 규정한다. 전자정부법(E-Government Act of 2002)에서 정부 정보와 서비스의 인터넷상 제공 및 각종 사이버보안 요건을 규정한다. 연방정보보안관리법(Federal Information Security Management Act of 2002)에서 연방정부기관의 사이버보안 책임을 명확히 규정하고 연방보안사고센터, 행정관리예산국의 사이버보안 기준 제정을 의무화하고 있다.

한편 주요기반시설의 사이버보안 강화를 위한 행정명령(2013)에서 통신, 에너지, 금융, 운송, 정부시설, 원자로 등 16개 주요기반시설에 대한 사이버위협에 대응하기 위하여 정부(국토안보부 등)는 위협 및 공격 정보를 기업에 제공하여 공유하고 국립표준기술연구소(NIST)를 중심으로 사이버위협 시 정책적, 기업적, 기술적으로 표준화된 대처방법 개발 및 프라이버시와 시민자유의 확실한 보호를 위한 평가를 하고 있다. 또한 2014년 1월, 조달청(General Services Administration)과 국방부(Defense Department)는 연방정부기관의 사이버보안의 취약점을 개선하기 위한 개혁보고서(reform report)를 발표하였는데, 동 보고서에서 사이버보안과 관련된 새로운 기술을 고려하도록 권고하고 있다.

이 밖에도 2015년 1월 8일 사이버 정보공유 및 보호법(안)(Cyber Intelligence Sharing and Protection Act)(H.R.234) 등 3개 법안이 상하원에 제출되었다.[5] 동 법안들은 연방의회를 거쳐 2015년 12월 18일 「사

이버보안 정보공유법(Cybersecurity Information Sharing Act of 2015, CISA)」으로 대통령의 서명을 받게 되었다. 이 법안의 가장 큰 특징은 사이버 침해 정보를 민간과 공공이 공유할 수 있도록 하고, 공유한 기업에 대해서 해당 사건과 관련된 책임으로부터 면제를 시켜주고 있다. 과거 이 법안은 사생활 침해 우려로 입법화되지 못하였으나 동 법안에서 개인의 프라이버시와 시민권을 보호하는 내용을 함께 담음으로써 보안과 프라이버시 보호 간 충돌을 해결하고 있다. 연방기관은 사이버보안 집행에 있어서 개인 사생활과 시민자유를 보호하기 위한 조치를 취하여야 하며, 정기적으로 이에 대한 영향을 평가하고 알려야 한다. 그리고 국토안보부는 비영리 민간단체를 지역별, 특정 위협별로 정보공유분석기관으로 지정하고, 이들 상호간의 유기적 연계성을 위하여 사이버보안통신통합센터(NCCIC)를 설치·운영하고 있는 점도 눈여겨 볼 필요가 있다.[6]

Ⅲ 국내 공공정보 개방과 보안 정책의 시사점

1. 공공데이터 개방과 보안

「공공데이터의 제공 및 이용 활성화에 관한 법률」(이하 "공공데이터법"이라 한다)은 공공기관이 보유 및 관리하고 있는 공공데이터를 기업과 국민이 이용할 수 있도록 권리를 보장하기 위하여 2013.10.31.부터 시행되고 있다. 정부는 이 법률 제정 이전부터 '정부 3.0' 정책에 따라 공공누리(Korea Open Government License, KOGL) 사업을 통해 공공정보를 민간영역에서 활용할 수 있도록 하여 문화적, 경제적 부가가치 창출하도록 지원해 왔다. 공공데이터법에서 공공데이터란 "데이터베이스, 전자화된 파일 등 공공기관이 법령 등에서 정하는 목적을 위하여 생성 또는 취득하여 관리하고 있는 광

5) 박영우, 미국 사이버보안 법제의 최근 동향, 2015.4.29 인터넷 법제도 포럼 발제자료
6) 박영철, 손승우 외, 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원, 2015.12 참조.

또는 전자적 방식으로 처리된 자료 또는 정보를 말한다."(제2조2호)고 정의하고 "공공기관"이란 국가기관, 지방자치단체 및 「국가정보화 기본법」 제3조제10호에 따른 공공기관을 말한다.(제2조1호)고 정의하고 있다.

한편 행정자치부는 2011년 7월, 공공정보활용지원센터(www.pics.or.kr)와 국가지식 포털(www.knowledge.go.kr)을 통합하여 데이터 포털(www.data.go.kr)을 구축하였다.

데이터셋 분야별 개방 현황

No.	분야	15대 전략분야	제・개정일	
			제정	개정
1	주차장 정보	국토교통	'14. 10. 10.	'15. 7. 29.
2	도시공원 정보	문화관광	'14. 10. 10.	'15. 7. 29.
3	어린이 보호구역	재해안전	'14. 12. 1.	'15. 7. 29.
4	공중화장실	공공정책	'14. 12. 1.	'15. 7. 29.
5	사회적기업	공공정책	'14. 12. 1.	'15. 7. 29.
6	무인민원 발급 정보	공공정책	'14. 12. 1.	'15. 7. 29.
7	전통시장	문화관광	'14. 12. 1.	'15. 7. 29.
8	문화축제	문화관광	'14. 12. 1.	'15. 7. 29.
9	민박/펜션업소	문화관광	'14. 12. 1.	'15. 7. 29.
10	공연행사정보	문화관광	'14. 12. 1.	'15. 7. 29.
11	무료급식소	보건복지	'14. 12. 1.	'15. 7. 29.
12	CCTV	재해안전	'15. 7. 29.	
13	어린이집	보건복지	'15. 7. 29.	
14	도서관	교육	'15. 7. 29.	
15	평생학습강좌	교육	'15. 7. 29.	
16	휴양림	문화관광	'15. 7. 29.	
17	관광안내소	문화관광	'15. 7. 29.	
18	농어촌체험마을	문화관광	'15. 7. 29.	
19	상수도 수질 검사	환경	'15. 7. 29.	
20	전기차 충전소	환경・교통	'15. 7. 29.	
21	무료 와이파이	과학기술	'15. 7. 29.	
22	공공시설 개방정보	공공정책	'15. 7. 29.	

행정자치부, "공공데이터 개방 표준"[행정자치부 고시 제2015-31호, 2015.8.4. 일부개정, 2015. 8. 4. 시행]. 5. 데이터셋 분야별 개방기준.

공공데이터법은 제3조 4항에서 “공공기관은 다른 법률에 특별한 규정이 있는 경우 또는 제28조제1항 각 호의 경우를 제외하고는 공공데이터의 영리적 이용인 경우에도 이를 금지 또는 제한하여서는 아니 된다.”고 규정학고, 제17조 1항에서 공공기관의 장은 해당 공공기관이 보유・관리하는 공공데이터를 국민에게 제공하여야 한다. 이 점에서 우리나라는 공공정보를 민간이 활용할 수 있도록 적극적인 정책과 법제도를 마련하고 있다고 평가된다.

공공정보 중에는 다음과 같은 정보는 제공할 수 없다. 1.「공공기관의 정보공개에 관한 법률」 제9조에 따른 비공개대상정보 2.「저작권법」 및 그 밖의 다른 법령에서 보호하고 있는 제3자의 권리가 포함된 것으로 해당 법령에 따른 정당한 이용허락을 받지 아니한 정보의 경우에는 그러하지 아니하다. 동법 제9조에 따른 비공개대상정보는 국가안전보장・국방・외교관계 등에 관한 사항으로 공개될 경우 국가의 중대한 이익을 현저히 해할 우려가 있다고 인정되는 정보이거나 개인의 사생활의 비밀 또는 자유를 침해할 우려가 있는 정보 또는 영업비밀 등이 해당한다.

공공정보의 적극적인 개방에 비해 정보 개방으로 인한 사이버 보안 문제는 상대적으로 미흡한 수준이다. 즉 실무적으로 개인정보 등이 포함된 공공데이터의 대상 범위가 불명확하고 그 기준이 미흡하다. 예를 들면, 공공기관이 작성한 연구보고서의 경우 개인정보가 포함된 경우가 다수가 있으나 그 기준이 미흡하고, 개인정보 처리를 강화할 경우 공공정보의 활용에 장애가 될 수 있다. 즉 개인정보 등이 포함된 공공데이터의 예시와 구분 기준이 필요하다. 또한 개인정보 등의 공개, 이용, 제공 처리 기준도 미흡한 실정이다. 공공정보 공개 등에 있어서 정보주체의 동의 및 고지의무 조항 등이 없으며(법 제21조 제3자 관련 정보 인정 시 통지 의무), 법 제4조에서 타법 특별 규정 준수를 규정하고 있으나 공공데이터 제공은 불특정다수를 대상으로 하고 있으므로 여전히 구체적인 기준이 필요한 실정이다.

이와 같이 우리나라는 공공정보 개방과 관련하여 사이버보안 및 정보보호는 관련 법률에 맡기고 있으나 그 특수성을 고려한 보안 기준이 미흡한 상태

이다. 미국의 경우 공공데이터 포털의 경우 특수목적의 분리된 네트워크를 사용하고 있는데 우리나라의 경우도 공공기관은 물리적 망분리를 통해 보안성을 강화하고 있다. 그러나 공공정보 사이버 보안의 필요성에 대한 인식은 미국에 비해 떨어지는 수준이며, 또한 미국과 같이 사이버 보안을 강화하려는 일련의 입법적 움직임이 부족한 상황이다.

2. 공공저작물 개방

문화체육관광부는 2006년부터 공유저작물 창조자원화를 추진하였는데, 이는 공유저작물 활용 기반을 구축하여 개인의 창조활동과 문화적·산업적 활용을 증진하기 위한 것이다. 이를 위해 저작권법상에 공공저작물의 자유이용에 관한 제24조의2를 신설하였다.

> **저작권법 제24조의2(공공저작물의 자유이용)** ① 국가 또는 지방자치단체가 업무상 작성하여 공표한 저작물이나 계약에 따라 저작재산권의 전부를 보유한 저작물은 허락 없이 이용할 수 있다. 다만, 저작물이 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
> 1. 국가안전보장에 관련되는 정보를 포함하는 경우
> 2. 개인의 사생활 또는 사업상 비밀에 해당하는 경우
> 3. 다른 법률에 따라 공개가 제한되는 정보를 포함하는 경우
> 4. 제112조에 따른 한국저작권위원회에 등록된 저작물로서 「국유재산법」에 따른 국유재산 또는 「공유재산 및 물품 관리법」에 따른 공유재산으로 관리되는 경우
>
> ③ 국가 또는 지방자치단체는 제1항제4호의 공공저작물 중 자유로운 이용을 위하여 필요하다고 인정하는 경우 「국유재산법」 또는 「공유재산 및 물품 관리법」에도 불구하고 대통령령으로 정하는 바에 따라 사용하게 할 수 있다.

그러나 동 규정은 공공기관의 대부분 정보가 저작권 보호를 받고 있는데 그 대상을 국가 또는 지자체의 업무상 저작물 기타 보유 저작물로 한정하고 있다는 제한이 있다. 한편 한국저작권위원회는 2006년부터 보호기간 만료 저작물을 수집, DB화하여 공유마당(gongu.copyright.or.kr)을 통해 약 786,272개의 저작물을 서비스하고 있다('07-14 조회· 원문보기· 다운로

드 등 1373만건 이용).

3. 공공저작물 개방과 보안

공공저작물의 개방과 보안을 추진함에 있어 그 균형을 이루기 위해 필요한 조치들을 언급하면 다음과 같다. 첫째, 안전한 저작물 이용을 위한 저작권 검증을 위하여 상시 모니터링 체계 구축이 필요하다. 둘째, 최소한의 정보 수집 및 안전한 개인정보 관리를 위한 규정 마련이 필요하다. 셋째, CCL (Creative Commons License) 마크를 부착하도록 규정할 필요가 있다. 예를 들면, Y 또는 BY-SA 두 가지만 선택할 수 있도록 공모전 조건을 부여하여 보다 개방적인 저작물 수집이 이루어지도록 한다. 넷째, 공공기관의 공공저작권 침해에 대한 대응을 위한 조치를 마련할 필요가 있다(공공저작물 저작권 관리지침 제24조). 현재 공공기관의 경우에는 침해 대응 조치를 의무화하고 있을 뿐 사이버 보안에 관한 언급은 부재한 실정이다.

한편 미국의 「사이버보안 정보공유법(Cybersecurity Information Sharing Act of 2015, CISA)」과 같이 사이버테러 위협으로부터 효과적으로 대처하기 위해 해킹 첩보 및 정보를 정부기관과 의무적으로 공유할 수 있는 법적 근거가 부재하다. 동 법안은 개인의 프라이버시와 사이버 보안 간 충돌을 해결하기 위한 장치를 마련하여 양자의 이익을 함께 고려하고 있다는 점에서 우리에게 시사점을 주고 있다.

정부3.0시대의 사이버안보 관련 법제 추진전략

이 정 현*

목 차

Ⅰ 서 론

1. 정부3.0

정부3.0이란 무엇인가? 이는 새로운 정부 운영 패러다임이다. 공공정보를 적극적으로 개방하며 공유하고 부처간 칸막이를 없애 소통하고 협력함으로

* 한국인터넷진흥원 법제팀장/법학박사

써, 국민 맞춤형 서비스를 제공하고 동시에 일자리 창출과 창조경제를 지원하는 새로운 정부운영 패러다임이라고 한다.[1)]

이 새로운 패러다임에 따르면 그간 수요자인 국민이 요구를 통해 얻었던 행정서비스가 국민 개개인 중심으로 수요자 맞춤형 서비스로 통합제공하는 정책을 의미하고 있다.

출처 : 정부3.0 홈페이지〈https://www.gov3.0.go.kr〉

운영방향	정부 중심	국민 중심	국민 개개인 중심
핵심가치	효율성	민주성	확장된 민주성
참여	관 주도 · 동원 방식	제한된 공개 · 참여	능동적 공개 · 참여 개방 · 공유 · 소통 · 협력
행정서비스	일방향 제공	양방향 제공	양방향 · 맞춤형 제공
수단(채널)	직접 방문	인터넷	무선 인터넷 스마트 모바일

이러한 정부3.0 전략을 추진하는 정부에서 사이버안보와 관련한 법제는 어떻게 추진 전략을 갖고 있는지, 혹은 갖추어야 하는지에 대하여 논해 보고자 한다.

1) <https://www.gov30.go.kr/gov30/int/intro.do>, (2015.6.14. 최종방문).

2. 사이버안보

한편, '사이버안보'라는 용어의 정의도 필요하다. "안보(安保)"의 사전적 의미는 두 가지가 있는데 첫째로, '편안히 보전됨. 또는 편안히 보전함'을 의미하고 둘째는 정치분야에서 '안전보장(安全保障)(외부의 위협이나 침략으로부터 국가와 국민의 안전을 지키는 일)을 줄여 이르는 말'이라고도 한다.[2)]

사이버안보, 사이버보안, 사이버안전 등은 영어로 모두 Cyber Security로 사용되고 있고 개념도 명확히 정리되어 있지 않은 상태이다.

좁은 의미에서 사이버안보는 사이버보안=사이버안전 등으로 혼합사용하는 용어로 비춰지고 있는 듯하다.

하지만, 기존의 여러 논문들에서 언급한 용어 정의를 인용한다면,[3)] '사이버안보'는 사이버위협이나 공격으로부터 국가 정보통신망의 위험요인을 제거하여 안정성을 유지하는 상태를 뜻하는 사이버보안보다는 동적이고 적극적인 개념으로 이해되며 국가의 안보와 밀접한 관련이 있는 개념으로 파악된다.[4)]

따라서 넓은 의미에서의 사이버안보는 물리적인 위협과 사이버 위협에 대한 방어와 공격의 수준을 높이는데 총력을 기울이는 국가적 차원의 큰 틀에서 사용되는 개념으로 정리하고자 한다.[5)]

2013년 3.20, 6.25 사이버공격 발생 이후 정부는 같은 해 7월 4일 '국가사이버안보 종합대책'을 발표했다. 그 주요한 내용은 다음과 같다. 첫째, 사이버위협 대응체계 즉응성을 강화하기 위하여 사이버안보 컨트롤타워는 청

2) 네이버 국어사전 참조.
3) 이완수, 국가 사이버 안보 구축전략에 관한 연구, 경기대학교 대학원 박사학위 논문, 2014.6. 36~37면 ; 남길현, "사이버테러와 국가안보", 국방연구.
4) 사이버안보, 사이버보안, 사이버안전, 정보보안(보호) 등에 관한 용어에 대해 자세한 사항은 이정현, "국가 사이버안보(cyber security) 추진체계의 이슈와 과제", 사이버안보법정책논집, 2014. 창간호, 55~63면에서 이를 비교하였으니 참고바란다.
5) 사이버안보를 위협하는 태양은 개인정보나 기업 및 국가의 중요정보를 해킹하는 행위나 금융권이나 기업 등의 영업비밀이나 산업비밀, 국방 및 국가기밀 등을 빼내려고 하는 행위 모두가 될 수 있다. 따라서 사이버안보를 논할 때 국방분야에 대한 언급도 필요하다 할 것이나 본 고에서는 국방에 대한 사항은 일부만 기술하기로 한다.

와대가 맡기로 하였고, 실무총괄은 국가정보원이 담당하며, 관계 중앙행정기관이 소관분야를 각각 담당하도록 대응체계를 확립하였고, 사이버상황을 즉시 파악하여 대처할 수 있도록 동시 상황전파 체계를 구축하였으며, 중요 사고에 대해서는 '民·官·軍합동대응팀'을 중심으로 상호협력 및 공조를 강화하기로 하였다. 둘째, 기관간 원활한 정보공유가 부족하다는 지적에 따라 유관기관 스마트 협력체계를 구축하기 위해 국가차원의 '사이버 위협정보 공유시스템'을 2014년까지 구축하고, 이를 토대로 민간 부문과의 정보제공·협력도 강화하기로 하였다. 셋째, 사이버공간 보호대책 견고성을 보강하기 위해 2017년까지 집적정보통신시설(IDC)·의료기관 등을 포함한 주요정보통신기반시설을 209개에서 400개로 확대하고 국가기반시설에 대해 인터넷망과 분리·운영하는 한편, 전력·교통 등 테마별로 특화된 위기대응훈련을 실시하기로 하였다. 넷째, 넷째, 사이버안보 창조적 기반 조성을 위해 최정예 정보 보호 전문가 양성사업 확대 및 영재교육원 설립 등 다양한 인력양성 프로그램을 추진하여 2017년까지 사이버 전문인력 5,000명을 양성하고, 미래시장 선점을 위한 10대 정보보호 핵심기술[6] 선정과 연구개발의 집중적 추진으로 기술 경쟁력도 강화해 나갈 계획이다.[7]

다행이 2015년 국내 정보보호 시장의 확대, 정보보호 전문가 양성, 세계최고 수준의 정보보호 제품개발을 위하여 수요확충과 신시장 창출, 정보보호 전문인력의 체계적 양성·관리 및 세계적 정보보호 기업 육성 지원 등의 법적 근거를 마련하고, 정보보호산업의 기반 구축과 경쟁력을 강화함으로써 국민생활의 향상과 국민경제의 건전한 발전에 기여하고자 하는 목적으로 「정보보호산업의 진흥에 관한 법률」이 5월 29일 국회를 통과하여 연말께에 시행될 예정이다.

6) 10대 정보보호 핵심기술은 5대 기반 분야(암호·인증·인식·감시·탐지), 5대 신성장 분야(스마트폰·IoT/M2M·클라우드·ITS·사회기반)이다.
7) 미래창조과학부, "정부, 「국가 사이버안보 종합대책」 수립 - 사이버안보 강화를 위한 4대 전략(PCRC) 마련 -", 2013. 7. 4.

국가안전보장의 견지에서 볼 때 더 이상 사이버공간은 국가의 규율이 가능하고 국가의 안전을 보장할 수 있는 안전한 공간은 아니다. 즉, 북한이 친북 활동을 위한 SNS 계정을 대폭 늘린 것으로 나타났는데, 해외에 서버를 둔 친북 사이트 162개와 SNS 계정 1622개에 이르고 있다. 즉, 군은 2010년부터 2014년 7월 말까지 해외에 서버를 둔 친북 사이트 162개와 SNS 계정 1,622개를 발견해 각각 125개 - 나머지 26개는 자진 폐쇄, 11개는 정밀 관찰 중 - 와 1,622개에 대해 국내 서버 접속을 차단한 바 있다. 특히 북한군 총참모부가 '지휘자동화국'을 만들어 우리 군에 대한 정보 수집을 목표로 한 해킹, 역정보 및 허위정보 유포 등 사이버전을 연구하고 있으며 정찰총국도 국가 공공망에 대한 사이버 공격을 연구하고 있는 것으로 분석했다. 이와 아울러 군당국은 국내 주요 기관의 홈페이지 게시판이나 인터넷 기사 댓글에 올라오는 친북 게시물은 연간 1만 2,000여 건에 이르는 것으로 파악하고 있으며 2012년부터 올해 8월까지 친북 게시물 3만 7,130건을 발견해 삭제한 바 있다.[8)]

정보통신기술의 발달로 인하여 더욱 다양한 방법과 경로를 통하여 국가안전보장을 위협하는 통신행위가 이루어지고 있고, 북한과의 대치가 계속되는 한 그 수는 계속 증가될 것이다. 이와 같은 환경에서 국가안전보장, 특히 사이버공간에서의 국가안보의 보장을 위한 합리적 법제추진 전략을 모색하여 합리적인 법적 방안의 마련이 필요하다.

이를 위하여 본 논문에서는 사이버안보를 둘러싼 미국, 유럽연합(EU), 일본 등의 국제동향과 최근 우리나라 국회에 발의되고 있는 사이버안보 관련 법제의 경향을 분석하고, 현행 사이버보안 법제도를 담당하는 추진체계와 법체계에 대해 개관한 뒤, 그 이슈를 살펴보고 개선 과제를 도출해 보고자 한다.

8) 아시아경제, 2014. 9. 11.

Ⅱ 주요국의 사이버안보 법체계

1. 미국

미국은 1990년대 냉전시대가 종식되고 국가 경제성장 및 발전을 위해 ICT기반의 다양한 공공사업을 추진하였다. 그러나 사회 전 영역으로 ICT가 확산되고 전세계에서의 초강대국의 위상에 따라 사이버 위협도 증가하였다.[9] 따라서 다양한 사이버위협에 대한 대응책에도 불구하고 다른 국가에 비해 사이버공격의 표적이 되는 경우가 빈번해 이른 시기부터 국가 사이버안보에 관심을 가지게 되었다. 클린턴・부시행정부(1993~2009년) 기간동안은 사회적 혼란 및 국가 안정성과 관련되는 주요 기반시설의 사이버보안 강화에 집중하며, 이를 주요 국정과제로 삼고 정책적인 노력을 기울였다. 사이버보안을 강화하기 위한 정책들은 법체계 정비에서 출발하게 되는데, 그 시작은 1980년대 중반의 컴퓨터관련 범죄와 사이버안보에 관한 법률들의 제정이다.[10] 이 시기에 국가 주요기반 시설 보호를 위해 중앙정부를 중심으로 전략개발이 이루어지기 시작하였으며, 1998년 5월 대통령령(Presidential Decision Directive, PDD) 63호 공표를 통해 주요기반 시설에 대한 범정부적 보호체계를 처음으로 마련하였다.[11]

2001년 출범한 부시정부는 9・11 테러를 기화로 주요기반시설 보호의 중요성이 더욱 커졌다. 부시행정부는 「국토안보법(Homeland Security Act)」

9) 미국은 사이버범죄로 연간 1,000억 달러(약 109조원) 규모의 피해액이 발생(2014.6, CSIS・McAfee 자료 참조).

10) 1980년부터 1990년대에 제정된 미국의 사이버안보 관련 법안은 아래와 같다. 「프라이버시 보호법」(Privacy Protection Act of 1980), 「위장접근수단・컴퓨터사기 및 컴퓨터남용법」(Counterfeit Access Device and Computer Fraud and Abuse Act)(1984), 「전자통신 프라이버시법」(Electronic Communications Privacy Act: ECPA)(1986), 「컴퓨터 보안법」(Computer Security Act)(1987), 「문서감축법」(Paperwork Reduction Act)(1995), 「정보기술관리 개혁법」(Information Technology Management Reform Act 또는 Clinger-Cohen Act)(1996) 등이다.

11) 김은혜・이재일, 미 오바마 정부의 사이버보안 주요 정책 및 법안, 인터넷 & 시큐리티 이슈, 2011.8.

을 제정(2002.11)하고 국가안보 강화를 위한 국토안보부(Department of Homeland and Security: DHS)를 설립, 기존에 다른 기관이 담당하던 국가안보, 정보보안, 특히 사이버안보 기능을 국토안보부에 많이 이전하였다.[12]

국토안보부는 오바마행정부가 들어선 2009년까지 미국의 사이버안보와 국토안보를 주도하였다. 오바마행정부가 수립된 이후에도 사이버안보는 핵심 국정과제였으며, 이에 따라 국가 사이버보안 강화를 위한 『사이버공간 정책 리뷰(Cyberspace Policy Review)』를 발표하게 된다(2009.5).[13]

사이버공간 정책 리뷰 발표 이후 기존 국토안보부 장관이 총괄하던 사이버보안 컨트롤 타워의 역할을 백악관 내 사이버보안조정관 직위를 신설하여 국가 사이버보안총괄 조정과 리더십 기능을 담당하도록 역할과 기능을 이전하였다. 국가안보위원회(National Security Council)내 사이버보안조정관[14]을 총책임자로 하는 사이버 보안국(Cybersecurity Directorate)을 설치하여, 사이버스페이스 정책 리뷰에 나와 있는 정책 방안을 더 자세히 설명하고 발전시킬 임무를 부여하였다. 이외에도 주요기반시설에 대한 사이버보안을 담당하고 있는 국토안보부와 사이버전에 대비를 위한 활동을 하고 있는 국무

12) 국토안보부(DHS)는 대통령 경호를 담당하는 재무부 산하의 비밀검찰부를 비롯해 해안경비대, 국경수비대, 이민귀화국(INS), 세관, 연방비상관리국(FEMA), 교통안전국(TSA) 등 22개 연방 기관이 합쳐져 탄생되었다. <http://www.dhs.gov/history> (2015.6.14. 최종방문).

13) ▶ 백악관, 연방정부 등 최상위 리더십에 따른 정책 추진(Leading from the top), ▶ 보안교육, 전문 인력 양성 등 디지털국가 구축을 위한 역량 제고(Building Capacity for a Digital Nation), ▶ 민·관 협력을 위한 파트너십 구축 등 공동 책임(Sharing Responsibility for Cybersecurity), ▶ 효율적인 정보 공유 및 사고 대응 능력제고(Creating Effective Information Sharing and Incident Response), ▶ 혁신 촉진(Encouraging Innovation) 등의 내용을 담고 있다. <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf> (2015.6.14. 최종방문).

14) 사이버보안조정관의 역할 : ① 대통령에게 직접 사이버보안 정책 직접 보고, ② 주, 지방정부 및 민간부문을 포함하는 미국의 모든 사이버보안 담당자들과의 긴밀한 협력이 가능하도록 규정, ③ 국방부, 국가안보국, 국토안보부 등과 협력하여, 대규모 침해사고 발생시 총지휘관 역할을 담당, ④ 국가안전보장회의에 상주하며 대통령과 안전보장회의에 사이버보안 관련 정책을 정기적으로 보고, ⑤ 미군과 민간기관의 연방정부 사이버안보정책마련을 위한 자문관 역할 수행.

부·상무부 등 관련 정부부처 내 담당 부서와 산하 기관을 통해 미국의 사이버보안 전략을 추진하는데 있어 필요한 업무를 지원받고 있다. 여러 부처에 걸쳐 있는 사이버보안 업무가 사이버보안조정관을 통해 대통령에게 리더십을 부여하고 있다는 것이 특징이다. 사이버공간 정책 리뷰의 발표는 기존 국토안보부에서 주도했던 국가 사이버안보 업무가 대통령을 중심으로 백악관에서 정책을 추진하는 체계로 재편된 것을 의미한다. 또한, 국가 기관의 사이버위협 대응 능력제고 뿐만 아니라 보안 교육과 인력 양성, 혁신 또한 중요시하기 시작했으며 여러 분야에서 민간 부문의 책임과 의무를 강조했다는데 의의가 있다고 볼 수 있다.

오바마가 대통령에 재선된 2013년 이후에도 주요 기반시설에 대한 사이버보안 정책이 강화되는 정책이 나왔다. 『주요 기반시설 사이버보안 강화를 위한 행정명령 제13636호』(Executive Order 13636 : Improving Critical Infrastructure Cybersecurity) 및 『주요 기반시설 보안 및 복원력 강화를 위한 정책지침 제21호』(Presidential Policy Directive-21 : Critical Infrastructure Security and Resilience) 등이 마련되었다(2013.2). 2014년 2월에는 국립표준기술연구소(NIST)에서 『국가 주요 기반시설의 사이버보안 위협감소를 위한 사이버보안 프레임워크(Cybersecurity Framework)』가 개발되어 국가 주요 기반시설 운영 주체가 사이버위협 상황에 대한 인식 및 적절한 대응을 수행할 수 있도록 하는 일종의 관리 지침을 제공하였다.

현재 국토안보부를 비롯한 각 부처들은 행정명령 제13636호와 정책지침 제21호의 이행사항을 추진 중에 있으며, 인센티브 제안, 사이버보안 프레임워크 최종안 확정, 시민자유 보호 관련 보고서 발간 등 2015년까지 제시된 이행사항은 모두 완료되었고, 오바마 대통령의 임기가 끝나는 2016년까지 이행상황 점검 의무가 각 부처에 부과되어 있는 상황이다.

2015년 들어서 오바마 행정부는 국가안보를 위한 여러 가지 정책을 발표하고 있다.

우선 2015년 2월 6일에는 전반적인 국가 안보 계획을 담은 『2015 국가

안보전략(The 2015 National Security Strategy)』을 발표하였다. 국가 차원의 안보 전략을 4대 분야(안보, 번영, 가치, 국제질서 등)로 구분하여 제시하였으며, 공유된 공간(shared space)으로의 접근성 보장을 위해 사이버 보안을 언급하였다.

이에 앞서 1월13일에는 국가 차원의 효과적인 사이버위협 대응을 위해 사이버보안 관련 입법을 再제안하였다. 이는 2011년 5월에 사이버공격으로부터 미국 시민과 주요 기반시설을 보호하기 위해 '사이버보안 입법 제안서(Cybersecurity legislative proposal)'를 의회에 제출하였다가 최종 입법화 가 실패(부결)되자 『주요 기반시설 사이버보안 강화를 위한 행정명령 제13636호(2013.2월)』로 그간 처리하였던 것을 재입법화하기 위한 것이었다.

2015년 2월 13일에는 『민·관간 효과적이고 신속한 사이버위협 대응을 위해 민·관 사이버보안 정보공유 촉진 행정명령(Promoting Private Sector Cybersecurity Information Sharing EXECUTIVE ORDER 13691)』을 발표하였다. 가장 중요한 내용은 기존 정보공유분석센터(ISACs, Information Sharing and Analysis Centers)[15]의 민·민 중심의 정보공유 활동을 민·관 분야까지 강화한 형태로 정보공유 협력의 중심 역할을 담당하게 하는 내용을 담고 있다. 이를 위해 주(州)간 정보 공유 등 기존 정보공유체계 확대를 하고자 하고 있으며, 국토안보부(DHS)는 비영리 조직들의 ISAOs 참여 유도를 위해 자발적 기준 마련에 필요한 자금을 지원하도록 하고 있다. 이 행정명령은 새로운 프레임워크에 기반한 정보공유에 있어 프라이버시와 시민자유의 강력한 보장을 포함하여 프라이버시 보호에 정부가 노력하고 있음을 보여주고자 하고 있다.

미국의 사이버안보 관련 법률은 2002년 「국토안보법」 제정 이후 주요한 제·개정이 없다고 평가되고 있으나, 지속적으로 사이버보안 관련 법안이 발

15) ISACs : 금융, 전기, 수도 등 산업 분야별 최신 멀웨어(Malware)와 사이버범죄 활동에 대한 정보를 공유하는 조직으로 각 산업별 회원사들에게 사이버위협 정보를 제공.

의되고 있다. 최근, 오바마 대통령의 효과적인 사이버위협 대응을 위한 사이버보안 입법제안(15.1.13.)이후 국토 안보 및 기반보호와 개인정보 보호를 위한 입법이 두드러지고 있다.[16]

2. 유럽연합

유럽연합(EU)은 단일 국가가 아닌 연합이기 때문에 사이버안보 추진 체계도 국가에서 볼 수 있는 구조와는 다소 상이한 구조이다. 사이버안보는 EU 집행위원회(European Commission)내의 네트워크콘텐츠기술총국(Communication Networks, Content and Technology)10)에서 총괄하고 있으며, EU 산하기관인 유럽네트워크정보보호원(ENISA)에서 지원을 받고 있다.[17]

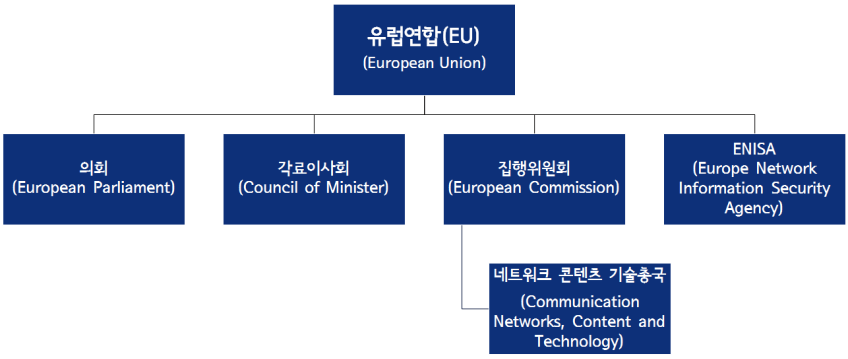
유럽연합의 사이버위기 상황에 대한 대응은 2004년 「사이버범죄방지조약(Cybercrime convention)이 체결되면서 본격화 되었다.[18] 그 후 국제적인 협조를 바탕으로 사이버범죄에 대한 대처가 이루어져야 한다는 인식 하에 정보시스템 공격에 대한 기본결정, 통신테이터 보관에 대한 지침 등을 제정하였다.

16) 2001년 10월의 애국법(USA PATRIOT ACT), 국토안보법(Homeland Security Act of 2002), 사이버보안 강화법(Cybersecurity Enhancement ACt of 2014) 외에는 많은 입법시도에도 불구하고 입법화되지 못하는 상황이다.

17) 유럽네트워크정보보호원은 EU회원국 네트워크 및 정보보안을 지원하며, 국가 간 정보교류 증대와 네트워크 보안 기능 조정 등의 역할을 수행하는 기관으로 EU규정에 따라 2004년에 설립됨. 또한 ENISA는 사이버범죄에 효과적으로 대응하기 위하여 유럽 각국의 컴퓨터비상대응팀(CERT, Computer Emergency Respose Team)구축을 지원하며 이를 네트워크로 묶는 초국가적 시스템 마련을 추진.

18) 사이버범죄방지조약(Cybercrime convention 2001)에 대해 자세한 사항은 이정현, “국제 사이버 범죄조약의 영향”, 제23회 정보보호와 암호에 관한 학술대회 논문집, WISC2012, 2012. 9, 109~118면 참조.

[유럽연합의 사이버안보 추진 체계]



EU는 사이버보안 및 개인정보 침해 사고 발생에 따른 관련 규정 법제에 기반한 보고 체계를 마련하는 등 공공과 민간부문의 사이버 대응 능력 개발 및 협력 지원하고 있다.[19] 특히, 네트워크 및 정보보호와 관련한 최소한의 공통요건 규정을 통한 네트워크 및 정보보호 전담 국가 지정 및 컴퓨터긴급대응팀 설치, 국가 네트워크 및 정보보호 전략 및 협력 계획 채택 장려하는 등의 내용을 담고 있는 네트워크 및 정보보호지침을 마련하는 등 EU 전반에 걸쳐, 국경을 넘어서는 사고 발생 시 국가 간 조율, 민간의 참여 대비 측면에서의 법률을 마련하는 노력을 기울이고 있다. 또한, 민・관협력을 통해 유럽 내 사이버위기 대응을 위한 기존의 표준절차와 협력 메커니즘을 점검하기 위해 격년으로 범유럽 차원의 사이버사고 대응 훈련을 지원하고 있다.[20] 이외에도 유럽집행위원회 차원에서 주요기반시설 운영자들과 함께 네트워크 및 정보보호취약점 파악과 복구 시스템 개발 노력을 기울이고 있는 중이다.

19) EU는 Regulatory Framework Directive for electronic communications (Directive 2002/21/EC) 및 EU data protection 입법 통해 전자통신서비스제공사업자 및 데이터 관리자들에게 보호 조치 및 침해사고 발생 시 보고조치 등을 하도록 명시하고 있다.

20) 2014년 4월 EU는 EU 차원의 사이버위협 대응 효율성 제고를 위한 사이버유럽 2014(Cyber Europe 2014) 훈련을 실시.

3. 일본

일본에는 그간 정보보호 전체를 포괄적으로 보호하기 위한 법령은 존재하지 않았다. 인터넷이 발전함에 따라 일본에서도 차츰 정보보호 문제에 대한 대응의 필요성이 증대됨에 따라 관련 법령이 다수 제정되었다. 기반 및 통신 보호와 관련된 주요 법률로는 「부정 접속 행위의 금지 등에 관한 법률」.[21], 「고도 정보통신 네트워크 사회형성 기본법」[22], 「프로바이더 책임 제한법」[23] 등이 있다.

일본은 정부의 사이버보안전략의 기반조성이라는 목표아래 「사이버시큐리티기본법」의 제정을 추진하였다. 입법에 관한 구체적인 동향과 관련해서는 자민당IT의 전략특명위원장인 히라이타구야(平井たくや)가 2014년 2월 개최된 강연에서 의원입법으로 「사이버 시큐리티에 관한 기본법」을 제정하려고 시도하고 있다는 것을 공개적으로 밝힌 후, 「사이버시큐리티기본법」을 2015년부터 본격적으로 시행하고 기능시키기 위해 2014년 6월 11일 의원입법으로 관련 법안을 국회에 제출하여, 같은 해 11월 6일 동 법안이 통과되었으며 11월 12일 공포되었다. 이 법은 정보보호 관련 일본의 IT기본법이라 할 수 있는 현행 「고도정보통신네트워크사회 형성 기본법」에 대하여 특별법적 지위에 있다.

21) 「不正アクセス行為の禁止等に関する法律」은 1999년 8월 13일에 제정(법률 제128호)되어 2002년 2월에 시행되었다. 일본 총무성 홈페이지 참고 <출처: http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/09.html> (2015.6.16. 최종방문).

22) 「高度情報通信ネットワーク社会形成基本法」; 일명 IT 기본법이라고 불린다. <출처 : http://law.e-gov.go.jp/htmldata/H12/H12HO144.html> (2015.6.16. 최종방문).

23) 「プロバイダ責任制限法」<http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/pdf/jyoubun.pdf> (2015.6.16. 최종방문).

《일본「사이버시큐리티기본법」구성체계 》

제1장	총 칙	▶ 사이버보안 기본법의 목적, 정의, 기본이념 등 제시 – 국가, 지방공공단체, 중요 사회기반사업자, 교육연구기관 등의 책무 규정(§4~§11)
제2장	사이버 보안전략	▶ 사이버보안 전략 추진을 위한 기본계획 수립 제시 – 종합적인 보안시책 수립・공표, 재정범위 내 실시 등(§12)
제3장	기본시책	▶ 사이버보안 기본시책의 주요 규정사항, 수립 방향 등 (§13–§23)
제4장	사이버보안 전략본부	▶ 사이버보안 전략본부의 구성 및 운영(§24–§29) ▶ 관련 자료 및 정보제공 요청권, 협력 요청권 등(§30–§35)

「사이버시큐리티기본법」의 주안점은 관련 시책을 종합적이고 효율적으로 실시하기 위한 컨트롤타워가 되는『사이버 시큐리티 전략본부(본부장은 내각관방장관)』를 법적 근거를 기반으로 하는 조직으로 설치하는 것이다. 즉, 종전 정보보안정책회의(의장은 내각관방장관)을 격상시켜 고도정보통신네트워크사회추진전략본부(IT종합전략본부) 및 국가안전보장회의(NSC)와 긴밀하게 연계하는 체제로 만든다는 것이다.[24)]

또한「사이버시큐리티기본법」은 이러한 정보보안체제뿐만 아니라, 산업진흥 및 국제경쟁력확보를 위한 규정도 포함하고 있다.

Ⅲ 국내 사이버안보 법제 개관

1. 국내의 사이버보안 추진체계

국내 행정기관 중에서 사이버보안과 관련이 있는 기관은 미래창조과학부를 비롯하여 국가정보원, 행정자치부, 국방부, 법무부(검찰청), 경찰청 등이 있다. 국방 분야에서는 국군기무사령부의 국방정보전대응센터가 있다. 이 중

24) <http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=1> (2015.6.16. 최종방문).

에서도 국가정보원과 미래창조과학부, 행정자치부가 주요 역할을 수행한다.

먼저 국가정보원의 경우는 일단 「국가정보원법」에 따라 정보 및 보안업무의 기획·조정을 업무 영역의 큰 틀로 삼고 「국가사이버안전관리규정」, 「정보통신기반 보호법」, 「국가정보화기본법」, 「전자정부법」에 따라 개별적인 업무를 수행하고 있다. 대통령훈령인 「국가사이버안전관리규정」에 따라 국정원은 국가사이버안전센터[25]를 설치하여 국가전산망에 대한 사이버위협 또는 침해에 대응·복구 업무를 담당하며, '국가사이버안전전략회의'[26]와 전략회의의 효율적 운영 및 지원을 위한 '국가사이버안전대책회의'를 설치하여 범국가적인 체계를 수립하고 기관 간 역할 조정 및 국가사이버안전에 관한 중요 정책사항을 심의하도록 하고 있다. 「정보통신기반 보호법」에서는 주요정보통신기반시설 보호대책 이행점검, 주요정보통신기반시설 지정권고, 국가안전보장에 중대한 영향을 미치는 도로·철도·전력·가스·방송 등의 주요정보통신기반시설에 대한 기술적 지원 등을 하도록 하며, 「전자정부법」에서는 전자적 대민서비스 보안대책 마련, 전자문서의 보관·유통 관련 보안조치 이행 점검 등의 업무를 수행하도록 정하고 있다.

미래창조과학부는 「정부조직법」에 따라 과학기술정책의 수립·총괄·조정·평가, 과학기술의 연구개발·협력·진흥, 과학기술인력 양성, 원자력 연

25) 국가사이버안전관리센터(National Cybersecurity Center)는 국정원 훈령 「국가사이버안전관리규정」에 의거, 사이버공격에 대한 국가차원의 체계적인 대응 업무를 총괄하는 기구를 말한다. 국가사이버안전센터(NCSC)는 사이버 위협정보의 수집 분석, 전파를 위한 '국가종합상황실'을 운영, 각급기관 네트워크에 대한 보안관제를 실시하고 경보발령 및 침해사고 발생 시 긴급대응·조사와 함께 복구기술을 지원하며 각급 기관에 침해 대응 실무지침인 '국가사이버안전매뉴얼'을 작성·배포한다(국가사이버안전관리규정 제8조).

26) 국가사이버안전전략회의는 사이버 안전체계를 위한 최고의 정책기구로서, 국가사이버안전과 관련된 사항을 심의하게 된다. 국가정보원장을 의장으로 하며 각 행정부의 차관급 공무원이 위원이 되어, 국가 사이버 안전체계의 수립 및 개선사항, 국가사이버안전정책 및 기관 간 역할에 관한 사항 대통령 지시사항에 대한 조치방안 그 밖에 의장이 부의하는 사항을 심의하게 된다. 그리고 사이버안전전략회의 산하에 국가사이버안전대책회의를 두어 대책방안이나 시행방안 등을 세부적으로 다루게 된다(국가사이버안전관리규정 제6조).

구・개발・생산・이용, 국가정보화 및 기획・정보보호・방송・통신의 융합・진흥 및 전파관리, 정보통신산업, 우편・우편환 및 우편대체에 관한 업무 영역을 담당하고 있다. 「정보통신망법」에 의하여 한국인터넷진흥원(KISA) 등 산하 전문기관과 함께 정보보호 관리체계 인증, 사이버 침해사고 대응 등의 업무를 담당하고 있다. 또한 「정보통신기반 보호법」에 따라 주요정보통신기반시설 보호대책 이행점검, 주요 정보통신기반시설 지정권고 등의 업무를 수행한다. 또한 「전자서명법」, 「국가정보화 기본법」에 따라 공인인증기관 지정・관리, 공인전자서명의 인증, 정보화시스템 보급・확산 등의 업무를 수행하고, 소위 ICT진흥특별법이라는 명칭으로 더 알려진 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」이 2013년 8월13일 제정되어 2014년 2월 14일부터 시행되고 있다. 또한 「정보통신산업진흥법」 등을 통해 정보보호와 관련한 산업과 보안인력 등을 육성한다.[27]

또한 행정자치부는 「개인정보보호법」에서 규율하는 개인정보 보호에 관련된 부분을 담당하고 「전자정부법」 등에 따라 국정원장과 협의하여 전자적 대민서비스와 관련한 보안대책 수립, 전자정부통합망의 관리・감독, 사이버위협 감시・전파, 전자정부통합관제센터 등의 운영업무를 수행한다. 또한, 「재난 및 안전관리 기본법」에 따라 국가기반체계의 마비와 관련한 안전관리체계의 확립, 예방 및 대응・복구 등에 관한 업무를 수행한다.

국방부는 「정보통신기반 보호법」에 따라 국방분야의 주요정보통신기반시설의 안전성 확인 및 국방분야 사이버안전정책 수립・집행 및 국방사이버위기관리기능을 수행한다. 또한 국방부 산하의 국군기무사령부에는 '국방정보

27) 또한 최근에는 「정보보호산업 진흥에 관한 법률」이 2015년 5월29일부로 국회를 통과하여 공포후 6개월 후에 시행예정에 있다. 이에 따라 종전에 「정보통신산업진흥법」 규정되었던 지식정보보안컨설팅전문업체 관련 규정 등 정보보호에 관한 사항들이 동법에 규정되는 등 국내 정보보호 시장의 확대, 정보보호 전문가 양성, 세계 최고 수준의 정보보호 제품개발을 위하여 수요확충과 신시장 창출, 정보보호 전문인력의 체계적 양성・관리 및 세계적 정보보호 기업 육성 지원 등의 법적 근거가 마련되게 되었다.

전대응센터'를 구축하여 사이버안전업무를 전담시키고 있다.[28]

그 외에도 경찰청에서는 사이버안전국을 두어 DDos공격, 사이버테러, 개인정보유출, 악성코드 배포와 같은 사이버범죄에 더욱 효율적이고 전문적인 수사 및 예방을 위한 노력을 하고 있다.[29] 검찰청 인터넷범죄수사센터는 첨단 인터넷범죄에 효율적으로 대응하기 위하여 감시 활동을 펼치고 있다.

2. 국내 사이버안보 법체계

(1) 현행 법제

최근 사이버 공격은 공공·민간 영역 구분 없이 발생하여 침해사고 유형 및 피해범위가 지속 확대[30]되고 있으며, 국민의 재산과 기본권뿐만 아니라 국가안보 전체에도 영향을 미치고 있다.

그러나, 현행 사이버안보 법제는 사이버 안보 전반을 규율하는 일반법 없이 공공·민간 분야별 개별법(Sectoral law)에 의한 규율체계를 유지하고 있다.

즉 공공부문에서는 「국가사이버안전규정」, 「전자정부법」 등이 있고, 민간부문은 「정보통신망법」과 「전자금융거래법」등이 있다. 또한 공공부문과 민간부문을 모두 규율하는 법률로 주요정보통신기반시설을 안전하게 보호하도록 하는 체계를 규정하고 있는 「기반보호법」과 「국가정보화 기본법」이 있으나, 이 법률들은 특정시설과 이용 등에 대해서만 규율하고 있다. 좀 더 세분화하는 다른 분류를 한다면 우리나라의 사이버안보추진체계는 「군사기밀보호법」과 「보안업무규정」에 의한 전통적인 '국가기밀보호체계'와 '정보보안체

28) 보다 더 자세한 사항은 우리 학회에서 개최한 2013년 정기학술세미나 자료집을 참고하기 바란다. 이창범, "국내외 사이버안보 관련 법제정 동향과 시사점", 사이버테러와 법정책적 대응, 한국사이버안보법정책학회, 27~33면 참조.

29) 2000년에 경찰청 사이버테러대응센터가 설립되었으나 새로운 사이버범죄에 대한 대응을 위하여 2014년 6월 11일 사이버안전국이 출범되어 업무가 확대·개편되었다.

30) 7.7 DDoS 공격('09년) 544억원 → 3·20 대란('13년) 8,800억원으로 침해사고 피해규모 급증.

계', 그리고 「국가사이버안전관리규정」에 의한 '사이버안전체계', 「정보통신기반 보호법」에 의한 '기반시설보호체계', 「전자정부법」에 의한 '전자정부보호체계', 마지막으로 「개인정보 보호법」, 「정보통신망법(개인정보 부분)」, 「위치정보의 보호에 관한 법률」, 「신용정보보호법」, 「통신비밀보호법」 등에 의한 '개인정보보호체계' 등 6개 체계로 분류할 수 있다.

(2) 입법동향

19대 국회[31]에 발의된 사이버보안 관련 입법은 총 10종이나 그중 4종은 정보통신기반보호 자체에 대한 개선안이고, 1종은 「악성프로그램확산 방지등에 관한 법률」 제정안이며 사이버보안 거버넌스와 관련된 법안이 4종이다.[32]

서상기의원과 하태경의원이 각각 발의한 「국가 사이버테러 방지에 관한 법률안」과 「국가 사이버안전 관리에 관한 법률안」은 국정원 중심으로, 정청래 의원과 변재일 의원이 각각 발의한 「정보통신기반 보호법」 개정안은 미래부 중심의 거버넌스를 주장하고 있는 바, 이 문제에 대해서는 이미 과거 여러 번 논의 되었으므로 여기서는 생략한다.[33]

분야	의안명	제안일자	주요내용
정보통신기반 자체 개선	기반보호법 (조명철의원)	2013.2.6	1년에 최소 2회 이상 주요정보통신기반시설보호 대책의 이행 여부를 확인하도록 하고, 이를 관계중앙행정기관의 장에게 통보하도록 의무를 부과하여 기반시설의 정보보호 조치를 강화

31) 회기는 2012년부터 2016년.
32) 「악성프로그램확산 방지 등에 관한 법률」(안)은 침해사고 예방 및 대응과 이용자 컴퓨터 보호를 목적으로 추진되고 있는 바 자세한 내용은 이창범, 앞의 글, 33~36면을 참고하기 바란다.
33) 이에 대해 자세한 사항은 이정현, "국가 사이버안보(Cyber security) 추진체계의 이슈와 과제," 사이버안보법정책논집, 2014. 창간호, 75~84면 참조.

분야	의안명	제안일자	주요내용
정보통신기반자체개선	기반보호법(권은희의원)	2013.5.30.(2014.12.29. 국회통과, 2015.1.20. 공포)	침해사고에 대한 데이터의 안전한 관리 및 복구를 위하여 관리대책에 관리 정보의 백업 시스템 구축 및 복구를 포함(제5조제1항, 제6조제3항2호), 개정안은 주요정보통신기반시설보호대책에 신속한 대응을 위한 백업・복구 뿐 아니라 침해사고 방지를 위한 예방 활동을 포함하는 것으로 수정의결됨
	기반보호법(김태원의원)	2014.1.28.	용역업체 직원 신원조사, 직무상 비밀 유출 시 처벌 등의 규정 신설, 정보통신기반시설 관리기관의 준수사항 마련, 취약점 이력관리 의무화 등 기반시설의 정보보호 조치 강화
	기반보호법(김한표의원)	2015.5.26.	취약점 분석・평가 기준에 실시간 보안감시 인력, 네트워크 모니터링 등을 위한 보안장비, 관리기관 소속 공무원 및 임직원에 대한 사이버보안 교육 및 침해사고 관리방안이 반드시 포함되도록 함
악성프로그램방지	악성프로그램 확산 방지 등에 관한 법률(한선교의원)	2012.6.14	컴퓨터보안프로그램 이용・보급 활성화, 웹사이트에 은닉된 악성프로그램 삭제, 악성프로그램 감염컴퓨터의 치료 지원, 심각한 침해사고 발생시 실효성 있는 대응체계 확립 등 이용자 컴퓨터의 보안 강화
사이버보안거버넌스	국가 사이버 안전관리에 관한 법률(하태경의원)	2013.3.26.	국정원 중심 국가차원에서 사이버안전에 관한 기본계획 수립・시행, 국무총리 소속으로 국가사이버안전전략회의, 사이버위기 대응훈련・사이버위기경보 발령・사이버공격으로 인한 사고의 통보 및 조사 등
	국가사이버테러 방지에 관한 법률(서상기의원)	2013.4.9.	국정원 중심으로 정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축, 사이버테러 사전 탐지하여 사이버위기 발생 조기에 차단, 사이버안전센터 운영
	기반보호법(정청래의원)	2013.7.4.	미래부가 사이버 안보 컨트롤타워 역할을 맡는 내용을 핵심으로 하여 기존 서상기의원안이나 하태경의원안에서 지적받는 국정원의 과도한 역할에 대해 주요 정보통신기반시설 관련 침해사고 대응체계를 미래부로 일원화

분야	의안명	제안일자	주요내용
사이버 보안 거버넌스	기반보호법 (변재일의원)	2014.1.9.	미래부와 국정원으로 이원화되어 있는 대응체계를 미래부로 일원화하고 주요정보통신기반시설의 보호 체계를 강화하는 등 대규모 침해사고 발생 시 보다 신속하고 적극적인 대응 시스템을 구축하도록 함
	사이버위협정보 공유에 관한 법률 (이철우의원)	2015.5.19.	국가 주요 정보통신망의 사이버위협에 대한 공공·민간의 정보 공유체계 활성화를 위한 범정부 차원의 정보 공유체계를 규정(총괄기관: 국정원)

입법 동향에서 특이할 점은 2015년 5월에 이철우 의원(새누리당, 국회 정보위)이 사이버위협정보 공유 체계 강화를 골자로 한 「사이버위협정보 공유에 관한 법률안」을 발의(2015.5.19)하였다. 이에 대해서는 사이버안보 추진전략 부분에서 후술한다.

Ⅳ 사이버안보 법제 추진전략

1. 추진체계 이슈

우리나라는 남북이 분단된 상황에서 남북한이 각기 다른 정치·경제 환경에서 상호 대립하고 있다. 이러한 환경속에서 그간 우리나라는 물리적 안보태세에만 집중하고 있었으나 국가차원의 사이버안보체계를 본격적으로 논의하게 된 것은 2003년 1.25 인터넷 대란이 원인이었다고 본다. 이후 2004년 중국 해커에 의한 우리나라 국가기관 기밀유출 사건을 비롯하여 7.7 DDoS 사건과 3.4 DDoS사건, 이어 2011년 농협 해킹사건, 2013년 3.20과 6.25 침해사고, 최근 2014년 12월 23일에는 한국수력원자력(한수원)에 대한 해킹사고가 발생하였다. 그 행위가 북한 소행이라고 추정 또는 확신됨에도 불구하고 사이버안보의 추진 체계를 명확히 확립하여 선제적 대응을 못하는 상

황으로 보인다. 이러한 사고가 있을 때마다 컨트롤타워의 부재, 위협정보 공유, 그리고 보안관제(모니터링) 및 조기경보를 통한 피해확산 조기 차단, 관련법 체계의 정비문제 등이 이슈화 되었다. 이러한 컨트롤타워 문제, 정책 집행체계 문제, 보안관제에 대한 문제가 우리가 직면한 사이버안보 추진체계의 이슈라고 본다.[34]

2. 외국의 사이버안보 입법 트렌드 분석

우리나라의 사이버안보 법제를 추진 전략을 수립함에 있어 밴치마킹할만한 사항을 찾는 것도 중요한 방안중 하나라고 판단된다.

(1) 미국

앞서 주요국의 사이버 안보에 대한 입법례를 살펴보면서 파악되었겠지만, 미국의 사이버안보 정책은 대통령을 중심으로 수립되며, 대통령 직속기관 등 관련 정부부처(국토안보부, 상무부 등)와의 협력을 통해 추진된다. 911테러 이전에는 국사사이버안보처(NCSD)가 사이버컨트롤타워 역할을 하였는데 국토안보부(DHS) 수립후에는 국토안보부의 국가사이버안보센터(NCSC)로 그 뒤 오바마정부에서는 대통령 직속 국가안보위원회를 중심으로 사이버안보정책이 수립되며 산하 사이버안보국(Cybersecurity Directorate)에서 사이버안보 관련 업무를 총괄하며, 사이버안보조정관(Cybersecurity Coordinator)이 총괄책임을 맡고 있다. 그리고 국가정보국(ODNI: Office of the Director National Intelligence)과 국토안보부를 중심으로 사이버위협 정보 공유 및 국가 주요기반시설의 사이버안보를 담당한다.

미국의 사이버안보 관련 입법 시도의 트렌드는 한마디로 사이버(안보)보안 정보의 공유다. 민・관간 원활한 사이버안보 정보공유 협력 촉진 이 필요하다는 인식하에 민간과 국토안보부(DHS) 국가사이버보안정보통합센터

34) 이에 대해 자세한 사항은 이정현, "국가 사이버안보(Cyber security) 추진체계의 이슈와 과제," 사이버안보법정책논집, 2014. 창간호, 89~92면 참조.

(NCCIC)간 사이버위협 정보 공유를 시도하고 있다. 민간기업을 대상으로 불필요한 개인정보 삭제 등 자국민의 개인정보보호를 위한 관련 규제 준수를 권고하고 민・관간 정보공유로 인한 정부의 빅브라더化에 대한 거부감을 상쇄시키기 위해 국토안보부, 법무장관(Attorney General) 등에게 프라이버시 및 시민 자유 감독위원회(Privacy and Civil Liberties Oversight Board)[35]와 함께 개인정보 수집・보유・이용・공개 가이드라인 마련 할 것을 요구하며, 관련법 개정을 통한 사이버범죄 퇴치를 위한 법집행권한의 현대화와 데이터 유출 금지 위반과 관련한 주법들을 연방법 차원으로 일원화하는 시도 등이 이루어지고 있다. 특히 「사이버 정보공유 및 보호법안(Cyber intelligence Sharing and Protection Act; CISPA)」의 입법 추진은 눈물겹다. 2011년부터 총 3회의 입법 시도가 있었으며 2015년 6월 현재 계류중에 있다.[36] 하지만, 최근 사이버보안과 관련된 법률은 지속적으로 발의되고 있지만 통과된 예가 없다. 이는 국가에서 사이버보안을 위한 정보의 이용의 필요성과 국민의 프라이버시 보호에 대한 중요성에 대한 대립이 합의를 이끌어내지 못하고 있기 때문으로 보인다. 소니 해킹사건을 이후로 오바마 대통령 역시 민간과 정부 간의 정보 공유의 내용을 담는 법을 지지하고 있어 미국 사이버 보안과 관련된 법제의 방향에 향후 이 법의 귀추가 주목되고 있다.

35) 프라이버시 및 시민 자유 감독위원회(Privacy and Civil Liberties Oversight Board) : 테러리즘과 관련한 법, 제도 실행에 있어 프라이버시와 시민 자유 침해 여부를 감독하고 대통령과 고위 행정관료에 조언 제공(5명의 위원으로 구성, '04년 설립).

36) 1. 마이크 로저스(Mike Rogers) 의원 하원 발의(H.R. 3523) : 11.30.2011.
- 4. 26, 2012 : 하원 통과되었으나 동일회기에서 상원을 통과하지 않아 입법만료 폐기 (112차 의회)

2. 마이크 로저스(Mike Rogers)의원 재발의(H.R. 624) : 2. 12, 2013.
- 4. 18, 2013 : 하원 통과
- 4. 22, 2013 : 상원에 접수되었으나 폐기 (113차 의회)

3. 더치 루퍼스버거(Dutch Ruppersberger)의원 하원 발의(H.R. 234) :1. 8, 2015. (114차 의회)
- 2. 2, 2015. : 2개의 위원회에 회부됨(Committee consideration by House Select Committee on Intelligence, Senate Select Committee on Intelligence).

답답한 오바마 대통령은 민・관간 효과적이고 신속한 사이버위협 대응을 위해 「민・관 사이버보안 정보공유 촉진 행정명령」을 발표('15.2.13.)하여 현재의 공백을 매우 우려하고 있다.

(2) EU

유럽연합 역시 앞서 입법동향에서 살펴본 바와 같이 EU전반에 걸쳐, 국경을 넘어서는 사고 발생 시 국가 간 조율, 민간의 참여 대비 측면에서의 법률을 마련하는 노력을 기울이고 있다. 또한, 민・관협력을 통해 유럽 내 사이버위기 대응을 위한 기존의 표준절차와 협력 메커니즘을 점검하기 위해 격년으로 범유럽 차원의 사이버사고 대응 훈련을 지원하고 있는 상황이다. 「EU 입법지침(안)(Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013 - EN)」은 EU 사이버 보안 전략(EU Cyber Security Strategy)의 핵심 내용들로 구성된 지침으로서, 모든 회원국, 주요 인터넷 제공자, 기간통신망운영자, 에너지, 교통, 금융, 의료(건강) 서비스통신망운영자 모두에게 EU 내에서 안전하고 신뢰할 수 있는 디지털환경을 보장하도록 요구한다. 2013년 2월 7일 EU 집행위원회가 제안하고 2014년 3월 13일 수정안이 EU 의회에서 압도적인 다수의 찬성으로 통과되었으며, 2015년 9월 채택과 18개월내 국내법 전환을 목표로 한다.

(3) 독일

독일 연방정부는 연방내무부가 제출한 「정보기술시스템의 보안성을 강화하기 위한 법률(안)(가칭 'IT 보안법')」[37]을 정부안으로 확정하여 의회에 제출하였다(2014. 12. 17.). 이 법률안은 새 법률을 제정하지 않고 「연방정보기술보안청(BSI) 설립법」(BSIG)[38], 「연방범죄수사청법」[39], 「텔레미디어

37) Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme(IT-Sicherheitsgesetz).

법」(TMG)[40], 「전기통신법」(TKG)[41] 중에서 정보기술보안과 관련한 일부 규정들을 신설하거나 개정하고 있다. 2014년 8월 18일 제출되어 각계의 의견[42]을 수렴한 후 내용을 보완하여 11월에 다시 제출된 것이다. 동 법안은 2015년 6월 12일 연방하원을 통과하여 상원 심의를 앞두고 있는데 통과가 유력시 되고 있다.

독일 정부는 이 법률을 통해 데이터 처리 시스템의 가용성, 무결성 및 기밀성의 보호를 강화하여, 증가하고 있는 위협상황에 대처하고자 한다. 즉, 기업에서의 IT 보안의 개선, 안전한 정보통신망을 통한 시민 보호 강화, 연방 정부의 IT 보안의 구축 및 이와 관련한 연방정보기술보안청(BSI: Bundesamt für Sicherheit in der Informationstechnik)과 연방범죄수사청(BKA)의 역할을 강화하고자 한다. 이로인하여 지금까지 데이터의 탐지, 취득 또는 변경에 대해서 주(州) 사법경찰이 관할하고 있었기 때문에 보안 흠결과 개발 연구와 공개가 위협을 받을 수 있었으나 연방범죄수사청(BKA)이 인터넷 범죄 영역에서 더 많은 권한을 가지게 되었다. BSI 외에 연방범죄수사청, 재난구조청, 헌법보호청 등도 연방의 IT 시스템과 주요기반시설의 공격에 더 많은 권한을 가지게 되었다.[43] 또한 외국에서 멜 웨어를 추적하는 권한 부여로 연방대외정보기관(BND)도 IT보안에 대해서 더 많은 기여를 하게 되었다.[44]

38) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
39) Bundeskriminalamtgesetz
40) Telemendiengesetz
41) Telekommunikationsgesetz
42) 이 법률안에 대한 쉴레스비히 홀스타인 주 데이터보호감독청(ULD)의 입장 : <https://www.datenschutzzentrum.de/uploads/it/20141021-it-sicherheitsgesetz.pdf> BITKOM의 입장 : <http://www.bitkom.org/files/documents/Stellungnahmelang_BITKOM_ITSIGv3.pdf> 통신정보보관 반대 시민단체의 입장: <http://www.vorratsdatenspeicherung.de/content/view/748/1/lang,de/> (2015.6. 17. 최종방문).
43) <https://netzpolitik.org/2014/it-sicherheitsgesetz-im-kabinett-beschlossen-die-kritischen-punkte-zusammengefasst/>
44) <http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Kritik-an-Aufruestung-Warnung-vor-nationalem-Alleingang-2499554.html>

(4) 일본

일본은 앞서 입법동향에서 파악한 바와 같이 「사이버시큐리티기본법」을 제정하였다. 일본의 기본법 제정에 따라 우리나라도 사이버보안에 대한 기본법 제정 의견도 제시될 수 있겠으나, 일본 「사이버시큐리티기본법」은 구체적인 규정이 없다는 문제점이 있다. 만일 우리나라가 일본과 같은 기본법을 만들고자 한다면 일본과 같은 형식의 입법은 지양해야 할 것이다. 이해를 돕기 위해 일본의 「사이버시큐리티기본법」과 국내법제와의 비교하여 보았다.

[일본 사이버시큐리티기본법과 국내법과의 비교]

<table>
<tr><th></th><th>일본</th><th>국내</th></tr>
<tr><th></th><th>「사이버시큐리티기본법」</th><th>정보보호 관련 법령</th></tr>
<tr><td>정보보호 컨트롤타워</td><td>○ 사이버보안 전략본부(내각총리 소속)
– 사이버보안전략(안) 수립・이행
– 국가 행정기관 및 독립법인에서의 대책기준의 수립, 기준을 근거로 이행 평가 등</td><td rowspan="2">○ 민간・공공・국방 등 분야별로 구분
<table><tr><td>민간</td><td>미래부</td><td>– 정보통신망법
– 정보통신기반 보호법</td></tr><tr><td>공공</td><td>국정원</td><td>– 사이버안전 관리규정 (대통령 훈령)</td></tr><tr><td>국방</td><td>국방부</td><td>– 국군사이버 사령부령 (대통령훈령)</td></tr></table></td></tr>
<tr><td>정보보호 시책 수립</td><td>○ ‘사이버보안 전략본부’에서 사이버보안 전략 추진의 일환으로 보안시책 수립 및 평가 등을 실시 (안§12, §25)</td></tr>
<tr><td>정보보호 예방・대응 조치</td><td>○ 침해사고 시의 신고, 처리절차 등 구체적 규정 없음
– 사이버보안을 위한 기본이념과 보안전략, 기본시책 등의 수립・이행 및 사이버보안 추진체계 등 규정
– 다만, 이를 바탕으로 각 개별법*에서 관련 사항을 규율 가능
* 「전기통신사업자법 등의 일부를 개정하는 법률」(2001년 법률 제62호), 「전기통신기반충실임시조치법의 일부를 개정하는 법률」(2001년 법 제43호 등)</td><td>○ 사이버보안을 위한 컨트롤타워, 기본이념, 종합적 보안전략과 시책 등에 대한 통합법은 없음
○ 다만, 각 개별법에서 침해사고 시의 신고, 처리절차 등을 규정
– 침해사고 대응조치는 피해정도* 에 따라,
* 관심 〈 주의 〈 경계 〈심각
– 범정부사이버위기대책본부(사이버 안전관리규정–‘주의’ 이상),
– 민관합동조사단(정보통신망법), 침해사고대책본부(기반보호법)을 구성하여 운영</td></tr>
</table>

3. 추진 전략

(1) 사이버 위협정보의 공유 및 분석을 위한 입법 추진

앞서 소개한 것처럼 2015년 5월에 「사이버위협정보 공유에 관한 법률(안)(이하 '사이버위협정보 공유법'이라 한다)」이 국회에 발의되었다. 동 법안은 사이버위협정보 수집・공유를 위한 '사이버위협정보 공유센터'(국정원 소속)의 설치・운영에 관한 규정 등 총 14개 조문으로 구성되어 있다(12개 조문, 부칙 2개). 「사이버위협정보 공유법」은 서상기 의원이 발의한 「사이버테러방지법(안)」중 논란이 있거나 불필요한 조항은 제외하고 사이버테러 대응에 가장 시급한 핵심사항(사이버위협정보 공유) 위주로 최소조항(12개)으로 구성하고, 국정원의 권한 강화, 프라이버시 침해 등 논란을 최소화하기 위해 활동결과 국회보고, 정보남용 방지대책 강구 운영 등 견제장치도 마련하였다고 입법 설명을 하고 있다.

외국의 사이버안보 관련 입법트렌드에서 파악하였듯이 최근의 전세계의 입법 동향은 사이버침해정보의 공유라고 할 수 있다. 외국의 입법 트렌드에 따라 우리나라도 이와 유사한 입법안이 발의됨에 따라 동 법안의 발의는 시의적절하다 판단된다.

그러면 이 법률안을 기준으로 주요내용을 살펴보고 검토의견을 제시하고자 한다.[45]

45) 제정안 주요내용은 다음과 같다.
가. 공공・민간 영역 간에 공유하는 '사이버위협정보'를 정의(안 제2조).
나. 국정원장은 국가안보실장, 미래창조과학부장관 등과 협의하여 범정부 차원에서 사이버위협정보를 공유하기 위한 방법과 절차를 마련함(안 제4조).
다. 국가의 주요 정보와 정보통신망을 관리하는 기관(이하 "사이버위협정보 공유기관")은 사이버위협정보를 수집하고 상호 공유하여야 함(안 제4조).
라. 사이버위협정보 공유를 효율적으로 수행하기 위하여 국정원장 소속으로 사이버위협정보 공유센터(이하 "공유센터")를 설치・운영함(안 제5조).
마. 공유센터의 장은 공유된 사이버위협정보를 종합 분석하고 결과를 사이버위협정보 공유기관 및 관련 업체에게 제공하여야 함(안 제6조).
바. 국정원장은 법무부장관 등 국가기관 및 전문가가 참여하는 협의회를 구성하여 사이버위협 정보의 남용방지 대책을 수립하여야 함(안 제7조).

「사이버위협정보 공유법」은 국가 주요 정보통신망의 사이버위협에 대한 공공・민간의 정보 공유체계 활성화를 위한 범정부 차원의 정보 공유체계를 규정하고 있다. 이는 최근 급증하는 국가 정보통신망에 대한 사이버위협을 조기 탐지・전파하여 국정원・미래부 등 유관기관 및 민간 사업자 간의 정보 공유체계를 강화하려는 것으로 파악된다. 우선 동법안은 범국가적 사이버위협정보 공유체계를 신설하고자 하고 있다(안 제4조 및 제5조).

국정원을 중심으로 "(공공・민간) 정보수집・제공 ⇔ (중앙행정기관) 정보공유 ⇔ (국정원) 정보종합・분석・배포" 등 범국가적 공유체계 구축을 목표로 하고 있다. 정보 공유체계 구축을 위하여 국정원장은 관계기관(국가안보실・미래부・금융위 등) 협의를 통해 공유방법・절차를 마련하고, 국가 주요 정보통신망이나 정보를 관리하는 "사이버위협정보 공유기관[46]"은 위협정보를 수집하여 제공할 의무가 있다.

공유기관에서 수집한 사이버위협정보는 국정원장 소속『사이버위협정보 공유센터』[47]에서 종합하여 분석・배포하도록 하고 있다.

동 법안의 두 번째 큰 내용은 일반 이용자에 대해서 사이버위협정보의 제공을 요청할 수 있도록 하는 규정이다(안 제8조제2항). 공유센터(국정원장 소속)의 장이 국가 안전보장을 위하여 "필요하다고 판단하는 경우"에는 악성프로그램 감염PC의 일반 이용자에 대하여 해당 악성프로그램의 제공을 요청할 수 있도록 규정하고, 해당 정보를 제공한 개인에 대하여는 공유센터의 장이 대통령령으로 정하는 절차와 방법에 따라 보상금을 지급할 수 있도록 하고 있다.

사. 사이버위협정보를 보유한 사람은 공유센터의 장에게 신고하거나, 공유센터의 장이 사이버위협정보의 제공을 요청할 수 있음(안 제8조).
아. 공유센터의 장은 사이버위협정보 공유 활동에 대한 결과를 평가하고 그 결과를 국회에 보고하여야 함(안 제9조).
자. 사이버위협정보 공유기관, 공유센터 등의 종사자는 직무상 알게 된 비밀을 누설하면 아니 되고 위반 시에는 벌칙을 부과함(안 제10조・제11조).

46) 주요정보통신기반시설 관리기관, 주요ISP, IDC, 전자금융 운영기관, 핵심기술 보유기관 등.

47) 정부기관(미래부, 금융위, KISA)・민간업체(백신SW업체 등)의 파견인력으로 구성.

「사이버위협정보 공유법」의 내용에 대해 다음과 같은 검토의견이 제시된다. 우선 동 법안은 적용 범위를 국가 주요기반시설이 아닌 일반 민간 사업자 등에 대한 사항까지 확장하여 법제화함에 따라 개인 프라이버시 침해 및 국가 권한의 오·남용 문제 등이 우려된다. 법안은 "(공공·민간) 정보수집·제공 ⇔ (중앙행정기관) 정보수집·공유 ⇔ (국정원) 정보종합·분석·배포" 등의 체계를 규정함으로써 「사이버테러방지법(안)」과 유사한 규율체계를 구축하고 있으나, 「사이버테러방지법(안)」에서 제외하고 있는 전자금융기반시설 운영기관을 "사이버위협정보 공유기관"에 포함하여 주요기반시설로 지정되지 않은 사업자 등에 대하여도 정보 수집·제공 의무를 부과하고 있다.[48]

또한, 수집된 정보를 정부기관(미래부, 금융위, KISA), 민간업체(백신SW 업체 등)의 파견인력으로 구성된 "사이버위협정보 공유센터"(국정원장 소속)에서 종합·공유하도록 규정함으로써 공공·민간의 협력체계를 보다 강화하도록 하고 있다.[49]

[사이버위협정보 공유체계 비교]

	「사이버위협정보 공유법(안)」 (이철우 의원안)	「사이버테러방지법(안)」 (서상기 의원안)
목적	공공·민간을 아우르는 범부처 사이버위협정보 공유체계 구축	
공유체계	사이버위협정보 공유센터 ⇒ 국정원장 소속 ⇒ 정부기관·민간업체 파견인력으로 구성	국가사이버안전센터 ⇒ 국정원장 소속 ⇒ 기존 사이버안전관리규정상 설치 근거 법제화
	사이버위협정보 공유기관 ⇒ 전자금융기반시설 운영 기관, 단체, 사업자 포함	책임기관 ⇒ 일반 전자금융기반시설 운영기관 불포함
역할	기관 간 사이버위협정보 수집·공유·분석·배포	

48) 「사이버테러방지법(안)」은 정보 수집·공유를 위한 책임기관의 범위에 주요정보통신기반시설로 지정된 시설의 관리 기관을 규정(안 제2조제1항제7호).

49) 「사이버테러방지법(안)」은 '국가사이버안전센터'(국정원장 소속)를 설치하고 민·관·군 합동대응팀을 운영할 수 있음을 규정하고 있으며(안 제9조제1항 및 제3항),

이와 같은 정보 공유체계 강화는 사이버위협 조기 탐지·전파를 통해 신속한 침해 대응을 가능하게 하는 반면, 정보기관의 과다한 권한문제를 야기할 위험이 있다.

예를 들어 국정원장 소속의 공유센터의 장이 국가 안전보장을 위하여 '필요하다고 판단하는 경우' 일반 감염PC 이용자에게 해당 악성프로그램의 제공 요청을 가능하도록 하여(안 제8조제2항), 불명확한 판단기준에 따른 정부개입의 문제 발생이 우려된다.[50] 이에 대하여 「사이버위협정보 공유법」은 ①정보공유에 따른 국회 보고, ②민·관 협의회 구성을 통한 사이버위협정보 남용 방지를 위한 절차 등 사후 통제절차를 규정하고 있으나, 사후적 통제절차만으로는 정부의 과도한 개입 등에 대한 우려를 근본적으로 해소하기 어려운 측면[51]이 있으며, 사이버안보를 위한 사이버위협정보 수집·공유의 필요성과 국민 프라이버시 보호간의 이익형량을 통해 입법 방향을 보다 신중히 검토하는 것이 바람직할 것으로 판단된다.

생각건대, 정보공유체계는 일반적으로 민간분야(일반법) 및 국가핵심시설 분야(특별법)로 구분하여 민간분야는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 적용되고, 주요기반시설에 대하여는 「정보통신기반 보호법」이 우선 적용되고 있는 바, 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「정보통신기반 보호법」과의 정합성을 유지하면서 공공·민간의 범국가차원의 공유체계를 구축하는 방향을 검토하는 개선안이 보다 바람직할 것으로 판단된다.

또한, 「사이버위협정보 공유법」은 공유센터(국정원장 소속)의 장이 사이버

50) "사이버위협정보"의 정의에 "사이버위협으로 판단되는 정보로서 사이버위협의 발신지와 목적지, 발생일시 등을 포함한 로그기록자료, 악성프로그램 및 이와 관련한 자료, 보안취약점 관련 정보"를 모두 포함(동법 제2조제7호).

51) 앞서 외국 트렌드로 美국토안보부 내에 사이버위협정보를 위한 협조기관을 설치하고 민간 연방기관으로부터 정보를 수집·제공받아 공유하는 CISPA법안이 발의('15.1.8)된 바 있으나, 국민 프라이버시 침해 위험성 등에 따른 반대로 입법이 지연되고 있음을 참고.

위협정보를 보유하거나 악성프로그램에 감염된 컴퓨터의 이용자에게 해당 정보의 제공을 요청할 수 있음을 규정하고 있어, 일반 이용자에 대한 기본권 제한 및 정부 권한의 오·남용 문제가 야기 될 우려 있으므로 일반 이용자 PC에 대한 정보 요청 절차 및 판단기준을 명확히 하고 신속한 침해 대응을 위해 정부가 이용자 감염PC에 관련 정보 제공을 요청할 수 있는 절차 개선 방안을 검토할 필요가 있다. 각국의 최신 트렌드에서 파악되었듯이 사이버안보를 유지하기 위해 민·관간 정보의 공유는 필수적이고 필요한 것으로 파악되고 있다. 따라서 우리나라도 정보공유 및 분석을 위한 입법이 필요하다 할 것이나 개인의 프라이버시 침해 우려를 불식시킬 수 있는 입법의 추진이 절실하다 할 것이다.

(2) 사이버안보 조직체계의 확립

정부는 우리나라의 사이버공간의 보호를 위해 2015년 4월부터 '국가 사이버안보 강화방안'을 마련하여 시행하고 있다.[52] 이 대책에는 범정부 차원의 사이버안보 역량 강화, 핵심기술 개발 및 인력양성, 국제공조확대, 업무수행체계 정비, 컨트롤타워 강화 등의 핵심과제가 포함되어 있다.[53]

이에 따라 정부는 우선 국가안보실 중심의 전반적인 사이버안보 컨트롤타워 기능을 보다 강화하기 위해 국가안보실 산하에 사이버안보비서관을 신설하고 국가안보실과 국가사이버안전센터를 통해 국가적인 사이버보안정책의 수립·시행·평가를 일원화하는 사이버안보 수행체계를 구축하고자 하고 있다.

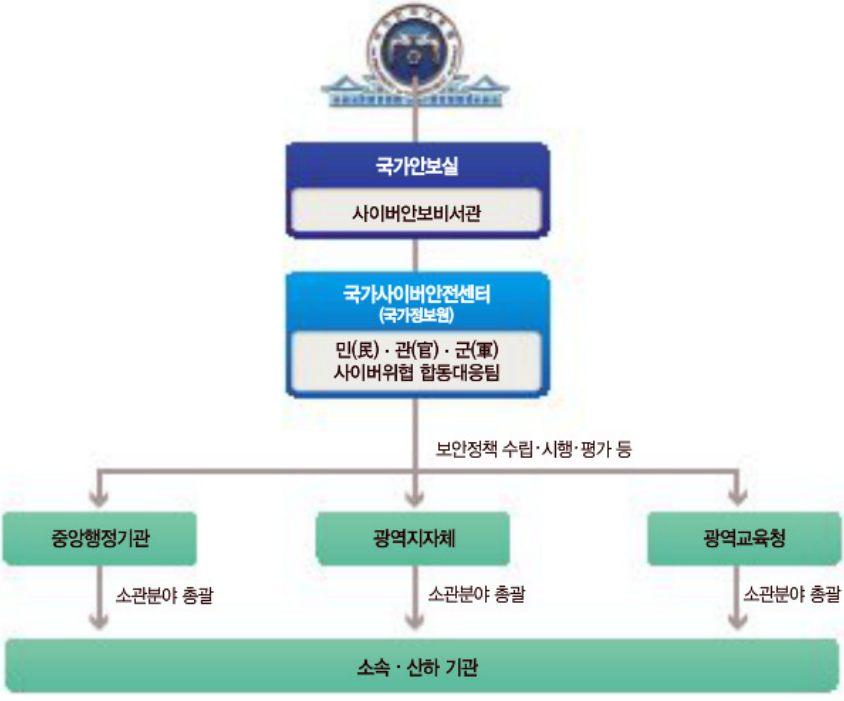
또한 중앙행정기관, 지자체와 주요기반시설 관리기관의 보안능력 확충을 위해 사이버보안 전담조직 신설·확대를 추진하는 것으로 하고 있다. 이러한

52) 국무총리실 보도자료, 국가 사이버 안보태세 역량 강화 (한수원 해킹사고 중간 수사결과 등, (2015.3.17.) <http://pmo.go.kr/pmo/news/news01.jsp?mode=view&article_no=47900&board_wrapper=%2Fpmo%2Fnews%2Fnews01.jsp&pager.offset=20&board_no=3&defparam:year_month=2015-03> (2015. 6.17. 최종방문).

53) 사이버안보 조직체계의 확립부분은 이 국가 사이버안보 강화방안을 토대로 체계를 확립하고자 하고 있으므로 이에 갈음한다.

과정을 통해 중앙행정기관과 광역지방자치단체, 광역교육청은 소관분야에 대한 보안관리를 총괄하게 된다. 그리고 각급기관의 정보보호예산을 별도 항목으로 분리하고 취약점 분석·평가지원, 사이버 공격징후 탐지·대응기구 운영, 업무망과 인터넷 분리 등 관련 예산을 확대하며, 민·관·군 합동 사이버위기 대응 실전훈련을 강화하고, 사이버 위협정보 종합수집·분석·공유 시스템을 보강하도록 하고 있다.

[국가사이버안보 수행체계 개선방향]



(출처 : 2015 국가정보보호백서)

사이버안보 핵심기술 개발 및 정예요원 육성을 위해 사이버능력이 우수한 특기자 전형의 사이버 특화고교·대학을 확대하고 군 전역이후 사회 각 분야에서 활용되도록 사이버인력 생태계를 조성해 간다. 또한 전문기관의 사이버

안보 핵심기술 개발 투자 확대와 함께, 벤처기업 펀딩 및 정부지원 사업 확대 등도 적극 추진한다.

사이버 대응역량 강화를 위해 조직・인력을 확충하고 관련 연구개발 예산을 확대하며, 주요 정보통신망에 대한 해킹 방지기술과 같은 보안기술 및 부품개발 등 관련 산업 육성도 적극 추진한다.

사이버공격에 대해 국제사회와 공조 대응하기 위해 주요국과 사이버안보 관련 정책 및 정보공유를 확대하고, 국제기구와의 긴밀한 협력을 통하여 사이버 공격에 대한 억지력 강화 및 국제규범 마련 노력에도 적극 동참할 계획이라고 한다.

끝으로 국가 사이버안보 정책 의사결정의 일원화 등을 위해 사이버안보 관련 법령을 보완하여 업무수행체계 기반을 지속적으로 정비할 계획임을 밝히고 있다.

(3) (가칭) 사이버안보기본법 법제화

현행 우리나라의 사이버 침해대응 관련 법제를 보면, 각 개별 법령에 산재된 침해사고 규정 및 단일화된 추진체계 미비로 인하여 신속・효율적인 침해대응 체계 구축이 곤란하다. 북한소행으로 여겨지는 수차례의 해킹사태나 DDoS공격(좀비PC 이용 DDoS공격은 공공・민간 구분없이 국가재난에 준하는 대규모 침해 야기) 등에서 알 수 있듯이 IT정보 환경에서 사이버안보체계의 공공・민간으로 구분・대응은 무의미한 것으로 파악된다.

또한, ICT의 급격한 발전에 따른 역기능을 서둘러 봉합하기 위해 다수 법의 무원칙적 제정으로 일관성・통일성 부족, 법간 충돌・모순이 발생하는 상황이다.

이러한 사이버안보 추진체계 관련 현행 법령의 명확하지 않은 태도는 신속하고 적절한 사전 예방・사후 대응책 마련에 부족한 것으로 파악된다.

따라서 사이버안보조직체계를 어떻게 정립할 것인지 정책이 확정되면, 정부・사업자・이용자 등 정보보호 관련 주체들의 역할을 명확히 분류하고 주

체 간 형평을 고려하여 책임이 배분될 수 있도록 법체계가 규정되어야 할 것이다.

결론적으로 국가차원의 사이버안보를 위한 포괄적 기본법 제정이 필요하지 않나 생각된다. 현행 사이버보안 법령간 집중과 분산이 조화를 이루는 사이버안보 법제 체계화가 필요하다. 아울러 종합적·全방위적 사이버안보 대응 체계 구축이 필요하다. 침해사고는 공공·민간을 구분하지 않으므로 악성코드 및 사고에 대한 정보공유 및 기술지원 등 협업체계를 마련하고, 사이버안보는 네트워크와 상호 연계가 필수적인 만큼 전문화된 총괄부처로 하여 일원적인 대응체계의 구축이 필요하고, 각 법령에 산재된 규정의 통합 및 주체별 역할을 명확화하며, 정보통신망·시스템 등 보호범위의 재구성, 침해사고 대응체계 명확화, 관련 주체들 간의 적절한 역할 분담, 중소기업 지원책 등의 마련이 필요하다.

「사이버안보기본법」을 제정한다면 그 제정방향은 다음과 같다. 첫째, 인터넷 기술 환경 변화에 대응한 선진화된 정보보호 기본법제의 제정, 둘째, 해외 주요국의 사이버안보 법제와의 조화 및 종전 법집행체계를 개선한 효율성·대응성 극대화 정책의 반영이 필요하다. 셋째, 사이버안보기본법은 사이버안보정책의 특성을 기반으로 하여 이를 구체적으로 실현하기 위한 정책입법이 필수적이므로 다양한 분야에 걸쳐 존재하는 사이버안보정책의 내용을 인정하면서 정부의 통합적 사이버안보정책을 가능하게 하는 입법이 되어야 한다. 이에 따라 정책의 개념적 범위를 설정하고 이에 대응한 정책체계를 확립하며 국가적 차원에서 사이버안보를 위한 자원동원의 효율성과 효과성을 보장해야 할 것이다. 넷째, 개별분야의 특수한 규율을 위한 입법 내용은 개별법에 두고 정책체계 효율화를 위하여 필요한 공통사항은 기본법에 두는 법제간 역할분담을 가능하게 하는 입법이 고려된다. 장기적으로 해당 정책이 경쟁과 협력을 지속하면서 일반법과 특별법의 관계 또는 기본법과 개별법의 관계를 발전시켜가는 정책환경을 제공할 수 있도록 입법 방향을 설정하는 것이 좋을 것이다.

V 결 론

사이버안보법제의 문제는 발전하는 ICT기술에 따라 국가적·사회적 위협이 계속 증가하면서 더욱 더 우리의 관심대상이 되고 있다.

자원이 부족한 우리나라가 세계속에서 위상을 정립함에 있어 ICT기술은 큰 몫을 담당하였고 정보화라고 하는 국가 발전 모델을 성공시켜오면서 등한시 하였던 사이버안보에 대한 부작용이 계속적으로 나타나고 있는 상황이다.

우리의 사이버안보법제는 다른 나라와 비교하여 볼 때 ICT발전에 따른 역기능을 해소 또는 감쇄시키기 위해 부단한 노력을 한 결과, 한편으로는 나름대로 잘 갖추어진 체계를 이루고 있다. 하지만 작금의 시대에서 우리는 역사적 또는 정치적 특성으로 인하여 더 이상 사이버안보법제의 체계적 발전을 도모하지 못하고 있다. 미국과 같이 국토안보부를 설치하여 체계적으로 운영하기에도 많은 제약이 따르고 있고, 현재의 정보기관을 활용하여 추진하겠다고 하더라도 우리나라 정치·사회적 역사의 트라우마로 인하여 반대여론에 부딪혀 진퇴양난에 빠져 있는 상황이다.

계속되는 사이버 침해사고에 따라 현 정부에서는 사이버안보정책에 대한 인식이 개선되고 안보특별보좌관을 정보보호분야 전문가로 임명하는 등 사이버안보체계 확립을 위해 많은 노력을 기울이고 있다.

우리나라 뿐만 아니라 최근 사이버안보에 대한 인식은 전세계적인 화두가 되고 있다. 특히 사이버침해에 관한 정보의 공유와 분석에 대한 열망은 미국, 유럽 여러 나라나 조직에서 제1순위의 관심사로 입법화를 서두르거나 정책을 개진하여 원하는 목적을 달성하고자 하는 상황이다.

우리나라에서 발생하는 주요 사이버 침해사고는 명백히 밝히기는 어렵지만 북한의 소행인 것으로 보여지고 있고 이후에도 미국의 소니사에 대한 해킹도 북한의 소행인 것으로 파악되고 있다. 중국이 미국에 대해 시도한 해킹사건이나 미국이 같은 우방인 영국이나 독일정부 요인에게 시도한 해킹도 빈번하다. 이로 인해 적성국은 물론 우방국간에도 관계가 껄끄러워질 수 있는

상황인바, 사이버테러가 국제화, 보편화하면서 심지어는 국가 간 사이버전쟁이 언제든 발생될 가능성이 있다.

그간 미봉책으로 위기를 모면하기 위해 패치형태로 개선하던 사이버안보에 관한 법체계의 개선을 하기 위해서는 일상적인 장애나 재난보다는 국가안보 차원의 대응체계 구축이라는 국가 전략적 차원에서 추진이 되어야 할 것이다.

그러나 사이버안보법체계의 개선을 함에 있어 국민의 개인정보나 프라이버시가 침해되지 않고, 자유와 권리가 지켜질 수 있도록 하는 노력이 필요하다.

최근의 외국 선진국들의 입법 트렌드는 살펴본 바와 같이 사이버침해사고를 미연에 방지 또는 속히 복구할 수 있도록 하기 위한 정보의 공유를 목적으로 입법이 추진되고 있다. 이는 정부3.0에서 주창하는 정보의 공유와 유통, 협력이다.

미국, 독일, 유럽연합, 일본 등에서 추진하고 있는 사이버안보와 관련해 적용되고 있는 법제들을 비교・분석하여 우리나라 실정에 맞게 법제화를 추진하고 그 체계를 공고히 해야 할 시점이다.

국회에서 공전(空轉)하고 있는 법률안들이 왜 입법이 안되는 가를 곰곰이 생각해 보고 모두가 동의하고 입법을 수긍할 수 있는 그러한 최상의 법안을 만들어야 할 것이다. 그 법령을 바탕으로 컨트롤타워를 수립하고 각 기관에 흩어져 있는 권한을 재정비하고 체계화한다면 안정된 국가안보가 확보될 것이다. 그 힘을 통해 국가간 공조도 앞장설 때 세계 속에 강력한 대한민국으로 자리매김 할 수 있지 않을까 생각한다.

[참고문헌]

김은혜・이재일, 미 오바마 정부의 사이버보안 주요 정책 및 법안, 인터넷&시큐리티 이슈, 2011.8.

남길현, “사이버테러와 국가안보”, 국방연구.

이완수, 국가 사이버 안보 구축전략에 관한 연구, 경기대학교 대학원 박사학위 논문, 2014.6.

이정현, “국가 사이버안보(cyber security) 추진체계의 이슈와 과제”, 사이버안보법정책논집, 2014. 창간호.

_____, “국제 사이버 범죄조약의 영향”, 제23회 정보보호와 암호에 관한 학술대회 논문집, WISC2012, 2012. 9,

이창범, “국내외 사이버안보 관련 법제정 동향과 시사점”, 사이버테러와 법정책적 대응, 한국사이버안보법정책학회,

아시아경제, 2014. 9. 11.

미래창조과학부, “정부,「국가 사이버안보 종합대책」수립 - 사이버안보 강화를 위한 4대 전략(PCRC) 마련 -”, 2013. 7. 4.

미래창조과학부 등, 2015 국가정보보호백서. 2015.

<https://www.gov30.go.kr/gov30/int/intro.do>

<http://www.dhs.gov/history>

<https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>

<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/09.html>

<http://law.e-gov.go.jp/htmldata/H12/H12HO144.html>

<http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/pdf/jyoubun.pdf>

<http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=1>

<https://www.datenschutzzentrum.de/uploads/it/20141021-it-sicherheitsgesetz.pdf>

<http://www.bitkom.org/files/documents/Stellungnahmelang_BITKOM_ITSIGv3.pdf>
<http://www.vorratsdatenspeicherung.de/content/view/748/1/lang,de/>
<https://netzpolitik.org/2014/it-sicherheitsgesetz-im-kabinett-beschlossen-die-kritischen-punkte-zusammengefasst/>
<http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Kritik-an-Aufruestung-Warnung-vor-nationalem-Alleingang-2499554.html>
<http://pmo.go.kr/pmo/news/news01.jsp?mode=view&article_no=47900&board_wrapper=%2Fpmo%2Fnews%2Fnews01.jsp&pager.offset=20&board_no=3&defparam:year_month=2015-03>

제3장 국가 사이버안전을 위한 법적 과제

주요 국가별 사이버안보 대응체계 연구

정 태 진*

목 차

Ⅰ 서 문

사이버 안보위협과 관련하여 세계 여러 국가는 사이버공격을 가장 심각한 위협이라고 정의하고 불순세력의 공격으로부터 국가의 주요 정보나 시설을 보호하기 위하여 노력을 기울이고 있다. 최근 들어 사이버안보위협에 국가간 협력을 통해 공동으로 대응하기 위한 움직임도 활발해지고 있다. 그리고 유럽에서는 ENISA를 중심으로 회원국들이 사이버 안보위협에 능동적으로 대응하는 체계를 꾸준히 갖추고 있다.

그러나 그 외의 국가들은 각국이 처한 입장, 이해관계 그리고 법률적 차이로 인해 통일된 법률이나 대응체계는 존재하지 않는다. 그리고 각국마다 사이버안보를 담당하는 기관도 다르다. 우리나라 같은 경우에는 국정원, 국방부, 경찰, 인터넷진흥원등이 영역별로 사이버안보를 담당하고 있다.

* 사이버폴리싱 연구센터장

그러나 사이버공격의 목표가 되는 곳은 민간시설에 집중되어 있다. 지난 몇 년간 북한의 사이버공격으로 인해 국가기관, 금융기관 그리고 방송국 등이 피해를 입었으며 대기업들도 많은 피해를 입었으나 외부로 많이 알려지지 않았다. 왜냐하면 기업이미지나 주가에 영향을 주기 때문이다. 이러한 민간의 피해는 해당기업이나 단체의 피해만이 아니라 궁극적으로는 국가적인 피해이다. 사익이 곧 국익이기 때문이다.

이러한 차원에서 우리나라 국정원이 사이버안보를 책임지고 효과적으로 대응하기 위해서 민간영역까지도 보호할 수 있도록 법으로 포함시켜야 한다. 그러나 과거 국정원의 정치개입 사건들로 인해 대국민 신뢰를 많이 잃었기 때문에 국정원이 추진하려는 사이버안보법은 야당의 반대로 제정이 어려운 상태이다. 더 이상 사이버 위협으로부터 국가안보를 등한시 할 수 없기에 이 법을 통과시키기 위한 대국민 설득이 필요하고 국민들을 설득하기 위해서는 다른 국가들의 사이버안보 대응체계는 어떠한지 알아보는 것이 필요하다.

Ⅱ 주요 국가별 사이버안보 대응기관 및 동향

1. 미국

미국의 사이버안보는 NSA와 사이버사령부를 중심으로 이루어진다. NSA는 원래 2차 세계대전 당시 암호해독을 하기 위해 만들어졌는데 1952년 해리 트루먼 대통령에 의해 NSA로 거듭 태어나게 되었다. 현재 예산이나 인원이 가장 큰 정보기관이며 국방부 산하에 있으며 최고 NSA국장은 국방장관과 국가정보국장(Director of National Intelligence)에게 동시에 보고할 의무가 있다.

위키피디아에 의하면, “미 정보기관중 가장 큰 규모와 막강한 정보수집력을 갖고 있는 것이 NSA다. NSA는 석사급 이상의 학력을 가진 3만8000여 명의 요원들이 근무하고 있다. 정보수집 대상국의 암호를 해독하기 위해 세계최대의 수학자 채용기관이며 슈퍼컴퓨터를 보유하고 있다. 한 해 예산은

80억달러(8조원)이다"[1].

미국 사이버사령부는 2009년 6월 만들어 졌으며 NSA국장직과 더불어 미국 사이버사령부 사령관(Commander of the US Cyber Command)은 마이클 로저스 제독이 겸직하는데 미국 사이버사령부는 미군 전략사령부 예하부대로써 모든 군의 사이버부대자원을 통해 국방정보네트워크시스템을 보호하고 사이버상의 군사 활동을 준비하여 미국과 그 동맹국의 사이버상의 모든 자유로운 활동을 보장한다. 이와 같이 미국은 NSA와 US Cybercom을 통해서 전 세계 사이버 및 통신정보를 수집하여 안보활동을 하고 있다.

미국은 2011년 오바마 대통령의 지시로 사이버공격을 받을 시에 물리적으로 타격할 수 있는지에 대한 국제법 검토했다. 이러한 정책의 일환으로 2014년 소니영화사 해킹사건 발생시에 미국은 즉각적으로 북한 인터넷망을 공격하였다. 물론 물리적 목표에 대한 타격은 아니었으나 그 맥락은 같다.

그리고 사이버안보 및 국방 태세를 강화하기 위해서 "플랜X" 프로젝트에 착수하여 미국방부의 사이버전 전략을 방어위주에서 공격위주의 전략으로 바꾸었다. 이를 위해서 미국은 고등국방연구원(Defense Advanced Research Projects Agency)을 통해 1억 2천만 달러 정도를 4년간 투입하고 있다[2]. 플랜X는 전 세계 사이버공간에 포진해 있는 수백억개의 컴퓨터 도메인과 서버를 총망라에 표시하고 이들의 연결 상태를 보여주는 디지털 지도를 작성하는 프로젝트이다. 이를 토대로 미국은 필요시 적국의 사이버시스템을 자동으로 공격할 수 있는 능력을 갖추려고 준비 중이다.

현재 미국 기업의 사이버공격은 기업체 스스로가 해결하는 것을 원칙으로 하고 문제의 심각성이 있는 경우에는 국토안보부가 개입을 하여 수사하고 국가안보에 직결되는 공격에 대해서는 사이버사령부를 통해 대응하고 있다.

1) 오에리 (2013년 6월 14일). "9・11이 낳은 '첩보外注' 시대… 1급 기밀 보안 무방비 노출". 문화신문. 2013년 7월 9일에 확인함.
2) http://www.army.mil/article/152979/New_Army_cyber_officers_hack_improvements_into_DARPA_s__Plan_X_/

미국 사이버사령 주요임무는 사이버전장에서의 작전을 구상하여 새로운 교전 규칙이나 전술 기술 및 절차를 만들어 내는 것을 비롯하여 신속한 정보 제공을 통해 국가지도자들의 의사결정을 돕는다. 그리고 지속적인 훈련을 통해 실전에 대비하고 사이버방어가 가능한 구조 설계를 통해 국가기반시설에 대한 보호를 강화한다.

미국 국방장관의 최근 발언에 의하면, 미국은 중국, 러시아, 이란, 북한을 미국사이버안보의 가장 큰 위협이 되는 국가로 지목했다. 그리고 이러한 국가들의 위협에 대비하기 위해 새로운 대응체계를 마련하기로 했다.

2015년 미국사이버사령부는 사이버공간에 대한 공격력을 강화하기 위해 46억불을 들여 사령부 업무의 대부분을 아웃소싱하기로 했다. 그리고 9월 30일, 총 114페이지에 달하는 계약서와 86페이지의 작업명령서를 공개했다[3].

문서에는 마이클 로저스 제독이 9월초에 발표한 비전이 반영되어 있다. 로저스 제독은 미국 NSA 국장도 겸직하는데 앞으로 우리의 파트너(민간)를 무장 시키는 것이 급선무라고 강조했다. 구체적인 전투력에 대해서는 밝히지 않으면서도 '사이버 합동군수지원'에 대해서 자세히 언급하였다.

사이버 합동군수지원 매뉴얼(Cyber Joint Munitions Effectiveness Manual (JMEM))[4] 은 2013년 여름 모델링 과 시뮬레이션 저널에 미군의 사이버 컨셉을 일반적인 전쟁터로 본다고 표현했다.

미국 국방부의 마크 갈라거 박사에 의해 쓰여진 요약문은 사이버전의 복잡성에 대해 잘 묘사했고 핵무기 사용에 준하는 모델과 데이터를 사용하라고 강조했다.

미국사이버사령부가 하청업체에게 요구하는 사이버공간에서의 작전지원 핵심사항은 문서에 나와 있듯이 "추천, 발전, 평가, 분석 그리고 사이버전에 사용하는 무기, 도구 그리고 전력에 대한 결합이다

3) http://www.theregister.co.uk/2015/10/06/uscybercom_460_million_contract/
4) http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx

특히나 지원 사항은 계획, 조정과 공격적 작전과 방어적 작전 그리고 방위 정보 네트워크에 대한 동시성에 대한 전문가들의 기술적인 자문을 의미한다.

계약자들의 핵심 경력은 제한은 없지만

1) 행정, 수송, 정보관리
2) 사이버공간 작전지원
3) 사이버공간 기획지원
4) 정보수집
5) 능력관리 및 개발지원
6) 사이버작업장에 대한 훈련 및 연습
7) 정보통신 지원
8) 전략/정책/원칙 개발 및 캠페인 평가
9) 교전지원
10) 보안 안정성과 감사

그리고 계약자는 보안감사와 같은 일반적인 사안에 대한 요구사항에 대해 답변해야 한다. 계약서는 계약자가 브리핑 사안에 대해서 발표할 것도 포함했다.

로저스 제독은 많은 전문가들이 정부영역 밖이나 미국 영토 밖에서 활동하고 있다고 경고하고 아직은 사이버사령부가 조금 앞서 있을지 모르나 이들을 빨리 흡수하지 않으면 안 될 것이라고 경고했다.

현재 사이버사령부는 잠재적인 적들에 대항하여 열심히 활동하고 있지만 국가적 차원에서 사이버공간에서의 경쟁적 위치에 있는 이들에 대해 정확히 파악해야 한다고 강조했다.

국가, 집단, 개인들은 최첨단 기술을 이용하여 미국과 미국의 우방국을 상대로 사이버협박, 사이버공격, 사이버강탈을 일삼고 있다. 그들의 목표는 정부를 넘어서 개인이 소유하는 기업까지 뻗쳐 있다.

미국사이버사령부는 연방정부, 외국, 기업파트너들과 협력하여 사이버스

파이 행위에 대해 강력히 대처하여 사전에 차단하고 적들의 도발 의욕을 억제하는데 노력을 하고 있다. 필요시 상부에 지시에 의해 공격을 감행하는 작전을 수행할 수 있다.

미국 사이버사령부는 군사작전에 필요한 의사결정을 내릴수 있는 전문가와 작전 지휘관을 일선 부대에 제공하여 언제든지 대응할 수 있는 태세를 갖출 것이라고 발표했다.

로저스 제독은 디지털 기술이 전통적인 군사작전의 형태를 많이 바꿔 놓았다고 주장하고 사이버사령부의 주요임무는 부대가 작전 가능하고 최적화되도록 하고 해커들에게 뒤지지 않아야 한다고 주장했다.

이러한 목적을 달성하기 위해서 사이버사령부는 육상, 해상, 공중 그리고 우주에서의 군사적 충돌을 대비하여 제 5지대를 설정해 놓아야 한다고 말했다. 그리고 주요 임무를 수행할 사이버 부대의 역량을 강화시키고 민관협력을 통해 목적을 달성해야 한다.

사이버전 용사들은 언제든지 항공모함, 비행편대, 육해공 부대, 특수전팀, 여단 등에 배치되어 능력을 발휘해야 한다. 사이버부대는 언제든지 작전 가능한 한 상태를 준비되어야 한다. 이런 태세를 갖추기 위해서는 다른 영역에서와 마찬가지로 플랫폼, 도구, 훈련 그리고 기반시설을 갖춰야한다고 말했다[5].

2. 영국

영국의 GCHQ(Government Communications Headquarters (GCHQ))는 1차 세계대전 중인 1919년 GC & CS(Government Code & Cypher School)로 만들어졌다. 영국의 정보기관중 전자신호 정보를 제공하고 영국정부와 군에 정보검증을 하는 기관이다[6]. GCHQ는 MI5, MI6 그리고 국방정보기관과 함께 합동정보위원회의 지휘를 따른다. GCHQ는 외무부 소속은 아니

5) http://www.theregister.co.uk/2015/09/10/cybercom_vision_statement_us_rogers/
6) https://en.wikipedia.org/wiki/Government_Communications_Headquarters

지만 외무부 장관이 책임을 맡고 있고 본부장은 차관의 지위에 있다.

영국의 GCHQ는 미국의 NSA와 비슷한 업무를 수행하는 기관인데 주로 정보통신망에 대한 보호를 담당하는 업무를 수행한다. 최근 밝혀진 문서에 의하면 GCHQ는 2007-2008년 암호명 KARMA POLICE작전을 만들어서 모든 인터넷 사용자들에 대한 감시를 시작하였으며 2009년에는 온라인라디오를 청취하는 사람들을 위주로 정보를 수집하였다[7].

2015년 5월에는 공개적으로 사이버 안보업무 전문가를 대대적으로 모집하였다. 이들은 사이버 테러리스트, 범죄자 그밖에 사이버위협에 대응하는 것이 주요 임무이다[8].

최근 들어 GCHQ는 해저케이블을 통한 글로벌 통신에 대한 도청 가능성을 염두에 두고 국제통신에 대한 감시를 강화하고 있다. 통상적으로 10-25 퍼센트의 통신이 국제통신에 속하는데, 여기에는 외국에 서버를 둔 페이스북이나 트위터가 포함 된다[9].

2015년 GCHQ는 이스라엘유닛8200 정보기관 모델을 본받아 우수대학원생들을 교육시킨 뒤 민간에 취업시키는 프로그램을 운영할 계획을 발표했다. 영국정부관계자에 의하면 GCHQ에는 많은 인재들이 일하고 있다. 이 프로그램의 시행에 있어서 문제는 민간업체와 GCHQ간의 상생하는 환경을 조성하는데 있다. 대학원생들은 GCHQ에 평생 근무해야 할 의무가 없고 언제든지 민간기업으로 취업 할 수 있다.

이러한 제안은 최근에 이스라엘을 방문한 프란시스 마드 의원(내각 각료)에 의해 제안 되었고 마드 의원은 유닛 8200 졸업생들을 만나고 왔다. 많은 정부 관계자들이 GCHQ가 민관과 협력을 잘 이루고 있다고 믿지만 앞으로도 더 긴밀히 산업체, 학교등과 파트너쉽을 이루어 기술을 발전시키는 것이

7) http://www.theregister.co.uk/2015/09/25/gchq_tracked_web_browsing_habits_karma_police/
8) http://www.theregister.co.uk/2015/05/12/gchq_recruitment_call_spying_snowden/
9) http://www.theregister.co.uk/2015/07/23/how_spies_spy/?page=2

사이버안보 목적이라고 했다[10].

그리고 영국정부는 700,000파운드를 들여 대학 교육기관들이 해커, 악성 소프트웨어 또는 사이버위협으로부터 영국을 지킬 수 있는 획기적인 교수법을 개발하도록 독려하였다[11].

3. 독일

독일은 사이버상의 안보와 보안역량을 강화하기 위한 중심기관(Zentralstelle)으로서, 연방내무부 외청으로 설치된 연방정보보안청(BSI)을 주목할 필요가 있다. 同기관은 원래 1957년부터 연방정보원(BND) 소속하에 설치되었던 암호국(暗號局, Zentralstelle fuer das Chiffrierwesen: ZfCH)이 확대 개편되어, 오늘에 이르게 된 것이다.[12]

同부서는 광범위한 업무를 수행하고 있는바, IT 사용과 관련된 안보/보안상의 리스크를 조사하고(investigate), 예방적 보안조치를 개발한다. 정보기술(information technology)의 활용과 관련한 불안 및 위협들에 관한 정보를 제공하고, 적절한 해결책을 제시한다. 민간기업과의 협력과 그들의 발전을 포함하여, IT 보안의 시험, IT 시스템의 평가를 수행한다. 심지어 정보 및 정보통신 시스템상의 리스크와 손상을 최소화 내지는 회피할 수 있도록, 연방정보보안청은 다양한 분야 목표에 대한 지원을 하고 있는바, IT 제조업체, 배급업체 그리고 사용자들에 대한 조언을 한다. 또한 IT 분야의 발전과 트렌드를 분석한다. 2015년 현재, 사이버보안국(Abteilung C: Cyber- Sicher-heit)을 비롯하여 5개국(C, B, K, S, Z)으로 편성되어 있으며, 各局(Ab- teilungen)에는 각 2개 課(Fachbereich 1,2)들이 설치되어 있다.[13] 연방정보보안청(BSI)은

10) http://www.theregister.co.uk/2015/01/02/gchq_tech_recruitment_scheme/
11) http://www.theregister.co.uk/2015/09/23/cyber_skills_fund_security_universities/
12) 초대 暗號局長(Leiter der Zentralstelle für das Chiffrierwesen)이 제1대 연방정보보안청장(BSI)이 된 셈이다.
13) 약 600명의 직원이 근무하고 있으며, 현재의 청장(Michael Hange)은 2009년 10월

유럽연합(EU)내 네트워크 및 정보보안청(ENISA: European Network and Information Security Agency)과 협력하고 있다.[14]

특히, 同연방정보보안청 관할 하에(beim federfuehrenden BSI), 2011년 4월부터 연방정부 산하 각급 정보보안기관들의 협력기구(Kooperationseinrichtung der Sicherheitsorgane des Bundes)로서, 국가사이버방어본부(Nationales Cyber-Abwehrzentrum: Cyber-AZ:NCAZ)를 가동하기 시작했다. 주요 업무는 사이버공격(Cyber-Angriffe)에 대한 "예방, 정보 그리고 조기경보(Fruehwarnung)"에 있다. 연방정부 및 민간경제영역의 IT(IT-Infra- strukturen des Bundes und der Wirtschaft)분야에 대한 전자적 공격을 방어(zur Abwehr elektronischer Angriffe)하기 위한 임무를 수행하고 있다.

연방정부의 사이버안보전략(Cyber-Sicherheitsstrategie für Deutschland)에 따라, 사이버공격(Cyber-Angriff)이라 함은 "사이버공간상(Cyber-Raum)의 IT-공격"으로 이해되고 있다. 연방정보보안청에서 설정하고 있는 Cyber공격의 유형으로는, 명의도용, 해킹,Trojaner공격, D DOS공격(Distributed Denial of Service-Angriff) 그리고 인터넷구조공격(예, Border Gateway Protocol-hijacking) 등이다.

국가사이버방어본부 설치의 필요성은 2005년부터 연방정부 내 공공기관 및 민간기업에 대한 전자적 공격이 점증하면서, 대두되었다. 2004년 연방범죄수사청(BKA)내에 설치된 연방 테러대책합동본부(Gemeinsame Terrorismusabwehrzentrum: GTAZ)가 국가사이버방어본부 출범의 기초가 되었다고 한다. 연방 내무부장관의 업무개시에 관한 공식발표(2011년 6월 16일)로부터 해당부서(NCAZ)의 업무가 개시되었다. 해당부서의 공식적인 책임자는 연방정보보안청장이 맡고 있다.

부터 재직 중이다.

14) 유럽연합내 해당부서의 책임자(Executive Director, 2009~)로 활동하고 있는 Udo Helmbrecht 는 전임 연방정보보안청장(2003-2009)이었다.

국가사이버방어본부(NCAZ)의 핵심 구성기관들은 내무부 외청인 연방정보보안청(BSI), 연방헌법보호청(BfV), 연방 국민안전 및 재난관리청(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: BBK) 등이다. 그리고 협력기관으로서는 연방범죄수사청(BKA), 연방정보원(BND), 연방경찰청(Bundespolizei), 국방부(Bundeswehr)의 기무사령부(MAD), 관세범죄수사청(Zollkriminalamt) 등이 상호협력하고 있다.

국가사이버방어본부는 독립적인 관청적 성격을 지닌 것은 아니며, 관련된 각급 연방 정보보안기관들간 상호 협력("Kooperationsvereinbarungen" der beteiligten Behörden)을 도모하고 있다. 연방정보보안청(6명), 연방헌법보호청(2명) 및 기무사령부(2명) 소속의 상근 요원들과 각급 기관의 전문요원들이 정기적으로 파견되어 근무하고 있다.

독일의 연방정보/보안기관들의 특징은 정치적 중립성, 부서 책임자의 임기가 장기간 보장되는 전통을 갖고 있으며, 정보공동체간 상호협력(co-operation)이 강조되고 있다. 뿐만 아니라, 연방제 국가로서, 특정부서에 권한이나 통제력/관할권이 집중되기 보다는 연방정부 내 각급 기관 간에 견제와 균형이 정착되고 있으며, 관련부서를 설치하기 위한 논의를 거친 후, 법령을 제정하여, 직무와 권한에 대한 명확한 근거를 갖춤으로써 법치주의 행정의 원칙을 견지하고 있다는 점이다. 또한 정보기관 근무자를 양성하기 위한 공동 교육과정, 해당부서 요원의 파견근무, 부서 책임자의 교류임명 등으로 정보보안기관간 상호협력을 증진하고 있다.

4. 일본

일본은 국가정보 보안센터(National Information Security Centre (NISC))가 사이버안보를 책임지고 있다. 2014년 11월 「사이버시큐리티 기본법」이 국회를 통과하였는데 사이버안보를 위해 국가정보 보안센터(National Information Security Centre (NISC))와 정부안보협력팀(Government Security Operation Coordination team (GSOC))에게 더

힘을 실어주는 법안이다.

현재는 기관을 초월하여 위협을 차단하는 법이 없기에 사이버공격에 취약하다. 새로운 법안으로 일본 내 13개 주요 기반시설 운영자들을 조정 할 수 있는 권한을 갖게 된다. 현재 「사이버시큐리티기본법」에 근거하여 관련 행정법규를 제정(사이버시큐리티전략본부령, 내각 사이버시큐리티 센터조직규칙 등) 사이버 안보 조직을 개편하여 시행하고 있는데 여기에는 재무, 교통 전력이 포함된다[15]. 2005년에 만들어진 NISC는 이러한 법률의 부재로 그동안 사이버안보 업무를 완벽하게 해내지 못했다.

최근 들어 일본은 서방의 여러 국가들과 중국의 군사도발과 함께 사이버공격에 공동대응하기 위해 협약을 맺었다. 그리고 프랑스와 공동으로 수중드론개발에 나섰다. 수중드론은 해저에 청음기를 설치해 중국 잠수정의 움직임을 포착하는 데도 사용하고 해저케이블을 끊고 통신정보를 수집하는데도 사용된다.

일본과 프랑스는 이미 공동으로 방위기술을 개발하기로 결정했고 일본은 프랑스와의 계약에서 프랑스가 3국에는 이 기술을 팔 수 없게끔 안전장치를 해 놓았다. 중국은 이러한 정보에 대해 민감한 반응을 보이면서 자세한 정보수집에 나섰다. 일본정부는 수중드론 개발에 약 50억원정도 예산을 책정해 놓았다.

이와 함께 독일, 영국, 스페인, 포르투갈, 프랑스와 함께 사이버보안에 대한 협력방안을 모색하고 있다. 처음 시작하는 일본과 유럽 사이버공간 정책대화에서 사이버안보의 중요성을 강조 했다. 그리고 국제외교무대에서 서슴없이 중국의 군사적 도발에 대한 우려와 사이버보안 위협에 대해 보다 적극적으로 대응하여야 한다고 주장했다.

일본정부는 이미 미국의 DARPA(Defense Advanced Research

15) http://www.theregister.co.uk/2014/03/12/japan_new_law_improve_cyber_readiness/

Project Agency): 고등국방연구원 같은 최첨단 무기를 개발 할 수 있는 연구소를 만들 계획에 있다. 사이버안보를 국가안보전략의 초석을 다지는 것으로 여기고 사이버국방력 향상에 심혈을 기울이고 있다[16].

5. 중국

중국 인민해방군은 상당한 수준의 사이버전을 수행할 수 있는 군인들을 양성하고 있다. 그리고 미국은 이를 심각한 군사작전의 리스크로 여긴다.

Northrop Grumman's[17] 리포트에 의하면 인민해방군은 정보전과 컴퓨터 네트워크 운영을 군사작전의 중요한 부분이라고 인식하고 '정보전'에 대비하여 기존의 작전계획을 수정하였다.

이 보고서에 의하면 중국군은 지속적으로 미군의 지휘체계에 대해 평가하고 유사시에 전자무기나 네트워크 공격 또는 다른 도구를 이용하여 전쟁을 수행할 준비를 갖추었다고 전한다.

중국의 사이버전 능력은 기술적으로 선진국에 대한 억제나 실질적 공격력으로 상대국의 전력을 사이버전력을 약화시키거나 주요기반시설의 작동을 멈추게 할 수 있다. 이러한 측면에서 중국은 미국이나 미국의 우방국에 대해서 그들의 전력을 공개할 수 없지만 대만이나 서태평양 국가와의 충돌 발생시 어쩔 수 없이 노출될 것이다.

이 보고서에 의하면, 중국은 대학과 민간기업체의 연구기관에 연구개발을 의존하고 있으며 50개의 공립 대학들이 정보보안과 사이버전 관련 연구자금을 지원받고 있다.

Huawei, ZTE, Datang 사들은 중국 인민해방군의 중요한 사이버전 기술을 제공하는 업체로 알려져 있다.

중국 인민해방국은 국방연구만 하는 연구소에 의존하기 보다는 민간 IT기

16) http://www.theregister.co.uk/2014/04/30/japan_china_unmanned_sea_drones_meeting/
17) http://www.theregister.co.uk/2012/03/08/northrop_grumman_china_pla/

업들과 대학교들과의 협력으로 연구개발을 진행하고 있고 민간의 최첨단기술에 접근 할 수 있어 민관협력의 중요성을 잘 알고 있다. 이러한 연구개발은 가끔 합법적인 투자를 통해 외국 업체로부터 아주 중요한 기술을 전수 받기도 한다.

중국 인민해방군의 민간협력 전력이 주는 장점은 외국기업과의 합병이나 국제상업시장을 통해 최신기술로 만들어진 정보통신기술을 아무런 제재 없이 구매하여 바로 사용하는 것이다.

이 보고서는 시만텍과 화웨이의 합병이 지적 재산권 침해와 서방기업에 대한 경쟁력 약화 등을 초래 할 수 있다고 경고했다.

중국 인민해방군과 중국의 최대 글로벌 정보통신서 및 하드웨어 제작사와의 협력은 유사시에는 상대국의 정부, 군사, 산업에 필요한 물품들에 대한 중단으로 큰 타격들 입힐 수 있다.

그러므로 미국의회는 화웨이나 ZTE에 대한 국가안보 리스크 차원에서 조사 중이고 법적으로 보호 할 수 있는 후속조치를 내어 놓고 있다.

작년 미국 정보기관 보고서에 의하면, 화웨이의 최고경영자 Ren Zhengfei가 인민해방군에 근무한 경력이 있고 최고여성경영자 Yun Safang이 중국안전부장의 내연녀로 밝혀졌다.

미국정부는 이러한 이유로 화웨이에 대해서 미국 내 서버운영 사업 합작을 할 수 없도록 압력을 행사했다. 최근 보고서 (2012)와 2009년 작성된 보고서를 비교해보면 중국 대학교와 IT기업의 국방 기술개발 참여 사업은 훨씬 더 발전하였다. 국무원 각 성, 자치구, 직할시 인민정부는 중요 사이버안전 기술산업, 사이버안전 기술의 연구개발, 응용 보급과 네트워크 기술의 지적 재산권 보호, 연구기관, 대학 및 기업이 참여하는 국가 사이버안전 기술혁신 사업을 지원한다.

한편, 중국 2015년 7월 전국인민대표회의에서 국가안전법을 제정하였고 사이버안전법 초안을 공개하고 제정을 추진 중에 있다. 국가안전법은 국가안전에 전반적인 내용을 정하면서 사이버안보에 관한 사항을 개괄적으로 포함

한다[18].

특히 사이버안보 대응에 있어서 국가는 사이버안보 관제시스템을 구축하여 국가인터넷 정보판공실은 유관기관의 사이버안보 정보수집, 분석, 통보를 총괄조정하고 경보 및 정보를 배포한다. 그리고 주요 국가시설에 대한 안전조치는 소관 분야의 사이버안보 정보수집, 분석, 통보를 총괄조정하고 경보 및 정보를 배포한다. 각 지방 인민정부의 사이버안보 관련 정보를 수집하고 필요한 정보를 배포하고 긴급대응과 조사를 실시한다. 국가안보 및 사회공공질서 보호를 위해서 네트워크 통신 제한 등의 임시조치가 가능하다. 한 예로 중국의 통치 이념에 위배된다는 이유로 트위터나 페이스북의 사용이 금지되어 있다.

6. 이스라엘

이스라엘에는 Unit 8200이라는 정보기관이 있는데 주로 통신정보 수집(SIGINT:signal Intelligence)과 암호해독 (Code decryption)을 담당하는 기관으로 국방부 소속이며 다른 이름으로는 Israeli SIGINT Natioanl Unit (ISNU)라고도 불리운다. 1952년 미군 장비를 가지고 만들어져 인원은 7000여명 정도 있다고 알려졌다. Unit 8200 산하에 Hatzav Unit이라는 조직이 있는데 이 조직은 모든 방송과 통신, 인터넷에서 공개된 정보를 수집하는데 이들이 수집한 정보가 사실상 모든 정보기관이 수집한 정보의 절반을 차지하는 중요한 기초 정보이다[19]. 대외적으로는 Unit 8200이 사이버안보를 전담하는 기관으로 알려졌다.

2014년 말, 이스라엘은 사이버방위국을 만들어서 이스라엘 국민들을 사이버공격으로부터 보호하는 임무를 맡겼다. 네타야후 총리의 명령으로 이미 이스라엘 사이버공간에 대한 테러리스트 공격에 대비하고 있으며 최고의 전

18) 박상돈, 동북아 주변국의 사이버안보 법제도 동향. 사이버평화안보포럼. 2015.11.06
19) https://en.wikipedia.org/wiki/Unit_8200

문가들로 구성하여 이스라엘 전체 사이버방위팀을 지휘하고 조정한다.

새로운 조직의 구성원들은 정부와의 계약으로 최고의 대우를 받고 근무하고 있다. 이스라엘은 전문가 영입에 있어서 아낌없이 투자한다.

모든 다른 기관들의 협력으로 단 60일 만에 성공적으로 새로운 기관을 만들었고 이는 국가의 시설만을 보호하는 것이 목적이 아니라 이스라엘 모든 국민을 보호하기 위해 만들었다. 최근 들어 이스라엘의 웹사이트들은 여기저기로부터 지속적으로 공격받고 있다.

하마스와 헤즈볼라 같은 테러리스트 그룹은 이란과 더불어 사이버테러에 많은 관심을 보이고 있다. 특히, 이란정부의 지원을 받는 해커들이 자주 사이버공격을 감행한다.

이스라엘 정보기관 신뱃트(Shin Bet)는 최근 최정예 사이버안보팀을 구성하여 이스라엘에 대한 조직적인 공격에 대응하고 있다[20]. 신뱃트 외에 모사드 역시 사이버스파이와 서비스거부 등에 대항하여 싸우고 있다. 이스라엘의 최대 적은 무슬림국가이다. 이스라엘의 최첨단 방위산업체들은 사이버스파이들의 가장 관심 있는 목표물로서 중국 정부의 지원을 받는 해커들의 침입이 빈번하다.

최근 이스라엘은 미국과 공동으로 세계 최초의 사이버무기인 '스턱스넷'을 개발하여 이란을 공격했다는 소문이 있다. 이 소문은 얼마 전에 은퇴한 가비 아쉬케나지 참모총장이 방송 인터뷰에서 자신이 근무하면서 쌓은 업적 중에 하나가 스턱스넷을 개발하여 이란의 우라늄 시설을 공격한 것이라고 밝히면서 퍼지기 시작했다.

누가 개발하였건 스턱스넷은 사이버공격에 대한 방어가 쉽지 않음을 보여주었고 할리우드 영화에서나 보듯이 발전소 전력이 끊기고 통신이 두절되는 사태가 발생 할 수 있다는 것을 보여주었다. 일단 사이버스파이행위나 서비스거부공격만 보더라도 심각한 문제가 아닐 수 없다.

20) http://www.israelnationalnews.com/News/News.aspx/185349#.VilFnn7hDIU

Ⅲ 국제 사이버안보 주요이슈

미국의 사이버보안 정보공유법, Cybersecurity Information Sharing Act(이하 CISA)이 연초 하원 통과 후에 최근 미국 상원을 통과하여 이제 CISA가 정식으로 발효되기 전까진 오바마 대통령의 결재만 남았다.

사이버보안 정보공유법(CISA)은 영향력이 막강한 구글, 페이스북, 트위터, 드롭박스 같은 기업들이 반대를 표명하고 있다. 이는 해킹과 관련된 위협첩보들을 반드시 공유해서 추가 피해를 막자는 것이 주된 내용이고 강제사항이다.

즉 관련업체가 사이버보안, 테러, 범죄 등의 위협에 대해 정부기관과 정보를 공유하는 것을 골자로 하고 있는데, 정보를 공유한 업체는 해당 사건에 대해 면책권을 주는 내용도 포함되어 있다. 하지만 정보를 공유하지 않고 어떤 사건이 발생했을 경우 책임을 물을 수도 있다는 내용이 포함됐다.

이와 같이 미국은 우리나라보다 더 민주주의 제도가 앞서고 개인의 사생활을 중요시 하는 국가인데도 불구하고 이러한 개인의 사생활 정보를 국가기관이 들여다 볼 수 있는 법안을 만들어서 국가 사이버안보를 강화하는 것을 보면 우리나라보다는 사이버안보 이슈에 대해 좀 더 심각성을 알고 있는 거 같다.

또한 2014년 소니 픽처스 해킹사건 때에도 북한의 인터넷망을 즉각적으로 공격하여 초기에 진압하는 대응태세를 전 세계에 보여 주었고 이를 통해 많은 나라에서 사이버공격에 대한 대응전략을 점검하는 계기가 되었다. 이러한 즉각적인 타격은 정확하게 공격의 진원지를 파악하고 있었기 때문이다.

특히 오바마 대통령은 취임초기부터 사이버안보에 관해서 많은 관심과 발전에 필요한 조치를 취하였다. 사이버안보보좌관 도입부터 국제법상 물리적 타격 가능성 검토까지 사이버안보에 필요한 많은 조치를 하고 있고 최근 중국의 시진핑 주석 방문시에는 서로 사이버공간에서의 산업스파이활동을 금하자고 약속했다[21]. 그러나 많은 외교적 노력에도 불구하고 이러한 약속이 현실세계에서 얼마나 효력이 있을지는 알 수 없다.

두 정상이 만나기 전까지 국토안보부 (DHS)의 지원을 받은 FBI가 5년간 중국 해커들의 사이버접근을 감시한 것은 얼마나 미국 정부가 사이버안보에 관심을 갖고 있는지 알 수 있다[22].

중국은 사이버안보를 위해 20여 년 전부터 소프트웨어, 하드웨어 그리고 네트워크를 자국산으로 개발하여 사용해 오고 있다. 그리고 PC의 운영체제를 리눅스 기반의 '기린'이라는 시스템을 만들어 사용한다. 모든 IT장비나 소프트웨어가 자국산이니 그만큼 사이버보안이 철저하게 이루어지는 것이다[23].

그리고 중국이 미국 등 다른 나라를 공격하고 있다는 보고는 많이 있으나 중국이 공격을 당했다는 소식은 많이 들을 수 없다. 파이어아이의 보고서에 의하면 중국이 한번 공격을 당하면 공격진원지는 사이버 인해전술로 마비 될 것이라는 추정도 있다[24].

일본의 사이버안보 차원에서 내년 1월부터 한국의 주민등록제도와 비슷한 '마이넘버' 제도를 도입한다. 그리고 더욱 안전한 개인정보 보호를 위해 망분리가 민간영역으로 확대 보급 될 것이다. 망분리는 인터넷을 통해 유입되는 위협을 차단 할 수 있다[25]. 일본은 다른 나라보다 사생활을 중요시 하는 나라이기에 망분리 솔루션을 통해 개인정보 보호에 만전을 다 할 것으로 예측된다.

일본은 국가적 차원에서는 국제컨퍼런스를 주최하여 세계 여러 국가들의 전문가들을 초청하여 정기적으로 필요한 정보를 수집하고 이에 따라 법과 정책을 바꾸면서 국제사회 일원으로 역할을 제대로 하고 있다. 최근에는 오키나와에서 사이버3 컨퍼런스를 개최하였는데 미국의 전직 NSA국장을 비롯하여 세계적인 고위급 인사들이 참여하여 변화하는 사이버안보 이슈에 대해

21) http://biz.chosun.com/site/data/html_dir/2015/09/26/2015092600292.html
22) http://www.boannews.com/media/view.asp?idx=48443&kind=3
23) http://news.joins.com/article/19043775
24) http://www.dt.co.kr/contents.html?article_no=2014012802019960800001
25) http://www.datanet.co.kr/news/articleView.html?idxno=94246

의견을 교환했다[26]. 일본의 사이버안보 정책은 외부로 많이 알리는 것보다는 내실을 기하는 방향으로 조용히 이루어진다.

독일은 중국과 경제스파이 방지를 위한 해킹금지 협약에 사인했다. 이는 중국과 미국, 영국의 협약에 이은 것이다[27].

독일의 메르켈 총리는 시진핑 중국주석과의 대화 후에 기자들에게 "독일은 협약 체결을 위해 아주 신속하게 이루어졌다"라고 말했다. 독일은 유럽에서 중국의 가장 큰 사업 파트너이다.

베를린에 소재한 유럽 경영기술 대학원의 사이버보안 전문가인 산드로 게이큰은 이번 체결로 인한 독일 사업의 전망을 설명했다.

독일은 아주 매력적인 공격 목표이다. 왜냐하면 독일중소기업 미텔 슈탄트(Mittelstand)의 경영혁신들이 IT 보안에 취약한 상태로 있었기 때문이다.

중국은 항상 상업적인 절도행각에 대한 혐의에 대해서 부인하지만 아주 적은 수의 전문가들만 믿는다. 중국의 인민해방군을 통해 큰 규모의 해킹을 일삼고 있으며 산업용 악성소프트웨어도 생산하고 있다.

공격 목표는 외국정부, NGO, 사회운동가와 최첨단 회사들(특히나 항공이나 방위사업권을 가진 회사들) 이다.

중국 관리가 말하기를 "우리는 독일과 함께 산업스파이와 사이버범죄에 대항하여 싸울 것이다. 우리는 사이버절도나 무역기밀절도행위를 비난한다"[28]고 전했다.

독일과 중국의 협약은 경제스파이에만 국한되고 통신정보나 외교해킹 그리고 국가안보 목표에 대한 것은 포함되지 않는다. 이는 중국과 미국의 협약에서와 같다.

최근 The Süddeutsche Zeitung의하면, 독일 정보기관 BND는 전략기

26) http://www.yonhapnews.co.kr/bulletin/2015/10/07/0200000000AKR20151007172000009.HTML?input=1195m
27) http://www.theregister.co.uk/2015/10/30/china_germany_no_hack_pact/
28) http://www.theregister.co.uk/2015/10/30/china_germany_no_hack_pact/

술계획를 추진하기 위해 3억 유로 예산을 구하고 있다. 그중 450만 유로는 SSL and HTTPS 안에 있는 컴퓨터 버그를 찾아내는데 사용된다.

독일 정보기관 (BND)가 찾고 있는 제로데이버그[29]는 버그를 고치기 위해서가 아니라 버그를 강탈하기 위함이다. 그래서 많은 NGO와 저작권 침해자 그리고 CCC(컴퓨터 혼돈 그룹)같은 그룹들은 정부의 의도를 비난한다. 독일 저작권 침해자 대표 코너 (Körner)는 사람들이 사이버테러보다 정부를 더 무서워 할 것이라고 주장한다. 그는 이 전략에 대해서 정부는 회색시장 보안 취약성을 위해서 예산을 사용하면 안된다고 반대했다.

더크 일그링 CCC대표는 이러한 제안이 독일 경제에 악영향을 끼칠 것이라고 주장했다. The Süddeutsche Zeitung 리포트에 의하면 심각한 리스크는 범죄자들이 범죄를 저지르기 위해서 블랙마켓에서 제로데이를 구입하는데 있다고 전한다.

독일 BND의 제안은 미국 NSA가 최근에 발표한 것과는 대조되는데 NSA는 모든 버그들은 찾아내어 고칠 수 있다고 전했다. 독일 BND는 이와는 별도로 110만 유로를 하니팟[30]을 만들기 위해 필요하다고 하는데 사회관계망 분석에는 좀 이르다. 시험 프로그램을 올해 6월에 마쳤다.

29) 운영체제(OS)나 네트워크 장비 등 핵심 시스템의 보안 취약점이 발견된 뒤 이를 막을 수 있는 패치가 발표되기도 전에, 그 취약점을 이용한 악성코드나 프로그램을 제작하여 공격을 감행하는 수법이다. 이런 경우, 별도의 대처방안이 없기 때문에, 가공할만한 피해를 발생할 수 있다는 점에서 그동안 보안 전문가들이 가장 우려해왔던 보안 위협이다. 최초의 제로데이 공격은 2005년 12월 28일 MS 그래픽처리엔진의 윈도메타파일(WMF) 취약점이 공개되자마자 발생했다. 취약적 노출 후 24시간도 지나지 않아 이 취약점을 이용한 악성 파일이 등장한 것이다.

30) 컴퓨터 프로그램에 침입한 스팸과 컴퓨터바이러스, 크래커를 탐지하는 가상컴퓨터이다. 침입자를 속이는 최신 침입탐지기법으로 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 한다. 크래커를 유인하는 함정을 꿀단지에 비유한 것에서 명칭이 유래한다. 1990년대 중반 미국 매사추세츠공과대학교수 데이비드 클록(David Clock)이 처음 제안한 뒤, 1999년 선마이크로시스템스의 컴퓨터 보안전문가인 랜스 스피츠너(Lance Spitzner)와 2002년 소프트웨어 제조회사 사익(SAIC:Science Applications International Corporation)이 실제 프로젝트를 시행하였다. 침입자를 오래 머물게 하여 추적이 가능하므로 능동적으로 방어할 수 있고, 침입자의 공격을 차단할 수 있다는 장점이 많이 활용되고 있다.

이스라엘은 유대인 국가의 생존권을 용납하지 않은 이란과 이슬람 극단주의 등으로부터 사이버공격에 맞설 수 있는 최첨단 방어망을 구축하는 한편 민간기업들을 사이버범죄 등으로부터 보호하는 소프트웨어 및 시스템을 개발하고 세계 정보보안시장을 이끌고 있다.

이스라엘 대테러 국제연구소의 보아즈에 의하면, 팔레스타인의 하마스가 최근 사이버 전담부대를 신설했다. 레바논의 시아파 조직 헤즈볼라는 이란에서 사이버 기술 지원을 받고 있을 가능성이 크다고 했다. 이스라엘 고위관계자에 따르면 하마스등은 무력도발과 동시에 사이버도발도 감행할 가능성이 커졌다고 전하면서 이 같은 하이브리드 공격의 수법은 세계 각지에서 무장세대교체가 진행되어 앞으로는 자살폭탄 테러보다 사이버테러가 더 상행하게 될 것이라고 전망했다.

최근 들어 IS가 소셜 네트워크를 통해 그들의 지하드운동을 선전하고 젊은이들을 모집하고 테러를 독려하는 것을 비롯하여 조만간 실질적인 사이버테러를 감행 할 것이라는 예측이 나오고 있다. 그러므로 서방 연합국은 IS의 사이버테러 공격에 대비하여 준비 중에 있다.

Ⅳ 결 론

주요 국가의 사이버안보 대응체계를 연구를 통해 각국의 사이버안보 전략의 특성 및 공통점을 찾게 되었다. 미국 NSA 국장 마이클 로저스 제독의 계획에서 보듯이 모든 사이버안보 업무의 민간 아웃소싱, 영국 GCHQ의 대학생 교육 프로그램, 이스라엘의 UNIT8200 프로그램, 중국의 대학 및 연구기관 지원 프로그램 등 모든 프로그램의 중심에는 사람과 교육 그리고 협력이 있다.

이는 아무리 첨단기술을 이용하여 공격과 방어를 행하는 사이버공간이라도 사람의 통제 없이는 아무것도 이루어지지 않기 때문이다. 세계 여러 국가들은 정부기관의 자원만으로는 사이버공격에 적절히 대응할 수 없음을 인지

하고 민관협력을 강화하는 길을 모색하고 있다. 또한 정부가 가지고 있는 사이버 감시체제를 민간에서도 사용할 수 있게 하자는 것이 추세이다. 왜냐하면 대부분의 사이버공격의 목표는 민간시설에 집중되어 있기 때문이다. 만약 국가가 사이버안보에 관하여 독점권을 가지고 활동 한다면 효율성에 있어서도 많이 뒤처진다. 특정한 기업의 환경을 모르기에 어떠한 곳에 취약점이 있는지도 잘 알지 못하기 때문이다. 그러므로 국가주도의 사이버안보 정책에서 민관협력의 사이버안보 정책으로의 전환과 그에 알맞은 전략적인 변화 또한 필요하다.

한국은 지구상에서 미국과 함께 가장 사이버공격을 많이 받는 나라중 하나이고 북한으로부터 사이버공격을 지속적으로 받고 있음에도 불구하고 사이버안보에 실질적으로 필요한 법률 제정의 어려움을 겪고 있다.

우리나라같이 주적의 개념이 확실한 나라는 얼마 되지 않는다. 그럼에도 불구하고 우리나라의 사이버안보 대응체계는 제대로 작동 할 수 있는 법적인 토대가 마련되어 있지 않아서 이제까지 발생한 것보다 더 심각한 수준의 사이버공격을 받을 시에 제대로 대응 할 수 있을 지 염려가 된다.

지금 세계는 방어위주의 사이버 대응에서 공격위주의 대응으로 전환하고 있고 나아가서는 물리적인 타격까지도 고려하고 있다. 그리고 스턱스넷 같은 사이버 무기제작에도 많은 투자를 하고 있다. 북한같이 사이버공격같은 비대칭전력을 선호하는 나라에서는 이미 스턱스넷과 유사한 웜바이러스를 만들고 있을지도 모른다.

사이버전에 있어서 방어 후 타격은 거의 불가능하다. 사실상 공격 받은 목표는 이미 피해를 입은 것이기 때문이다. 그러므로 선제적이고 적극적인 감시활동이 필요하다. 이를 실현하기 위해서는 민관협력은 기본이고 이를 뒷받침 해주는 법률적 지원이 있어야만 가능하다. 다른 선진국에서 민관협력이 쉽지 않았으나 법률적으로 그들의 자산을 보호해주면서 사이버안보활동 참여를 독려함으로써 일부 반대에도 불구하고 국가안보 수호라는 공공의 목적을 실현하기 위해 노력하고 있다.

사이버안보 입법환경 변화에 따른 입법전략

김 재 광*

목 차

* 선문대학교 경찰행정법학과 교수

I 머리말

서울 지하철 1-4호선을 운영하는 서울메트로의 핵심 컴퓨터 서버를 북한으로 추정되는 사이버테러 조직이 해킹해 최소 5개월 이상 장악했던 사실이 뒤늦게 밝혀졌다고 조선일보가 2015년 10월 5일자로 보도했다. 이 보도가 사실일 경우 서울시민 420만명이 매일 이용하는 서울메트로의 지하철 2000량이 테러의 위험에 장기간 노출된 셈이어서 논란이 예상된다.[1)]

위의 사례에서 보듯 우리나라는 북한의 사이버테러, 각국 범죄단체의 사이버범죄 등 다면적인 안보 위협에 노출되어 있으며 정부에 대한 직접적 공격 외에 민간 IT인프라 해킹 등이 지속적으로 이루어지고 있다.[2)] 국가 및 공공기관을 대상으로 한 사이버 테러는 매년 수만 건씩 발생해 2010년부터 2014년까지 최근 5년간 약 7만6천여 건의 사고가 발생한 것으로 나타났다.[3)] 또한 아래 표에서 보는 바와 같이 세계적으로도 사이버공격 사례가 증가하고 있으며 그에 대한 대응 또한 강경해지고 있다. 그 이유는 사이버전쟁은 선전포고도 없이 가상의 적국을 초토화시킬 수 있기 때문에 군사시설은 물론이고 전력, 통신, 금융망, 송유, 가스, 수도관 등 한 나라의 주요 기반시설을 순식간에 마비시킬 수 있다. 핵 공격 못지않게 더 큰 피해를 초래할 수 있는 것이 바로 사이버공격이기 때문이다.

1) 한국경제신문 2015년 10월 5일자 “북한 추정 사이버테러 조직, 서울메트로 서버 5개월 간 장악” 기사 참조
2) 사이버안보 위협이 지속적으로 늘어나고 있는데, 시만텍자료(2013년 보고서[1)])에 따르면 1인당 사이버범죄로 인한 금전피해가 2012년 197달러에서 2013년 208달러로 약 50% 증가하였고, 전 세계 사이버범죄 피해비용 역시 2012년 1,110억 달러에서 2013년 1,130억 달러로 증가하였다. 사이버위협이 범죄 단계를 넘어서 국가안보에 대한 위협이 될 수 있는 수준으로 증가하고 있다. 배병환송은지, 주요국 사이버보안 전략 비교 분석 및 시사점, 2014. 11. 17 참조
3) 쿠키뉴스 2015년 5월 22일자 “범정부 차원의 사이버테러 대응 컨트롤타워 구축 추진” 기사 참조

[세계 주요 사이버공격 사례]

시기	내용	
2015년	중국 → 미국	인사관리처 해킹으로 공무원 2,150만명 신상 유출[4]
2014년	러시아 → 미국	백악관 전산망에 침입해 오바마 일정 정보에 접근
2014년	북한 → 미국 미국 → 북한	소니픽쳐서 사이트를 공격해 정보를 유출하고 협박 노동신문 등 주요사이트를 마비시키는 보복조치
2012년	이란 → 미국 이란 → 친미국가	미국 금융회사의 이스라엘 정부에 대한 공격 사우디, 카타르 등 국영기업에 대한 악성코드 공격
2010년	이스라엘 → 이란	사이버미사일 '스턱스넷' 공격으로 핵시설 파괴[5]
2008년	러시아 → 조지아	물리전과 연계해 정부, 금융, 방송사이트 공격
2007년	러시아 → 에스토니아	디도스 공격으로 국가 전체 인터넷 2주간 마비

출처: 손영동, 사이버전 대응태세, 무엇이 문제인가, 2015. 9. 16

사이버안보 관련법령들에 대한 입법이 전혀 진전이 없는 우리나라와는 달리 미국과 일본 등 선진국가들은 사이버안보 관련법령들을 체계적으로 정비하여 사이버테러, 사이버공격에 효과적으로 대응할 수 있는 법제도적 기반을 구축하고 있다.

소프트웨어 얼라이언스(이하 BSA, www.bsa.org)가 사이버테러 문제가

4) 2003년 8월14일 미국은 대규모 정전사태를 맞았다. 미 동북부와 중서부 7개주, 그리고 캐나다 온타리오 주가 암흑으로 변했다. 이 정전으로 22곳의 원전이 멈추었다. 10개 이상의 공항이 폐쇄되고 지하철이 마비됐다. 인터넷과 전자제품은 모두 먹통이 됐다. 이런 사태가 무려 3일 동안 지속되면서 발생한 경제 손실은 60여억 달러. 직접적인 피해를 입은 주민만 5000만에 달했다. 미국은 당시 사이버공격의 주범으로 중국을 지목했다. 중국의 사이버부대가 미국의 컴퓨터에 침입해 전력관리시스템을 공격했다는 것이다. 전기가 흐르는 한 바이러스는 침투와 복제를 멈추지 않는다. 다른 말이 아니다. 사이버공격을 100% 차단할 방법은 아직까지는 없다는 것이다.

5) 이란의 핵시설에 '스턱스넷' 공격을 가해 단순히 자료를 지우거나 빼내는 수준을 넘어 원심분리기 시설 자체를 못 쓰게 파괴한 것을 계기로, 사이버전쟁의 위협은 새로운 차원으로 접어들어 핵전쟁 위협 수준을 보이고 있다. 세계가 직면한 사이버안보 위협은 핵위협을 대체하는 게 아니라 핵위협과 결합하는 양상마저 보이고 있다. 연합뉴스 2015년 10월 15일자 "세계적 사이버안보 위협 통제위해 사이버군비 정보공개해야" 기사 참조

세계 각국의 중요한 이슈로서 부각되고 있는 가운데 아태지역 국가들의 사이버보안 실태를 조사한 “APAC 사이버보안 실태 보고서(Asia-Pacific Cybersecurity Dashboard)”를 발표했다. 한국의 경우 국가보안에 초점을 두고 있어 ‘보안’보다는 ‘방어’에 가까운 사이버보안 전략을 취하고 있는 것으로 분석됐다. 또한 체계적인 민관 사이버보안 협력 시스템도 미흡한 것으로 조사됐다. 보고서에 따르면, “한국과 중국의 경우 사이버보안에 대한 국제적 접근 방식에 반하는, 고립된 자체 표준평가인증 제도가 오히려 효율적인 사이버보안 전략 수립에 걸림돌이 되고 있다. 한국과 중국, 말레이시아, 베트남의 등의 국가는 임시방편의 대응책은 가지고 있으나 국가 수준의 포괄적인 사이버보안 정책 기반은 아직 개발 중인 상태이다.[6]” 결론적으로 국가 수준의 포괄적인 사이버보안정책 기반이 부족하다는 평가이다.

우리를 둘러싸고 있는 사이버안보환경도 급변하고 있다. 우리의 인접국가인 중국, 북한, 일본 등은 사이버전력을 지속적으로 증원하고 있다. 또한 IoT, 빅데이터, 클라우드컴퓨팅으로 대표되는 초연결사회의 도래는 사이버안보 법정책적 전환을 강력히 요구하고 있다. 더군다나 사이버안보입법의 프라이버시 참해가능성에 대한 우려 때문에 개인정보보호에 터잡은 사이버안보입법을 요구하는 목소리가 높아져 가고 있다.

따라서 사이버안보입법은 이러한 엄중한 법현실을 고려하여 추진되어야 한다. 또한 사이버안보입법은 국가안보에 관한 사항이기 때문에 초당적 협력이 요청된다. 그런 측면에서 사이버안보에 대해 초당적으로 대처하고 있는 미국의회의 자세는 시사하는 바가 크다. 이러한 입법환경이 20년 가까이 일관성 있게 사이버안보정책을 추진한 원동력이라고 생각한다.

이 글은 이러한 문제인식을 가지고 지금까지 추진되었던 사이버안보 관련법안에 대한 검토와 함께 앞으로의 입법전망을 모색하는데 목적을 두고 있다.

6) K・BENCH 2015년 10월 8일자 “BSA, 아태지역 사이버보안 실태 보고서 발표” 기사 참조

Ⅱ 우리나라와 인접한 주요 국가의 사이버안보 법정책

미국은 국토안보법을 필두로 사이버안보와 관련한 법규를 체계적으로 정비하고 있다. 일본은 2014년 11월 사이버안보기본법을 제정해 후속 정책 마련에 분주하다. 중국은 지난 7월 시행한 신(新)국가안전법에 사이버주권 수호를 명시했고 사이버 통제를 강화하는 포괄적 사이버안보법을 올해 안에 통과시킬 예정이다. 이렇듯 미국·일본을 비롯한 여러 국가는 사이버안보라는 분명한 틀 아래에서 국가조직 기능 강화와 체제 확충이 이루어지고 있으며 민간부문과 연계도 강조되고 있다. 기본법을 구체적으로 시행하기 위한 지침이 마련돼 각 정부기관이 취해야 할 대응방안을 명확히 제시하고 있다. 이에 비해 우리는 총력전 개념에 입각한 통합방위법에 사이버영역이 포함돼 있지도 않다. 사이버테러방지법 제정은 유명무실한 상태고 통신비밀보호법 개정도 계류 중이다. 개인정보보호는 상대적으로 강화돼 기업들이 사업하기 어렵다고 토로하는 단계까지 왔지만, 국가 사이버안보와 관련해서는 대통령 훈령인 「국가사이버안전관리규정」이 전부다.[7)]

1. 중국

(1) 사이버안보 정책

중국은 미국에 버금가는 사이버안보 역량을 갖추기 위해 많은 투자를 하였다. 인민해방군은 1997년 “악성코드 침투가 원자폭탄보다 효율적”이라는 내용의 보고서를 중앙군사위원회에 제출했다. 이후 위원회 직속의 컴퓨터 바이러스 부대, 사이버공격 및 정보교란 모의훈련을 주된 임무로 하는 넷포스(Net Force), 베이징, 광저우, 지난, 난징 등 4대 군구 산하에 전자전 부대를 잇달아 창설했다. 2010년 7월 전 군의 사이버 관련 전략·정보기구를 창

7) 전자신문 2015년 8월 11일자 “[손영동의 사이버세상]<5>사이버 법제조차 없는 디지털 강국” 기사 참조

설했다. 특히 자국의 컴퓨터 영재뿐만 아니라 미국에서 유학한 고급 인재를 파격적인 조건으로 채용해 편제에도 없는 사이버특수부대에 배치하고 있다.

서방 선진국들이 중국을 두려워하는 것은 이들 사이버부대만이 아니다. '홍커(red hacker)'라 불리는 150만 명에 달하는 민간 해커가 있다. 이들은 정부의 통제를 거의 받지 않기 때문에 더욱 공격적이고 무차별적인 해킹을 감행한다. 맹목적이라 싶을 정도의 애국심으로 무장하고 미국, 일본, 한국을 비롯한 전 세계 정부나 기업, 개인까지 타깃이 된다. 중국 공산당은 이같은 홍커의 행동에 대하여 자국 내 사이트를 공격하지 않는한 처벌하지 않는 것으로 알려져 있다. 미국은 중국 정부가 프리랜서 해커들을 직간접적인 국가통제 아래에 두면서 민간 해커들의 애국적 해킹활동을 조장한다고 보고 있다. 이에 반해 중국은 미국 정보기관이 나서서 대놓고 사이버감청을 하고 자국의 사이버정책에 쓸데없이 관여한다며 불쾌감을 감추지 않고 있다.

2014년 10월 중앙군사위원회는 '군 정보보안 강화안'을 발표했다. 강화안은 군 정보보안을 위해 전 군과 무력경찰부대가 따라야 할 지도사상, 기본원칙, 보장정책 등을 제안하면서 정보보안이 군에 있어서 기본적인 사항으로 간주되어야 함을 강조하고 있다. 주요내용은 ‣전 분야에 걸친 정보보안의 총체적인 설계와 종합적인 관리, ‣정보보안 강화작업은 필수적 요소로 사이버강군의 임무와 군사투쟁을 위하 돌발상황 대처, ‣정보보안의 보안등급 뷴류와 위협 평가의 전면적 시행 등이다.[8]

(2) 최근의 사이버안보 입법 동향

1) 사이버보안법안

2015년 7월 중국 전국인민대표회의(전인대)는 사이버상에서의 공격과 범죄, 유해정보 확산 위협으로부터 사이버주권과 국가안보를 수호하기 위한 「사이버보안법」 초안을 마련했다. 초안은 중국내 모든 분야의 네트워크를 대상으로 정부, 기관, 기업, 개인이 이행해야 할 역할과 의무를 담고 있다. 또한

8) 손영동, 사이버전 대응태세, 무엇이 문제인가, 2015. 9. 16 참조

공공질서를 파괴하는 사이버위협 발생시 인터넷 접속을 차단하는 방안이 명시됐다.[9)]

2) 국가안전법의 제정

중국이 지난 7월 1일 새로운 「국가안전법」 제정을 계기로 온라인과 정보보안 능력을 키울 것이라는 관측이 나오고 있다. 새 국가안전법은 7월 6일부터 시행에 들어갔다. 새로운 「국가안전법」은 지난 1993년 제정된 기존 국가안전법의 대체입법이다.

모두 7장으로 이뤄진 새 「국가안전법」은 정치 안전, 국토 안전, 군사 안전, 문화 안전, 과학기술 안전 등 11개 영역에서 국가 안전을 수호하는 것에 관한 임무와 책임을 규정했다. 또 국가안전 제도, 국가안전 보장, 국민과 조직의 의무와 권리 등을 명시하고 있다.

이 법은 국가는 국가안전의 수호를 위해 자주 창신 능력 건설을 강화해야 하며, 자주적으로 통제 가능한 전략적 첨단 신기술, 중요한 영역의 핵심기술의 발전을 가속화해야 한다고 요구했다. 새 국가안전법은 또 지식재산권의 운용, 보호 및 과학기술 비밀보호 능력 건설을 강화하고, 중대한 기술과 공정의 안전을 보장해야 한다고 강조했다. 제정이유로는 현대 국가의 안보는 엄중한 위협과 도전에 직면하고 있고, 특히 테러와 사이버 해킹 등 예측 불가능한 영역에서 (안보)위협이 더욱 커지고 있다는 것을 들 수 있다. 새 국가안전법이 '사이버 안전' 강화에 중점을 뒀다는 것이 일반적인 평가이다.

실제로 새 「국가안전법」은 국가가 네트워크와 정보 안전을 보장하는 체계를 구축하고, 네트워크와 정보안전 보호 능력을 향상시키며, 네트워크와 정보기술의 혁신 연구・개발 응용을 강화해야 한다고 명시했다. 새 법은 또 네트워크와 정보 핵심기술, 핵심 기초시설과 중요 영역 정보시스템 및 데이터의 안전에 대한 통제 가능성을 실현해야 한다고 강조했다.

하지만 중국 일각에서는 새 「국가안전법」이 국가안보 적용 범위를 크게 넓

9) 손영동, 사이버전 대응태세, 무엇이 문제인가, 2015. 9. 16 참조

힌 까닭에 사회에 전방위적인 통제를 가할 것이란 우려도 나오고 있다. 지난 1993년에 제정된 「국가안전법」은 안보 위협의 범위와 법 적용 범위를 국가 전복과 분열 선동, 매국 행위, 국가기밀 누설 등으로 규정했다. 그러나 새 국가안전법은 이 범위를 경제, 금융, 문화, 인터넷, 식량, 에너지, 종교, 우주, 심해, 극지방 등으로까지 넓혔다.[10]

2. 일본

(1) 사이버안보 정책

미국의 사이버정책에 가장 적극적으로 호응하는 나라가 일본이다. 2013년 10월 미-일 안전보장협의회에서 사이버국방분야 협력에 관한 양해각서를 교환했다. 2015년 4월 아베 신조 일본 수상은 미 상하 양원 합동연설을 하고 미-일 방위협력을 위한 지침, 이른바 '가이드라인 2015'를 공동 발표했다. '가이드라인 2015'는 아태지역 안보에 대한 공동의 목표와 대응방식을 담고 있는데, 종전의 가이드라인에 비해 미-일동맹의 연합작전 태세를 한층 강화했다. 특히 상호 협력범위를 아태지역을 넘어 글로벌로 확장했고, 우주 및 사이버공간을 포함시켰다. 이로써 일본 역할이 나토동맹에서의 영국, 프랑스, 독일과 비슷한 수준으로 올라갔다. 그간 미국은 사이버방어를 둘러싼 국제적 규범을 서두르면서 일본의 동참을 호소해 왔고, 해외로부터 해킹 공격에 시달려온 일본도 미국의 협조를 요청하고 있다.

2012년 9월 신카쿠(중국명 다오위다오) 국유화 이후 국회를 비롯한 정부, 금융기관, 무기개발업체에 대한 해킹이 더욱 거세지고 있다. 2015년 5월 최대 규모의 해킹 공격으로 연금기구의 정보시스템에서 125만명의 신상정보가 유출되기도 했다. 이에 일본은 경찰청에서 담당해오던 사이버수사를 대폭 강화함과 동시에 국가 주요시설에 대한 대응을 자위대 수준으로 끌어올렸다.

10) 보안뉴스 2015년 7월 6일자 "中 새 '국가안전법' 제정..."정보보안 능력 키울 것" 기사 참조

일본이 사이버테러 대응조직을 만든 건 2000년 1월 16개 정부기관 사이트가 중국 해커들에게 마비된 사건이 계기가 됐다. 이후 사이버방어 조직을 꾸준히 증강시켜오다 2014년 3월 자위대 예하에 사이버공간방위대를 창설했다. 방위대는 100명 규모의 적은 인원으로 발족했지만 예산은 무려 212억 엔(약 2,000억원)에 달한다.[11]

일본정부는 2013년 6월 11일에 종전의 '국민을 지키는 정보시큐리티 전략'을 대신할 새로운 국가전략으로서 '사이버시큐리티 전략'을 결정하였다. 이 전략은 2013년부터 2015년을 대상기간으로 하며 사이버공간의 확대에 따라 리스크도 점차 확대되고 국제화되고 있는 추세에 대응하기 위한전략을 제시하고 있다.[12]

일본 사이버공간의 환경이 급속하게 변화함에 따라 새로운 전략의 수립이 필요하다고 보았다. 사이버공간은 다양한 정보 등이 유통되는 가상의 공간으로 급속하게 확대되고 있으며 실생활에도 급속하게 침투하고 있다. 이에 따라 사이버공간과 실공간이 '융합・일체화'가이루어지고 있으며 글로벌화되고 있는 상황이다. 이에 따라 사이버공간에서 발생하는 리스크도 점차 심각해지고 있으며 그 확산속도도 매우 빠르다. 또한 사이버공간이 점차 글로벌화됨에 따라 리스크도 글로벌화되는 등 문제점도 더욱 심각해지고 있다. 일본정부는 이러한 환경에 적절하게 대응하여 ① 강인한 사이버공간의 구축, ② 활력있는 사이버공간의 구축, ③ 세계를 솔선하는 사이버공간의 구축을 통해 '사이버시큐리티 입국'의 실현을 목적으로 새로운 정책을 제시하고 있다.

국가는 사이버공간에 관한 국가의 기본적 기능을 강화하는 것이 필요하다. 국외로부터의 사이버공격등에 대응하여 사이버공간의 방위 및 사이버공간의 범죄대책등을 마련하는 것이 필요하다. 또한 스스로 정보시스템을 운용하는

11) 손영동, 사이버전 대응태세, 무엇이 문제인가, 2015. 9. 16 참조
12) 곽관훈, "최근 일본의 사이버안보 관련법령 현황과 시사점"「사이버 안보위협 대응전략의 법정책적 검토 및 전망」2013년 한국사이버안보법정책학회 월례세미나 발제문, 2013. 12. 17, 11쪽 이하 참조

주체로서 정부기관 및 공공기관의 시큐리티를 강화하기 위한 조치를 취할 필요가 있다.

(2) 최근의 사이버안보 입법 동향: 「사이버시큐리티기본법」의 제정

2014년 11월 사이버안보를 위한 주체별 책임을 규정한 「사이버시큐리티기본법」을 제정했다. 일본은 사이버안보 분야의 기본법으로서 「사이버시큐리티기본법」을 제정하여 시행함으로써 사이버안보를 강화하고 있다.

일본의 「사이버시큐리티기본법」은 사이버시큐리티 관련 시책 추진의 기본이념과 각 주체별 사이버시큐리티 확보의 책무를 정하고 있다. 또한 정부가 사이버시큐리티전략을 수립하도록 하고, 내각에 사이버시큐리티전략본부를 두면서 내각관방이 그 사무를 처리하도록 하는 추진체계를 정립하였다. 「사이버시큐리티기본법」은 그밖에도 사이버시큐리티의 강화에 필요한 다양한 조치들을 정하고 있다. 「사이버시큐리티기본법」은 사이버안보 분야의 기본법이 제정되었다는 점, 연성규범에 대한 의존도를 감소시키고 법치국가원리를 준수한다는 점, 기본 이념에 바탕한 범국가적 사이버안보 추진의 법적 근거를 마련하였다는 점, 사이버안보 총괄기구의 위상을 높이고 이를 법제화하였다는 점, 사이버안보 강화 활동의 투명성을 확보하여 일반 국민의 참여 여건을 조성하였다는 점, 사이버안보 국제질서 형성에 대한 적극적인 참여를 선언하였다는 점 등에서 큰 의미가 있다. 「사이버시큐리티기본법」은 한국의 사이버안보 관련 입법활동에 중요한 참고대상이 될 것으로 보인다.[13]

3. 북한

북한의 사이버전 능력은 세계 최고수준인 미국에 버금간다는 평가를 받는다. 북한은 1990년대부터 사이버전 역량을 축적해왔다. 경제난으로 재래식 전력 증강에 어려움을 겪자 적은 비용으로 큰 효과를 낼 수 있는 사이버 전력

13) 박상돈, "일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점을 중심으로" 「경희법학」 50권 2호(경희대 법학연구소, 2015), 초록 참조

강화에 박차를 가했다. 2003년 이라크 전쟁 당시 미국이 지휘통제자동화시스템을 통해 소수 인력으로 이라크군 전체를 무력화시키자, 북한은 더 심혈을 기울여 사이버전 능력 배양에 집중하고 있는 것으로 알려졌다. 김정일 국방위원장은 생전인 2005년 "현대전은 전자전이다. 전자전을 어떻게 하느냐에 따라 승패가 좌우된다"고 강조하기도 했다. 현재 우리 군이 파악하고 있는 북한군 사이버 전사는 5900여명이다. 일각에선 1만2000명이 넘는다는 말도 나온다. 즉, 이미 12,000여 명의 해커부대를 운용하고 있고, 연구기관까지 합치면 30,000여 명의 사이버전사를 보유해 역량이 미국 중앙정보국(CIA)수준에 필적한다는 평가도 있다.

북한은 우리나라 초등학교에 해당하는 인민학교의 영재들을 발탁해 금성 1,2학교에서 매년 500시간 컴퓨터 전문교육을 실시한다. 이들 가운데 우수한 학생들은 총참모부산하 지휘자동화대학(전 미림대학)이나 김책공과대학 등에서 전문교육을 받는다. 지휘자동화대학 한 곳을 통해서만 매년 100여명의 사이버전사들이 배출된다. 바로 이들이 인민군 정찰총국에 배치돼 사이버전을 전담한다. 정찰총국 산하 '전자정찰국(121국)' 소속의 해커 500~1,000명이 남한 군・전략기관에 대한 해킹과 바이러스・악성코드 유포를 도맡아 한다. 100명으로 편제된 사이버 심리전부대 '적공국 204호'는 남한 시민들을 대상으로 심리전을 수행하고 있는 것으로 알려졌다. 김정은 노동당 제1비서는 아버지 김 위원장 유지를 이어받아 지난해 8월 전략사이버사령부를 신설하라고 명령한 것으로 알려졌다. 우리 군은 아직 이 사령부의 활동내용은 밝혀내지 못하고 있다.[14]

북한은 사이버 공간에서의 방어와 분열, 불법 이용에 집중하고 있다. 사이버 간첩행위, 전산망 공격, 역정보의 유통 등이 북한 사이버 전략의 핵심이다. 북한의 사이버공격은 정보기술 연결에 취약한 다른 우월한 적들에 대한

14) 최현수, "[세계는 사이버 전쟁중] 北 사이버전 능력 세계최고 수준… 南보다 한수 위", 국민일보 2014년 11월 25일자 기사 참조

비대칭전력[15]이다. 적들의 즉각적인 무력 대응을 유발할 가능성도 낮다. 북한이 출처라는 사실이 밝혀질 즈음이면 이미 흔적은 사라질 수밖에 없다.[16]

북한의 사이버공격은 자신들의 능력을 검증하기 위해 수시로 실전 훈련 형태로 진행돼 온 것으로 파악되고 있다. 이들은 한국군을 상대로 하는 것이 특징이며, 군사정보 수집과 해킹, 허위정보 확산 등 사이버 심리전을 담당하고 있다.

국군 사이버사령부가 공개한 자료에 따르면 2009~2013년 기간 동안 북한의 대남 사이버 공격으로 발생한 피해액만 8,600억 원이라고 한다. 북한은 특히 우리 군(軍)을 대상으로 홈페이지 공격, 악성코드 유포, 해킹메일 발송 등의 방법으로 2010년부터 총 6,392건의 사이버 공격을 감행한 것으로 드러났다.[17]

최근 북한의 대남도발 양상은 중국 공산당의 군사교리를 모방한 '점혈전략'(點穴戰略)이다. 인간으로 치면 인체의 급소가 되는 '점'(點)을 공략해 상대방을 무력화시키는 전략이다. 가장 많이 적용되고 있는 분야는 역시 사이

15) 일반적으로 전쟁에 이용되는 전력은 대칭전력과 비대칭전력을 나뉘는데, 비대칭전력은 핵무기・생화학무기・탄도미사일 등 대량살상이 가능한 무기를 포함한 땅굴로 침투하는 무장공비・잠수함 등을 통한 기습공격, 게릴라와 같은 비정규군 등의 전력을 말한다. 반면 대칭전력은 탱크, 전차, 군함, 전투기, 포, 미사일, 총 등 실제 전투에서 사용되는 무기를 말한다. 재래식 전력을 구축하기 위해서는 많은 시간과 비용이 들지만 투자한 만큼 효과를 나타내기 때문에 대칭전력이라고 하며, 전통적으로 사용되고 있는 무기라는 의미에서 재래식전력(무기)라고도 한다. 비대칭전력은 재래식 무기에 비해 인명을 살상하는 데 있어 월등한 위력을 발휘하고, 상대방의 취약점을 최대한 공략할 수 있으며, 비교적 적은 비용으로 효과를 극대화할 수 있다. 북한은 남한에 비하여 재래식 무기가 부족하기 때문에 비대칭전력 위주로 군사력을 강화하고 있는 것으로 알려져 있다. 시사상식사전 참조

16) 안찬일, "[통일논단] 북한의 사이버 전력: 실력과 실체", 천지일보 2014년 12월 7일자 칼럼 참조. 몇 년 전 사이버 부대에서 일하다 나온 탈북자는 북한이 소유한 중국의 호텔에서 작전을 폈다고 증언했다. 심양과 심지어 상해 등지에도 북한 사이버 전사들의 진지는 무역회사 간판을 내걸고 버젓이 활동하고 있다. 국제사회가 북한에 교환교육의 기회를 제공했지만 북한은 이를 차세대 해커와 사이버 전사들을 교육하는 기회로 활용했다.

17) 김필재, "北 대남 사이버 총공격시 5분 내 南韓 주요시설 초토화", 뉴데일리 2014년 8월 3일자 기사 참조

버전이다. 정보시스템의 약점과 급소 부위의 혈(穴)을 눌러 전체를 마비시킴으로써 최대의 효과를 추구하는 것이다. 북한의 사이버 전술은 크게 3가지로 다음과 같다. ▲대남 도발 전 악성코드를 남한의 컴퓨터에 잠복-은폐시키는 방법 ▲컴퓨터 인터페이스를 통해 악성코드 침투 후 본 시스템으로 확산시키는 방법 ▲공장에서 컴퓨터를 생산할 때 발생하는 자기장(磁氣場)을 활용해 악성코드를 침투시키거나 또는 간접 자장(磁場)을 만들어 컴퓨터에 장애를 일으키는 방법 등이다.[18]

2003년 1월의 1.25 인터넷대란, 2009년 7.7 디도스(DDoS)공격, 2011년 3.4 DDoS공격, 4월 12일 농협전산망 중단사건, 2013년의 3.20공격 및 6.25공격 등 북한에 의한 사이버공격으로 인한 침해사고가 지속적이고 계획적으로 발생하고 있다.[19] 특히 2013년의 3.20사이버공격의 경우, 20일 KBS를 비롯한 MBC, YTN 등 주요 방송사 및 신한은행 등 금융기관 전산망 마비사태로 사회적 혼란이 초래되었다.

2013년 8월 김정은 국방위원장은 "사이버공격은 무자비한 타격력을 보장하는 만능의 보검"이라고 사이버전을 독려했다. 여기서 우리는 김정은이 주한의 사이버부대 창설과 운영에 깊이 관여하고 있다는 점과 사이버전이 비대칭 전력으로서 필수불가결하다는 인식을 가지고 있다는 점에 유의해야 한다.

2015년 8월 남북 고위급 화담 중에도 북한으로 추정되는 해커들이 사이버 도발을 끊임없이 감행한 것으로 확인됐다, 남북 화해무드가 조성되는 상황과 달리 사이버공간에서의 긴장감은 여전히 팽팽하다.

지구상에 대한민국을 향해 동시다발적이고 정교한 사이버공격을 단행할 집단은 북한뿐이다. 2003년 1월의 1.25 인터넷대란, 2009년 7.7 디도스

18) 김필재, "北, 무인기 활용한 對南 '핵(核)테러' 가능성", 뉴데일리 2014년 4월 11일자 기사 참조

19) 디도스(DDos: Distributed Denial of Service. 분산 서비스 거부 공격)이란 해킹 방식의 하나로서 여러 대의 공격자를 분산 배치하여 동시에 '서비스 거부 공격(Denial of Service attack ; DoS)'을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 것을 말한다. 두산백과 참조

(DDoS)공격, 2011년 3.4 DDoS공격, 4월 12일 농협전산망 중단사건, 2013년의 3.20공격 및 6.25공격 등에 이르기까지 북한의 사이버공격은 간단없이 자행되었다.

서울의 한 대학병원 전산망이 2014년 8월 해킹을 당한 채 8개월 동안 방치됐던 사실이 밝혀지기도 했다. 경찰에 따르면 사이버공격을 1년여 지속적으로 추적, 분석한 결과 공격 근원지가 평양시 소재 인터넷주소(IP)로 나타났다. 2014년 12월 시작된 한수원 해킹 사건은 지금까지 무려 아홉 차례에 걸려 원전 관련 도면 등 한수원 자료를 공개하면서 사이버심리전을 펼치고 있다.

2015년 7월 탈북자모임 등 북한문제를 다루는 웹사이트 5곳을 장악하고 이용자가 해당 사이트에 접속하는 것만으로 악성코드에 자동 감염되도록 했다. 북한은 2005~2007년 홈페이지나 이메일을 해킹하다 2008년부터는 채팅, 백신, 자료공유(P2P) 사이트 등을 이용해 범위를 넓히고 있다.[20]

4. 미국

(1) 사이버안보 정책

사이버안보에 대한 직접적 입법전략의 대표적인 사례로는 미국을 들 수 있다. 미국의 경우 주요 기반 시설을 겨냥한 사이버 공격에 대비한 사이버안보 보호법, 사이버 전쟁 시 민-관 협력을 규정한 사이버안보강화법 등 5개 관련 법률을 제정·시행하고 있다.

미국의 사이버안보정책은 1980년대에 시작된 이래 시대의 변천에 따라 대상과 목표가 수정되어 왔다. 초기 국방이나 연방정부의 정보시스템의 보호가 중점이 되던 사이버안보정책은 최근 주요기반시설의 보호로 이행하고 있으며, 최근에는 상호보완적으로 보호하는 체계로 진행되고 있다는 평가를 받고 있다.[21]

20) 박상돈, "일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점을 중심으로"「경희법학」 50권 2호(경희대 법학연구소, 2015), 초록 참조

국가차원의 사이버안보정책을 추진한 것은 민주당의 클린턴정부이다. 클린턴정부는 주요기반시설의 보호의 필요성을 인식하고 1996년 7월 클린턴 대통령에 의한 대통령령 행정명령 제13010호를 발령하면서 종래 컴퓨터보안과 주요기반시설의 보호를 연동한 사이버안보정책을 추진한 것이다. 특히 2001년 9.11테러의 발생은 미국내 주요기반시설의 대테러 취약성에 대한 재인식의 계기가 되었고, 이를 기점으로 국가차원의 안보정책을 재정비하면서 사이버안보정책의 강화에도 박차를 가하고 있다.

오바마정부 출범 이후 설립초기 대테러 활동에 중점을 두었던 국토안보부(Department of Homeland and Security: DHS)로 하여금 주요정보통신기반시설을 포함하여 연방정부 차원의 국가사이버안보정책을 총괄하며, 각 분야의 업무를 담당하는 부처가 소관 분야를 선도하도록 책임과 임무를 집중·분산시키며, 대통령실에서 사이버안보보좌관으로 하여금 사이버안보 관련 정책과 활동을 조정하는 체계를 구축·운영하고 있는 점에서 확인할 수 있다.[22]

미국은 국토안보법을 필두로 사이버안보와 관련한 법규를 체계적으로 정비하고 있다. 아래의 표는 미국의 사이버안보 관련 법률 현황을 나타내고 있다. 이하에서는 이 중 대표적인 법률들을 개관하는 것으로 한다.

(2) 최근의 사이버안보 입법 동향

1) 사이버안보법안

2012년에 입법 추진하던 「사이버안보법안(Cybersecurity Act of 2012)」는 상원에서 폐기되었다. 반대이유는 프라이버시 및 자유권 침해였다. 이 법안은 해커나 외국정부의 사이버공격으로부터 원자력시설, 수도시설, 전기시설, 금융시스템 등 미국의 주요기반시설을 강력하게 보호하고자 하는 것으로, 그 배경에는 사이버공격이 단지 이론적이거나 상상적인 것이 아니라 현

21) 이에 대해 자세한 것은 김현수, "국가 사이버안보 법정책의 현황과 인식제고방안" 「사이버위협의 현황과 법제도 개선방안」(제1회 사이버안보법정책학회 월례세미나, 2013. 3. 20), 2쪽 이하 참조

22) 김현수, 앞의 논문, 5쪽 참조

실적이고도 급박한 위험으로 존재하고 있다는 인식에서부터 출발하고 있다. 즉 이와 같은 사이버공격은 미국의 경제와 미국인의 생활방식에 심각한 피해를 줄 뿐만아니라 미국의 국가안보에도 영향을 줄 수 있다. 사이버공격이 이른바 "진주만 공격"보다 더 큰 피해를 줄 수 있다는 것이다.

2) 사이버안보 정보공유법안

「사이버안보 정보공유법안(Cybersecurity Information Sharing Act of 2015: CISA)」은 지난 2015년 3월 12일 상원 정보위원회에서 14대 1로 통과되었다. 이 법안은 정보위원회의 리차드 버르(Richard Burr) 위원장과 부위원장인 다이엔 페인스타인(Dianne Feinstein)이 공동발의한 것으로 사이버안보와 위협에 대한 정보를 공유하는 것을 촉진하고, 아울러 개인의 프라이버시와 시민권을 보호하는 것을 목적으로 하고 있다. 또한 이 법률은 기업으로 하여금 정보공유에 동참할 때 책임을 면제할 수 있는 내용을 포함하고 있다.[23]

CISA는 공공과 민간 분야 사이에 사이버위협 정보에 대한 기밀정보는 물론, 공개된 정보의 공유까지도 증대시키는 것을 목표로 한다. 각자의 정보 공유와 더불어 그 대응방안에 대한 정보까지도 상호간, 그리고 정부와의 공유를 촉진한다. 부가적으로 동 법안은 국토안보부를 사이버위협에 대한 정보수집과 대응 방안을 전파하는 일차적인 관문으로 상정하고 있다. 아울러 기업이 사이버안보 관련 당국에 적절한 고지 및 정보 공유행위를 수행할 경우 법적인 책임을 면제해 주도록 하고 있다. 그리고 기관책임자, 감사 그리고 프라이버시 시민권 감시 이사회(Privacy Civil Liberties Oversight Board: PCLOB)에 의한 프라이버시 영향 및 이행 등에 대한 보고서 제출을 의무화하고 있다.

프라이버시 보호 측면에서 CISA는 공공부문에서 사이버위협정보의 자발

23) 이 법안의 통과에 대한 언급에 대해서는 KISTI 미리안, 「글로벌동향브리핑」, 2015. 03-25 참조하였다.

적으로 공유하도록 하고 있다. 아울러 어떠한 정보가 공유될 지, 그리고 어떠한 사이버안보 목적으로 이의 사용을 제한할지 정의하고 있다. 마지막으로 법안은 공유되는 정보에서 개인식별 가능한 정보를 제거하도록 하고 있다.

3) 사이버 네트워크보호 법안

「사이버 네트워크보호 법안(The Protecting Cyber Networks Act: PCNA)」이 2015년 4월 22일 미국 하원을 통과하였다. 사이버공격으로 인한 피해 확대가 이어짐에 따라 관련 법안의 도입 필요성에 대한 공감대가 형성되었다. 이에 미국 하원은 사이버 위협 징후나 대응조치 관련 정보를 기업 기업간 혹은 미국 정부와 공유하려는 사업자들에 대한 법적 보호(liability protection) 보장을 주요 골자로 하고 있다.[24]

이 법안 역시 최종 발효 앞두고 프라이버시 침해 논란에 직면하고 있다. 그러나 동시다발적으로 발생하는 사이버 공격을 단일 기업이 대응하는 것이 사실상 불가능하다는 점에서 정보 공유 및 협력을 통한 사이버안보 강화를 모색하는 본 법안은 긍정적으로 평가받고 있다. 하지만 정보 공유과정에서 프라이버시가 침해될 수 있으며 사업자들로부터 수집된 정보들이 어떻게 활용될지도 불분명하다는 점에서 이 법안에 대한 시민들의 반대가 만만찮다. 그러나 이미 유사한 법안이 상원을 통과했다는 점에서 최종 발효 가능성이 높은 것으로 보고 있다.

Ⅲ 사이버안보 일반법 및 개별법 추진사례 분석

1. 사이버안보 일반법 추진사례

종래 사이버안보 일반법 제정을 위한 대표적인 사례는 「국가 사이버테러 방지에 관한 법률 안」(2013년 4월 9일 발의)과 「국가 사이버안전 관리에 관

24) 정보통신기술진흥센터, “미국 사이버 네트워크보호 법안(PCNA)을 둘러싼 논란 분석” 「ICT R&D 정책동향」(2015. 6. 30) 참조

한 법률안」(2013년 3월 26일 발의) 등을 들 수 있다.

(1) 국가 사이버테러 방지에 관한 법률안

1) 제안이유

사이버공간은 정보통신기술의 비약적인 발전과 더불어 정보기기와 컴퓨터 그리고 인터넷 등의 네트워크로 연결된 가상의 공간으로 이미 국민 생활의 보편적인 영역으로 자리매김하였고, 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있다. 이러한 특수성으로 말미암아 복잡·고도화되며, 시공간의 제약을 벗어나 발생하는 모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있다. 게다가 사이버테러로 초래되는 사이버상의 위기는 현실세계의 물리적 질서혼란과 달리 특정개인에 대한 것일지라도 국가전체의 위기로 확대될 수 있다. 그리고 과거 1.25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비 사태 발생과 해외로부터 조직적인 사이버테러로 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대하고 있다. 그러나 우리나라는 아직 국가차원에서 사이버테러 방지 및 위기관리업무를 체계적으로 수행할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있다.

따라서 이 법에서는 정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버테러를 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 한다.

2) 주요내용

가. 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련 정보를 상호 공유하기 위하여 민·협의체를 구성·운영할 수 있음(안 제5조).

나. 국가정보원장은 국가사이버테러 방지 및 위기관련 기본계획을 수립하고 이에 따라 시행계획을 작성하여 책임기관의 장에게 배포하여야 함(안 제7조).

다. 사이버테러에 대한 국가차원의 종합적이고 체계적인 대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제9조).

라. 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제12조).

마. 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 피해가 중대할 경우 관계 중앙행정기관의 장 및 국가정보원장에게 그 결과를 통보하여야 함(안 제13조).

바. 국가정보원장은 사이버테러에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취해야 함(안 제15조).

사. 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등을 위하여 관계 기관 및 전문인력이 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제16조).

아. 정부는 사이버위기관리에 필요한 기술개발·국제협력·산업육성·인력양성 등 필요한 시책을 추진할 수 있음(안 제19조, 제20조 및 제21조).

자. 정부는 사이버테러 기도에 관한 정보를 제공하거나 사이버테러를 가한 자를 신고한 자에 대하여 포상금을 지급할 수 있음(안 제24조).

차. 직무상 비밀을 누설한 경우에는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 보안관제센터를 구축하지 아니한 경우에는 2천만원 이하의 과태료에 처할 수 있음(안 제25조 및 제26조).

(2) 국가 사이버안전 관리에 관한 법률안

1) 제안이유

최근 사상 초유의 방송·금융 전산망 마비 사태를 비롯하여 북한의 GPS 교란, 국가기관 홈페이지에 대한 디도스(DDos) 공격 및 농협 전산망 해킹 등 다양한 사이버공격으로 인하여 사회·경제적 혼란이 발생하고 있다. 그러나 현재 우리나라는 국가차원에서 사이버위기를 체계적으로 관리할 수 있는 제도와 구체적 방법 및 절차가 정립되어 있지 아니한 바, 사이버위기로 인하여 국가안보에 중대한 위험이 초래되고 국민의 재산과 국가의 이익에 막대한 손해가 발생할 우려가 있다.

따라서 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 이바지하려는 것이다.

2) 주요내용

가. 국가정보원장은 국가 사이버안전에 관한 정책을 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관과의 협의를 거쳐 국가사이버안전기본계획을 수립하여야 함(안 제5조).

나. 국가 사이버안전에 관한 중요사항을 심의하기 위하여 국무총리 소속으로 국가사이버안전전략회의를 둠(안 제6조).

다. 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제7조).

라. 국가정보원장은 국가 차원의 사이버위기 발생에 대비하여 사이버안전 관리책임기관이 참여하는 사이버위기 대응 훈련을 실시할 수 있도록 함(안 제9조).

마. 중앙행정기관, 지방자치단체, 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 보안관제센터를 설치·운영하여야 함(안 제11조).

바. 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향 및 피해규모 등을 고려하여 수준별 사이버위기경보를 발령할 수 있도록 함(안 제12조).

사. 중앙행정기관, 공공기관 및 지방자치단체의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우 국가정보원장에게 통보하도록 함(안 제13조).

아. 국가정보원장은 사이버공격으로 인하여 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있도록 함(안 제14조제1항).

자. 국가정보원장은 사이버공격으로 인한 피해가 심각하다고 판단되는 경우나 심각 수준 이상의 사이버위기경보가 발령된 경우에는 관계 중앙행정기관의 장과 협의하여 사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위한 범정부적 사이버위기 대책본부를 구성·운영하도록 함(안 제14조제3항).

(3) 평가

두 법안의 국회통과 실패 원인은 첫째, 사이버테러 전담 기관이 법률 및 제도적으로 확립되는 경우 이 기관에 공공 및 민간의 정보가 집중돼 막강한 권력을 가지는 소위 빅 브라더(Big Brother)가 탄생할 가능성이 있다는 지적에 대한 고려가 되어 있지 않다. 따라서 사이버테러와 관련한 전담 기구가 일반 국민들이 우려하는 빅브라더화 되는 것을 견제하는 장치로 전담 기구가 국회 정보위원회에 보고하고 감사를 받도록 법률에 명시하는 방안 등을 제시할 필요가 있었다고 본다. 둘째, 사이버테러를 방지하기 위한 정보의 수집과 일반적인 개인정보 침해에 대한 개념을 법률로 명확하게 구분하는 노력이 흠

결되었다. 따라서 사이버테러를 방지하기 위한 정보의 수집과 일반적인 개인정보 침해에 대한 개념을 법률로 명확하게 구분하여 관련 규정을 모호하게 둘 경우 제기될 수 있는 국가 권력에 의한 민간인 사찰 의혹이 발생되지 않도록 투명화해야 할 것이다. 셋째, 전담 기구의 역할과 책임이 법률상 불명확하다. 따라서 전담 기구의 역할과 책임을 법률상 명확하게 규정하고, 보안 전문인력 양성을 위한 정책적인 대안 마련도 필요하다.

2. 최근 사이버안보 개별법 추진사례

(1) 사이버위협정보 공유에 관한 법률안

이철우 의원이 2015년 5월 19일 「사이버위협정보 공유에 관한 법률안」을 발의하였다. 19대 국회 임기만료로 폐기되었다. 이 법률안은 제정법으로 사이버테러 대응과 관련 있는 국가정보원, 국가안보실, 미래창조과학부, 금융위원회 등 유관부처와의 협의 및 위협정보 공유를 위한 절차를 마련하고 효율적인 업무수행을 위해 국가정보원 내에 '사이버위협정보 공유센터'를 설치해 운영하는 내용을 담고 있다.

1) 제안이유

2013년 3.20, 6.25 사이버테러로 청와대 홈페이지 변조는 물론 민간 방송·금융사 전산시스템이 대량으로 파괴되는 피해가 발생하였으며 지난해에는 한국수력원자력 제어시스템 가동을 중단시킬 목적으로 대량의 해킹메일이 유포되는 등 최근의 사이버위협은 단순 정보절취를 넘어 국민생활과 직결되는 사회기반시설의 안전까지 위협하여 우리의 경제와 국가안보를 저해하는 가장 심각한 위협 중의 하나로 대두되었다. 특히 일부 지역에 국한해 발생하는 물리적 위협과 달리 사이버위협은 초국가적으로 시·공간을 초월하여 공공·민간 영역 구분이 없이 동시 다발적으로 발생함으로써 사이버위협 요인을 조기에 파악하여 차단하지 않을 경우 피해가 순식간에 확산되는 특성이 있다.

따라서 이러한 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 함에 있다.

2) 주요내용

가. 공공・민간 영역 간에 공유하는 '사이버위협정보'를 정의(안 제2조).

나. 국정원장은 국가안보실장, 미래창조과학부 장관 등과 협의하여 범정부 차원에서 사이버위협정보를 공유하기 위한 방법과 절차를 마련함(안 제4조).

다. 국가의 주요 정보와 정보통신망을 관리하는 기관(이하 "사이버위협정보 공유기관")은 사이버위협정보를 수집하고 상호 공유하여야 함(안 제4조).

라. 사이버위협정보 공유를 효율적으로 수행하기 위하여 국정원장 소속으로 사이버위협정보 공유센터(이하 "공유센터")를 설치・운영함(제5조).

마. 공유센터의 장은 공유된 사이버위협정보를 종합 분석하고 결과를 사이버위협정보 공유기관 및 관련 업체에게 제공하여야 함(안 제6조).

바. 국정원장은 법무부 장관 등 국가기관 및 전문가가 참여하는 협의회를 구성하여 사이버위협 정보의 남용방지 대책을 수립하여야 함(안 제7조).

사. 사이버위협정보를 보유한 사람은 공유센터의 장에게 신고하거나, 공유센터의 장이 사이버위협정보의 제공을 요청할 수 있음(안 제8조).

아. 공유센터의 장은 사이버위협정보 공유 활동에 대한 결과를 평가하고 그 결과를 국회에 보고하여야 함(안 제9조).

자. 사이버위협정보 공유기관, 공유센터 등의 종사자는 직무상 알게 된 비밀을 누설하면 아니 되고 위반 시에는 벌칙을 부과함(안 제10・11조)

Ⅳ 주요 사이버안보 관련법률 개정필요성 검토

1. 정보통신망법

정보통신망법은 정보통신망의 안전성 및 안정성 확보를 위한 보호조치의 구체적인 내용을담고 있어 정보통신망 및 정보시스템 보호 관련 법제의 일반법과 같은 역할을 수행한다.[25]

최근 인터넷기술 및 정보통신서비스의 발전과 더불어 지능형지속공격(APT), 분산서비스거부공격(DDoS), 개인정보 침해사고 등 사이버 침해사고가 점차 지능화·고도화되고 있으며, 인터넷 등의 네트워크로 연결된 사이버공간의 특성상 일반 개인에 대한 물리적 피해는 국가 사이버안보 전체에 대한 위협으로 확산될 수 있다.

특히, 이와 같이 사이버 침해사고 발생 초기에 신속·효율적으로 대응하지 못할 경우 단시간 내에 정보통신 시스템 전체와 사회 질서의 혼란이 야기될 수 있는 바, 침해사고 예방을 위하여 웹사이트 게시자료에 대한 점검 등 보호조치를 취하는 한편, 정보통신서비스 제공자 등 정보통신망을 운영하는 자의 침해사고 긴급대응 조치를 강화하고 이용자의 컴퓨터 등에 신속히 접근하여 원인조사를 할 수 있는 절차를 마련하며, 악성프로그램 전달 및 유포행위 등 정보통신망 침해 범죄에 대한 제재수준을 상향하는 등 현행법의 운영상 나타난 문제점들을 개선할 필요가 있다.

25) 정보통신망의 안전성 및 안정성 확보를 위한 보호조치의 구체적인 내용을 담은 정보보호지침의 제정·고시 및 권고, 정보보호 사전점검, 정보보호 최고책임자 지정, 집적정보통신시설(IDC) 보호, 정보보호관리체계(ISMS) 인증 권고 및 의무화, 이용자의 정보보호기준 제정·권고 및 침해사고의 예방 및 확산 방지를 위한 취약점 점검·기술 지원 등의 이용자 보호조치, 정보통신망 접속의 일시적 제한, 침해사고 대응을 위한 침해사고정보의 수집·전파/예보·경보/긴급조치, 침해사고의 유형별 통계/해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보의 제공, 침해사고의 신고, 침해사고 원인분석 및 피해확산 방지, 중대한 침해사고의 피해 확산 방지/사고대응/복구 및 재발 방지를 위한 민·관합동조사단 구성 등에 관해서 규정하고 있다.

2. 정보통신기반보호법

정보통신기반보호법은 정보통신망 중에서도 국가안전보장・행정・국방・치안・금융・통신・운송・에너지 등의 업무와 관련된 전자적 제어・관리시스템 등에 대해서만 적용되므로 정보통신망법에 대한 특별법의 지위에 있다고 할 수 있다.[26]

한수원 사이버 침해사고 등 국가 중요시설에 대한 전자적 침해행위로 인한 국가 주요정보통신망 장애 및 국가기밀 유출 등 국가・사회적으로 혼란을 야기하는 침해하는 사고가 발생하였으며, 발생 가능성도 날로 증대하고 있으나, 현행법체계상 전자적 침해행위에 대해 신속하게 대응하고 피해를 최소화하기에는 한계가 있다.

이에 주요정보통신기반시설에 대한 사이버 침해사고 예방 및 대응에 관한 업무수행체계의 혼선을 해소하고, 정보통신기반보호위원회의 심의항목을 명시적으로 규정함으로써 관리기관 및 관계행정기관이 실효성 있는 보호대책을 수립할 수 있도록 할 필요가 있다.

또한 침해사고 발생 등 유사시에 대비하여 침해사고 대응을 위한 모의훈련을 실시하여 신속하고 효율적인 대응 역량을 확보할 수 있도록 하고, 기술적・관리적 기준을 정부가 사전에 정하여 주요정보통신기반시설에 대해서는 일정기준 이상의 보안수준을 유지하도록 함으로써 사전 예방체계를 강화할 필요가 있다.

현행 정보통신기반보호법에 따르면 국가안전보장・행정・국방・치안・금융・통신・운송・에너지등의 업무와 관련된 주요정보통신기반시설에 대하여 국가 위급 상황시에 정부가 규제하고 명령할 수 있는 권한을 가지고 있다.

26) 주요정보통신기반시설의 지정, 주요정보통신기반시설의 취약점 분석・평가, 주요정보통신기반시설 보호계획 및 보호대책의 수립, 주요정보통신기반시설 침해사고 대응, 주요정보통신기반시설 침해사고 통지, 정보공유・분석센터(ISAC)의 구축・운영, 정보통신기반 침해사고대책본부의 구성・운영, 정보통신기반보호위원회의 구성・운영 등에 관해서 규정하고 있다.

하지만 사이버공격 징후를 사전 탐지하여 수집된 정보를 종합적으로 분석·대응한다거나 발생한 사이버공격에 부처별 대응이 아닌 국가적인 차원에서 대응하기 위한 시스템은 아직 법제도화되어 있지 아니하다.[27]

3. 정보통신비밀보호법

헌법 제18조는 "모든 국민은 통신의 비밀을 침해받지 아니한다"라고 하여 통신의 비밀과 자유를 보장하고 있다. 통신에 대한 기본권의 보장에서 볼 때, 법문의 표현은 "모든 국민은 통신의 비밀과 자유를 가진다"라고 하는 것이 타당하다.[28] 통신의 비밀과 자유도 절대적으로 보장되는 것이 아니므로 헌법 제37조제2항에 따른 제한이 가능하다.[29] 통신의 자유의 제한에 관하여 정하고 있는 대표적인 법률로 통신비밀보호법이 있다. 통신비밀보호법은 범죄수사 또는 국가안전보장을 위한 경우에는 엄격한 요건하에 특정 국가기관에 의한 감청을 허용하고 있다. 즉 예외적으로 범죄수사를 위한 검열·감청 등 '통신제한조치'를 허용하고 있다.[30]

어느 나라나 공동체의 안전과 국민과 국가의 이익을 위하여 국가정보기구를 설치하여 국가정보활동을 하고 있다. 국가정보활동은 그 사안에 따라 통상적인 행위도 있지만 고도로 비상적인 행위도 있다. 국민과 국가의 안전을 위한 행위, 사이버 전쟁행위, 국민과 국가의 이익을 위하여 고도의 정보를 수집해야 하는 행위, 특수한 활동을 행해야 하는 경우 등 각종의 행위에서 감청의 방법이 필요하다. 예외적인 경우에 행해지는 감청에는 영장 또는 허가를 받을 것을 요구하는 것이 국가정보활동의 성질과 기능에 부합하지 않는 경우

27) 정준현, "국가 사이버안보를 위한 법제 현황과 개선방향", 「디지털 시대와 국가 정보발전」, 2012, 94쪽 참조
28) 정종섭, 「헌법학원론」(박영사, 2015), 655쪽
29) 헌재결 1995. 7. 2, 92헌마144
30) 독일연방헌법은 제13조에서 이러한 예외적으로 허용되는 감청에 대하여 명시적 요건을 정하여 인정하고 있다. 일본에서는 1999년 '범죄수사를 위한 통신방수(通信傍受)에 관한 법률'을 제정하여 범죄수사를 목적으로 한 감청을 일정한 요건하에 예외적으로 인정하고 있다.

가 있다.[31]

우리나라는 1.25인터넷대란, 7.7디도스공격, 3.4대란, 3.20 및 6.25 사이버공격 등은 국가의 사이버안보가 구조적인 문제에 봉착해 있다는 점을 시사하고 있다. 이제는 '정적 사이버안보'에서 '동적 사이버안보'로, '후발적 대응'에서 '선제적 대응'으로 그 패러다임을 전환하여야 한다. 선제적 사이버안보가 가능한 동적 안보체계의주요 수단 중의 하나가 통신제한조치, 특히 감청이라 할 수 있다.

급속한 통신기술 발달로 인한 납치, 유괴, 살인 등 흉악범죄 뿐만 아니라, 첨단기술의 해외유출 범죄가 날로 지능화・첨단화되고 있고, 테러・간첩 등 국가안보를 위협하는 요소가 급증하고 있으나, 첨단통신 서비스를 악용하는 강력범죄 및 국가안보 위협요소에 대해서는 속수무책인 것이 현재의 실정이며, 첨단통신을 악용하는 최근의 범죄 추세에 효과적으로 대처할 수 있는 제도적 장치마련이 시급한 상황이다. 현행법상 휴대전화를 포함한 모든 통신에 대한 감청을 합법화하고 있지만, 수사기관은 감청절차의 투명성 문제로 현재 첨단통신에 대한 자체 감청 설비를 갖추지 못하고 있으며, 첨단통신을 악용하는 범죄에 대한 수사과정에서 통신사업자의 도움을 받으려 해도 감청 협조 설비의 구비를 의무화한 법적 근거가 없어 실효성이 부재한 상황이다. 이로 인해 법원의 엄격한 심사를 거쳐 영장을 통한 감청허가를 받더라도 강력범죄자나 간첩 등 국가보안법 위반사범이 휴대전화를 사용하는 경우, 선제대응 및 범증 확보가 어려운 상황이다. 이에 일반 국민들의 통신의 자유와 개인 사생활을 보호할 수 있는 법적 장치를 마련하는 등 투명한 법 집행 절차에 따른 합법적인 감청을 보장함으로써 휴대전화를 포함한 모든 통신수단에 대한 감청제도를 허가・승인(법원・대통령)-집행(정보수사기관)-협조(통신업체) 체제로 3원화한 선진국 수준의 감청제도를 마련할 필요가 있다. 다만, 세계 각국이 통신제한조치를 통하여 테러와 국가안보 침해범죄 등 범죄예방을

31) 정종섭, 앞의 책, 662쪽

할 수 있는 제도적 장치를 도입하되, 그로 인하여 발생할 수 있는 프라이버시 침해나 개인정보의 유출 등 기본권 침해를 방지하기 위하여 필요한 법적 조치를 강구하고 있음을 유념할 필요가 있다.

V 사이버안보 입법환경 변화와 법체계 정당성의 요청에 따른 입법전략 모색

1. 사이버안보 입법환경 변화에 따른 입법전략

(1) 개인정보보호에 터잡은 사이버안보 입법

2015년 5월 19일 아시안리더십콘퍼런스의 '조선 디베이트(debate)'를 참관한 청중은 프라이버시와 안보 중 더 중요한 가치로 프라이버시를 선택했다. '스마트 시대, 프라이버시 vs 안보'라는 주제로 진행된 이날 토론에서 태블릿PC를 이용한 투표 결과 프라이버시는 56%, 안보는 44%의 지지를 받았다.[32]

가장 큰 쟁점은 과연 프라이버시와 안보가 공존할 수 있는가였다. 옥스퍼드대 쇤베르거 교수는 "안보와 프라이버시는 양립할 수 없다"며 "9·11 테러 이후 미국, 유럽 등에서도 프라이버시를 파괴하는 모습이 계속되고 있는데, 자유 없는 안보는 아무 의미가 없다는 것을 알아야 한다"고 했다. 이에 대해 타이페일 스틸웰硏 총괄이사는 "자유(프라이버시)는 안보가 있어야 지켜질 수 있다"며 "테러 단체들이 지속적으로 활동하면서 위협을 주고 있는데 이를 지킬 수 있는 것이 바로 안보"라고 반박했다.

(2) 초연결사회에 기반한 사이버안보 입법

클라우드, 빅데이터, 사물인터넷(IoT) 등으로 인한 초연결사회(Hyper-

32) 조선일보 2015년 5월 20일 "[아시안리더십콘퍼런스] 스마트 시대, 프라이버시와 안보는 공존할 수 있나" 기사 참조

connected Society)[33]의 도래는 경제와 산업 분야에서 새로운 기회를 창출하고 인류에게는 더 나은 편의를 제공하고 있다. 그러나 대규모의 정보가 수집되고 초고속으로 처리하는 과정에서 개인정보 등의 유출과 오남용, 해킹 등의 우려가 커지고 이에 대한 피해는 개인, 기업, 정부 등 모든 경제주체의 큰 부담이 되고 있다. 정보보호가 선행되지 않는 초연결사회, 디지털 세상은 오히려 해커들의 놀이터로 전락하고 국가안보와 국민의 삶의 질에 심각한 위협이 될 수 있다.[34]

사물인터넷, 빅데이터, 클라우드 컴퓨팅의 속성으로 인하여 여러 사이버범죄 및 사이버공격이 발생할 수 있으며 때로 이들은 테러리즘의 성격까지 띠기도 한다. 특히 마이닝된 빅 데이터 정보에 국가기밀 등이 들어있는 경우 여기에 침투하거나 클라우드 공간에서 처리 및 저장된 중요 정보가 유출된 경우 등을 상정할 수 있다.[35]

따라서 빅데이터, 클라우드컴퓨팅 등 초연결사회를 맞이하여 국가사이버안보전략 실행을 위한 구체적인 실행 전력 및 매뉴얼 마련이 필요하다. 즉, IoT를 통한 초연결사회, 민간・정부의 클라우드 중심 환경 변화를 고려한 실행 전략 및 매뉴얼 마련이 필요하다. 그리고 그에 부합하는 입법이 이루어져야 한다. 사물인터넷, 빅데이터, 클라우드컴퓨팅 등 초연결사회의 진입으로 인하여 사이버안보 입법환경도 급변하고 있다. 초연결사회의 도래로 사이버안보에 대한 접근방법도 근본적으로 변화될 수밖에 없다.

미국에서 「사이버 네트워크보호 법안(The Protecting Cyber Networks Act: PCNA)」이 2015년 4월 22일 미국 하원을 통과한 것도 이런 의미에서

33) 초연결사회란 인터넷, 통신기술의 발달에 따라 네트워크로 사람, 데이터, 사물 등 모든 것을 연결하는 사회를 말한다.

34) 석호일, "[IT 칼럼] 정보보호는 비용이 아니라 투자이자 미래 유망산업이다" 뉴스천지 2015년 3월17일자 기사 참조

35) 장철준, "빅데이터・클라우드 환경과 사이버안보의 법정책적 문제", 「초연결사회와 사이버안보」 2014년 한국사이버안보법정책학회 추계학술대회 발제문, 2014. 11. 28, 77쪽 참조

시사하는 바가 크다고 하겠다.

(3) 사이버투명성을 기반으로 한 사이버안보 입법

인터넷이 실제 세계에 위험스러운 결과를 가져올 전장으로 변하고 있는 상황에서 이런 새로운 종류의 전쟁 위험을 낮추는 방안을 생각하기 시작해야 한다. 이를 위해선, 세계가 핵무기 위협을 완화하는 체제를 만드는 과정에서 관련 정보공개를 통해 핵무기의 위험과 이익에 관해 대중이 이해할 수 있도록 했던 것처럼, 디지털 무기에 관해서도 같은 수준의 정보공개가 이뤄져야 한다. 어떤 디지털 무기를 보유하고 있고 그것들이 어떻게 사용되며, 그것을 통제하는 규범은 어떠한지 공개돼야 한다는 것이다.

오바마 대통령과 시진핑 중국 국가주석이 최근 정상회담에서 양국 간 주요 충돌현안인 사이버 해킹의 방지에 합의했으나, 실질적이고 구체적인 합의가 조만간 이뤄질 전망이 회의적인 것도 양국의 디지털 군비 경쟁의 불투명성과 관련 있다. 사이버 불투명의 가장 기본적인 사례로는 각 나라 군대의 사이버전 조직이 사실은 공격용임에도 국민에겐 방어용이라는 생각을 주입시키는 것이다.

따라서 이른바 '사이버군비 정보공개에 관한 법률'을 제정하여 사이버투명성을 확보하는 것도 검토할 필요가 있다. 왜냐하면 그지 멀지 않은 장래에 사이버군비에 대한 정보공개 및 무기감축에 관한 국제적 논의가 이루어질 것으로 예상되기 때문이다.

(4) 정보공유를 기반으로 한 사이버안보 입법

미국은 각 분야마다 정부내 협력을 위한 정부조정위원회(Government Coordinating Council: GCC)와 해당 분야내 협력을 위한 분야조정위원회(Sector Coordinating Council: SCC)를 각각 설치하도록 하고 있다. 그리고 각기 다른 분야에 관련되어 있는 정부부처간의 협력을 위한 분야간 정부조정위원회(Government Cross-Sector Council: GCC)를 설치하고 있다.[36]

미국의 대표적인 정보공유조직은 미국에서 운영중인 정보공유센터

(Information Sharing andAnalysis Center: ISAC)이다. 이 조직은 1984년에 운영된 국가통신조정센터(National Coordinating Center for Commucations: NCC)가 그 기원이다. 1999년 재정서비스ISAC(Financial Services ISAC)이 최초로 창설되었으며, 현재 16개의 ISAC이 활동중이다. 이들 센터들은 ISAC Council을 구성하고 있다.

정보공유센터는 각 분야에 특화되어 사고・위협・취약성 정보를 전파하는 것 이외에도 사고정보를 수집・분석하여 경보를 발령하며 보고하는 것을 기본임무로 수행하고 있다. 그 밖에도 위협이 해당 분야에 미치는 영향에 관해서 정부가 보다 잘 이해하도록 돕거나, 사이버・물리적 및 모든 위협에 관한 정보를 회원간 교환・공유하는 창구역할을 수행한다. 정부나 다른 분야 ISAC의 기술적 상세분석을 지원함으로써 기술과 경험을 전파하는 역할도 한다.

사이버안보 측면에서 주요정보기반보호를 총괄하고 있는 국토안보부 산하 국가사이버보안국은 제어시스템 보안 프로그램(Contral Systems Security Program)을 통해 제어시스템 보안에 관련된 설명서・지침서・경보 등을 제작하여 배포하거나, 관련된 표준 등과 같은 자료를 홈페이지를 통하여 제공하고 있다. 특정 분야를 담당하는 책임기관도 관련분야에 적용할 수 있는 경험공유 문서를 제작・배포한다. 예를 들어, 에너지부는 주요기반보호 대통령위원회(PCIPB)와 함께 에너지분야의 SCADA 시스템 보호를 향상시키기 위한 경험을 21단계로 구분 설명하는 문서를 제작하여 배포하고 있다.

이철우 의원이 2015년 5월 19일 「사이버위협정보 공유에 관한 법률안」을 발의하였다. 이 법률안은 제정법으로 사이버테러 대응과 관련 있는 국가정보원, 국가안보실, 미래창조과학부, 금융위원회 등 유관부처와의 협의 및 위협정보 공유를 위한 절차를 마련하고 효율적인 업무수행을 위해 국가정보원 내에 '사이버위협정보 공유센터'를 설치해 운영하는 내용을 담고 있다. 일

36) 이에 대해서는 김현수, 「주요정보기반보호(CIIP) 동향」, (한국법제연구원, 2010. 10), 23-26쪽 참조

부 지역에 국한해 발생하는 물리적 위협과 달리 사이버위협은 초국가적으로 시·공간을 초월하여 공공·민간 영역 구분이 없이 동시 다발적으로 발생함으로써 사이버위협 요인을 조기에 파악하여 차단하지 않을 경우 피해가 순식간에 확산되는 특성이 있다. 따라서 이러한 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 구축하려는 이 법률안은 의미가 크다고 하겠다.

(5) 민－관 파트너십을 기반으로 한 사이버안보 입법

미국을 비롯한 EU 그리고 영국 등 대부분의 선진국가들은 사이버안보 민-관 파터너십(Public-Private Partership: PPP)의 중요성을 강조하고 있다. 유럽의회는 주요정보기반을 대상으로 하는 위협에 대해서는 정부와 민간이 공동책임이 있으며 단독대응은 적절하지 않다고 보고 있으며 영국은 첨단 민간영역과 밀접히 연계하되, 필요하다면 새로운 체계를 세우는 것이 장기적으로 중요하다고 인식하고 있다.

민관협력과 정보공유는 1990년대 후반 미국의 주요기반보호에 대해 고민한 때부터 제시된 개념이지만, 최근 들어 그 중요성이 더욱 부각되고 있는 추세이다. 미국은 정부의 사이버안보보좌관이 관련 정부부처·기관 및 민간기관과 협력하여 민-관 파트너십을 점검하고, 정보공유체계를 검토하여 효과적 모델을 제시하도록 하고 있다. 이에 따라 미국의 국가정책은 민-관간 협력강화를 지속적으로 강조하고 있으며, 특히 최근 들어서는 분야간 협력도 강화할 것을 강조하고 있다. 미국에서는 민-관 파트너십을 강화하기 위하여 2004년 이후 3억2천7백만 달러를 들여 70여개의 정보융합센터를 설립하고 정보공유를 강화하고 있다. 이러한 목적의 일환으로 2009년 국토안보부의 국가사이버안보국(National Cybersecurity Division)은 산업제어시스템합동작업반(Industrial Control Syatems Joint Working Group: ICSJWG)을 출범시키기도 하였다.

우리나라의 경우에 국가정보원은 정부・공공기관 및 산・학・연 등이 자율적으로 참여, 상호 협력함으로써 국가 정보보안 역량을 제고하기 위하여 국방부・경찰청 등 정부부처와 공기업, 산・학・연 전문가가 참여하는'국가정보보안연합회(NISA: National Information Security Agency)'를 운영해오고 있다. 2002년 설립된[37] 국가정보보안연합회는 정보화로 인한 각종 정보보안 위협에 효과적으로 대응하기 위하여 정부・공공기관 및 산・학・연 등이 자율적으로 참여, 상호 협력함으로써 국가정보보안 역량 제고를 추구하기 위하여 설립된 단체이다.

한국CSO협회는 비영리 사단법인으로서 사이버 위협에 대한 민・관 협력체계 구축과 민-관 분야별 CSO(최고보안책임자, Chief Security Officer) 간 협력 및 정보공유 활성화를 위해 2009년 6월 창립되었다. 한국CSO협회는 중앙 행정기관, 지방자치단체를 비롯하여 산하기관 및 공공기관과 일반기업의 CSO 의견수렴을 통해 실용적이고 효율적인 정보보호 정책 및 미래전략 수립을 위한 자문 역할을 하고 있다.

정보통신기반 보호법 제16조에 의해 설립된 정보공유・분석센터(Information Sharing & Analysis Center: ISAC)로서 대표적인 것으로는 방송통신ISAC, 금융ISAC 등이 있다. 방송통신ISAC은 정보보호 관련 업무 수행에 있어 민간분야의 자생적 공동대응체제를 구축하여 전자적 침해행위로부터 회원사의 정보통신관련 시설을 보호함으로써 정보통신역무의 안전성과 신뢰성을 제고하기 위한 목적에서 설립되었다. 현재 통신정보공유분석협회라는 이름의 사단법인 형태로 운영중이며 KT, SK텔레콤 등 주요 기간통신사업자가 가입되어 있다.[38] 금융ISAC은 은행・보험 등을 담당하는 금융결제원 금융ISAC과 증권・선물 등을 담당하는 코스콤 금융ISAC이 있다. 금융결제원 금융ISAC은 금융부문 정보통신기반시설을 보호하기 위하여 설립된 금융부문 정보공유・

37) 국가정보원・미래창조과학부・방송통신위원회・안전행정부, 2013 국가정보보호백서 중 정보보호 연혁 참조.
38) 방송통신ISAC 홈페이지(http://www.isac.or.kr) 참조.

분석센터로서 17개 국내은행을 비롯한 보험사, 카드사 등 32개 금융회사가 업무에 참가하고 있다. 코스콤 금융ISAC은 증권·선물사 및 금융유관기관을 중심으로 금융회사 대상 실시간 통합보안관제, 취약점 분석·평가 및 사이버침해 관련 정보 분석·제공 등의 서비스를 주업무로 하고 있다.[39]

(6) 교육친화적 사이버안보 입법

사이버안보에 관한 관심이 증가하면서 사이버안보의 인식제고 및 교육정책이 국가차원의 계획으로 수렴되어 시행될 필요가 있다.

미국에는 「사이버안보 교육 강화를 위한 법률안」(Cybersecurity Education Enhancement Act of 2011)이 마련되어 있음을 참고할 필요가 있다. 즉, 사이버공간의 안전에 관한 관심이 증가하면서, 미국에서는 사이버공간의 안전성 확보를 위한 사이버안보의 인식제고 및 교육 정책이 국가차원의 계획으로 수렴되어 시행되고 있다. 동 법안에서는 사이버안보 담당 차관보(the Assistant Secretary of Cybersecurity)를 통해 국토안보부 장관에게 국립과학재단과 공동으로 고등교육기관을 대상으로 장학금(grant)를 지급하는 프로그램을 설치하도록 명하고 있다. 동 프로그램은 다시 세 가지로 나누어 설명할 수 있다. 첫째, 사이버보안 전문가 개발 프로그램(cybersecurity professional development programs), 둘째, 사이버보안 학위 프로그램, 셋째, 전문가 개발이나 학위 프로그램을 위한 사이버안보 훈련에 필요한 장비(equipment)의 구입. 동 법안은 국립과학재단의 장에게 이들 프로그램을 실질적으로 운영하도록 요구하고 있다.

2. 사이버안보 법체계 정당성 확보를 위한 입법

(1) 초당적 협력에 기반한 사이버안보 입법 추진: 미국사례의 시사점

「사이버안보 정보공유법안」(Cybersecurity Information Sharing Act

39) 상세한 내용은 국가정보원·미래창조과학부·방송통신위원회·안전행정부, 2013 국가정보보호백서, 26~28면.

of 2015: CISA)은 공화당과 민주당의 지지를 받아 상원을 통과하였다.[40] 이 법안의 특징은 사이버위협의 증가 속에서 미국을 지키기 위해 초당적으로 추진되었다는 점이 높이 평가받고 있다.

법안 통과를 주도한 정보위원회 바르 위원장은 이 법안이 양당의 지지를 받아 상원을 통과하게 된 것을 기쁘게 생각한다고 밝혔다. 상원에서 통과된 이 법안은 사이버위협에 대한 기관 간 정보 공유와 함께 개인들에게 보다 강력한 프라이버시 보호 수준을 담보할 수 있을 것이라고 그는 말했다. 위협이 매일 증가하고 있는 상황에서 이 법안을 통해 사이버 공격자에 대해 보다 잘 대응할 수 있는 체제를 갖출 수 있을 것이라고 그는 주장했다. 그리고 공동발의자인 페인스타인 부위원장은 2014년 한해만 해도 수억명에 이르는 미국인의 개인정보가 유출되었고, 수많은 미국 기업이 해킹 공격을 당했으며, 지적재산권의 피해와 기반시설에 대한 해킹 시도가 발생했다고 지적했다. 이 법안은 순전히 자발적으로 사이버위협에 한정된 정보공유를 통해 사이버공격에 대한 대응수준을 높임으로써 민간분야와 정부가 이들 위협에 대해 보다 잘 이해하고 대응할 수 있도록 할 것으로 판단한다고 말했다. 강력한 프라이버시 보호 요건과 책임면제 등의 조항을 통해 이 법안이 더욱 균형있는 법제도가 될 수 있다고 주장했다.

지난 2월 「사이버위협공유법」(Cyber Trreat Sharing Act)을 제안한 국토안보 및 정무위원회 소속 톰 카퍼(Tom Carper) 상원의원은 이번 위원회의 결정에 환영의 뜻을 표했다. 사이버공간에 상존하는 위협을 고려하면, 의회는 물론 행정부와 다양한 이해관계자들이 미국의 사이버공간 방어능력 개선을 위해 모두 협력해야 한다고 커퍼는 성명을 통해 지적했다. 이번 법안을 제정하기 위해, 협력과 투명성 원칙에 입각하여 함께 노력하고, 더불어 사이버안보를 개선하며 시민권을 보호하기 위한 조치들을 취할 필요가 있다고 주

40) 이 법안의 초당적 협력에 대해서는 KISTI 미리안, 「글로벌동향브리핑」, 2015. 03-25 참조

장했다.

이 법안에 모든 사람들이 찬성하는 것은 물론 아닌데, 예를 들면 최근 일단의 프라이버시 옹호단체들은 위원회에 서한을 보내 동 법안이 프라이버시와 시민권을 침해할 수 있다고 주장한 바 있다.

위와 같은 미국의 사이버안보에 대한 초당적 협력사례는 우리에게 시사하는 바가 크다. 미국의 공화당과 민주당도 '기름과 물'과 같은 사이이지만 국가안보(사이버안보)에 있어서만큼은 찰떡궁합을 과시하여 미국의회와 국회의원의 품격을 여실히 보여주고 있다. 우리나라의 여당과 야당 모두 국가안보를 매우 중요시하는 정당이다. 그런 만큼 국가안보의 문제인 사이버안보 입법에 있어서도 초당적 협력을 통해 안보의 사각지대가 생기지 않도록 하여야 할 것이다.

(2) 이른바 「국가 사이버안보 기본법」의 제정의 필요성

1) 우리나라의 사이버안보 관련법령의 법체계 정합성문제

현행 사이버안보 관련 법률은 정보통신망법을 필두로 분야별 또는 적용대상별로 개별적·산발적으로 규정을 두고 있다. 그러나 현재의 사이버안보 관련 추진체계 및 법령체계는 다음과 같은 한계를 가지고 있다고 할 수 있다.

첫째, 정보통신망·정보시스템에 대한 중복규제 또는 공백이 발생하고 있다. 정보통신망 및 정보시스템이라는 유사한 보호대상에 대해서 분야 및 세부대상만 달리하여 규정함으로써, 동일한 주체에 대해서 여러 가지 법률이 동시에 적용되는 경우가 생기고 있다. 또한 정보통신망법이나 정보통신기반보호법 등에서 정보통신망과 기반시설 등 많은 영역을 규율하고는 있으나, 관련 법률의 어느 부분에서도 다루지 않는 공백도 존재한다고 할 수 있다. 예를 들어, 정보통신망법의 경우 정보통신서비스제공자를 중심으로 규정이 되어 있으며, 시스템과 정보통신망과의 연결을 전제로 하기 때문에 네트워크에 연결되지 않은 개별 컴퓨터 보호의 문제가 발생된다. 이에 대해서는 형법상의 컴퓨터 관련 규정도 적용되지 않아 법 적용의 사각지대가 된다 할 것이

다. 개별 법률의 소관부처가 다를 경우 추진체계의 분산을 초래하며, 문제 발생시 책임부처의 불명확으로 인해 대응에 혼선 발생이 가능하다. 최근의 침해사고의 경우 그 대응결과를 보면 확연히 문제가 됨을 알 수 있다.

둘째, 관련 주체들간 역할 분담의 형평성 문제가 있다. 정부・사업자・이용자 등 정보보호 관련 주체들의 역할이 명확치 않고 규제가 불균형적으로 이루어지는 경우가 존재한다. 또한 역할이 명확한 경우에도 형평을 고려하여 책임이 배분되지 못하고 일부에만 과중한 부담이 지워지는 경우가 있다.

셋째, 민・관 협력 및 중소기업・개인이용자 보호 규정이 미비하다. 여러 가지 사업자 대상 의무에 대해서 중소규모사업자의 이행에 실질적인 도움을 줄 수 있는 규정이 없어 실효성 확보가 어렵다는 것이 현재의 체계라고 할 수 있다. 마찬가지로 개인이용자가 본인의 PC를 쉽고 편리하게 보호할 수 있도록 국가차원에서 지원하는 규정도 거의 찾아볼 수 없다는 문제가 있다.

끝으로 국제적인 협력 관계 구축의 미비를 들 수 있다. 점차 대규모화 되고 있는 전자적 침해사고에 대응하기 위해서는 비상시의 국제적인 대응체계 구축이 필수적인데, 현행 법률의 국제협력 관련 규정은 대부분이 동향 파악 및 추상적인 협조 의무 규정에 불과하다고 할 수 있다.

국가 차원의 선제적 예방・대응능력을 확보할 수 있도록 민・관・산 협력을 바탕으로 국가차원의 종합정책의 추진이 가능할 수 있도록 하는 체계의 구축과 국가 중요시설에 대한 침해사고의 효율적 대응을 위하여 사이버안보 관련 추진체계 및 법령체계의 한계를 극복하고자 하는 노력이 필요하다.

2) 사이버안보 일반법의 제정방안

이른바 「국가 사이버안보 기본법」을 제정해서 사이버안보에 대한 종합적이고 체계적인 접근을 할 필요가 있다. 사이버안보에 관한 국가와 국민의 책임을 정하고 사이버안보정책의 방향과 그 추진에 필요한 기본적인 사항을 규정함으로써 사이버안보의 가치와 위상을 높여 사이버안보가 국가사회의 발전에 중요한 역할을 할 수 있다는 것을 입법목적으로 제시하여야 한다.

그리고 사이버안보가 자유민주주의의 수호와 국민 개개인의 안전된 삶을 위하여 가장 중요한 가치 중의 하나임을 인식하고, 사이버안보의 가치가 우리 사회 영역 전반에 확산될 수 있도록 국가가 그 역할을 다하도록 하며, 개인의 기본적인 권리와 조화롭게 실현되도록 하는 것을 기본이념으로 제시하여야 한다.

법안에 담길 주요 내용으로는 ① 사이버안보의 개념정의, ② 국가, 기업 및 국민의 책무, ③ 다른 법률과의 관계, ④ 사이버안보정책 수립·시행상의 기본원칙 – 개인정보보호에 터잡은 사이버안보 –, ⑤ 사이버안보기본계획의 수립, ⑥ 사이버안보를 위한 분야별 사이버안보정책의 추진, ⑦ 사이버안보 인식제고를 위한 조치, ⑧ 사이버안보를 위한 인력의 양성, ⑨ 사이버안보를 위한 조사·연구와 개발, ⑩ 사이버안보 정보제공 및 정보공개, ⑪ 사이버안보 국제협력, ⑫ 개별 사이버안보 관련 법률과의 기본적이고 원칙적인 연계조항 등을 들 수 있다.

이와 관련된 논의로 (가칭) 「사이버보안 기본법」을 제정하자는 주장이 있다.[41] 이정현 박사는 정보통신망·시스템 등 보호범위의 재구성, 침해사고대응체계 명확화, 관련 주체들간의 적절한 역할 분담, 중소기업 지원을 통한 보호의 실효성 확보, 개인 이용자의 인식제고 및 보호·지원, 국제적인 공조체제 구축 등 IT환경 변화를 수용하는 법률의 등장이 필요한 시점이라는 데에 착안한 것으로 보인다. 그리고 법률의 목적은 국가정보원, 미래창조과학부, 행정자치부, 국방부, 검찰 및 경찰 등에 분산된 정보보안기능을 리드하고, 통제하여 효율적으로 기능할 수 있는 컨트롤 타워를 만들고, 정보보안정책의 수립과 집행, 그리고 정보보안의 기반조성과 관련 산업의 발전에 관한 원칙을 제시하고 있다. 그리고 정보통신망법을 발전적으로 정리하여 사이버보안, 개인정보보호, 그리고 이용자보호로 3분하여 사이버보안을 중점적으로 규율하는 별도

41) 이정현, "국가 사이버안보 추진체계의 이슈와 과제", 「국가 사이버안보 추진체계의 이슈와 과제」 제3회 한국사이버안보법정책학회 월례세미나 발제문(2013. 7. 18), 32쪽-34쪽 참조

의 법률을 제안하는 방안도 제시되고 있다.[42] 특히 사이버보안이 날로 중요해진다는 점을 고려하여 현재와 같이 산재되어 있는 보안 관련 법령들보다는 사이버보안 영역에서 기본법 역할을 할 수 있는 「사이버보안 기본법」을 제정하자는 것이 주요골자이다. 이러한 새 법안에는 현행 「국가정보화 기본법」의 정보보안시책 수립에 관한 책무 등을 포함하고, 공공과 민간영역을 모두 아우르는 단일의 정보보안 추진체계를 갖추고, 국회에서 잠자고 있는 「악성프로그램 확산방지 등에 관한 법률(안)」에 갈음하여 침해사고에 대한 사전적·사후적 대응체계를 갖추며, 정보보안 평가·인증, 그리고 각종 점검제도에 대한 사항도 담자고 주장한다. 아울러 「사이버보안 기본법」을 제정하더라도 기왕의 개별 법률들은 현재 체제로 그대로 존속하되, 사이버보안에 관하여 기본법과 개별법의 상하 체계 구조로 개선하는 것이 낭비와 혼란을 막을 수 있는 방법이라고 한다. 개별적으로 국가정보화 기본법의 정보보안에 관한 규정은 「사이버보안 기본법」으로 이관하고, 정보통신기반보호법과 「국가사이버안전관리규정」은 상당 부분 서로 중복 또는 상충될 수 있으므로 조정하되, 정보보안 계획수립이나 추진체계 및 사이버보안 진흥정책 등은 「사이버보안 기본법」으로 이관하고, 폐지가 필요한 경우는 폐지도 고려하되, 각 개별 법령의 고유한 행위규제는 그대로 개별법에 존치시키는 방법을 채택하자고 한다.[43]

생각건대, 위에 제시된 방안들은 현행 사이버보안 관련 법령 등의 체계정합성 도모 측면에서 통폐합하자는 논의라고 볼 수 있다. 필자가 제안하는 법안은 모두가 공감할 수 있는 사이버안보와 관련한 가장 기본적이고 원칙적인 사항 위주로 가자는 것인 반면, 위에 제시된 이정현 박사의 방안들은 실체적인 사항들 위주로 규정하자는 것이기 때문에 접근방법이나 내용적인 측면에서 차이가 있다. 그리고 입법과정에서도 종래와 같은 전철을 밟을 가능성이

42) 한국인터넷진흥원, 「사이버보안법제 선진화 방안 연구」 (방송통신정책연구 11-진흥-라-02), 2011. 12 참조

43) 예를 들어, 정보통신망법의 해킹의 처벌과 같은 정보보안 관련 행위규제에 관한 법규정이 그것이다.

적지 않다고 본다. 그래서 필자가 의도하는 바는 사이버안보의 필요성에 관한 국민적 합의 도출을 먼저 하자는 것이다. 이는 추진체계문제 등이 전면에 부각되어서는 논의 자체가 어려워진 경험을 바탕으로 하고 있다. 참고로 현재 사이버안보 관련 법제는 정보통신망·정보시스템보호 관련법(정보통신망법, 정보통신기반보호법, 전자정부법, 국가사이버안전관리규정), 개인정보·사생활 보호 관련법(개인정보보호법, 정보통신망법, 위치정보법, 신용정보법, 통신비밀보호법), 사이버안전 인력·산업 육성 관련법(정보통신산업진흥법, 정보통신망법, 국가정보화기본법, 산업기술보호법, 국가사이버안전관리규정) 등 너무 많은 법들이 서로 중첩되거나 산재돼 있기 때문에 법체계 정합성 측면에서 관련 법률의 정비가 필요하다는 지적이 많다.

결론적으로 위와 같은 다양한 형태로 존재하는 사이버안보 관련법제의 체계정합성을 위해서는 「국가사이버안보 기본법」의 제정이 선결적으로 필요하다고 본다.

Ⅵ 결론: 사이버안보 입법의 전망

머리말에서도 밝혔듯이 세계적으로 사이버공격 사례가 증가하고 있으며 그에 대한 대응 또한 강경해지고 있다. 그 이유는 사이버전쟁은 선전포고도 없이 가상의 적국을 초토화시킬 수 있기 때문에 군사시설은 물론이고 전력, 통신, 금융망, 송유, 가스, 수도관 등 한 나라의 주요 기반시설을 순식간에 마비시킬 수 있다. 핵 공격 못지않게 더 큰 피해를 초래할 수 있는 것이 바로 사이버공격이기 때문이다.

우리나라를 둘러싸고 있는 인접 국가들인 중국, 일본, 미국 등은 사이버전을 대비하여 오래전부터 체계적으로 준비해 왔으며 사이버안보 관련법제를 지속적으로 정비해 왔다. 특히 미국의 경우에는 20여 년 동안 일관되게 사이버안보 법정책을 추진해 왔으며 미국의회의 초당적 협력이 있었다. 이러한

사이버안보 입법에 있어서 보여준 초당적 협력은 헌법수호기관으로서 미국 의회의 위상과 품격을 나타내기에 부족함이 없었다. 타산지석으로 삼아야 할 것이다.

그리고 사이버안보 입법환경 변화에 따른 입법전략을 모색할 필요가 있다. 그것에는 (1) 개인정보보호에 터잡은 사이버안보 입법, (2) 초연결사회에 기반한 사이버안보 입법, (3) 사이버투명성을 기반으로 한 사이버안보 입법, (4) 정보공유를 기반으로 한 사이버안보 입법, (5) 민-관 파트너십에 기반한 사이버안보 입법, (6) 교육친화적 사이버안보 입법 등에 대해 고찰하였다.

그리고 사이버안보 법체계 정당성 확보를 위한 입법과 관련해서는 (1) 초당적 협력에 기반한 사이버안보 입법 추진: 미국사례의 시사점, (2) 「국가사이버안보 기본법」의 제정의 필요성 등에 대해 생각한 바를 밝혔다.

[참고문헌]

강달천, “최근 사이버테러의 현황과 법적 의의 -”「사이버테러와 법정책적 대응」 2013년 한국사이버안보법정책학회 정기학술세미나 발제문, 2013. 5. 3

곽관훈, “최근 일본의 사이버안보 관련법령 현황과 시사점”「사이버 안보위협 대응전략의 법정책적 검토 및 전망」 2013년 한국사이버안보법정책학회 월례세미나 발제문, 2013. 12. 17

권현준, “IOT환경과 사이버안보의 법정책적 문제”「초연결사회와 사이버안보」 2014년 한국사이버안보법정책학회 추계학술대회 발제문, 2014. 11. 28

김성천, “최근 독일의 사이버안보 관련법령 동향과 시사점”「외국의 사이버안보 관련법제 동향 및 법정책적 과제」 2014년 한국사이버안보법정책학회 춘계학술대회 발제문, 2014. 5. 29

김성천, “사이버보안 법제에 관한 연구”, 중앙법학 제13집제3호, 2011. 9

김인중, “사이버안보 추진체계의 이슈와 과제”「사이버테러와 법정책적 대응」 2013년 한국사이버안보법정책학회 정기학술세미나 발제문, 2013. 5. 3

김일환, “독일 기본법상 대테러관련기관과 법제도들에 관한 고찰”「성균관법학」 제15권 제1호(2003)

김재광, 「국가 정보보호 추진체계 관련법제 분석」, 한국정보화진흥원, 2009. 12

김재광, 「전자정부법」, 한국법제연구원, 2010. 8

김재광, “사이버안보의 사회적 인식 제고를 위한 법정책적 개선방안”「사이버안보법정책논집<자료집>」 제1호, 한국사이버안보법정책학회, 2014. 12

김재광・김정임, “일본의 사이버위기 관련 법제의 현황과 전망”「법학논총」 제33권 제1호(2009. 6, 단국대 법학연구소)

김정임, “인도의 IT법제(사이버안보)의 분석과 시사점”「외국의 사이버안보 관련법제 동향 및 법정책적 과제」 2014년 한국사이버안보법정책학

회 춘계학술대회 발제문, 2015. 5. 29
김현수, 「주요정보기반보호(CIIP) 동향 -미국과 EU를 중심으로-」, 한국법제연구원, 2012. 10
김현수, “국가 사이버안보 법정책의 현황과 인식제고방안 - 미국의 사례를 증심으로 -” 「사이버위협의 현황과 법제도방안」 제1회 한국사이버안보법정책학회 월례세미나 발제문, 2013. 3. 20
박상돈 · 박현동 · 홍순좌, “미국 사이버보안 입법의 신경향 연구”, 정보보안논문지 제11권 제4호, 2011. 9
박영철, “사이버안보와 통신비밀보호법” 「사이버안보법정책논집<자료집>」 제1호, 한국사이버안보법정책학회, 2014. 12
양근원, “사이버테러 대응과 현행 절차법 검토”, 「인터넷법연구」 제3권 제1호, 2004
윤장홍, “초연결사회의 사이버안보와 관련한 기술적 기반” 「초연결사회와 사이버안보」 2014년 한국사이버안보법정책학회 추계학술대회 발제문, 2014. 11. 28
이정현, “국가 사이버안보 추진체계의 이슈와 과제” 「국가 사이버안보 추진체계의 이슈와 과제」 제3회 한국사이버안보법정책학회 월례세미나 발제문, 2013. 7. 18
이창범, “국내외 사이버안보관련 법제정 동향과 시사점” 「사이버테러와 법정책적 대응」 2013년 한국사이버안보법정책학회 정기학술세미나 발제문, 2013. 5. 3
이창범 · 강이석, 「프랑스의 정보보호 행정체계 및 법제 개요」, 한국인터넷진흥원, 2009. 12
이창범 · 강이석, 「독일의 정보보호 행정체계 및 법제 개요」, 한국인터넷진흥원, 2009. 12
이창범 · 이명아, 「영국의 정보보호 행정체계 및 법제 개요」, 한국인터넷진흥원, 2009. 12
장철준, “빅데이터 · 클라우드 환경과 사이버안보의 법정책적 문제” 「초연결사회와 사이버안보」 2014년 한국사이버안보법정책학회 추계학술대회 발제문, 2014. 11. 28

정준현, “국가 사이버안보를 위한 법제 현황과 개선방향” 「디지털 시대와 국가 정보 발전」, 2012

정필운, “스마트 환경에서 인터넷 침해사고 대응 조직과 추진체계”, 2012년 인터넷법제도포럼 발표자료

정태진, “인적 정보(HUMINT)의 역할강화를 통한 사이버 안보위협 대응전략” 「사이버 안보위협 대응전략의 법정책적 검토 및 전망」 2013년 한국사이버안보법정책학회 월례세미나 발제문, 2013. 12. 17

지성우, “독일의 사이버위기 관련 법제의 현황과 전망” 「사이버위기관련 법제의 현황과 전망」, 단국대 법학연구소, 2009. 5. 29

최경진, “정부 조직 개편에 따른 사이버안보법체계 개선방안” 「사이버위협의 현황과 법제도방안」 제1회 한국사이버안보법정책학회 월례세미나 발제문, 2013. 3. 20

한국인터넷진흥원, 「사이버보안법제 선진화 방안 연구」(방송통신정책연구 11-진흥-라-02), 2011. 12

현대호, “미국의 사이버위기 관련 법제의 현황과 전망” 「법학논총」 제33권 제1호, 단국대 법학연구소, 2009. 6

사이버안보와 개인정보보호법령의 상관성

최 경 진*

목 차

Ⅰ 머리말

사회의 거의 모든 설비와 서비스뿐만 아니라 중요기반시설이 대부분 인터넷에 연결되고 네트워크와 정보처리장치를 통한 제어가 가능해지면서 안보 개념에도 변화가 불가피해졌고 소위 '사이버안보'의 중요성을 고려하여 대통령실에 안보특보가 임명되고 사이버안보 강화대책의 마련을 위한 노력이 집중되고 있다. 그러나 사이버안보가 기존의 안보와 어떤 관계에 있고, 사이버안보에 대하여 누가 어떠한 권한과 의무를 가지는가 혹은 가져야 하는가에 대한 명확한 결론이 내려져 있지 않다. 나아가 사이버안보에 관하여 기존의 법률이 어떻게 작용하고 있는지에 대하여도 아직 정밀한 검토가 충분히 이루어지지 않고 있다. 반면, 정보통신기술의 발전으로 국민 개개인의 기본적 권리와 자유를 신장하고 보호해야 한다는 점은 강조되어, 안보 목적의 기본권 제한이나 정보기관의 활동을 위한 법적 근거를 마련하는 것은 매우 어려운

* 가천대학교 법과대학 교수

반면 국민의 기본적 권리의 보장을 강화하기 위한 관련 법령의 제개정은 상대적으로 쉽게 이루어지고 있다. 이로 인하여 국익을 위한 사이버안보 활동이 불가피한 경우에도 자칫 불법적인 사이버 안보활동을 묵인할 수밖에 없는 경우가 발생할 수도 있고 반대로 국가안보 차원의 불가피한 사이버안보 활동이 억제될 가능성도 있다. 어느 경우이든 국가 이익에 반하고 결과적으로 국민 개개인의 법익을 중대하게 해치는 결과로 이어질 수 있다는 문제가 있다. 이러한 문제는 여러 분야에서 나타날 수 있지만, 이 글에서 다루고자 하는 개인정보보호법령 영역에서 특히 문제된다. 사이버안보 활동의 상당수는 개인·단체 혹은 그 정보처리장치·네트워크의 활동에 대한 감시나 정보수집으로부터 이루어지기 때문에 개인정보보호법령과 충돌할 수 밖에 없다. 최근 우리나라는 은행권의 개인정보유출이나 카드사태 등으로 인해서 개인정보보호법령을 지속적으로 강화해오고 있다. 이러한 개인정보보호법령의 강화는 불가피하게 정부의 활동, 특히 정보수집을 핵심 기능으로 하는 정보기관에 의한 사이버안보 활동에 제약을 가하게 된다. 결국 개인정보보호를 통한 개인의 권리의 보장과 국가안보를 위한 사이버안보활동의 보장이라는 두 가지 법익의 충돌을 적절히 조화할 필요가 생겨난다. 이러한 문제의식을 바탕으로 이 글에서는 과거 및 현행 개인정보보호법령에서 사이버안보 활동에 대하여 어떻게 규율하고 있는가를 살펴본 후 주요 국가에서는 개인정보보호법규에서 어떻게 이를 다루고 있는지를 비교법적으로 검토하여, 최종적으로 바람직한 개인정보보호법령의 규율태도를 도출하고자 한다.

Ⅱ 우리나라의 개인정보보호법제와 사이버안보

1. 개인정보보호법 제정 이전

(1) 일반적 적용대상

2011.3.29. 「개인정보 보호법」[1](이 글에서 "개인정보보호법"이라 함)이

제정되기 이전에는 1994.1.7. 제정된 「공공기관의 개인정보보호에 관한 법률」[2](이하 "공공기관개인정보법"이라 함)이 공공기관에서의 개인정보보호를 규율하였다. 공공기관개인정보법은 "공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호"하는 것을 목적으로 하며(제1조), 그 적용대상은 공공기관이었다. 공공기관이란 "국가행정기관·지방자치단체 그 밖의 공공단체 중 대통령령이 정하는 기관"을 말하기 때문에 국가정보원과 같은 정보기관도 이에 포함되었다. 공공기관개인정보법이 보호하는 대상은 개인정보인데, 동법에 따른 개인정보란 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"(동법 제2조 제2호)를 말한다. 정보기관이 수집하는 개인에 관한 정보는 대부분 특정 개인에 관한 정보인 경우가 많고, 사이버안보 활동에서 수집되는 각종 정보도 궁극적으로 그 목적을 달성하기 위해서는 처음에는 비식별정보였다고 하더라도 다른 정보와 결합하여 특정 개인을 식별할 필요가 있기 때문에 이 법에 따른 보호대상이 된다.

(2) 국가안보에 대한 일반적 적용 제외

공공기관의 컴퓨터 등에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 공공기관개인정보법이 적용된다. 그러나 공공기관의 컴퓨터등에 의하여 처리되는 개인정보 중 「통계법」에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보분석을 목적

1) 이 법률은 2011.3.29. 법률 제10465호로 제정되어 2011.9.30.부터 시행되었다.
2) 이 법률은 1994.1.7. 법률 제4734호로 제정되어 1995.1.8.부터 시행되었다. 이 글에서는 개인정보보호법에 의하여 폐지되기 직전의 공공기관개인정보보호법을 기준으로 한다.

으로 수집 또는 제공 요청되는 개인정보의 보호에 관하여는 이 법을 적용하지 않는다(제3조 제2항). 이러한 예외에 따라 정보기관이 국가안보 목적으로 수집하거나 다른 공공기관에 제공을 요청하여 수집하는 개인정보에 대해서는 공공기관개인정보법이 적용되지 않는다. 이처럼 국가안보 목적의 일반적 적용제외 규정으로 인하여 공공기관개인정보법은 사이버안보를 포함하는 국가안보 영역에는 개입하지 않았었다. 또한 나아가 국가안전보장과 관련된 국가중요시설 중 원자력발전소 등 대통령령으로 정하는 시설에 대하여는 폐쇄회로 텔레비전을 설치하는 경우 정보주체가 이를 쉽게 인식할 수 있도록 일정한 사항을 기재된 안내판을 설치하는 등 필요한 조치를 취할 필요가 없다(제4조의2 제4항).

2. 개인정보보호법 제정 이후

(1) 일반적 적용대상

개인정보보호법이 제정됨에 따라 종래의 공공기관개인정보법은 폐지되고 개인정보보호법으로 통합되었다. 이에 따라 민간과 공공을 불문하고 일원적으로 개인정보보호법이 적용된다. 현행 개인정보보호법은 “개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함”(제1조)을 목적으로 한다. 이 법에 따라 보호되는 개인정보는 “살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)”를 말하는데, 이는 공공기관개인정보법과 일부 문구에 차이가 있을 뿐 동일하다. 개인정보보호법을 준수하여야 하는 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. 이 때 개인정보파일이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으

로 배열하거나 구성한 개인정보의 집합물(集合物)을 말하며, 공공기관이란 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체, 「국가인권위원회법」 제3조에 따른 국가인권위원회, 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관, 「지방공기업법」에 따른 지방공사와 지방공단, 특별법에 따라 설립된 특수법인, 「초·중등교육법」, 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교를 말한다. 국가정보원은 대통령 소속 기관으로서(「국가정보원법」 제2조) 개인정보보호법 제2조 제6호에 따른 공공기관에 해당하고, 국가정보원은 「국가정보원법」 제3조에 따른 직무를 수행하기 위하여 정보를 수집하고, 개인정보를 포함하여 수집된 정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 온오프라인에서 구축·운영하고 있기 때문에 개인정보처리자에 해당한다. 즉, 국가정보원도 개인정보보호법에 따른 개인정보처리자로서 동법이 적용된다.

(2) 국가안보에 대한 부분적 적용 제외

1) 국가안보에 대한 적용 제외

원칙적으로 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보보호법이 적용된다(제4조). 그러나 공공기관개인정보법과 마찬가지로 개인정보보호법도 "국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보"의 경우에는 개인정보보호법 제3장(개인정보의 처리), 제4장(개인정보의 안전한 관리), 제5장(정보주체의 권리 보장), 제6장(개인정보 분쟁조정위원회), 제7장(개인정보 단체소송)의 규정이 적용되지 않는다(개인정보보호법 제58조 제1항 제2호). 이에 따라 주요 개인정보보호 관련 규정은 사이버안보 활동에 적용되지 않는다. 또한 개인정보보호법은 공공기관의 장이 개인정보파일을 운용하는 경우에는 행정자치부장관에게 등록하도록 요구하는데(제32조 제1항), ① 국가 안전, 외교상 비밀, 그 밖에

국가의 중대한 이익에 관한 사항을 기록한 개인정보파일, ② 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일, ③ 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일, ④ 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일, ⑤ 다른 법령에 따라 비밀로 분류된 개인정보파일에 대하여는 등록이 면제된다. 결국 국가정보원은 국가 안전에 관한 사항을 기록한 개인정보파일을 운용하더라도 행정자치부장관에게 등록할 필요가 없다.

이상과 같이 개인정보보호법은 국가안보에 대한 적용을 제한하고 있지만, 공공기관개인정보법과는 달리 개인정보보호법의 전 규정을 적용 배제하는 일반적 적용 제외 방식으로 규정하지 않고 대부분의 규정은 제외하되 기본원칙이나 개인정보보호정책을 비롯한 추진체계와 일부 보칙 규정의 적용에 대해서는 적용을 배제하지 않아서 사이버안보 활동 과정에서의 개인정보처리에 대하여 일정한 제한을 가할 수 있는 여지를 남기고 있다. 사이버안보에도 적용되는 규정을 살펴보면 다음과 같다.

2) 예외 - 국가안보에도 적용되는 규정

(가) 기본원칙

개인정보보호법의 기본원칙(제3조)은 국가안전보장을 위한 개인정보의 처리에도 적용된다. 즉, ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다. ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다. ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야

한다. ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다. ⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다. ⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다. ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다. 국가정보원이 사이버안보 활동 과정에서 최소한의 범위에서 위와 같은 기본원칙을 준수하여야 한다. 이러한 기본원칙을 위반한 경우에 별다른 제재조항은 없지만, 기본원칙을 준수하지 않은 경우에 국가배상청구의 대상이 될 수도 있다.

(나) 정보주체의 권리 보장

정보주체는 자신의 개인정보 처리와 관련하여 ① 개인정보의 처리에 관한 정보를 제공받을 권리, ② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리, ③ 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함)을 요구할 권리, ④ 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리, ⑤ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리를 가진다(제4조). 이러한 정보주체의 권리를 보장하지 않는 경우에 별다른 제재조항은 없지만 국가배상청구의 대상이 될 수도 있고, 정보주체는 법원에 이러한 권리를 실현하기 위한 소를 제기할 가능성도 있다.

(다) 책무

정보기관도 국가기관으로서 일정한 책무를 가진다(제5조). 즉, 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다. 또한 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다. 개인정보의 처리에 관한 불합리한 사회적 관행을

개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진・지원하여야 하며, 개인정보의 처리에 관한 법령 또는 조례를 제정하거나 개정하는 경우에는 개인정보보호법의 목적에 부합되도록 하여야 한다. 이러한 책무는 정보기관의 고유 업무와의 충돌을 야기할 수 있다.

(라) 정책 추진 체계

개인정보보호법은 개인정보보호정책의 효과적인 추진을 위하여 대통령 소속으로 개인정보보호위원회를 설치하여 운영토록 하였다. 개인정보보호위원회의 기능으로는 ① 개인정보보호 기본계획 및 시행계획, ② 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항, ③ 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항, ④ 개인정보 보호에 관한 법령의 해석・운용에 관한 사항, ⑤ 개인정보의 이용・제공에 관한 사항, ⑥ 영향평가 결과에 관한 사항, ⑦ 의견제시에 관한 사항, ⑧ 조치의 권고에 관한 사항, ⑨처리 결과의 공표에 관한 사항, ⑩ 연차보고서의 작성・제출에 관한 사항, ⑪ 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항, ⑫ 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의・의결하는 사항에 대한 심의・의결을 수행한다. 이 중에서 개인정보의 처리에 관하여 정보기관인 국가정보원과 다른 공공기관 사이의 의견조정이 필요한 때에는 개인정보보호위원회가 심의・의결할 수 있다(제8조 제1항). 또한 공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의・의결을 거친 경우는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있도록 규정하고 있는데(제18조 제2항 제5호), 이 규정에 따라 예외적으로 국가정보원이 개인정보를 목적 외 용도로 이용하거나 제3자에게 제공하고자 하는 경우에도 개인정보보호위원회의 심의・의결을 거쳐야 한다.

(마) 금지행위

국가정보원에서 개인정보를 처리하거나 처리하였던 자는 ① 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위, ② 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위, ③ 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위를 하지 말아야 한다(제59조). 이러한 금지행위를 한 자에게는 5년 이하의 징역 또는 5천만원 이하의 벌금(②와 ③의 금지행위)이나 3년 이하의 징역 또는 3천만원 이하의 벌금(①의 금지행위)에 처해진다(제71조 제5호, 제6호 및 제72조 제2호).

3. 해외 주요국의 동향

(1) 미국의 입법 동향

미국은 1947년 국가안보법(National Security Act), 중앙정보부법(Central Intelligence Agency Act), 국가안보국법(National Security Agency Act), 국가안전법(Internal Security Act), 해외정보감시법(Foreign Intelligence Surveillance Act), 비밀정보절차법(Classified Information Procedures Act), 정보요원신분보호법(Intelligence Identities Protection Act), CIA정보법(Central Intelligence Agency Information Act), 국토안보법(Homeland Security Act), 애국법(USA Patriot Act) 등에 기초하여 광범위한 개인정보 수집 권한을 부여받았지만, 기관간 사이버 보안 정보의 신속한 공유 및 보호를 위한 입법을 추진 중에 있다. 이하에서는 그 동안 추진되었던 사이버안보 관련 법률안에 대하여 간략하게 소개한다.

1) 사이버 정보 공유 및 보호법 「Cyber Intelligence Sharing and Protection Act (H.R.624)」

정보기관과 사이버 보안 기관 사이의 사이버위협 정보의 공유를 목적으로 한 법률안으로서 사이버 보안과 관련된 연방정부의 협력 활동, 협력 정보 공유,

사이버보안 범죄를 위한 협력 조직 할당, 협력 조직에 의한 정보 공유 등을 규정한다. 특히, 연방기관 웹사이트에 개인정보를 게시할 경우, 각 웹사이트별 프라이버시 요건 및 프라이버시 지침을 수립하도록 하였다.

2) 보안정보통신법 「SECURE IT (H.R.1468)」

사이버위협정보의 공유 및 연방정보보안정책의 협력에 관한 사항을 규정하여 정보보안 증진을 목적으로 하여, 사이버위협정보의 공유를 촉진하기 위하여 사이버위협정보 공유 허가, 연방정부에 의한 정보공유, 검사, 비밀 정보에의 접근을 규정하고, 연방정보보안정책의 협력을 위하여 연방정보보안정책의 협력과 정보기술의 관리 등에 관한 사항을 규정한다.

3) 사이버보안 증진법 2014 「Cybersecurity Enhancement Act of 2014 (S. 1353)」

사이버보안의 증진 및 사이버보안 연구・개발, 작업인력 개발, 교육, 공적 감시 및 준비태새를 강화 하기 위한 지속적이고 자발적인 공공민간 파트너쉽을 규정한 법률안으로서 사이버보안에 관한 공공-민간 협력, 교육 및 작업인력 개발, 사이버보안 기술 표준 고도화 등을 규정하였다. 특히, 사이버 보안에 관한 공공-민간의 협력체계를 구축하기 위하여, 연방사이버보안 연구・개발을 촉진하는 규정을 두고, 컴퓨터・네트워크 보안 연구 센터를 설치, 정부 시스템을 위한 사이버보안 자동화 및 체크리스트, NIST(National Institute of Stnadards and Technology)의 사이버보안 연구・개발을 규정하고, 사이버보안 연구・개발을 위하여 연방 사이버보안연구개발에 관한 규정을 두고, 컴퓨터・네트워크 보안연구센터 설치, 정부 시스템을 위한 사이버보안 자동화 및 체크리스트 명확화, NIST의 사이버보안 연구・개발 지원을 규정한다. 또한 사이버보안 감시 및 준비태세를 위하여 연방사이버보안 감시 및 교육프로그램을 운용토록 하였고, 사이버보안 기술 표준 고도화를 위하여 국제 사이버보안 기술표준, 클라우드 컴퓨팅 전략, 신원 관리 연구・개발을 규정한다.

4) 사이버보안 정보 공유법 2014 「Cybersecurity Information Sharing Act of 2014 (S.2588)」

사이버 보안 위협에 대한 정보 공유의 증진을 통하여 미국 내 사이버보안을 증진하기 위한 법률안으로서 연방정부에 의한 사이버보안 위협정보의 공유에 대한 법적 근거를 규정하면서, 사이버보안 위협을 예방, 탐지, 분석 및 억제하기 위한 권한을 규정하고, 사이버위협 표지자 및 대응책을 연방정부와 공유하는 규정을 둠. 아울러 책임으로부터 보호와 정부 활동이나 사이버보안 위협에 관한 보고 등을 규정한다.

5) 사이버 정보 공유 및 보호법 「Cyber Intelligence Sharing and Protection Act (H.R.234)」

정보기관과 사이버 보안 기관 사이의 사이버위협 정보의 공유를 목적으로 한 법률안으로서 사이버 보안과 관련된 연방정부의 협력 활동, 협력 정보 공유, 사이버보안 범죄를 위한 협력 조직 할당, 협력 조직에 의한 정보 공유, 감시의 제한, 정보의 이용 및 보유 기준, 비참여에 대한 비책임 등을 규정한다.

6) 사이버 네트워크 보호법 「Protecting Cyber Networks Act (H. R. 1560)」

사이버안보 위협에 대한 정보의 증진된 공유를 통하여 미국에서 사이버안보를 증진하고, 사이버안보 위험과 관련된 정보의 다면적 공유를 증진하고 프라이버시 및 시민의 자유 보호를 증진기 위하여 국토안보법을 개정하기 위한 법률안으로서 사이버안보 위협을 예방, 탐지, 분석 및 억지하기 위한 권한, 사이버 위협 표지자 및 방어 조치의 공유, 연방사이버보안보호선진화법으로서 국가사이버안보 및 통진 통합 센터 설립 운영에 관하여 규정한다.

7) 사이버위협공유법 2015 「Cyber Threat Sharing Act of 2015 (S.456)」

정보시스템을 더 잘 보호하기 위하여 민간간 및 공공과 민간 사이의 사이버보안 위협 표지자 공유를 가능하게 하기 위한 체계를 입법하기 위한 법률안으로서 민간 사이 또는 공공과 민간간의 사이버보안 위협 표지자 정보에

대한 공유를 가능하게 하는 체계를 구축하는 법적 근거를 규정한다.

8) 국가 사이버안보 보호 선진화법 2015 「National Cybersecurity Protection Advancement Act of 2015 (H.R.1731)」

사이버안보 위협과 관련된 정보의 다면적 공유를 증진하고 프라이버시와 시민의 자유를 강화하기 위하여 2002년 국토안보법을 개정하기 위한 법률안으로서 국가 사이버안보 및 통신 통합센터(National Cybersecurity and Communications Integration Center)의 설치·운영, 정보 공유 체계 및 절차, 내부자고발 보호, 다른 법률과의 관계 등을 규정한다.

9) 사이버안보 정보 공유법 「Cybersecurity Information Sharing Act of 2015 (S.754)」

사이버안보 위협에 대한 정보의 공유 증진을 통하여 미국의 사이버안보를 증진하기 위한 법률안으로서 연방정부의 정보 공유, 사이버안보 위협을 예방, 탐지, 분석 및 제거하기 위한 권한, 사이버위협 표지자 및 방어 조치를 연방정부와 공유, 책임으로부터의 보호 등을 규정한다.

10) 소결

이상과 같이 미국은 기존의 다양한 법률에 따라 국가안전보장과 관련된 광범위한 정보 수집 및 처리 권한을 허용하고 있었지만, 최근 사이버안보의 중요성이 강조되고 기관간 효율적인 정보의 공유를 촉진하기 위하여 여러 법률안을 발의하여 입법을 추진하고 있다. 나아가 사이버안보정보의 공유를 통한 프라이버시 침해를 막기 위한 최소한의 보호막으로서 프라이버시 지침을 수립하도록 하거나 내부 고발자 보호를 통한 투명성 촉진 등의 법제도적 기반도 일부 법안에서 함께 추진되고 있음을 알 수 있다.

(2) EU의 입법 동향[3)]

EU는 회원국 국민의 기본권과 자유를 보호하고 개인정보 처리와 관련한

3) EU의 입법동향에 대하여는 최경진, "EU와 미국의 개인정보 규율체계 개선 동향", 「개인정보 보호의 법과 정책」(고학수 편), 박영사, 2014 참조.

프라이버시권을 보호하며 EU 회원국 간의 개인정보의 자유로운 유통을 촉진하기 위하여, 1995년 10월 24일 “개인 정보의 처리와 자유로운 유통에 관한 개인정보보호지침(Directive of the European Parliament of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC)”(이하 “DPD”라 함)을 제정하여 현재까지 EU 역내에서 개인정보의 처리에 관한 중요한 지침으로 작용하고 있다. 그러나 DPD는 EU 회원국에 대하여 직접적인 강제력을 가지거나 직접 적용될 수 없는 지침(directive)의 형태로 되어 있어서 각국은 국내법에 따라 서로 상이한 보호수준을 채택하여 회원국간 불균형이 발생하였고, 인터넷을 통한 개인정보의 유통으로부터 개인을 보호할 필요성도 더욱 강조되었다. 결국, 인터넷 상에서의 개인정보 처리의 중요성 및 EU 회원국 내의 단일한 규율체계 정비의 필요성 등을 바탕으로 하여 2011년 7월 6일 유럽의회(European Parliament)가 “유럽연합에서의 개인정보보호에 관한 종합적 접근”을 의결하면서 입법이 가시화되기 시작하였다.[4] 이후 EU 역내의 강화된 단일 개인정보보호 입법을 목표로 2012년 1월 25일에 2012 GDPR(안) 및 “형사범죄의 예방, 수사, 기소 또는 형 집행 및 그 정보의 자유로운 이동을 위한 관할 관청에 의한 개인정보의 처리와 관련한 개인의 보호에 관한 유럽 의회 및 유럽 이사회 지침안(Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data)”이 발표되면서 입법이 구체화 되었다. EU 차원의 개인정보보호를 위

4) European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union(2011/2025(INI)) 16.

한 입법 노력은 1995년 EU가 DPD를 제정한 이후 16년여 만이다. 더욱이 이번 발표에서 주목할 만 한 점은 지침의 전면개정에 머무르지 않고 EU 회원국의 국내에 직접 법적 효과가 발생하는 'Regulation'의 형태로 추진된다는 점이다. EU 법체계 하에서 'Regulation'은 EU 전체에 직접 적용되는 매우 강력한 규범이고, 'Regulation'이 발효되면 회원국의 국내법에 우선하여 적용된다. 따라서 회원국은 국내법을 EU 규정에 일치시키는 입법을 하거나 기존 법을 개정하여야 한다. 규정안이 발효되려면 27개 회원국 정부 대표로 구성된 유럽 이사회와 유럽 의회의 승인을 받아야 한다. 최초 GDPR(안)이 제안되었을 때에는 2014년 발효를 목표로 하였지만, 2013년에 유럽의회를 통과할 때까지 4,000개 이상의 수정안 및 수정의견이 제시되었을 정도로 많은 논란과 논의가 진행되어 실제 입법이 완료될 때까지 많은 어려움이 있을 것으로 예상되었다. 그런데 스노든(Edward Snowden) 사건을 전기로 하여 EU 역외, 특히 외국 국가기관에 의하여 처리되는 EU 회원국 국민의 개인정보보호의 강화 논의가 촉발되었고 결국 2013년 10월 22일에 유럽의회를 통과하였다. 그리고 2014년 유럽 선거 이전에 최종 통과를 목표로 하였지만, 2013년 10월 25일에 유럽이사회는 최종 기한을 2014년이 아닌 2015년으로 수정하여 향후 일정을 최종 확정하였다.[5)]

(3) 최근 유럽사법재판소 판결

1) 사건 개요

DPD는 개인정보의 적절한 보호수준(adequate level of protection of the data)을 제공하는 경우에는 제3국으로의 개인정보를 이전할 수 있도록 규정하고 있고, EU 위원회(EU Commission)는 미국과의 사이에서 개인정보의 국가간 이전에 관한 Safe Harbor 협정을 체결하여 미국 기업들이 EU 회원국 국민의 개인정보를 수집·이용할 수 있도록 근거를 마련하였다. 이 사건에서는, 2008년부터 페이스북(Facebook) 이용자였던 Maximillian

5) EUCO 169/13.

Schrems이라는 호주 시민이 페이스북에 제공했던 개인정보가 페이스북 아일랜드 자회사로부터 미국에 있는 서버로 이전되어 처리되었는데, 미국 정보기관(NSA)가 미국 스노든 사건에서 드러난 사실관계를 바탕으로 미국의 법과 실무가 미국으로 이전된 정보의 공적 기관에 의한 감시에 대한 충분한 보호를 제공하지 못한다고 주장하면서 아일랜드 정보보호청에 청원을 제기하였다. 아일랜드 감독기구는 그러한 청원을 거절하였다. 그 이유는 2000년 7월 26일 EU 위원회가 미국 상부부와 적절한 보호 수준을 제공하기 위한 자발적인 체계를 구축하기 위하여 Safe Harbor Agreement를 체결하여 시행되고 있다는 점이었다. 이 Safe Harbor 협정에 의하여 현재까지 4,000개 이상의 미국 기업들이 EU로부터 미국으로 개인정보를 이전할 수 있었다. 그런데 2015.10.6. 유럽사법재판소(ECJ)가 지난 15년 가까지 유지해 온 Safe Harbor를 무효화하는 판결을 선고하였다. Safe Harbor 협정에 대하여는 EU가 GDPR(안)의 입법을 추진하는 과정에서 개정 논의가 진행 중이었고, 2013.11.27. EU 위원회는 투명성, ADR 체계의 구제, 집행 개선, 미국 당국에 의한 접근 등 13개 권고를 마련하였었지만, Safe Harbor 협정의 개정은 난항을 겪어왔었다. 그러던 중 이번 ECJ 판결을 계기로 Safe Harbor 협정 개정 논의에 속도가 붙을 것으로 예상된다.

2) 판결 주요 내용

ECJ 판결의 핵심 내용은 DPD 하에서 요구되는 적절한 개인정보보호 수준이 Safe Harbor 체계 하에서 충족되지 못한다는 것이다. 그 이유는 미국 정보기관에 의하여 미국으로 전송되는 EU 회원국 국민의 개인정보에 대한 접근이 - 특히 Safe Harbor 협정에 대한 문언적 검토에 비추어 Safe Harbor 협정이 엄격하게 필수적이고 필요한 범위를 초과하여 미국 집행 당국의 개인정보에 대한 접근을 허용한다는 점에서 - 유럽 기본권 헌장에 의하여 보장되는 사생활의 자유와 권리 및 개인정보보호에 대한 권리를 침해한다는 것이고, 미국이 감청이나 감시하는 것과 관련하여 유럽시민이 질의하는

경우에 적절한 회신을 받을 수 없는 상황은 유럽 기본권 헌장에 의하여 보호되는 효과적인 침해 제거 및 보상에 대한 유럽 시민의 권리가 침해되는 것에 상응한다는 것이다.

ECJ는 EU 위원회가 Safe Harbor 협정과 같은 결정을 채택하였더라도, EU 회원국 내의 개인정보보호 감독기구는 개인정보가 제3국으로 이전되는 것이 DPD의 요건을 준수하였는지를 완전히 독자적으로 검토할 권한을 가진다고 판단하였다. 궁극적으로는 ECJ가 EU 위원회의 결정이 유효한지를 결정할 권한을 가진다는 것이다. 이러한 판단 하에 위와 같은 Safe Harbor 협정의 무효를 선언한 것이다.

3) 판결에 따른 효과

ECJ 판결에 따라 개인정보보호감독기구가 허가하거나 DPD의 예외에 해당하지 않는 이상 Safe Harbor 협정에 따른 EU로부터 미국으로의 개인정보의 이전은 불법이 되었다. Safe Harbor 협정에 따라 EU 자회사로부터 미국 모회사나 다른 미국 법인으로 개인정보를 이전하던 다국적 기업은 BCRs과 같이 개인정보 국외이전을 위하여 Safe Harbor 협정을 대체할 수 있는 체계를 모색하여야 한다. 그러나 이번 판결을 기초로 즉각적인 법집행이 이루어질 것으로 예상되지는 않는다. EU 회원국 내의 정보보호감독기구들은 일정한 유예기간을 허용할 것으로 예상되며, EU DPD에서 요구하는 적절한 보호 수준과 조화하기 위한 노력을 기울일 것으로 예상된다.

Safe Harbor의 향후 방향과 관련해서는 현재 EU와 미국이 Safe Harbor 2.0 체결을 위하여 2013년 EU 위원회의 권고와 관련한 논의를 진행해 왔지만, 특히 개인정보 침해 시의 구제(Redress)와 관련해서는 미국 내 법률의 제개정이 필요한데 선거를 앞두고 있어서 입법 여부가 불투명하다는 문제가 있다. 한편 2014.1. 오바마 정책 지침 28(Presidential Policy Directive 28)은 정보보호 관점에서 NSA의 업무수행에 일정한 제한을 가하고 있다는 점에서 향후 Safe Harbor 2.0의 채택 가능성은 낮지 않다. 특

히 이번 판결로 미국은 개인정보보호 관점에서 미국 정보기관의 활동에 많은 압박을 받을 것으로 보인다.

Ⅲ 최근 국내 입법 동향

1. 사이버위협정보 공유에 관한 법률안

사이버보안과 관련된 개인정보의 처리와 관련된 법률안으로서 사이버위협정보 공유에 관한 법률안이 있다. 이 법안은 2015.5.19. 이철우 의원이 대표발의하였고, 현재 상임위 심사를 받고 있다. 이 법안은 2013년 3.20, 6.25 사이버테러로 청와대 홈페이지 변조는 물론 민간 방송·금융사 전산시스템이 대량으로 파괴되는 피해가 발생하였으며 2014년에는 한국수력원자력 제어시스템 가동을 중단시킬 목적으로 대량의 해킹메일이 유포되는 등 최근의 사이버위협은 단순 정보절취를 넘어 국민생활과 직결되는 사회기반시설의 안전까지 위협하여 우리의 경제와 국가안보를 저해하는 가장 심각한 위협 중의 하나로 대두되고 있다는 인식 하에 발의되었다. 특히 일부 지역에 국한해 발생하는 물리적 위협과 달리 사이버위협은 초국가적으로 시·공간을 초월하여 공공·민간 영역 구분이 없이 동시 다발적으로 발생함으로써 사이버위협 요인을 조기에 파악하여 차단하지 않을 경우 피해가 순식간에 확산되는 특성이 있고, 따라서 이러한 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 구축하려는 것을 입법목적으로 한다. 이는 미국 의회에서 논의 중인 사이버위협정보의 공유와 관련된 입법과 그 맥을 같이 한다.

동 법률안의 주요 내용을 살펴보면, 공공·민간 영역 간에 공유하는 '사이버위협정보'를 정의(안 제2조)하고, 국정원장은 국가안보실장, 미래창조과학부 장관 등과 협의하여 범정부 차원에서 사이버위협정보를 공유하기 위한 방

법과 절차를 마련하도록 하였다(안 제4조). 국가의 주요 정보와 정보통신망을 관리하는 기관(이하 "사이버위협정보 공유기관")은 사이버위협정보를 수집하고 상호 공유하여야 하며(안 제4조), 사이버위협정보 공유를 효율적으로 수행하기 위하여 국정원장 소속으로 사이버위협정보 공유센터(이하 "공유센터")를 설치·운영토록 하였다(제5조). 공유센터의 장은 공유된 사이버위협정보를 종합 분석하고 결과를 사이버위협정보 공유기관 및 관련 업체에게 제공하여야 하며(안 제6조), 국정원장은 법무부 장관 등 국가기관 및 전문가가 참여하는 협의회를 구성하여 사이버위협 정보의 남용방지 대책을 수립하여야 한다(안 제7조). 사이버위협정보를 보유한 사람은 공유센터의 장에게 신고하거나 공유센터의 장이 사이버위협정보의 제공을 요청할 수 있고(안 제8조), 공유센터의 장은 사이버위협정보 공유 활동에 대한 결과를 평가하고 그 결과를 국회에 보고하여야 한다(안 제9조). 사이버위협정보 공유기관, 공유센터 등의 종사자는 직무상 알게 된 비밀을 누설하지 말아야 하고 이에 위반한 때에는 벌칙을 부과한다(안 제10·11조).

2. 사이버테러 또는 사이버안전과 관련한 법률안

사이버테러나 사이버안전과 관련한 일반적인 사항을 규정하는 법률안으로서 2015.6.24. 발의된 "사이버테러 방지 및 대응에 관한 법률안"(이노근 의원 대표발의안), 2013.4.9. 발의된 "국가 사이버테러 방지에 관한 법률안"(서상기 의원 대표발의안), 2013.3.36. 발의된 "국가 사이버안전 관리에 관한 법률안"(하태경 의원 대표발의안)이 제19대 국회에 계류 중이다. 이들 법안의 주요 내용은 사이버안전, 사이버위기, 사이버공격, 사이버테러의 중요성을 인식하여 이에 효과적으로 대응할 수 있는 체계를 만들고, 민관협력, 국가정보원장의 권한, 사이버안전센터의 설치·운영, 사이버테러대응체계의 구축 등을 규정하고 있다.

Ⅳ 제언

개인정보보호와 사이버안보는 서로 긴장관계에 있으면서도 불가분의 관계에 있다. 사이버안보를 꾀하기 위해서는 개인정보의 처리가 불가피하지만, 개인정보보호를 함으로써 사이버안보도 도모할 수 있으며, 사이버안보가 확보되면 개인정보보호도 함께 이루어질 수 있는 긴밀한 관계이다. 또한 사이버안보는 국가안전보장이라는 측면에서도 매우 중요한 부분을 차지하고 있기 때문에 사이버안보를 위한 개인정보의 처리는 적절한 범위에서 허용할 필요가 있다. 이처럼 개인정보보호와 사이버안보는 적절한 균형관계를 꾀하여야 하는데, 특히 ECJ 판결에서 보는 것처럼 자칫 과도한 개인정보보호에 대한 제한은 민간 분야에서의 국가간 개인정보의 이전 및 이를 기반으로 한 무역을 가로막는 장애가 될 수도 있다. 최근 우리나라도 EU 적절성 평가를 비롯한 국제적인 개인정보의 이전에 적극적으로 대응하고자 준비를 하고 있는 상황에서 국내 정보기관에 의한 무제한적이고 무분별한 개인정보에 대한 접근이나 처리를 허용하는 것은 바람직하지 못하다. 반면, 사이버안보를 꾀하기 위한 정보 수집의 은밀성이나 불가피성 등을 고려할 때 너무 많은 제한을 하거나 모든 절차를 투명하게 공개하도록 강제하는 것도 국익에 반한다. 따라서 사이버안보를 위한 개인정보처리의 근거는 현재처럼 유지하면서도, 사이버안보 활동 과정에서 개인정보가 부당하게 침해된 경우에 적절한 구제가 이루어질 수 있는 체계를 유지하는 것이 필요하다. 이런 관점에서 현행 개인정보보호법 상 개인정보분쟁조정위원회에 의한 개인정보분쟁해결 규정을 적용제외한 것을 재고하거나 아니면 다른 적절한 구제절차를 마련토록 하는 것이 필요하다. 또한 미국 대통령 정책 지침에서와 같이 정보기관 내부적으로 자율적인 통제가 이루어지기 위한 법적 기반을 강화하는 정책을 추진하는 것도 바람직한 방향이다. 이런 관점에서 현행 「국가정보보안 기본지침(국가정보원)」, 「보안업무규정」, 「국가사이버안전관리규정」의 제정 및 운영은 하나의 중요한 법적 기반이 될 수 있다.

제4장 사이버안보를 위한 기술과 법의 만남

최근 사이버 위협동향과 기술적 대응방향

정 용 욱*

목 차

Ⅰ 서 론

일상생활에서 가깝게 사용하는 컴퓨터에는 표면적으로 나타나지 않은 사이버 위협들이 인터넷과 연계되어 존재하고 있다. 사이버위협이란 악의적인 사용자가 컴퓨터를 이용하고 네트워크를 경유하여 타인에게 위험적 요소를 전달하는 모든 행위를 말한다. 최근 대중화되어 알려진 IOT를 이용한 드론(무인항공기) 위협이 있으며 개인의 신상을 폭로하고 파멸시키는 평판위협이 있다. 또한 인터넷 소셜 네트워크를 사용한 정보교환 및 공격에 대한 방어가 있다. 본 논고에서는 이러한 위협들에 대한 용어 및 기술을 정리하고 적용사례, 위험요소, 대응방안에 대해 알아본다.

* 경찰청, 박사.

Ⅱ 본 론

1. IOT를 이용한 드론(무인항공기)의 위협

(1) 사물인터넷(IOT)의 이해

드론에 대한 위협을 알기 위해서는 사물인터넷(IOT)에 대한 이해가 필요하다. 사물 인터넷과 관련된 용어에는 M2M, 유비쿼터스, 사물인터넷, 만물인터넷 등이 있으며 다음과 같이 정의하고 있다.

- M2M: 사람이 직접 제어하지 않고 장비나 사물간의 양방향 통신을 의미한다.
- 유비쿼터스: 사용자가 시간에 상관없이 자유롭게 네트워크에 접속할 수 있는 환경(Ubiquitous)을 의미한다.
- 사물 인터넷: 인터넷 기반으로 M2M(사람+ 사물, 사물+ 사물)을 연결해 서로간의 정보를 상호 소통하는 지능형 기술 및 서비스(IoT)를 의미한다.
- 만물 인터넷: 사물 인터넷이 정의하는 대상을 모든 사물환경으로 확대하여 상호소통하는 지능형 서비스(IoE)를 의미한다.

사물 인터넷 3대 기술에는 센서를 사용하는 기술, 유무선 통신 네트워크를 사용하는 기술, 사용자 서비스에 대한 인터페이스 제공기술 등이 있다.

- 센싱 기술: 온도/습도/초음파 센서, 원격감지, 영상센서 등이 사물과 주위환경에서 정보를 수집하게 된다.
- 유무선 통신 및 네트워크 인프라: 블루투스, 와이파이, RFID 등 근거리 무선통신, WCDMA, LTE 같은 이동통신기술, GPS 등을 사용한다.
- 서비스 인터페이스: 정보수집, 가공추출 처리, 저장, 판단, 보안 및 프라이버시 보호, 객체 정형화 등을 포함한다.

사물 인터넷에는 크게 디바이스, 이동통신망, 시스템사업자, 서비스 및 어플리케이션 분야 등이 분포되어 있다. 디바이스에는 칩셋, 모듈, 단말기가 속하며 이동통신망에는 GSM/CDMA, LTE 휴대폰들이 있으며 시스템사업자는 제품기기 제조사, 시스템 통합 사업자, 특정 어플리케이션 임대사업자, B2B, B2C 서비스 사업자를 의미한다. 서비스 및 어플리케이션 분야에는 자동차 텔레메틱스, 차량관제, 스마트그리드 및 관리, 고정형 무선 통신, 생활 가전제품들이 이에 속한다. 사물 인터넷 기반으로 사물에 적용된 사례를 보면 다음과 같다.

- 버스도착 안내시스템: 버스운행 관리시스템과 연계해 도착 예정시간을 정류소 단말기, 교통 안내 앱에서 제공한다.
- 스마트 계량기: 에너지, 가스, 수도 사용량을 체계적으로 모니터링한다.
- 스마트 시티: 교통체증, 폐기물, 가로등을 관리하고 휴대폰 기지국의 전자파 방출에 대해 모니터링한다.
- 공장 자동화기기: 공장 내 설치된 센서를 통해 100밀리 초 간격으로 부품 가동률과 온도, 진동 데이터 수집, 가동상태를 모니터링한다.
- 자동주차 시스템: 차량에 부착된 센서를 통해 주위 데이터를 분석해 자동으로 핸들을 조정한다.
- 포드 컨셉트카 에보스: 에어백 센서를 통해 사고 유형을 분석해 해결책을 제공, 해당 지역 도로와 날씨, 사고 상황 등의 데이터를 분석한다.
- 자동차 부품의 인터넷 연결: 자동차 플랫폼, 부품이나 유지보수, 업그레이드 등 자동차 시장에 적용한다.
- 규제약품 모니터링: 마취약물 추적, 자동화 보안 캐비닛, 약제 재고 관리 컨베이어 등에 적용한다.
- 바코드를 이용한 의료자동화 시스템: 약제 이동의 각 단계를 추적하여 정확한 약제가 정확한 양만큼 환자에게 전달여부를 확인한다.
- 기숙사 화장실/세탁실 정보제공: 비어있는 화장실, 세탁기와 건조기 사

용 정보를 제공한다.

- 개 목걸이: 체온을 측정하여 애완견의 온도가 화씨 72도가 넘으면 주인에게 SMS 메시지를 발송한다.
- 고양이 급식기: 외출이나 여행 시 고양이에게 먹이를 주는 급식기를 사용하고 웹캠을 통해 전 과정을 감시한다.
- 가축건강관리: 가축의 귓속에 무선 인터넷센서를 이식해 가축을 감시하며 질병을 예방한다.
- 무선 기저귀: 기저귀에 내장된 칩이 기저귀 교체 시간을 감지해 부모에게 SMS로 알려준다.
- 인터넷 슬리퍼: 착용자의 발걸음에서 건강의 이상 신호를 감시하여 가족과 의사에게 전달한다.

사물 인터넷 기반으로 서비스에 적용된 사례를 표로 보면 다음과 같다.

서비스 종류	내 용
위치추적	사물 및 사람 추적, 주문관리, 물류추적, 친구 찾기 등
자동차	차량관리, 교통정보, 통행료, 차량도난방지, 시내버스관제 및 도착안내
원격제어	가스/물/전기등 사용량의 원격검침, 산업자동화, 센서, 조명, 펌프, 자판기 제어 등
물류, 유통, 금융	ATM기, POS시스템, 휴대폰결제 솔루션, 택배 배달 서비스 등
보안, 공공안전	CCTV 보안, 빌딩 관리, 자연재해 모니터링 등
의료	혈압, 당뇨 등 개인건강 체크솔루션, 생체신호 모니터링, 노약자 및 장애인 지원, 원격 의료 등
자산관리	자동판매기, 복사기, 디스플레이 기기에 대한 원격관리 등
가전	디지털 액자, 디지털 카메라, 전자책, 가정관리 허브 등
환경감시	대기오염 모니터링, 하천 오염도 측정, 해수 측정 등

실제 생활 속에서 사물 인터넷을 사용하는 과정에서 다양한 문제점들이 나타나고 있다. 예를 들면, 무료 사물 인터넷 서비스를 위한 개인정보, 상황정보, 광고 등을 통하여 보이지 않는 무형 비용에 대해 지불하게 되며 스마트 TV의 네트워크 해킹을 통한 개인의 생활모습을 감시하고 TV를 하이재킹 하여 금융정보를 도난한 후 전압 과부하를 주어 TV 폭파를 할 수 있다. 원격 CCTV 카메라의 해킹에 성공하면 외부인이 침입 가능하도록 무방비 상태로 설정할 수 있다. 또한 당뇨병 환자에게 제공하는 인슐린 펌프의 해킹을 통하여 오동작으로 환자 목숨에 위협을 가할 수가 있으며, 스마트 자동차에 대한 해킹으로 가속페달의 속도 조절과 브레이크 조작을 통하여 운전자 생명에 위협을 가할 수도 있다. 이러한 문제점에는 고령자와 어린이 등이 함께 사용하고 있는 스마트 가전제품에 대한 보안 업데이트가 부족한 것이 주요원인이다.

사물 인터넷에서 발생하는 전자파가 인체에 미치는 영향에 대한 조사가 시급한데 현재 휴대폰 사용 시 뇌종양 확률이 증가하며(스웨덴국립연구소), 2시간씩 50일간 전자파를 노출시킨 쥐의 뇌세포가 파괴되는 것을 확인할 수 있다(미국국립보건원). 신체와 밀착된 스마트폰과 웨어러블 기기에 사용되는 적외선 통신, 근거리 무선통신 주파수에 대한 유해 테스트가 필요하다. 사물 인터넷 해킹으로 인간의 생명에 위협을 줄 수 있는 위험한 수준에 대한 보안 부족한 게 사실이다. 예를 들면, 전기다리미와 전기 주전자에 스파이 마이크로칩이 탑재되어 도청 등을 통해 수집된 정보를 해외의 서버에 전송할 수 있으며 주요 기업 CEO, 각국 정상들을 대상으로 호텔 내 스파이 도청기 및 모니터링을 통해 계획적인 암살 시도가 이루어질 수 있다. 스마트 홈 해킹에 성공하면 누구나 집에 무단으로 침입 가능하며 기업공장내의 생산설비를 경쟁사가 해킹하여 공장 자동화 시설을 중단하는 등 여러 문제가 발생하게 된다.

(2) 무인항공기와 드론의 차이점

미국 국방장관실(OSD) UAV 로드맵에서는 무인항공기(unmanned aerial vehicle, UAV)를 “조종사를 태우지 않고, 공기역학적 힘에 의해 부양하여

자율적으로 또는 원격조종으로 비행을 하며, 무기 또는 일반화물을 실을 수 있는 일회용 또는 재사용할 수 있는 동력 비행체" 라고 정의하고 있다. 미국 FAA(Federal Aviation Administration)에서는 무인항공기를 "원격/자율조종으로 시계 밖 비행이 가능한 민간용 비행기" 라고 정의하고 있다. 이 정의에 따르면 취미로 날리는 상업용 드론이나 무선조종 모형항공기(model aircraft)는 무인항공기에 포함되지 않는 것으로 해석된다. 일상적으로 주변에서 언급하는 드론(drone)은 상업용 드론을 말하며 군사용 무인항공기와 용도 및 비행시간의 차이로 구분하고 있다.

(3) 드론의 등장배경

유인항공을 이용하여 촬영하기 위해서는 탑승인원 및 안전문제와 비행허가에 관련된 각종 규제에 직면하게 된다. 이에 신속한 기동성과 경제성을 확보한 촬영방식에 대한 요구가 생겨나면서 원격 리모트컨트롤 비행체, 즉 무인조종비행체를 활용한 촬영방식을 사용하는 드론이 등장하게 된다. 사람이 타지 않고 무선전파의 유도에 의해서 비행하는 비행기나 헬리콥터 모양의 비행체인 드론은 사용목적과 크기, 형태에 따라 다양하다. 무인항공기에는 전파를 이용해 원격 조정하는 RC(Remote Control), 사람이 탑승하지 않는 UAV(Unmanned Aereial Vehicles), 원격으로 사람이 조정하는 RPA(Remotly Piloted Aircraft) 등 다양한 종류가 있다.

(4) 드론의 분류

드론은 국가마다 적용하는 중량기준이 다르다. 보편적인 방식은 군사적 용도에 따른 분류에 전술/전략/특수임무 무인기가 있으며, 비행반경에 따른 분류에 근거리/단거리/중거리/장거리 체공형 무인기가 있다. 비행고도에 따른 분류에 저고도/중고도/고고도 무인기로 나누며, 크기에 따른 분류에는 초소형/소형/중소형/중형/대형 무인기로 분류한다. 비행, 임무수행 방식별 분류에는 정찰기/공격기/폭격기/전투기/표적기/무인헬기/초소형비행체 무인기가 있으며, 이착륙방식별 분류로 이륙/착륙/자동 이착륙 무인기로 이루어진다.

국내 항공법상 초경량비행장치의 무인비행장치가 이에 해당하나, 보다 규모가 큰 무인기에 대해서는 정의가 없는 바, 법적으로 드론을 규정하기는 다소 모호한 상황이다.

(5) 드론의 구성 및 정의

드론은 하드웨어 및 소프트웨어 요소로 구성되어 있으며 하드웨어 요소로는 비행체가 있으며 컴퓨터, 항법장비, 송수신기, 가시광선 및 적외선 센서 등의 장비로 구성한다. 드론의 어원은 여왕벌 앞에서 번식을 위해 존재하는 숫벌들이 윙윙 거린다는 뜻의 영어단어에서 나왔다. 드론은 비행기나 헬리콥터와 유사한 형태로 제작된 소형 무인 비행체를 말하며 적군을 정확히 겨냥해 공격하거나 테러 조직에 은밀히 접근해 타격을 입히기 위한 군사 목적으로 개발되었다. 1916년, 과학자 아키볼드 로(Archibald Low)가 비행체에 무기를 싣고 원격으로 적을 타격하는 무기를 개발하는 'Aerial Target' 프로젝트로 진행했으며, 1930년대 드론이라는 용어로 탄생하였다. 최초의 드론 사용은 오래된 전투기들을 대상으로 방공포 훈련을 실시하는 과정에서 개발되었다. 세계대전을 거치며 무인항공기에 대한 연구 및 실험이 확산되면서 1973년 대공포사격 훈련에 최초 무인항공기 드론이 사용되었다. 1982년 1차 레바논 전쟁에서는 이스라엘이 무인기를 투입했으며, 현재 20??년 기준 51개국에서 158종의 무인항공기를 개발・운용하고 있다. 우리나라는 2000년부터 무인기 개발을 시작해 무인정찰기 '송골매'와 대한항공에서 개발한 근접감시용 무인기 'KUS-9' 등을 개발하고 있다.

드론은 현재 90%가 군사용이지만 원격탐사, 통신 중계, 환경감시 등에 활용되고 있으며 영화제작이나 농업 등 산업 분야에서 활용하고 있다. 예를 들면, 일본의 야마하는 농약 살포용 무인항공기를 개발하여 20년 동안 2400기 이상의 무인헬기를 판매했고, 일본 전체 논 40%에 비료와 살충제를 뿌리고 있다. 독일 철도회사 도이체 반은 4개의 프로펠러를 달고 있는 드론을 활용하여 기차 차고와 정비소 경계에 활용하고 있다. 이 드론은 최고 지상 500

피트 상고에서 지상을 감시하고 영상을 전송할 수 있는 기능을 탑재하고 있다. 호주 폭스 스포츠는 크리켓 시합에서 드론으로 중계방송을 실시했으며, 이후 스포츠 중계나 재난 보도 등에서 드론을 활용한 촬영이 활발하게 이루어지고 있다. 미국 아마존과 DHL 등 주요 물류회사들은 물품 배달용 드론을 개발하여 상용화를 앞두고 있다. 특히 아마존은 '프라임에어(PrimeAir)'라는 드론을 이용한 택배 배송 서비스의 시험 동영상을 공개했다. 그러나 미국 연방항공청(FAA)에서는 항공법 규제로 실제 사용에 적용하지는 못하고 있는 실정이다. 미국 구글에서는 '룬(Loon)' 프로젝트를 통해 뉴질랜드에서 열기구를 통해 전 세계 인터넷망을 연결시키는 사업을 진행 중이며 프로젝트 및 다양한 사업에 드론을 적용시킬 예정이다.

드론 시장은 2013년 60억 달러 규모까지 성장했으며 군사용 드론이 90% 이상 차지하고 있지만 향후에는 민간 드론 시장도 2020년까지 연평균 8% 이상 성장해 2022년에는 114억 달러 이상 규모로 성장할 것이다. 미국 내 민간인이 등록한 드론은 2009년 146대, 2013년에는 545대가 등록되었고 2018년에는 7500대 이상 민간 드론이 승인을 받을 것으로 전망했다. 한국 국토교통부에서는 1999년 무인비행장치에 관한 안전관리 기준을 항공법에 반영하였고 비행장치 신고 및 안전성 인증, 비행계획 승인 제도를 운영해왔다. 2004년 초경량비행장치 전용 공역 지정, 2013년 무인비행장치 조종자 자격증명제 도입, 2014년 무인회전익 조종자 안전교육 실시 등 제도적인 보완을 추진하고 있다. 국토교통부 법령에서는 무인항공기 기체무게 150KG을 기준으로 초과하는 무인항공기는 항공기급 무인항공기라고 말하며, 그 이하는 무인비행장치로 구분해서 관리한다. 2014년 3월 31일까지 신고된 무인비행장치는 240대이며 12KG 이하 무인항공기는 신고대상에서 제외하고 있다. 백령도 등지에 추락한 북한국 무인항공기가 논란이 되면서 국토교통부는 안전관리를 강화하기 위한 제도를 보완하는 중이다. 현재 언급되고 있는 내용은 다음과 같다.

- 현행 안전관리 대상 분류 기준인 12킬로그램을 현실성 있게 재조정한다.
- 비행장치 성능, 비행지역, 비행 목적에 따라 안전관리 차등화를 둔다.
- 유사시 소유주 정보 등을 파악하도록 무인비행장치 신고관리 시스템을 구축한다.
- 비행금지구역내 무허가 비행에 대한 처벌기준을 강화한다.

현재 드론의 핵심적 기술은 무인항공기 항로를 통제하는 GPS 기술로 휴대폰에 넣어 상용화 할 수 있다. 민간용 드론은 규제와 배터리・모터(엔진) 기술이 더 발전시켜야 한다. 국내 (주)엑스드론의 경우 40분 비행시간이 가능하며 가동시간과 적재 무게를 늘리기 위해서는 배터리를 용량을 늘리고 경량화로 제작해야 한다.

드론은 두 가지 방식으로 분류할 수 있다. 기체에 부착된 프로펠러의 수로 분류하는 방식과 채널 수로 분류하는 방식이 있다. 프로펠러 수에 따라 프로펠러가 4개인 경우 쿼드콥터, 6개인 경우 헥사콥터, 8개인 경우 옥토콥터로 부른다. 채널수에 따라 2채널, 3채널, 4채널, 6채널로 분류되며 2・3채널 드론은 상하로 뜰 수만 있거나, 앞뒤로만 동작한다. 4채널 드론은 상하로 뜨면서 앞뒤좌우로 움직일 수 있고, 6채널 드론은 배면 비행까지 할 수 있다.

(6) 드론의 용도

용도	구 성	특 징
배달	스마트폰, 전용앱, 웹캠	장매물 탐지 및 운반
정찰	조종기, 시뮬레이션 프로그램, 헬리캠	실시간 감시, 정찰 및 정보수집
전투	조종기, 시뮬레이션 프로그램, 헬리캠	공중전 및 지상폭격
전자	조종기, 시뮬레이션 프로그램, 헬리캠	통신감청, 전자정보 수집
통신	조종기, 시뮬레이션 프로그램, 헬리캠	통신 중계 및 저궤도 위성 대체

드론은 배달용, 군사용, 정찰용으로 다양하게 사용되고 있으며 예를 들면, 항공 촬영을 통한 치안 유지, 교통법규 위반 단속, 재난 발생 시 피해 파악과 생존자 발견, 정밀타격 작전, 경찰의 도난 차량 추적이나 마약수사, 재난 지역의 실종자 수색, 미디어 업계의 항공 촬영 등 활용 범위의 확산에 적용되어 졌다. 드론은 국가 안보를 위해 만들어졌으며 전 세계 주요 국가들이 각각 군사용, 민간용 드론 개발에 박차를 가하고 나서고 있다.

(7) 국가별 드론 사용현황

<미국>

- 아마존 : 드론 배달시스템 'Amazon Prime air' 개발하여 캐나다, 호주 등에서 진행
- 구글 : 드론 'Project Wing'을 진행, 호주에서 1주일간 드론 택배서비스 실험
- 페이스북 : 인구가 적고 광활한 지역에서 인터넷을 돕는 통신용 드론 프로젝트 착수
- UPS : 드론을 활용하여 무인 배송서비스 도입을 위한 프로젝트를 진행
- 스테이트팜 : 대형 손보사로 재난 지역 피해규모 조사와 손해액 산정에 드론을 활용

<영국>

- BBC : 태국과 홍콩 시위 현장 촬영 등 뉴스 취재 촬영에서 드론을 활용
- 도미노피자 : 'DomiCopter'를 활용한 피자 배달 프로젝트를 진행

<독일>

- DHL : 드론을 활용하여 12km 떨어진 섬에 소포(의료품) 배달에 성공

<한국>

- 유플러스 : 세계최초 LTE망을 통한 드론을 조정하였고 드론으로 결혼식 생중계

- CJ 대한통운 : 드론을 이용한 물류 배달 시험 비행 계획을 준비

[드론 시범 사업자 목록 – 국토교통부 제공]

구분	대표기관	공동참여기관
1	강원정보문화진흥원	강원대, 애니품
2	경북대 산학협력단	원신스카이텍, 유콘시스템, 한국감정원, 그리폰다이나믹스, 한국전기비행, 동아하이테크, 유시스, 대구테크노파크
3	국립산림과학원	엑스드론, 제이와이시스템, 메타빌드
4	대한항공	–
5	랜텍커뮤니케이션즈	스타로직스
6	부산대 부품소재 산학협력연구소	드론 프레스
7	성우엔지니어링	디브레인, 더파워브레인스, 하이브시스템
8	에스아이에스	–
9	에이알웍스	한국전자통신연구원, 브이티더블유, 케이아이티밸리
10	유콘시스템	한국과학기술원
11	케이티(KT)	유콘시스템, 편진, 메티스메이크
12	한국국토정보공사	호정솔루션, 대영측기, 성진에어로
13	항공대 산학협력단	포워드벤처스(쿠팡)
14	현대로지스틱스	유콘시스템
15	CJ대한통운	한서대, 엑스드론, 바이크로드론코리아

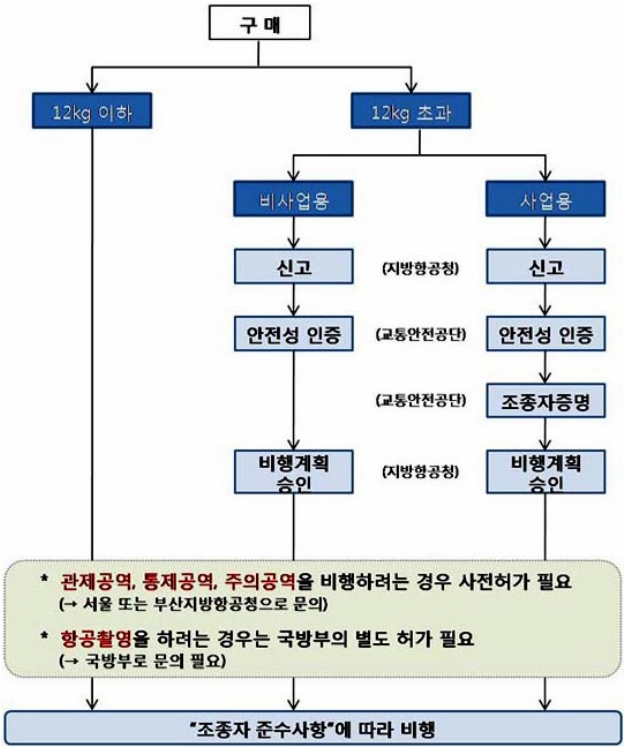
드론의 뛰어난 이동성과 다양한 활용성은 단순히 드론을 영상촬영에 활용하는 단계를 넘어서, 드론을 통해 영상 및 데이터를 수집하는 데 활용 가능하게 되어, 드론을 통해 대량의 데이터를 수집, 분석, 처리하는 SW도 발전하고 있다. 구글과 페이스북은 드론 기술을 활용하여 인터넷이 지원되지 않는 지역까지 인터넷 연결을 확대하는 프로젝트 진행 중이며, 드론을 농업 분야에

활용할 경우 인건비 하락, 생산 효율성 증대를 기대할 수 있어 일본에서는 살충제 배포, 농업용수 관리 등에 드론을 활용중이다. 또한 미국과 프랑스의 와이너리는 포도밭 관리를 위해 드론 이용을 추진하고 있다. 환경 보호를 위해 드론을 활용하는 프로젝트도 다양하게 시도되고 있으며, 인도네시아 오랑우탄 서식지 연구, 불법 어획 감시, 알래스카 빙하 및 고래 관찰 등에 드론을 이용하고 있다. 드론의 뛰어난 이동성과 다양한 센서의 이용 가능성은 인간이 접근하기 어려운 환경에서 다양한 임무를 수행할 수 있으며, 드론의 소형화 및 제작 가격의 하락으로 일반 소비 계층에게도 다양한 활용방안을 제시하고 있다. 재난시 생존자 탐색, 산림 화재시 소화, 화산, 허리케인, 토네이도 등 위험한 자연재해 조사 등에 드론의 활용이 가능하다. 미디어 및 영화산업에서도 드론을 '헬리캠'으로 사용해 화면을 전달하는데 사용하고 있으며, 일반 개인들은 취미용 드론으로 촬영한 사진과 동영상을 SNS에 올리며 개인의 레저 활동에 새로운 트렌드로 부상하고 있다.

(8) 드론(무인항공기)의 위험요소

미국에서 드론을 이용한 무인 꽃 배달 서비스를 시작하였다. 하지만 드론이 시민의 주거지를 무단 침입해 서비스가 중단되었다. 드론은 물건을 배달하기 위해서 정확한 위치 확보가 필요하다. 국내에서 단독빌라, 단독주택, 아파트의 동호수를 정확히 찾는 것은 GPS 위성으로는 힘들다. 가동시간, 제어범위 이탈, 접근센서 미동작 등으로 드론이 추락해 1년에 평균 2번씩 사람이 사망하는 사고도 생기고 있다. 국내 해킹 커뮤니티(POC)가 진행한 POC 2015 콘퍼런스에서 위성항법장치(GPS) 관련 오픈소스 도구 등을 통해 GPS 신호를 조작해 휴대전화, 자동차, 드론에 대한 GPS 스푸핑 공격을 시연하였다. 일본에서 원자력발전소 재가동에 반대하는 한 시민이 드론을 이용해 총리 관저에 방사성 물질을 실은 채 충돌하는 사건이 벌어졌고, 미국에서는 백악관 인근에서 취미용 드론을 조종하던 공무원의 실수로 비상 상황이 발생하는 소동이 벌어지기도 하였다. 우리나라에서도 지난해 북한이 보낸 정

찰용 드론이 발견되면서 국가 안보에 대한 위기감이 조성된 사례가 있다. 부산 해운대구에서는 드론을 활용해 해수욕장 피서객의 안전을 관리하다 추락 사고가 나면서 운행을 보류하기도 하였다. 국내에는 국토교통부가 정한 규정에 따라 서울 시내 비행금지구역에서 허가 받지 않은 드론은 비행할 수 없고, 최악의 경우 군이 격추 조치를 취할 수도 있다. 국토교통부는 현재 강원 영월 등 전국 4개 지역에 무인비행장치 전용 시범공역을 지정해 각종 실험을 진행하고 있다. 미국에서는 소형 드론과 항공기의 충돌 위험 발생 건수는 늘어나고 있으며 드론 사용자의 불안감이 커지고 있으며 무분별한 사용으로 인한 대형사고의 발생 가능성도 염두에 두고 있다. 드론의 고장이나 작동 오류로 사용자가 컨트롤 할 수 없는 상태를 하드웨어 결함, 주변 환경의 영향으로 인한 리모컨과의 교신 단절 현상 등 다양한 원인으로 발생한다. 이러한 드론을 활용한 상업적 여러 기회에도 불구하고, 충돌문제, 사생활 침해, 범죄 활용 등 부정적인 요인도 존재한다. 현재 조정자 없이 비행하는 완전 자율운행 기능이 완벽하게 개발되지 않아 충돌 및 추락에 따른 위험성이 존재하고 있다. 드론을 범죄에 활용하거나 무분별한 촬영으로 인한 개인정보침해 문제 발생에 대한 우려도 큰 현실이다. 드론은 첨단 로봇 산업이 실용화되기 전 중간단계의 가능성과 IT 서비스와 융합되어 새로운 상업적 가치 창출 등의 기대로 많은 기업과 투자자의 관심이 집중되고 있다. 현재 영상 촬영 또는 개인 취미용으로 많이 이용되고 있으나 드론을 통한 영상과 음성 등 데이터를 수집, 분석, 서비스하는 사물인터넷의 한 축으로 활용성을 기대하며 향후 첨단 로봇과 IT 서비스의 융합체로 빠른 성장이 기대된다. 상업용 드론 시장에서 한국이 경쟁력을 가지기 위해서는 국내 기술력 확보 및 시장 진출을 위한 지원이 필요하다. 첨단기술을 보유한 선진국, 가격적 측면에서 유리한 중국 등과의 경쟁 에서 우위를 차지하기 위해 차별화된 새로운 기술 개발 및 전략 모색이 필요하다. 또한 상업용 드론의 신뢰성 있는 이용 환경 마련을 위한 법・제도 정비가 시급하다.



드론을 구매한 후에는 안전을 위해 복잡한 도심에서 드론을 날리면 안 된다. 드론을 활용한 상업 촬영은 항공청 등록 이후에 가능하고, 일반 항공촬영의 경우도 3000만 원 이상 법인에서만 촬영이 가능하다. 드론을 활용한 사진 촬영은 국방부의 허가를 받아야 하고 주요시설의 경우 청와대 허가까지 받아야 한다.

스마트폰 크기에 촬영 성능도 탁월한 이 드론들이 그동안 불가능했던 각도에서 촬영한 영상들을 경험하며 즐거움을 만끽할 수 있다. 드론이 제작한 영상이 SNS를 타고 전파되면서 개인 사생활에 대한 논란이 발생하게 된다. 드론의 비행 안전성 확보도 문제다. 비행체가 작다 보니 바람, 눈 등 주변 환경에 취약하다. 비행 중 기능 이상으로 방향을 잘못 잡으면 사람이 다칠 수 있다. 높은 고도로 비행할 경우 항공기와 충돌 위험성도 가지고 있다.

2. 개인의 신상을 폭로하고 파멸시키는 공격

(1) 평판관리시스템의 등장배경

디지털 공간에서 '잊혀질 권리'가 전 세계적으로 이슈화되면서, 디지털 장의사에 대한 관심도 높아졌다. 디지털 장의사란 온라인상의 흔적을 없애주는 회사를 말한다. 디지털시대 사람들은 자신의 의지대로 혹은 의지와 상관없이 타인에 의해 디지털 족적을 남기게 되는데, 이런 인터넷상의 인생을 지워주는 역할을 디지털 장의사가 맡고 있다. 미국 인터넷 상조회사인 랑이프인슈어드닷컴은 300달러를 받고 가입회원의 사망 시 고인의 온라인 족적을 지우는 서비스를 제공한다. 디지털 장의사는 평판 관리(ORM, Online Reputation Management) 서비스의 일부다. 평판 관리에서는 사람・회사・브랜드의 '온라인 평판'을 모니터링 하는 것뿐만 아니라 적극적으로 관리해주는 서비스를 제공해 주고 있다. 한국에서는 맥신코리아・산타크루즈캐스팅 컴퍼니가 디지털 장의사 서비스를 제공하고 있다.

한국의 디지털 장의사 활동에는 법적・윤리적 쟁점들이 존재한다. 정보통신망법이나 개인정보보호법에 따르면 개인에게 온라인상의 자기 정보를 통제・삭제할 수 있는 모든 권한을 인정하지만, 본인이 죽으면 누구도 권리를 행사할 수 없어 디지털 장의사 활동에 제약이 있는 상태다. 온라인에서 떠도는 사생활을 청소해주는 서비스를 '디지털 세탁소'라 부르며 망자의 기록을 정리하고 지워주는 서비스를 '디지털 장례식'이라고 정의한다.

(2) 온라인 평판 피해사례

과거에 B양은 청소년 시절 호기심에 누드사진을 찍어 인터넷에 올렸다가 곧바로 사진을 삭제했고, 그동안 잊고 지내다가 몇 달 전 문제의 사진이 다시 유포되고 있음을 알게 되었다. 혼자서 개인 간 파일공유 사이트(P2P)를 찾아 삭제했지만 중간 유포자를 찾아내 신고해도 100만원 벌금형이나 집행유예로 풀려나게 되었다. 한 사람의 인생을 망가뜨리고 경미하게 법적 처벌이 내려진 경우다. 대학생 A씨는 여자 친구와 장난삼아 찍은 성관계 동영상을

페이스북에 올렸다가 공개 범위를 잘못 설정하여 주변 지인들에게 전파되었고 자극적인 제목으로 SNS와 P2P를 통해 급속도로 퍼져나가 두 사람이 정신적 피해를 입은 사례다. 과거 철없는 행동으로 이성친구와 교제 과정이나 채팅 등을 통해 찍었던 화상채팅이 무단으로 녹화돼 유포되어 친구를 통해 발견하고 피해사실을 요청한 경우도 있다. 과거의 흔적과 관련되어 삭제하려는 키워드에는 '왕따', '성적질문', '특정 정치인 욕설' 등 뒤늦게 후회하는 내용들로 구성되어 있다.

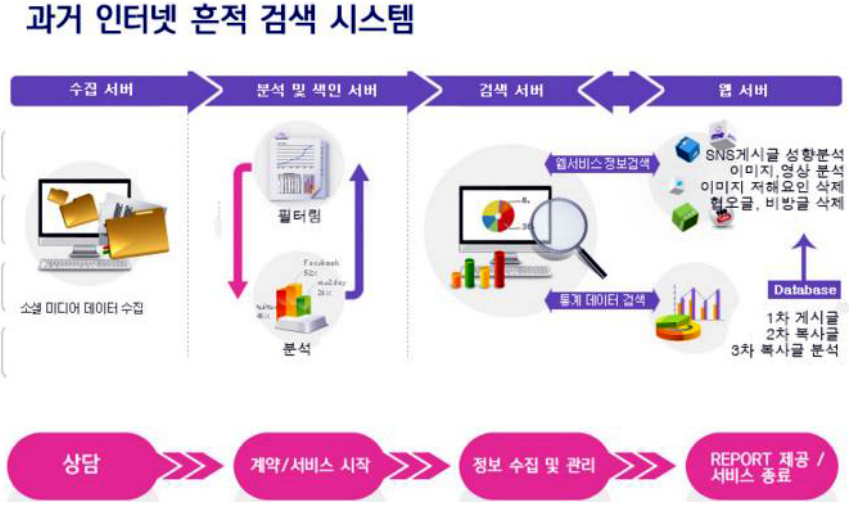
개인의 기록이 담긴 일기와 사진, 영상의 저장매체가 온라인으로 옮겨가면서 정보 유출로 인한 피해가 늘어나고 있다. 정보가 유출되면서 단 몇 초 만에 온라인으로 급속도로 확산하기 때문이다. 개인이 시간 내서 대응하기엔 지나치게 범위가 넓으며 개인의 은밀한 사생활이 유출되어 사람의 인생이 바뀌어 파멸하는 경우도 있다. 이를 제도적으로 잡아주기 위해 '임시조치'란 제도가 있다. 포털 사이트에 게시된 게시물로 인해 명예훼손을 당했다고 요구하게 되면 블라인드 처리가 되고 30일 동안 해당 글이 차단되고 부당성이 증명되지 않으면 영구적으로 자료가 삭제된다.

(3) 디지털 세탁소의 정의

디지털 세탁소는 온라인 개인정보 관리대행 서비스로 2000년대 유명 연예인이나 정치인, 기업체 등 온라인 평판에 민감한 사람들이 이용했던 서비스가 일반인에게 알려진 것이다. 인터넷, SNS에 노출된 개인의 정보나 게시글, 사진・동영상 등을 삭제해주는 업종으로 개인의 명예를 실추시킬 수 있는 게시물을 검색해 이를 지워주는 '평판 관리' 서비스를 제공한다. 평판 관리 서비스란, 악성 댓글이나 루머에 시달리는 사람들로부터 의뢰를 받아 인터넷에 올라간 개인의 정보를 모두 지워주는 일이다. '산타크루즈컴퍼니'는 고객이 홈페이지에 평판 관리를 의뢰하면 정부에서 구매한 프로그램을 통해 고객의 데이터를 수집하고 분류한 다음, 다시 그것이 비평인지 비방인지 직원의 판단을 거친다. 이렇게 해서 지울 정보가 결정되면 업체가 변호사를 통

해 해당 글이 올라간 사이트 관리자에게 삭제 요청을 보낸다. 보안IT 전문가팀, 법률 자문팀, 평판 분석팀, 기술지원팀 등 평판 관리에 필요한 모든 서비스를 종합적으로 제공하고 있다. 이 업체들은 의뢰인의 유출된 온라인 정보를 삭제하거나 과거에 남긴 게시판 글 및 사적인 내용들을 지워주는 대리인 역할을 한다. 의뢰인에 대한 모욕적인 비방, 음담패설 행위, 개인정보(휴대전화, 근무처, 집주소 등) 노출 등 명예훼손 기록에 대한 법률자문을 대행하기도 한다. 자신의 불명예스러운 과거를 지워 온라인의 이력을 '세탁'하려는 개인 및 기업체들도 디지털 세탁소 서비스를 이용하고 있다. 민감한 개인정보를 다루는 서비스의 특성 때문에 대부분 운영 자체도 비공개로 하는 회사가 많다. '프라이버시앤컴퍼니'의 경우 사무실 주소를 공개하지 않고 전화와 온라인 상담을 통해 서비스를 이용하는 고객만 방문센터에서 면담을 통해 진행한다. 정식으로 홈페이지를 만들어 사업장 주소와 연락처 등을 공개하고 영업하는 '산타크루즈 캐스팅 컴퍼니'는 국내 한 곳이다.

[산타크루즈 캐스팅 컴퍼니 서비스 구성도]



(4) 디지털 장의사의 정의

디지털 장의사는 사망한 사람의 인터넷 홈페이지나 웹사이트 아이디 등을 쉽게 파악해 정리할 수 있는 서비스로 평소 죽음에 대비해 각종 인터넷 계정과 기록들을 정리하는 서비스를 제공한다. 고인의 사이버 흔적을 정리해주는 업종으로 사후 고인에게 오는 연락에 대해 고인의 사망 사실을 알려주게 된다. 의뢰인이 전자메일, 블로그, 개인홈페이지 기록들 중 가족에게 남겨줄 것, 삭제하고 싶은 것을 구분해서 살아있을 때에 공개 콘텐트와 비공개 콘텐트를 계정별로 나눠 관리하고 있다. 현재 구글은 휴면계정 관리자 서비스를 통해 일정 기간 서비스를 이용하지 않으면 자신의 콘텐트를 사전에 설정된 사람에게 미리 보내고 있다. 구글의 계정 설정 페이지에서 확인할 수 있는 '비활성화 계정 관리자(IAM, Inactive Account Manager)' 서비스를 이용하면 이용자에게 어떤 불가피한 상황이 벌어질 경우 자신의 Gmail 메시지 및 데이터 등을 어떻게 처리할지에 대한 주문을 구글에 하며 사용자들이 자신의 디지털 사후에 어떠한 계획을 세울지에 대비할 수 있다. 야후는 망자의 콘텐트를 정리해주는 '야후 엔딩' 서비스를 제공한다. 페이스북은 유가족의 요구에 따라 망자의 계정을 기념 계정으로 보존해준다. 다음과 네이버 등 국내 포털들은 유족에게 가입 정보를 제공한다. 디지털 장의사 서비스에 가입하면 자신이 죽은 뒤에 디지털 장의사가 삭제할 기록과 가족에게 남길 기록 등을 생전에 구분해놓은 대로 처리해준다. 미국 캘리포니아주에서 '온라인 지우개법'이라 불리는 이 법은 SNS와 인터넷 등의 게시물에 대해서 해당 인터넷 업체에 삭제를 요청할 수 있는 권리를 보장한다. 법이 시행되면 게시물의 성격이 반사회적이거나 불법적이지 않더라도 최초 작성자가 원하면 삭제해야 한다. 청소년기에 우연히 올린 게시글이나 사진, 영상물 등의 정보가 당사자에게 악영향을 끼치는 것을 예방하는 것이다. 디지털 장의사는 고인으로부터 개인정보를 받아 살아있을 때 인터넷에 남긴 기록들을 모두 지운 후 그것들을 한 곳에 수집하여 디지털 추모관을 만든다. 요즘은 인터넷 디지털 기록까지 삭제를 해야만 진정하게 사람의 장례를 치른다고 말할 수 있다.

[디지털 장의사 장례비용]

(5) 평판관리 서비스 범위

네이버, 다음 등 대형 포털사이트에 있는 개인 블로그, 카페, 커뮤니티 등 인터넷 기록, SNS 기록, 방문객이 남긴 게시글, 사진, 동영상 파일 등 의뢰인이 원하는 모든 요구사항을 완전삭제 하는 것을 지원해 준다. 평판관리의 목적은 과거의 불리한 기록을 남기지 않고 현재의 삶을 보다 행복하게 나아가도록 하는 게 목적이다. 현재 잊어버리고 지냈던 과거의 인터넷 사용기록은 그 사람이 살아온 인생의 흔적으로 남는다. 새로운 친구를 사귀거나 회사에 입사하는 경우, 과거 인터넷 기록 검색을 통하여 상대방을 평가하는 중요한 기준으로 활용하고 있다. 요즘은 소개팅 및 결혼하기 전에 상대의 SNS를 검색해 과거 기록을 통해 상대방의 성격, 주변 환경, 지인들을 분석하는 경우가 많다. 평판관리 서비스는 먼저 의뢰인 주민등록번호 등 개인정보를 이용해 인터넷 사용 기록을 검색하고 정리할 데이터를 찾아낸 후 데이터가 보관

하는 포털 사이트 관리업체 담당자를 통해 개인기록을 삭제하며 가처분신청 등 법적인 절차를 거쳐서 삭제하게 된다. 평판관리 서비스를 사용하는 대부분은 여자들이며 결혼을 앞두고 과거의 이성교제 기록을 지우거나, 불륜 상대와 찍은 동영상을 없애주는 것을 의뢰하고 있다. 청소년들은 과거 학교기록 때문에 친구들에게 소외당하는 것을 걱정하는 경우가 많고, 성인의 경우, 유출된 은밀한 개인정보 때문에 불이익을 받을 것을 두려워하는 경우가 많다. 기업에서는 인터넷 악성 댓글, 언론사 오보 등을 실시간으로 확산되는 것을 차단하기 위해 평판관리 서비스를 사용한다.

(6) 온라인 평판관리 서비스의 위험요소

'잊혀질 권리'와 '기억할 권리'의 상관관계에 대해서 알아보도록 한다. '잊혀질 권리'를 주장하는 쪽은 과거의 인터넷 기록이 개인의 인생을 낭떠러지로 몰고 갈 위험이 있다고 한다. 개인이 디지털 세탁소의 도움을 받는 데는 한계가 있어 확산력이 강한 인터넷의 특성에 대응하는데 무리가 있다. 단, 인터넷에서 떠돌아다니는 불필요한 유해한 정보들을 어느 정도 정리하는 효과는 기대할 수 있다. 국내에서 '잊혀질 권리'는 상당히 강력하게 인정하고 있는 분위기다. 타인이 작성한 정보 중 명예훼손 및 사생활 침해의 우려가 있는 정보는 정보통신법에 따라 삭제를 요구할 수 있으며, 제3자가 수집한 개인정보도 수집 목적에 따라 기한이 지났을 경우 개인정보보호법에 따라 삭제를 요구할 수 있다.

반면 '기억할 권리'를 주장하는 쪽에선 개인에게 불리한 정보를 마음대로 삭제한다면 특정인에 대한 다양한 의견을 통한 공정한 평가가 이뤄질 수 없다고 생각한다. 개인의 표현의 자유와 알 권리를 제한해온 주체가 국가에서 의뢰인으로 바뀐 것뿐이다.

국내에서는 산타크루즈컴퍼니(http://www.santacruise.co.kr), 맥신코리아(http://maccine.net) 등의 회사들이 평판관리 및 게시 중단 서비스를 지원하고 있다. 유사하게 '시큐어세이프(SecureSafe)'란 회사도 클라우드 저장창고에 저장된 고인의 디지털 정보를 사후 유족이 삭제 및 관리하는 서

비스를 제공하고 있다.

3. 인터넷 소셜네트워크를 사용한 정보교환 및 공격에 대한 방어

(1) 트위터・페이스북 가입자정보 획득

일반적인 공조에는 외국과 공조는 국제법에 의한 것과 경찰 간 공조를 통한 것이 있으며 국제법은 증거물 교환 등을 위한 형사사법공조와, 범죄인인도를 목적으로 하는 범죄인인도조약이 있다. 경찰공조는 인터폴을 통한 것과 각국 사이버수사부서간 직접적인 컨택을 통한 것이 있다. 트위터와 페이스북은 미국 캘리포니아 소재 기업으로, 가입자정보의 획득을 위해서는 수사기관을 위한 가이드라인을 홈페이지에 게재하고 있다. 원칙적으로 형사사법공조 절차에 의한 미국 법원의 소환장(subpoena)과 법원 명령, 메시지 내용을 위해서는 압수수색영장이 필요함을 명시하고 있다. 형사사법절차로 검찰을 경유하여 법무부에서 요청사항을 외교라인을 통해 해당국 외교부에 발송 한다, 해당국 외교부는 법무부에 다시 전달하여 법적절차 진행하여 6개월 이상 소요된다. 트위터와 페이스북에 법집행기관을 담당하는 자와의 전자메일 교환에서도 형사사법공조 요청이 필요함을 재확인한다. 예외적으로 미국하고 동시에 수사개시가 될 수 있는 경우, 즉 피해자 또는 피의자가 미국인이거나, 미국 내에서 범행이 발생한 경우는 미국 경찰 또한 수사를 착수할 수 있다. 국제공조에는 한계가 있어 형사사법절차를 거치더라도 쌍방가벌성원칙에 따라 미국에서 범죄가 되지 않는 사항은 공조가 불가능 하다. 대표적으로 공직선거법 중 후보자 비방, 단순 명예훼손은 미국에서 표현의 자유를 폭넓게 인정하여 형사사건으로 취급하지 않기 때문에 요청이 불가하다.

(2) 트위터 조사방법

위와 같이 미국 SNS에 대한 조사가 어렵기 때문에 사회공학적인 방법이 필요하다. 친구 분석, 게시글 분석, 페이스북 및 트위터 ID 분석 등을 활용하고 페이스북의 경우 본인은 '계정설정'에서 최근 로그인 내역을 확인할 수 있

으므로 조사 대상자로부터 임의제출 받아 수사가 가능하다. 최근 로그인 내역 : 로그인 IP, 접속 기기(PC, 아이폰, 안드로이드 여부), 브라우저 타입 등 확인 가능하다. 사용자 정보를 요청하기 위해서 트위터는 미국 캘리포니아 샌프란시스코에 위치하며 미국 법에 따라 유효한 법적요청에 한하여 응답한다. 법집행기관으로부터 모든 요청사항은 팩스 또는 우편으로 접수한다. 사용자 정보를 요구할 때에는 1. 사용자 이름과 URL, 2. 요청하는 정보가 정확히 무엇인지, 3. 현재 수사 중인 사건과 관련성, 4. 접수사실을 통보할 수 있는 유효한 전자메일 주소가 필요하다. 법집행기관에서 발송한 전자메일 주소만 인식되고, 다른 민간에서 보낸 것은 자동으로 수신 거부된다.

(3) 페이스북 법집행기관 가이드라인

외국법집행기관을 지원토록 계정 기록은 Facebook 서비스 이용약관과 준거법에 의해서만 공개되며 계정 내용 공개를 위해 사법공조조약(MLAT) 또는 로거토리 레터가 필요할 수도 있다. 계정은 법적절차에 의한 요청을 받는 것을 전제로 공식적인 형사사건 수사와 관련하여 90일 동안 계정 기록 보존 조치가 가능하다. 긴급 요청 시에는 아동에 대한 긴급한 위험이나 사망 위험 또는 심각한 물리적 부상 및 지체 없이 정보 공개가 필요한 사안에 대해 법률 집행 관리는 records@facebook.com으로 연락하여 긴급 양식을 얻을 수 있다. 비법률 집행 관리가 보낸 이메일 주소의 메시지는 검토 또는 답변하지 않는다. 긴급 상황을 인식하고 있는 사용자는 즉시 지역 법률 집행 관리에게 직접 연락해서 해결하게 된다. 모든 요청에는 다음 사항이 구체적으로 명시되어야 한다.

1) 요청기관
2) 담당자(신분증 번호 포함)
3) 법집행기관임이 나타나는 전자메일 주소
4) 직접 연락 가능한 전화번호
5) 페이스북 사용자의 이메일 주소, 사용자 ID 번호 또는 사용자 이름

사용자가 법집행기관에서 본인의 정보를 취득한다는 조건에 동의한 경우, 법집행기관은 사용자를 직접 접촉하여 관련 정보를 얻어야 한다. 메시지, 사진, 동영상, 담벼락 게시물 등 계정 내용의 경우, 사용자는 Facebook의 계정 패널에 있는 “정보 다운로드” 기능을 이용할 수 있다. 또한 사용자는 보안 설정/로그인 내역 아래에 있는 계정 설정에서 최근 IP 주소를 볼 수 있다. 사용자들은 법률절차 없이 과거 IP 정보에 액세스할 수 없다. 사용자 통지의무 조항이 조사에 영향을 미칠 것이라고 판단되는 경우 수사관은 적절한 법원 명령서 또는 통보가 금지된다는 내용의 절차를 획득해야 한다. 법집행기관에서 요청한 사항이 페이스북의 이용약관 침해에 해당하는 경우, 우리는 사용자들에게 행위 파악 상태를 공지하는 등 추가 악용을 방지하기 위한 조치가 취해질 것이다.

Ⅲ 결 론

최근 사이버 상에서 발생되는 3가지 유형별 공격 및 위협요소 등에 알아보았다. 공격기법은 갈수록 다양해지고 치밀한 기술로 상상을 초월한 방법들로 발전되어 가고 있다. 현재 초중고생들을 대상으로 유투브 게임 동영상이 중독성에 가깝게 시청되고 있다. 해당 동영상내의 주인공이 제안하는 창작물을 제작하거나 특정회사 제품 구매를 유도 하는 경우가 많다. 이러한 소셜 네트워크를 통한 미디어의 영향은 군사적으로, 정치적으로 활용되면 특정인의 메시지를 순식간에 악의적으로 전파 시킬 수 있기 때문에 소셜 네트워크 서비스에 대한 부작용 연구가 절실히 필요하다. 예를 들면 IS(이슬람 국가)의 활동전사를 인터넷상에서 전 세계적으로 모집하고 홍보 동영상을 통하여 컴퓨터 사용자들이 심취할 수 있도록 유도하는 전술 등이 이에 해당한다. 향후 연구에는 인간을 보조할 수 있는 지능적 드론 및 격투용 드론에 대한 위협요소를 시뮬레이션 환경에서 실험을 통하여 연구하고자 한다.

사이버안보를 위한 형사법적 대응방안

김 성 천*

목 차

Ⅰ 들어가는 말

2009년 7월 7일 오후 6시를 기점으로 청와대를 포함한 국내 주요 인터넷 사이트에 대한 분산서비스거부(Distributed Denial of Service / DDoS) 공격이 이루어져 접속장애를 야기하고 일부 좀비 PC는 하드디스크 손상이라는 피해까지 입었다.[1] 서비스거부(Denial of Service)란 전산설비가 감당할 수 없는 과부하로 인하여 정보처리가 중단되는 현상을 말한다. 서비스거부 현상을 일으키는 가장 좋은 방법은 동시에 수많은 트래픽을 유발하는 것

* 중앙대학교 법학전문대학원 교수

1) 2009년의 7·7 DDoS 공격 이후에도 2011년의 3·4 DDoS 공격과 같은 2011년의 농협 서버 해킹(농협 IT본부에 위치한 서버상의 파일을 모두 삭제하는 명령이 수행되었다.) 사건이 세간의 많은 관심을 끌었다. 최근 2015년에는 서울메트로의 서버가 외부인에 의해서 5개월 동안 장악되는 사건이 벌어지기도 하였다고 한다.

이다. 분산된 수많은 좀비 PC에 특정 시점이 되면 특정 사이트에 업로드와 다운로드를 반복 실행하여 엄청난 트래픽을 유발시키도록 하는 명령(컴퓨터 바이러스)을 심어두는 방법이 사용된다. 그리고 이들 좀비 PC는 공격이 끝난 후 바이러스의 명령에 따라 스스로 하드디스크를 손상시켜서 부팅이 불가능하게 되기도 한다.

분산서비스거부 공격은 인터넷 공간에서 발생되는 업무방해 행위 중 비교적 심각한 유형에 속한다. 이러한 공격행위는 일단 형법 제314조 제2항의 컴퓨터 손괴 등에 의한 업무방해죄를 구성할 것이다. 컴퓨터 등 업무방해죄의 보호법익은 '컴퓨터 등을 이용한 정보처리 업무수행의 자유'이다[2]. 이 범죄는 분류상 개인적 법익을 침해하는 범죄에 해당된다.

컴퓨터가 개인적인 업무를 처리하는 전산기기로 이용되던 초창기에는 컴퓨터 등 업무방해 행위가 개인적 법익을 침해하는 범죄라고 하더라도 크게 틀린 말이 아니었다. 컴퓨터가 공공의 이익과 깊이 관련이 있는 영역에 적극적으로 활용되고 있지 않았기 때문이다. 그러나 지금은 상황이 많이 변화하였다. 우선 컴퓨터가 활용되지 않는 영역이 거의 없게 되었다. 그리고 인터넷으로 연결되지 않는 컴퓨터가 또한 거의 없는 상황이 되었다. 결국 우리 사회의 모든 영역이 인터넷을 통한 공격의 사정거리 안으로 들어온 것이다.

상황이 이렇게 되면 더 이상 컴퓨터 등 업무방해 행위가 단순히 개인적 법익을 침해하는 범죄라고 하기 곤란하다. 예를 들어 공항을 관리하는 컴퓨터를 마비 또는 교란시켜서 항공기끼리 충돌하게 만든다면 이는 이미 공공의 안전을 침해하는 범죄행위가 된다. 나아가 컴퓨터 및 인터넷 정보망을 이용해서 수집・가공・저장・검색・송신・수신되는 정보의 안전을 위태롭게 하는 행위는 상당한 경제적 손실도 유발시키고 있는 실정이다.[3]

2) 김성천, 형법, 도서출판 소진, 2009, 753면.
3) 현대경제연구원은 2009년 7월 7일의 분산서비스거부 공격의 피해액을 최소 363억원 최대 544억원으로 추산하였다. ("한국경제연구원 ddos" 한국일보 <http://news.hankooki.com/lpage/it_tech/200907/h20090723 11023823700.htm>)

컴퓨터 및 인터넷 정보망을 이용해서 수집・가공・저장・검색・송신 또는 수신되는 정보를 훼손・변조 또는 유출하는 행위로부터 정보의 안전(Datensicherheit / Information Security)을 지키는 일은 개인적 차원을 넘어 공공의 안전과 전자정보에 대한 공공의 신용 등 사회적 법익을 보호하고 나아가 국가의 안전보장을 도모하는 일이 되었다. 이와 같은 정보 및 정보통신기반시설의 안전을 지키는 것을 지칭하는 표현으로는 대략 정보보안, 정보보호, 사이버보안 또는 사이버안보 등 네 가지 정도가 사용되고 있다.[4)]

이 가운데 정보보안과 정보보호라는 표현은 보호의 객체에 초점을 맞추는 개념으로 보인다. 이에 비해 사이버보안과 사이버안보는 인터넷 정보망을 보호의 중심부에 끌어 들이고 있는 표현이다. 사이버스페이스는 가상공간을 의미하고 이를 구성하는 필수적인 요소가 인터넷 정보망이기 때문이다. 그런데 정보의 수집・가공・저장・검색・송신 또는 수신을 하는 과정에서 인터넷 통신망이 없어서는 안 될 중요한 수단이 되었다. 따라서 그것 자체를 보호하는 것이 곧 정보의 무결성(Integrität / integrity) 및 신뢰성(Vertraulichkeit / confidentiality)을 유지하는 일과 분리할 수 없게 된 것이다. 그러한 관점에서 보면 사이버공간의 안전을 보장한다는 측면에서 사이버안보라는 개념이 현재로서는 가장 적절한 표현인 것으로 생각된다.

이 논문의 목적은 사이버안보를 침해하는 행위의 유형을 정리해 보고 이에 대한 형사법적 대응방안을 모색하는 것이다. 사이버안보를 지키기 위한 사전예방 법제, 신속한 침해복구를 위한 법제 그리고 침해행위의 재발을 방지하기 위한 사후처벌 법제 등 세 가지 가운데 마지막 부분을 다루는 것이다.

4) 정필운, 사이버보안이란 개념 사용의 타당성 재론, 인터넷법제도포럼 제13회 월례발표회 (2011. 7. 21.) 발표문, 1면 참조.

Ⅱ 형사처벌 규정의 필요성

사이버안보를 침해하는 행위는 범죄로 평가된다. 범죄를 방지하기 위해서는 발생되는 범죄에 대한 빈틈없는 형사처벌이 이루어져야 한다. 그리하여 범죄행위를 하면 그에 따른 형사처벌이 있게 됨을 사회구성원들이 기정사실로 받아들이게 되면 그 범죄는 예방되는 것이다. 그 형벌이 그다지 가혹하지 않더라도 빈틈없는 형사처벌은 뛰어난 예방효과를 가지고 있다.[5]

이는 형사처벌제도가 정착된 문명국가와 그렇지 못한 원시사회를 비교해 보면 잘 알 수 있다. 살인범죄를 비교해 볼 때 원시사회의 경우에는 고의적인 폭력에 의해서 동족의 남성이 다른 남성에 의해서 살해되는 비율이 30% 정도에 이른다.[6] 이는 우리나라의 2009년도 살인범죄율인 0.003%와 비교해 볼 때 아주 높은 비율이다.[7]

원시인류와 현재의 인류가 유전적으로 서로 다르기 때문에 형사처벌제도의 존재만으로 범죄율의 차이를 설명할 수 없다는 반론도 가능하다. 그러나 비교대상으로서 30%의 살인범죄율을 보인 원시사회는 현재 지구상에 남아있는 문명화 되지 않은 곳이기 때문에 유전적 차이는 없는 상황이다.

5) 김성천, 사이버범죄에 대한 법적 대응, "중앙법학" 제12집 제1호 (2010), 211면. 과거에는 형벌이 가혹할수록 범죄예방 효과가 크다고 생각하여 범죄자를 공개된 장소에서 잔혹한 방식으로 처형하였으나, 잔인한 형벌이 가해짐에도 범죄는 근절되지 않았다. 아무리 가혹한 형벌이 예정되어 있다고 하더라도 거의 1만명에 한 명 꼴로만 잡혀서 처벌을 받는다면 형벌의 예방효과는 그리 크지 못할 것이다. 또한 범죄행위의 불법성과 비교해 볼 때 지나치게 가혹한 형벌은 형사법체계에 대한 반감만 드높이고 국민들이 사법적 정의를 신뢰하지 않게 될 것이다. 법이 지켜지게 하는 가장 좋은 길은 일반국민이 그 법질서를 신뢰하고 따르게 하는 것이라는 측면에서 가능한 한 가혹하게 형벌을 부과해야 효과적이라는 입장의 부정적 일반예방이론은 이제 더 이상 지지를 받을 수 없게 되었다.

6) 정혜욱, 아동성범죄의 근본원인과 대책, 중앙대학교 박사학위논문, 2011, 53면.

7) 대검찰청, 범죄분석, 2010, 108면에 의하면 2009년도 살인범죄 발생건수는 1,390건이다. 작년도 우리나라 전체 인구는 4천 874만 7천명이었으므로("남녀별 연령별 인구구조" e-나라지표 <http://www.index.go.kr/egams/stts/jsp/ potal/ stts/PO_STTS_IdxSearch.jsp?idx_cd=1010&stts_cd=101002&class_div= &idx_clas_cd=>) 살인범죄율은 약 0.003%가 된다.

사이버안보를 침해하는 범죄의 경우도 마찬가지라고 생각된다. 물론 살인범죄와 사이버안보 침해범죄의 특성이 상당히 다르기는 하다. 살인죄는 사람의 생명을 침해하는 범죄이고 사이버안보 침해범죄는 공공의 안전, 전자정보에 대한 공공의 신용 또는 사람의 업무를 침해하는 범죄이다. 범죄의 특성이 다르기 때문에 그에 대한 대처도 달라질 수 있을 것이다.

그런데 범죄예방이라는 측면에서 범죄 특성에 따라 서로 다른 예방대책을 이야기 할 때 형사처벌이라는 방법론과 관련해서는 특별예방의 경우만 다양한 교정처우대책이 거론되고 있다. 특별예방의 경우에는 각 개별 범죄의 특성에 따라 그 범죄를 저지른 범죄인의 성향도 다를 것이기 때문에 특성에 맞는 개별적인 처우를 하여야 한다는 주장이 가능하지만 일반예방의 경우에는 그렇지 않기 때문이다.

예를 들어 아동성범죄와 같은 특수한 범죄를 제대로 예방하기 위해서 전자발찌 제도를 실시하고 초등학교를 중심으로 폐쇄회로 카메라 설치 대수를 확대한다거나 보안관 제도를 도입한다는 등의 대처방안이 논의되는데 이는 형사 정책적 대응방안이기는 하지만 형사 사법적 대응방안은 아니다. 형사처벌이 이루어지면 그것을 통하여 일반예방이라는 효과가 나타나는가에 대하여 이를 부인하는 견해는 없다. 또 범죄유형에 따라 형사처벌을 하더라도 일반예방효과가 나타나지 않는다거나 그 예방효과에 경중이 있다는 견해도 찾아볼 수 없다.

그러한 의미에서 사이버안보 침해범죄도 예외가 아니라는 말이다. 사이버범죄는 익명성과 비대면성 때문에 검거와 처벌이 매우 어려워서 범죄억제가 힘들다는 것이 중론[8]인데, 이 말은 곧 사이버범죄도 형사처벌이 효과적인 일반예방 방법론임을 의미한다. 또한 예를 들어 일반청소년을 대상으로 처벌의 확실성이 사이버범죄 억제에 효과적인 영향을 미치는가에 대한 경험적 연구

8) 김성천, 인터넷과 형사법상의 과제, 『법제연구』 제18호 (2000), 56면 이하; 이성식, 사이버범죄의도에 대한 공식처벌의 억제효과, 『형사정책』 제20권 제1호 (2008), 187면.

결과[9]를 보더라도 처벌의 확실성이 범죄예방이라는 측면에서 가지는 효과는 매우 긍정적이다. 이처럼 사이버범죄의 경우에도 형사처벌이 효과적인 범죄억제 대책으로 평가되므로 이를 위한 처벌규정은 반드시 필요한 존재라고 할 수 있다.

Ⅲ 사이버안보에 대한 침해유형

「정보통신기반 보호법」에서는 침해의 유형을 해킹, 컴퓨터 바이러스, 논리·메일폭탄, 서비스 거부 그리고 고출력 전자기파 공격 등으로 세분하고 있다. 이 가운데 논리·메일폭탄과 서비스 거부 공격은 넓은 의미의 바이러스 공격에 포함되므로 함께 논하기로 하고 고출력 전자기파 공격은 물리적 공격이기 때문에, 통신망을 절단하는 등의 보다 적극적이고 물리적인 공격행위와 구별하기 어려운 점이 있어서 논의에서 제외하기로 한다.

1. 해킹

인터넷이 형성되기 시작하던 초기에는 해킹이라는 표현이 그다지 부정적인 의미를 가지고 있지 않았다.[10] 초창기에는 전화설비를 기술적으로 조작해서 전화를 공짜로 사용하거나 회의통화를 가능하게 하거나 음악을 송신하는 데 이용하는 등 사회적으로 그다지 큰 폐해를 유발하지 않는 행위유형(Phreaking[11])이었다. 물론 지금 현재는 사람의 생명을 위협할 수 있을 정도의 수준에 도달하였다. 앞에서 언급한 것처럼 공공의 안전을 침해하는 범죄행위로 분류할 수 있을 정도가 되었다.

정보통신망에 침입하여 정보를 손괴, 변조 또는 유출하기 위한 해킹 방법

9) 이성식, 사이버범죄의도에 대한 공식처벌의 억제효과, 201면 이하.
10) Ernst, Stefan: Hacker und Computerviren im Strafrecht, 『Der Sachverständige』 2004, S. 14.
11) Phreaking은 영어의 phone과 freak를 합성한 단어이다.

은 매우 다양하게 발전한 상태이다. 해킹 방법은 대략 다음과 같다.

① 비밀번호 도용 : 타인의 아이디와 비밀번호를 알아내어 이를 이용해서 '권한 없이 정보를 입력'하는 행위이다. 형법 제314조 제2항에는 허위의 정보를 입력하는 행위와 부정한 명령을 입력하는 행위만 명시하고 있는데, 아이디와 비밀번호의 도용은 부정한 명령 입력에 해당된다는 해석도 가능하고 그렇지 않으면 '기타의 방법'에 해당되는 것으로 보면 될 것이다.

타인의 아이디와 비밀번호를 알아내는 가장 손쉬운 방법은 당사자의 메모를 몰래 확인하는 것이다. 단 하나의 아이디와 비밀번호로 모든 사이트에 다 접속하는 사람이 아니라면 여러 가지의 아이디와 비밀번호를 항상 외우고 있기는 힘들기 때문에 어디엔가 메모를 하기 마련이다. 그리고 비밀번호를 기억해내야 하는 일은 항상 모니터 앞에서 생기므로 대부분의 메모는 모니터에 붙어있다.

물리적인 접근이 가능한 관계가 아닐 경우에 요사이 주로 사용되는 방법이 이른바 Social Engineering이다. Social Engineering은 사람들이 전형적으로 저지르게 되어 있는 오판(cognitive bias)을 활용하여 필요한 정보를 알아내는 방법론이다. 이와 같은 전형적인 오판은 인간이 진화과정에서 자연선택압력(natural selection pressure)에 의하여 획득하게 된 행동양식이다.[12] Social Engineering의 대표적인 기법이 피싱(Phishing)이다.

해킹 프로그램을 이용하는 Trapdoor는 이용자가 정확한 비밀번호를 입력하였음에도 다시 비밀번호를 입력하라는 에러메시지가 뜨게 하고 그 창에 비밀번호가 입력되면 이를 담아서 가져가는 방법이다.

12) 예를 들면 다른 사람들이 다 하는 행동이라면 그것이 맞는 것이라고 판단하고 따라서 하는 bandwagon effect, 자신의 결정이 틀렸을 가능성에 대한 새로운 증거를 찾기보다는 기존의 결정이 타당하였음을 입증할 증거를 찾는데 점점 더 많은 투자를 하게 되는 성향(irrational escalation) 또는 외부 상황을 제어할 수 있는 자신의 능력을 과대평가하는 성향(illusion of control)과 같은 것이 이에 해당된다.

② 시스템 보안상의 빈틈 활용 : Port Scanning을 통해서 시스템 보안상의 빈틈을 발견하고 그 지점을 통해서 침입하여 정보를 손괴, 변조, 유출하는 방법이다.

③ 트로이 목마 이용 : 겉으로는 무해한 정보인 것으로 보이는 프로그램을 이식시켜서 이를 통하여 정보통신망으로 침입하는 방법이다.

④ 제3의 신뢰인 이용 : 농협 전산망 침입에 이용되었던 방법이다. 공격대상 정보통신망에 접속할 수 있는 사람 가운데 보안에 취약한 자를 찾아내어 그 사람의 단말기를 통해서 그 사람의 아이디와 비밀번호를 이용하여 침입하는 방법이다. 이 방법을 이용해서 침입한 해커는 농협 IT본부 서버의 파일을 모두 삭제하라는 정보 손괴 명령을 내렸고[13] 그 결과 복구가 불가능한 많은 부분이 영구적으로 유실되었다.[14]

⑤ 침입 흔적 인멸 : 해커는 정보통신망에 침입할 때 자신의 IP주소를 비롯한 모든 흔적을 인멸한다. 농협 해킹 사건은 물론 7·7 DDoS 공격과 3·4 DDoS 공격의 행위자가 누구인지 수사기관에서 아직 찾아내지 못하고 있다.[15]

13) 농협 서버 587개 가운데 273개의 정보가 모두 삭제되었다. (전성철, 검찰 북 정찰총국 사이버테러 결론,『동아일보』2011. 5. 4.)

14) 김재영, 농협 상상초월 삭제명령,『동아일보』2011. 4. 19.

15) 검찰에서는 북한의 정찰총국이 농협 해킹사건의 범인이라는 발표를 하였지만(전성철·장관석, 농협 해킹 북 정찰총국이 7개월간 준비,『동아일보』2011. 5. 4.) 사실관계를 입증할 증거는 제시하지 못하였다. 증거가 하나도 없음에도 불구하고 북한 정찰국의 소행이라고 결론을 내린 이유는 3·4 DDoS 공격에 사용된 프로그램에 담긴 삭제대상 파일의 확장자명 목록이 일치하는 등 행위수법이 동일하다는 것이었다. 그리고 3·4 DDoS 공격이 북한 정찰국의 소행인 이유는 ① 그 공격에 사용된 프로그램상의 삭제대상 파일의 확장자명 목록과 7·7 DDoS 공격의 그것이 거의 일치하고, ② 70개국 748개의 IP가 공격에 사용되었는데 그 가운데 3개가 7·7 DDoS 공격 때와 일치하는 등 역시 범행수법이 같기 때문이라는 것이다. 결국 2009년에 발생한 7·7 DDoS 공격이 북한의 소행이고 3·4 DDoS 공격과 농협 해킹은 범행수법이 일치하기 때문에 결국 북한 정찰총국이 한 일이라는 말이다.
7·7 DDoS 공격 당시 국정원은 ① 한국의 통신망을 파괴하라는 북한 지도부의 지령이 있었고, ② 국군기무사령부가 미국이 실시하는 사이버 위협 대응훈련에 참여하겠다고 선언하자, 북한의 조국평화통일위원회가 이를 전쟁도발이라고 비난하면서 자신들도 고도의 기술전쟁을 할 준비가 되어 있다고 하였으며, ③ 북한이 한국정보보호진

2. 컴퓨터바이러스

인터넷망이 확대되면서 동시에 증대되고 있는 것이 컴퓨터바이러스에 의한 정보 침해의 위험이다. 사이버공간에 대한 최초의 대규모 공격은 1988년에 한 학생이 퍼뜨린 internet-worm에 의해서 이루어졌다. 당시 이 바이러스에 의해서 6천대의 컴퓨터가 동시에 작동을 멈추었다.

컴퓨터바이러스는 10대 청소년의 장난일 수도 있지만 공항 정보통신망이나 군부대의 무기 관리 전산망이 공격대상이 될 경우에는 대규모 인명피해까지 야기할 수 있는 심각한 행위유형에 속하게 된다. 행위자에 의해서 실시간으로 부정한 명령이 입력되는 해킹과 마찬가지로 바이러스 유포행위도 공공의 안전 또는 전자정보에 대한 공공의 신용이라는 사회적 법익을 침해하는 행위가 된다.

해킹과 다른 점은 바이러스는 프로그램의 일종으로서 미리 입력되어 있는 명령이 자동으로 수행된다는 것이다. 컴퓨터바이러스에 의한 정보침해는 프로그램의 유형에 따라 대략 다음과 같이 그 양상을 분류할 수 있다.

① 웜 : 프로그램 자체 또는 아무 것이나 불필요한 파일을 계속 복제해서 결국 감염된 컴퓨터가 과부하로 작동을 멈추게 만든다.

② 바이러스 : 특정 파일을 삭제(손괴)하거나 변조하여 이용가능성을 침해한다. 심한 경우에는 감염된 컴퓨터의 모든 파일을 삭제해 버리기도 한다. 또한 BIOS(Basic Input Output System) 파일에 변경을 가하도록 프로그래밍 된 바이러스는 냉각팬의 작동이 정지되도록 설정을 바꾸

흥원과 부산 동명대 컴퓨터학과를 상대로 모의훈련을 하였다는 정황이 파악되었고, ④ 북한이 과거에 즐기던 수법과 유사하다는 점을 근거로 북한이 저지른 사이버 공격 행위라고 발표하였다(정원수・윤상호, 북 사이버전 지령-예고-훈련까지, 『동아일보』 2009. 7. 11.).
이 가운데 정말로 북한이 그와 같은 공격행위를 하였을까에 관한 합리적 의문을 해소해 줄 수 있는 증거자료는 하나도 없다. 모두 국정원에서 보기에 그런 것 같다는 정도의 추정에 불과하다. 따라서 7・7 DDoS 공격 자체를 북한의 정찰총국이 저지른 일이라고 보기 힘들고, 이와 수법이 유사하기 때문에 3・4 DDoS 공격과 농협 해킹이 북한의 소행이라고 하는 것은 무리한 주장으로 보인다.

어 CPU 등 핵심부품이 물리적으로 손상되도록 할 수도 있다.

③ DDoS 바이러스 : 전 세계의 수많은 좀비 PC에 잠복해 있다가 행위자가 지정한 시각에 특정 사이트에 대한 파일 업로드와 다운로드를 무한 반복하는 명령이 수행되기 시작하도록 프로그래밍 된 바이러스이다. 분산된(distributed) 여러 PC로부터 업로드와 다운로드가 쉼 없이 반복되면 과도한 트래픽이 유발되어 피공격 사이트는 이를 감당하지 못하고 서비스거부(Denial of Service) 상태에 빠지게 된다.

사람들이 짜증을 느끼기는 하지만 스팸은 바이러스에 속하지 않는다. 스팸이란 ① 전자우편이나 그 밖에 대통령령으로 정하는 매체를 이용하여 전송되는 것으로서 수신자의 명시적인 수신거부의사에 반하는 '영리목적의 광고성 정보' 또는 ② 수신자의 동의를 받지 않은 채 수신자의 전화·모사전송기기에 전송되는 '영리목적의 광고성 정보'를 말한다(정보통신망법 제50조 제1, 2항). 불필요한 정보가 유입되기는 하지만 메일폭탄 수준에 이르지 않는 한 이를 통해서 정보나 정보통신망에 대한 이용가능성 침해의 결과가 야기되지는 않기 때문에 사이버안보 침해 행위로 보기 곤란하다.

Ⅳ 사이버안보 침해행위에 대한 가벌성 판단

1. 정보통신망 침입 행위

누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 안 된다(정보통신망법 제48조 제1항). 이 규정을 위반하게 되면 정보통신망법 제72조 제1항 제1호에 의해서 형사처벌 대상이 된다.

이 규정의 보호법익은 정보통신망 및 이를 통해서 접근할 수 있는 정보의 안전(사이버안보)라고 할 수 있다. 일단 행위내용에 해당되는 행동을 하기만 하면 범죄가 성립하고 별도로 정보훼손 등의 결과를 필요로 하지 않기 때문에 추상적 위험범으로 파악된다.

행위객체는 정보통신망이다. 정보통신망이란 '전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제'를 말한다(정보통신망법 제2조 제1항 제1호).

행위내용인 침입이란 '관리자의 의사에 반하여 들어가는 것'이라고 정의할 수 있다. 예를 들어 경찰청 전산망에 접근권한을 가진 사람은 많이 있을 수 있는데 그 가운데 한 사람이 경찰 데이터베이스의 정보 유출을 돕기 위해서 제3자에게 아이디와 비밀번호를 알려주었을 경우, 그 제3자의 접속 행위는 정보의 무결성·신뢰성·기밀성을 위협하는 것이어서 처벌대상으로 보아야 하기 때문이다. 따라서 관리자가 접근권한을 부여한 사람이 아니라면 누구라도 접속할 수 없다고 보아야 하겠다.

정보통신망은 여러 사람이 함께 이용하는 시스템이고 항상 관리자가 누구에게 어느 영역까지 들어올 수 있도록 허용하는가 하는 점이 명확하게 설정되어 있다. 예를 들어 포털 사이트의 서버에는 접근권한이 각기 달리 설정되어 있는 수많은 파일이 존재한다. 완전 공개되어 있는 파일은 누구나 접근할 수 있다. 그러나 그 파일을 변경할 수 있는 권한은 일부에게만 제한되어 있다. 인터넷을 통해서 이러한 공개파일을 검색하기 위해서 접근하는 행위는 침입이 아니다. 그러나 같은 인터넷에 들어와 있더라도 이 파일에 변경을 가하기 위해서 해킹을 통하여 관리자 아이디로 로그인을 하면 침입이 된다.

어차피 사이버공간은 물리적 경계가 없기 때문에 로그인 여부를 기준으로 침입 여부를 판단하는 수밖에 없을 것으로 보인다.

2. 정보 손괴 행위

(1) 컴퓨터 손괴 등 업무방해

특수매체기록을 손괴하여 사람의 업무를 방해하게 되면 형법 제314조 제2항에 해당되어 형사처벌 대상이 된다. 보호법익은 정보의 안전과 업무수행

의 자유라고 할 수 있다. 형법 제314조 제1항의 업무방해와 마찬가지로 추상적 위험범으로 해석된다.[16]

행위객체는 특수매체기록이다. 특수매체란 종이 이외의 전자적 기록매체를 의미한다. 특수매체에 저장되어 있는 정보가 특수매체기록이다. 컴퓨터 파일은 일반적으로 재산적 가치를 가지고 있겠지만 반드시 그러하여야만 행위객체에 포함되는 것은 아니다.

행위내용 중 손괴는 이용가능성을 침해하는 것을 말한다. 이용가능성은 파일을 삭제하거나 심하게 변화시켜서 본래의 정보를 인식할 수 없게 되면 침해되는 것이다.

이를 통하여 사람의 업무를 방해하여야 범죄가 성립되는데 업무방해는 업무수행 자체가 불가능해지거나 부당한 업무집행이 이루어지게 하면 성립된다. 추상적 위험범이기 때문에 업무방해의 가능성만 유발하면 충분하다.

(2) 전자무역촉진법 위반

형법 제314조 제2항과는 달리 전자무역촉진법[17]은 제31조 제2호에 전자무역기반사업자・전자무역전문서비스업자・무역업자・무역관계기관의 컴퓨터 파일에 기록된 전자무역문서 또는 데이터베이스에 입력된 무역정보를 훼손하는 행위 자체에 대하여 처벌규정을 두고 있다.

(3) 주요정보통신기반시설 교란・마비・파괴

나아가 정보를 손괴하는 행위가 단순히 사람의 업무수행에 지장을 초래할 정도의 위험을 야기하는 정도에 그치는 것이 아니라, 주요정보통신기반시설을 교란・마비・파괴하는 결과를 야기하게 되면 정보통신기반 보호법 제28조에 따라 가중처벌 대상이 된다.

16) 김성천, 형법, 753면.
17) 「무역업무자동화 촉진에 관한 법률」 제정 1991. 12. 31. 법률 제4479호, 「전자무역촉진에 관한 법률」 전부개정 2005. 12. 23. 법률 제7751호, 최근개정 2011. 4. 14. 법률 제10591호.

결과적 가중범인 본죄의 기본범죄는 정보통신기반 보호법 제12조이다. 기본범죄의 행위내용은 ① 부정하게 정보를 조작・파괴・은닉하거나, ② 컴퓨터바이러스를 투입하거나, ③ 일시에 대량 신호를 보내거나, ④ 부정한 명령을 처리하게 하는 것이다.

주요정보통신기반시설을 교란・마비・파괴하였다고 보기 위해서는 상당한 시간 동안 정보통신망의 운용이 불가능하게 만드는 정도에는 이르러야 할 것으로 생각된다. 일시적으로 서비스 속도가 낮아진 정도로는 가중처벌을 위한 결과가 발생한 것으로 보기는 곤란할 것이다.

(4) 정보통신망법 제48조 제2항 위반

“누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손・멸실・변경・위조하거나 그 운용을 방해할 수 있는 프로그램(이른바 악성프로그램)을 전달 또는 유포하여서는 아니 된다.” 이를 위반할 경우 정보통신망법 제71조 제9호에 의거하여 형사처벌대상이 된다.

3. 정보 변조 행위

특수매체기록을 변조하는 행위는 그 기록이 공전자기록일 경우에는 형법 제227조의2에 의해서 사전자기록일 때에는 형법 제232조의2에 의거하여 처벌대상이 된다. 이들 처벌규정의 보호법익은 전자기록에 대한 공공의 신용이다.

행위객체인 전자기록은 일반적인 문서와 기록 형태만 다를 뿐 공공의 신용을 담보한다는 측면에서는 다를 것이 없으므로, 문서가 갖추어야 할 요건인 ① 의사표시 기능, ② 증명 기능 그리고 ③ 작성명의자 확인 기능 등을 갖추고 있어야 한다. 따라서 이러한 요소를 갖추지 않은 단순한 풍경 사진 파일 등은 행위객체에서 제외된다.

본 죄는 목적범으로서 ‘사무를 그르치게 할 목적’을 가지고 정보를 변조하여야 범죄가 성립된다. 예를 들어서 교통법규위반 벌점 누적으로 면허정지

등의 행정처분이 내려져야 함에도 그러한 사무가 제대로 이루어지지 못하게 할 목적으로 벌점의 합계를 하향조정하는 경우가 이에 해당될 것이다.

한 편 정보통신망법은 정보 변조 행위 자체를 처벌하는 규정을 가지고 있다(같은 법 제48조 제2항, 제71조 제9호). 누구든지 정당한 사유 없이 정보의 내용을 변경하는 행위를 하면 그 자체로서 처벌대상이 되는 것이다.

4. 정보 유출 행위

(1) 도청

정보통신망을 통해서 타인 사이에 송신·수신되는 정보의 내용을 취득하게 되면 통신비밀보호법 제3조 제1항 및 제16조 제1항에 따라 처벌대상이 된다. 이들 처벌규정의 보호법익은 정보에 대한 자기결정권이다. 정보자기결정권이란 자신에게 속한 정보가 언제 누구에게 어느 범위까지 공개되도록 할 것인가를 결정할 수 있는 권리를 말하며 헌법상의 기본권이다.[18]

(2) 비밀침해

비밀장치가 되어 있는 특수매체기록의 내용을 기술적 수단을 이용해서 알아내면 형법 제316조 제2항에 따라 형사처벌 대상이 된다. 본죄는 친고죄이다. 보호법익은 비밀장치가 되어 있는 정보의 불가침성이다.

행위객체는 비밀장치가 되어있는 특수매체기록인데 국가 또는 공공기관의 정보는 행위객체에서 제외시켜야 한다는 견해가 있다[19]. 그러나 ① 형법 제

18) 통신비밀의 법적 성격에 대해서는 자유권적 기본권 가운데 사생활 보호와 관련된 정보자기결정권에 해당하는 것으로 보는 견해(권영성, 헌법학원론, 법문사, 1997, 398면 이하; 김일환, 통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰,『형사정책』(한국형사정책학회) 제16권 제1호 (2004), 32면; 성낙인, 통신에서의 기본권 보호,『공법연구』(한국공법학회) 제30집 제2호 (2001), 35면 이하)와 표현의 자유로 보는 입장(박용상, 표현의 자유, 현암사, 2002, 620면 이하)이 있다. 비밀은 누설되지 않도록 지켜지는 것이 본질이므로 사생활의 불가침과 관련된 정보자기결정권으로서의 자유권적 기본권으로 보는 것이 타당하다고 생각한다.

19) 배종대, 형법각론, 제3판, 홍문사, 1999, 294면; 오영근, 형법각론, 박영사, 2005, 251면; 임웅, 형법각론(상), 법문사, 2000, 228면; 진계호, 형법각론, 제3판, 대왕사,

316조가 친고죄이더라도 문제가 되는 경우에 고소권자는 얼마든지 지정이 될 수 있으므로(형사소송법 제228조) 친고죄라는 점 때문에 공공기관의 정보를 보호대상에서 제외할 이유는 없고, ② 개인의 정보보다 공공기관의 정보를 덜 중요하게 취급할 이유가 전혀 없으므로 국가・공공기관의 비밀장치 정보도 제316조의 보호대상으로 보는 것이 타당하다고 생각한다.

특수매체기록의 비밀장치는 비밀번호 또는 지문인식장치 등을 통해서 권한 없는 자의 접근을 제한하는 것을 의미하는 것으로 이해된다. 그러나 내용 자체를 암호화한 것은 비밀장치라고 할 수 없다.[20]

행위내용은 기술적 수단을 이용해서 내용을 확인하는 것이다. 이는 본래 비밀장치를 그대로 둔 채 기술적인 수단을 동원해서 내용을 알아내는 것을 의미한다. 따라서 비밀번호를 알아내서 비밀장치를 해제하고 내용을 인지하는 것은 본죄에 해당되지 않는다.[21] 비밀장치를 열지 않고 특수매체기록의 내용에 접근한다는 것은 지문인식장치 등 시스템 보안상의 빈틈을 찾아내어 이를 통해서 침입하는 것을 의미하는 것으로 볼 수 있다.

V 사이버안보 사후처벌 법제 전반에 대한 평가

사이버안보를 침해하는 범죄에 대한 처벌규정은 거의 빠짐없이 마련되어 있다는 점에서는 문제가 없어 보인다. 다만 이들 처벌조항들이 형법, 정보통신망법, 전자무역촉진법, 정보통신기반 보호법 등 여러 법규에 분산되어 있는 것은 수범자가 처벌대상의 내용을 파악하기 힘들게 한다는 측면에서 문제라고 생각된다.

이러한 측면에서 사이버안보에 관한 사항을 총괄하는 기본법이 제정되고

1996, 229면.
20) 김성천, 형법, 797면.
21) 김성천, 형법, 798면.

사이버안보를 침해하는 범죄행위에 대한 처벌규정은 형법에 독립된 장으로 새로 정리하여 제정하는 것이 타당할 것으로 보인다. 하지만 만약 사이버안보 기본법과 형법이 분리되어 있어서 수범자 입장에서 처벌규정을 찾기 힘들다는 문제점이 크다고 느껴질 경우에는 사이버안보 기본법 안에 형사처벌 규정을 두어도 무방할 것으로 생각된다.

어떻게든 일목요연하게 정리가 되면 사이버안보와 관련하여 사후처벌 법제는 얼추 완비되는 것으로 볼 수 있다. 완결성의 의미를 어떻게 이해할 것인가도 문제일 수 있겠지만 범죄유형과 관련하여 사이버안보를 침해하는 모든 행위유형에 대하여 빈틈없이 처벌규정이 마련되어 있으면 공백이 없다는 측면에서 완결성을 인정할 수 있을 것으로 보인다. 사이버안보 사후처벌 법제는 실체 형법적인 측면에서는 전반적으로 우수하고 완결적이라는 평가가 가능하다.

그런데 실제로 사후처벌과 관련하여 문제가 되는 것은 처벌규정의 완결성보다는 행위자를 발각하는 것이 아주 어렵다는 수사실무상의 장애요소들이다. 이제 장을 달리하여 그에 대해서 검토해 보기로 한다.

Ⅵ 형사처벌의 곤란성과 그 극복에 관한 문제

1. 사이버범죄의 익명성

사이버안보를 침해하는 행위에 대한 처벌규정은 현재로서는 큰 결함 없이 모든 범죄유형을 대상으로 규율하고 있는 것으로 보인다. 문제는 처벌규정상의 빈틈이 아니라 범죄를 발각해서 처벌하는 것이 매우 힘들다는 현실적인 측면에 놓여 있다.

사이버범죄가 전반적으로 동일하게 직면하고 있는 문제는 행위자를 알아내는 것이 곤란하다는 점이다. 사이버공간에서의 행위는 사람이 직접 인식할 수 있는 형태의 흔적을 남기지 않는다. 유일하게 찾아낼 수 있는 것은 행위자가 사용한 단말기의 IP주소이다.

이를 추적해서 행위자를 특정 한다는 것이 쉬운 일은 아니다. 2009년의 7·7 DDoS 공격 때 동원된 좀비PC의 IP주소는 모두 70개국의 748개이었는데 이 가운데 하나가 북한 체신청이 중국에 임대해서 사용하는 IP주소이었다는 점을 근거로 7·7 DDoS 공격의 행위자가 북한 정찰총국이라고 단정 짓는 것처럼 어처구니없는 결론에 도달할 가능성이 많다.

더구나 DDoS 공격과 같은 경우 일시에 과도한 트래픽을 유발하는데 동원되는 좀비PC의 IP는 확인할 수 있지만 정작 좀비PC에 DDoS 바이러스를 이식시킨 단말기의 IP는 확보가 되지 않고 있다. 행위자를 찾는 것이 불가능한 상황이다.

농협 해킹 사건의 경우에도 협력업체 직원의 노트북을 경유해서 삭제명령이 주어졌는데 행위 이후 모든 로그기록이 인멸되었기 때문에 누구에 의한 해킹이었는지 지금까지도 알아내지 못하고 있다. 물론 검찰에서 북한 정찰총국의 행위이었다고 발표하기는 하였지만 합리적인 증거를 근거로 내린 결론이라고 보기 힘들다. 다소 무책임한 수사결과라고 생각된다.[22]

그나마 경찰이 현대캐피탈 해킹사건의 용의자를 체포할 수 있었던 것은 행위자가 피해자 쪽에 금품을 요구하였고 이에 따라 현대캐피탈에서 입금한 돈을 현금인출기에서 찾아가다가 얼굴이 노출되었기 때문이었다.

2. 익명성 극복을 위한 방안

(1) IPv6에 의한 고정 IP 부여

익명성을 극복하기 위해서 일단 생각해 볼 수 있는 방안은 인터넷 실명제이다. 인터넷 사용을 위한 아이디를 발급받을 때 실명을 확인해 두면 그 아이디를 통해서 이루어진 행위는 바로 그 실명의 보유자의 행위로 특정할 수 있어서 범죄를 예방할 수 있을 것이라는 생각에서 출발한 것이다.

인터넷 실명제를 통해서 예방하고자 하는 범죄는 주로 사이버명예훼손과

22) 앞의 각주 19에서 왜 미덥지 못한 수사결과인가에 대하여 언급하였다.

사이버모욕 행위이다. 정작 사이버안보에 문제가 되는 해킹이나 컴퓨터바이러스 유포행위 등은 이를 통해서 방지하기가 힘들다. 자신이 발급한 아이디를 이용해서 로그인 하고 해킹을 시도하는 사람은 없기 때문이다. 앞에서 언급하였듯이 해킹은 권한 있는 타인의 아이디와 비밀번호를 도용하는 것이 기본이다.

무엇보다 필요한 것은 우선 지구상의 모든 인터넷 접속 가능 단말기에 고정 IP를 할당하는 것이라고 생각된다. 현재의 IP주소 체계로는 물론 불가능한 일이다. 따라서 차세대 IP주소 체계(Internet Protocol version 6 / IPv6)로 전환하고 전세계의 모든 단말장치별에 각각 다른 고정 IP주소를 부여하여야 할 것이다. 이것이 행위자 특정을 위한 첫걸음이라고 생각한다.

(2) 국제공조체제의 정립

사이버범죄 진압을 방해하는 또 하나의 요소는 사이버공간에는 공간적 제한이 존재하지 않는다는 점이다. 7·7 DDoS 공격이 70여 개국의 PC를 동원해서 이루어졌다는 것이 그 좋은 예이다. 전 세계 모든 인터넷 단말기에 고정 IP를 부여하는 것에서부터 시작하여 사이버범죄를 예방·진압하기 위한 국제협력체계의 정립이 필요하다.

이를 위해서는 IP표준제정과 사이버범죄의 행위내용에 대한 표준화가 있어야 할 것이고 인터폴과 같은 형태의 수사협조체제가 이루어져야 할 것이다. 각 국가별로 자국의 법익을 보호하는 차원에서 작동되고 있는 국가 단위로 고착되어 있는 형벌권 체계가 사이버범죄를 진압하기 위해서 변화를 맞아야 하는 시기가 도래하였다.

3. 익명성 극복의 현실적 한계

IPv6를 기반으로 한 모든 단말기에 대한 고정 IP 부여와 긴밀한 국제공조체제의 구축을 통해서 익명성이라는 장애요소를 어느 정도 극복할 수 있기는 할 것으로 생각된다. 하지만 이와 같은 해결방안은 지금 현재 적극적으로 추

진이 되고 있는 것은 아니다. 그와 같은 이상적인 범죄 예방·진압 체계가 갖추어질 때까지 사이버안보 침해 행위를 그대로 방치할 수도 없는 일이다.

상황이 이와 같기 때문에 당분간 사후처벌보다는 사전예방을 중심으로 하는 사이버안보 법제가 운영되어야 할 것으로 생각된다. 범죄가 발생하였을 경우에 이를 빠짐없이 처벌하는 것이 범죄예방을 위해서 매우 중요한 일이기는 하지만 행위자를 찾아내기 위한 도구가 아직 확보되어 있지 못한 상태이기 때문에 사전예방 체제부터 먼저 갖추어야 하겠다는 말이다.

사실 사전예방과 사후처벌은 어느 것 하나 소홀히 할 수 없는 사항이다. 다른 범죄의 경우에도 마찬가지이다. 사전예방을 게을리 해서 전과자를 양산할 이유도 없는 일이고, 아무리 예방조치에 만전을 기하더라도 보안에는 빈틈이 있을 수 있으니까 사후처벌도 안 할 수 없는 일이다.

따라서 사후처벌을 빠짐없이 할 수 있도록 하기 위해서 행위자를 특정할 수 있는 법적·기술적 장치를 마련해 나가면서, 또 한편으로는 당장 시급한 사전예방 법제를 구축하는데 초점을 맞추어야 할 것이다.

Ⅶ 형법의 국제적 적용범위 문제

1. 속지주의를 근거로 한 대한민국 형법의 적용

현재 전 세계의 육지는 거의 빈틈없이 국민국가 단위로 분할되어 있고 이들 국민국가의 주권이 그 영토에 대하여 형벌고권을 행사하고 있다. 국제적 형벌고권이라는 것을 형성하기 위한 노력도 있고 그러한 발상이 지금도 유효하기는 하지만 아직은 그것이 지구상에 구축되었다고 보기 어렵다.

따라서 모든 국가는 기본적으로 자신의 영토에 한하여 효력을 미치는 형법을 운용하고 있다. 현대 사회에서는 속지주의가 원칙인 것이다. 첫 번째 원칙인 속지주의를 보완하는 측면에서 다음으로 적용되는 원칙은 속인주의이다. 우리나라 국민이 저지른 범죄행위에 대해서는 그 행위지가 어디인가를 상관하지 않고 무조건 우리나라 형법을 적용한다는 것이다.

이처럼 각 국가의 형법 적용범위는 일방적이며 타협을 용납하지 않는다. 심지어 다른 국가에서 범죄행위를 저지르고 그 나라에서 이미 형사처벌을 받고 나서 귀국했다고 하더라도 다시 우리나라 법원이 재판권을 행사해서 처벌하는 것이 허용된다. 형법의 국제적 적용범위는 타국의 형법과 우리나라의 형법이 서로 충돌하여 어느 형법이 적용될 것인가 문제되는 경우에 어느 나라 형법을 준거법으로 선택할 것인가 하는 점과 완전히 무관하다. 그저 어느 경우에 우리나라 형법을 적용할 것인가 하는 점만 생각하고 고민하고 있는 것이다.

그런데 사이버안보를 침해하는 행위를 생각해 볼 때 판단을 어렵게 만드는 것은 그 침해행위가 물리적·공간적 한계를 초월해서 발생한다는 점이다. 속지주의라는 측면에서 침해 행위자가 어느 곳에 앉아서 공격을 감행하였는가 하는 점은 별 의미가 없다. 세계 어느 곳에서 공격행위를 하였건 관계없이 우리나라의 사이버안보를 침해하는 결과를 발생하였다면 결과발생지가 대한민국이라는 측면에서 형법 제2조의 속지주의를 적용하는데 문제가 없다.

2. 보호법익 관련 구성요건 내재적 한계

그런데 사이버안보를 침해하는 범죄행위에 대한 처벌규정이 보호하고자 하는 법익이 만약 국가적 법익이라면 이들 처벌규정은 대한민국의 법익을 침해하는 행위에 대해서만 적용되어야 한다는 구성요건 내재적 한계를 인정하여야 할 것이다. 예를 들어 우리나라에 소재하는 해킹 회사에서 필리핀 정보기관의 의뢰를 받고 필리핀 내에 위치한 통신사 서버를 해킹해서 통신내역을 확인하여 알려주었다면, 이는 필리핀의 정보통신망에 침입한 행위이고 따라서 필리핀의 사이버안보를 침해하는 행위인데 그러한 행위에 대해서 대한민국의 형법을 적용할 필요는 없다. 이집트 군부가 이집트 정부를 무력으로 전복시킨 행위에 대해서 굳이 우리나라 내란죄를 적용해서 처벌할 이유가 없는 것과 마찬가지이다.

사이버안보 침해행위가 전부 국가적 법익 침해범죄라고 할 수는 없겠지만

그 행위가 개인적 법익을 침해하는 성격을 동시에 가지고 있지 않은 경우에는 그 침해행위가 우리나라 정보통신망과 주요기반시설에 피해를 야기하였을 때에만 국내 형법을 적용하여야 할 것이다.

Ⅷ 맺는 말

사이버안보란 정보통신망을 통해 수집·가공·저장·검색·송신·수신되는 정보의 안전을 침해하는 손괴·변조·유출 행위로부터 정보의 무결성과 신뢰성을 보호하는 것을 의미한다. 컴퓨터의 사용범위가 확장되고 대다수의 컴퓨터가 인터넷으로 연결됨에 따라 사이버안보를 침해하는 행위는 개인적 법익을 침해하는 범죄의 차원을 벗어나 공공의 안전 또는 전자정보에 대한 공공의 신뢰라는 사회적 법익을 침해하는 범죄로 변모하였다.

사이버안보를 지키는 것은 공공의 안전과 전자정보에 대한 공공의 신뢰라는 중요한 사회적 법익을 수호하는 공적 임무가 되었다. 이를 보호하기 위한 법제는 사전예방과 사후처벌이라는 두 가지 영역으로 분류해서 고찰해 볼 수 있다.

먼저 사전예방 법제는 ① 주요정보통신기반시설을 보호하기 위한 정보통신기반 보호법, ② 정보통신망과 그것을 통해 연결되어 있는 정보 자체를 보호하기 위한 정보통신망법 그리고 ③ 국가사이버안전의 보호를 목적으로 하는 국가사이버안전관리규정 등으로 구축되어 있다. 이와 같은 법제를 운영하는 주체는 현재 정보통신기반보호위원회와 방송통신위원회처럼 모두 위원회 조직으로 되어 있다.[23]

사이버안보 업무는 그 속성상 공격행위가 이루어지거나 임박한 것으로 예상될 때 아주 신속한 대처를 필요로 하는데 회의체 기구인 위원회 조직으로는 임무를 수행하기에 벅찰 것으로 생각된다. 따라서 독일의 예처럼 독립된

23) 또 하나의 위원회인 국가사이버안전전략회의는 법령상의 업무 대부분이 정보통신기반보호위원회와 중복되어 사실상 불필요한 조직이다.

청 단위 조직으로 사이버안보 업무를 전담하도록 할 필요가 있을 것으로 판단된다.

사후처벌 법제는 범죄를 예방한다는 차원에서 반드시 있어야 할 부분이다. 사이버안보 침해행위를 유형별로 분류해 보았을 때 그에 대한 처벌규정이 빠짐없이 마련되어 있는지 확인해 본 결과 누락된 부분은 없는 것으로 판단된다. 다만 처벌규정들이 형법과 여러 특별법에 분산되어 있는 것은 처벌조항의 내용을 쉽게 이해할 수 없도록 만든다는 측면에서 문제점이라 할 수 있다.

사후처벌과 관련하여 실질적으로 문제가 되는 것은 사이버공간의 익명성으로 인한 처벌의 곤란성 부분이다. 이를 극복하기 위해서는 IPv6를 기반으로 하는 모든 인터넷 단말기에 대한 고유 IP 부여가 필요하다. 또한 사이버공간의 공간적 무제한성을 극복하기 위해서 수사상의 국제협력 체계가 완성되어야 할 것이다.

그런데 이와 같은 해결방안은 시간이 걸리는 사항이고 현재 적극적으로 추진되고 있지도 않은 형편이다. 따라서 행위자를 특정하기 위한 법적·기술적 보완조치가 완성될 때까지는 사전예방에 좀 더 많은 투자가 이루어져야 할 것으로 생각된다.

[참고문헌]

권영성, 헌법학원론, 법문사, 1997
권창범, 사이버보안을 위한 국가적 추진체계의 검토 및 발전방안, 인터넷법제도포럼 제14회 월례발표회 (2011. 8. 18.) 발표문
기광도, 법위반에 대한 처벌의 억제효과분석: 인지적 측면을 중심으로,『형사정책』제16권 제2호(2004)
김성천, 독일의 사이버 보안 관련 해외 법제 동향과 시사점, 인터넷법제도포럼 보안법제선진화연구반 제1차 발표회 (2011. 6. 20.) 발표문
김성천, 사이버범죄에 대한 법적 대응,『중앙법학』제12집 제1호 (2010)
김성천, 사이버보안 법제에 관한 연구,『중앙법학』제13집 제3호 (2011)
김성천, 인터넷과 형사법상의 과제,『법제연구』제18호 (2000)
김성천, 형법, 도서출판 소진, 2009
김일환, 통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰,『형사정책』(한국형사정책학회) 제16권 제1호 (2004)
대검찰청, 범죄분석, 2010
배종대, 형법각론, 제3판, 홍문사, 1999
성낙인, 통신에서의 기본권 보호,『공법연구』(한국공법학회) 제30집 제2호 (2001)
오영근, 형법각론, 박영사, 2005
이성식, 사이버범죄의도에 대한 공식처벌의 억제효과,『형사정책』제20권 제1호 (2008)
임 웅, 형법각론(상), 법문사, 2000
진계호, 형법각론, 제3판, 대왕사, 1996
정필운, 사이버보안이란 개념 사용의 타당성 재론, 인터넷법제도포럼 제13회 월례발표회 (2011. 7. 21.) 발표문
정혜욱, 아동성범죄의 근본원인과 대책, 중앙대학교 박사학위논문, 2011
Ernst, Stefan: Hacker und Computerviren im Strafrecht,『Der Sachverständige』2004
김재영, 농협 상상초월 삭제명령,『동아일보』2011. 4. 19.

전성철, 검찰 북 정찰총국 사이버테러 결론,『동아일보』2011. 5. 4.
전성철・장관석, 농협 해킹 북 정찰총국이 7개월간 준비,『동아일보』2011. 5. 4.
정원수・윤상호, 북 사이버전 지령-예고-훈련까지,『동아일보』2009. 7. 11.

사이버안보를 위한 공법적 대응방안

이 창 범*

목 차

Ⅰ 국가안보 관점의 인터넷 관리 필요성

파리 테러(2015), 러시아 여객기 폭파(2015), 뭄바이 테러(2008), 911 테러(2001) 등에서 보는 바와 같이 이제 테러는 장소와 시간을 가리지 않고 발생하는 일상이 되고, 한수원 원자력발전소 자료해킹(2014), 스노든 사건(2013), 에스토니아 공화국 정부, 언론, 방송, 은행 전산망 디도스 공격(2007) 등과 같이 정치적, 이념적, 종교적 목적으로 행해지는 해킹 및 사이버테러 행위는 경제적 피해를 넘어 국가의 안보와 국민의 안전을 위협하고 있다. 최근 발생한 이들 테러의 대부분은 인터넷을 통해 이루어지고 있다고 해도 과언이 아닐 정도로 인터넷은 테러와 밀접한 관련을 맺고 있다.

테러리스트들이 테러 활동에 인터넷을 이용하는 이유는 인터넷의 보편화로 테러의 진입장벽이 낮아진 데에도 있지만, 언제 어디서든지 테러의 모의 및 실행이 용이하고, 인터넷의 생활 필수품화로 인해 테러의 파급 효과가 크

* 경희대학교 법무대학원 교수

다는 것에서도 큰 이유를 찾을 수 있을 것이다. 또한 인터넷은 항상 흔적을 남기게 되어 수사기관 등이 자주 이용하는 압수·수색 및 감청의 단골 대상이지만, 동시에 기술적으로는 접속경로, 공격루트 등의 조작이나 변조가 가능하여 수사기관 등의 추적을 피하기 쉽다는 특징도 가지고 있다. 이처럼 테러리스트들은 익명성의 뒤에 숨어 온·오프 상에서 각종 테러와 공격 행위를 전천후로 전개하고 있다.

그러나 우리는 그동안 인터넷이 자유로운 표현의 공간이라는 이유로 인터넷을 주로 보호의 대상으로만 생각하고, 인터넷이 파괴적 수단으로 악용되는 것에 대해서는 대응이 부족하였다. 인터넷의 부작용에 대해서는 기껏해야 개인정보 침해, 명예훼손, 음란물 유포, 소비자피해 등과 같은 일반적인 범죄적 이용에 대한 대응 수준을 넘지 못하고 있고, 정보통신망법, 정보통신기반보호법 등에서 침해사고[1] 또는 전자적 침해[2]에 대해서 규정하고 있으나 이 역시 테러대응 또는 국가안보 관점에서 보다는 일반적 "사고" 예방 및 대응 관점에서 다루고 있다.

따라서 각종 테러 및 사이버공격으로부터 국민의 생명, 신체 및 재산을 안전하게 지키고 국가안보를 보다 튼튼하게 하기 위해서는, 인터넷의 편리성과 자유로운 표현수단으로서의 측면뿐만 아니라, 인터넷의 파괴적 이용 현상도 직시하는 균형 잡힌 시각이 필요하며, 테러대응 또는 국가안보 관점에서 인터넷의 위협에 대처하는 예방 및 대응 체계 수립이 시급하다.

1) "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다(정보통신망법 제2조 제1항 제7호).

2) "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다(정보통신기반보호법 제2조 제2호).

Ⅱ 우리나라의 사이버위협 대응 체계

인터넷은 때로는 그 자체가 공격의 대상이 되고 때로는 공격의 수단이 되고 있다. 예컨대 테러리스트들은 1) 특정국가의 인터넷망에 장애를 초래하거나 2) 사회기반시설을 공격·파괴하여 경제·사회적으로 혼란을 야기하기도 하며, 3) 이메일, SNS 등을 이용하여 테러를 공모·집행하거나 4) 정보시스템에 침투하여 각종 기밀정보를 유출하기도 하며, 5) 인터넷을 이용하여 허위사실을 유포함으로써 불안조성, 국론분열 등을 시도하기도 한다. 이와 같은 사이버위협 행위에 대응하기 위해 현행법에서는 아래와 같은 제도를 도입하고 있다.

1. 정보보호계획 등의 수립 및 시행

(1) 주요정보통신기반시설보호계획(정보통신기반보호법)

주요정보통신기반시설을 관리하는 기관의 장은 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 주요정보통신기반시설보호대책을 수립·시행하여야 하고, 관리기관의 장이 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관의 장에게 제출하여야 한다(제5조). 미래창조과학부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다(제5조의2).

한편, 관계중앙행정기관의 장은 관리기관이 제출한 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(주요정보통신기반시설보호계획)을 수립·시행하여야 한다. 미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정

기관의 장에게 통보할 수 있다. 주요정보통신기반시설보호계획에는 1) 주요정보통신기반시설의 취약점 분석·평가에 관한 사항, 2) 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항, 3) 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항이 포함되어야 한다(제6조).

(2) 전자정부기본계획(전자정부법)

중앙사무관장기관의 장은 전자정부의 구현·운영 및 발전을 위하여 5년마다 행정기관 등의 기관별 계획을 종합하여 전자정부기본계획을 수립하여야 한다. 전자정부기본계획에는 행정정보 공동이용의 확대 및 안전성 확보에 관한 사항이 포함되어야 한다. 관계 중앙행정기관의 장이 「국가정보화 기본법」 제7조에 따른 국가정보화 시행계획을 수립·시행할 때에는 전자정부기본계획을 고려하여야 한다(제5조). 또한 행정기관 등의 장은 5년마다 해당 기관의 전자정부의 구현·운영 및 발전을 위한 기본계획을 수립하여 중앙사무관장기관의 장에게 제출하여야 하고, 중앙사무관장기관의 장은 행정기관 등의 기관별 계획 추진현황 및 성과를 점검할 수 있다(제5조의2).

(3) 국가정보화기본계획(국가정보화기본법)

정부는 국가정보화의 효율적, 체계적 추진을 위하여 5년마다 국가정보화기본계획을 수립하여야 한다. 기본계획은 미래창조과학부장관이 국가와 지방자치단체의 부문계획을 종합하여 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회의 심의를 거쳐 수립·확정하며, 기본계획에는 분야별 정보보호, 개인정보 보호, 건전한 정보통신윤리 확립, 이용자의 권익보호 및 지식재산권의 보호, 국가정보화와 관련된 국제협력의 활성화 등에 관한 사항이 포함되어야 한다. 미래창조과학부장관은 국가와 지방자치단체의 부문계획의 작성지침을 정하고 이를 관계 기관에 통보할 수 있으며, 매년 기본계획의 주요 시책에 대한 추진 실적을 점검·분석하여 그 결과를 전략위원회에 보고하여야 한다(제7조).

한편, 중앙행정기관의 장과 지방자치단체의 장은 기본계획에 따라 매년 국가정보화 시행계획을 수립·시행하여야 하며, 전년도 시행계획의 추진 실적과 다음 해의 시행계획을 미래창조과학부장관에게 제출하여야 한다. 이 경우 행정자치부장관은 지방자치단체의 전년도 시행계획의 추진 실적과 다음 해의 시행계획을 종합하여 미래창조과학부장관에게 제출하여야 한다. 미래창조과학부장관은 제출된 추진 실적과 시행계획을 점검·분석한 후 그 의견을 기획재정부장관에게 제시하여야 하고, 기획재정부장관은 시행계획에 필요한 예산을 편성할 때에는 미래창조과학부장관의 의견을 참작하여야 한다(제7조).

(4) 정보통신망 이용촉진 및 정보보호 시책(정보통신망법)

미래창조과학부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보보호 등을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다. 정보보호 등에 관한 시책에는 정보통신망에 관련된 기술의 개발·보급, 정보통신망의 표준화, 정보통신망을 통하여 수집·처리·보관·이용되는 개인정보의 보호 및 그와 관련된 기술의 개발·보급, 정보통신망의 안전성 및 신뢰성 제고, 그 밖에 정보통신망 이용촉진 및 정보보호 등을 위하여 필요한 사항이 포함되어야 한다. 미래창조과학부장관 또는 방송통신위원회는 정보보호 등에 관한 시책을 마련할 때에는 「국가정보화 기본법」 제6조에 따른 국가정보화 기본계획과 연계되도록 하여야 한다(제4조).

(5) 정보보호산업진흥계획(정보보호산업발전법)

미래창조과학부장관은 정보보호산업의 진흥에 관한 정책목표 및 방향을 설정하기 위하여 5년 마다 정보보호산업 진흥계획을 수립·시행하여야 한다. 1) 정보보호산업진흥계획에는 정보보호산업 진흥을 위한 정책의 기본방향에 관한 사항, 2) 정보보호 전문 인력 양성, 원천기술 개발, 정보보호서비스 이용 확산 등 기반 조성에 관한 사항, 3) 정보보호기술등의 표준화와 지식재산권 보호에 관한 사항, 4) 정보보호기업의 육성 및 지원에 관한 사항, 5) 정보

보호 관련 중소기업, 벤처기업, 1인 창조기업의 경쟁력강화를 위한 지원에 관한 사항, 6) 정보보호산업과 그 밖의 산업 간 융합의 진전에 따른 정보보호 정책에 관한 사항, 7) 이용자의 권익보호에 관한 사항, 8) 정보보호산업에 관한 국제협력과 해외진출 지원에 관한 사항, 9) 정보보호산업 진흥을 위한 재원 확보 및 배분에 관한 사항, 10) 정보보호산업 진흥을 위한 법·제도 개선에 관한 사항, 11) 정보보호산업과 관련된 중앙행정기관 간의 업무협력 및 조정에 관한 사항, 12) 그 밖에 정보보호산업의 진흥을 위하여 필요한 사항이 포함되어야 한다. 미래창조과학부장관은 진흥계획의 수립을 위하여 관계 중앙행정기관, 지방자치단체 및 관련 공공기관의 장에게 소관 분야별 계획이나 자료의 제공 등을 요청할 수 있으며, 이 경우 계획이나 자료의 제공 등을 요청받은 기관은 특별한 사유가 없으면 이에 협조하여야 한다. 또한 정보보호산업진흥계획은 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제5조에 따른 기본계획과 연계되도록 하여야 한다(제5조).

(6) 정보통신 진흥 및 융합 활성화 기본계획 (정보통신융합법)

미래창조과학부장관은 정보통신 진흥 및 융합 활성화를 위하여 3년 단위의 기본계획을 수립하여 한다. 기본계획에는 1. 정보보호와 정보보안에 관한 사항 2. 관계 중앙행정기관 간 정책 및 업무 협력에 관한 사항 3. 그 밖에 정보통신 진흥 및 융합 활성화를 위하여 필요한 사항이 포함되어야 한다. 미래창조과학부장관은 기본계획의 수립을 위하여 관계 중앙행정기관, 지방자치단체 및 관련 공공기관의 장에게 소관 분야별 계획이나 자료의 제공 등을 요청할 수 있으며, 이 경우 계획이나 자료의 제공 등을 요청받은 기관은 특별한 사유가 없으면 이에 협조하여야 한다. 또한 미래창조과학부장관은 기본계획의 시행과 그 추진실적을 평가하여 다음 기본계획 수립 시 그 평가 결과를 반영하여야 한다(제5조).

관계 중앙행정기관의 장은 기본계획을 구체화하기 위하여 정보통신 진흥 및 융합 활성화 실행계획을 매년 수립하여 시행하여야 하고, 관계 중앙행정

기관의 장이 실행계획을 수립할 때에는 정보통신 전략위원회의 심의 결과를 반영하여야 하며, 전년도 실행계획의 추진실적과 함께 실행계획을 정보통신 전략위원회에 제출하여야 한다. 관계 중앙행정기관의 장은 실행계획의 수립을 위하여 필요한 경우 지방자치단체 및 관련 공공기관의 장에게 자료의 제공 등을 요청할 수 있다. 이 경우 자료의 제공 등을 요청받은 기관은 특별한 사유가 없으면 이에 협조하여야 한다(제6조).

2. 정보보호책임자 등의 지정

(1) 정보보호책임자 및 정보보호책임관(정보통신기반보호법)

정보통신기반보호법에 따라, 관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 정보보호책임자를 지정하여야 하고(제5조), 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 정보보호책임관을 지정하여야 한다(제6조).

(2) 정보보호 최고책임자(정보통신망법)

정보통신서비스 제공자는 정보통신망법에 따라 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정할 수 있다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하고 미래창조과학부장관에게 신고하여야 한다. 정보보호 최고책임자는 1. 정보보호관리체계의 수립 및 관리·운영 2. 정보보호 취약점 분석·평가 및 개선 3. 침해사고의 예방 및 대응 4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등 5. 정보보호 사전 보안성 검토 6. 중요 정보의 암호화 및 보안서버 적합성 검토 7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행에 관한 업무를 총괄하여야 한다(제45조의3).

(3) 정보보호최고책임자(전자금융거래법)

금융회사 또는 전자금융업자는 전자금융거래법에 따라 전자금융업무 및

그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하여야 한다. 다만, 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자는 정보보호최고책임자를 임원으로 지정하여야 한다. 정보보호최고책임자는 1. 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립 2. 정보기술부문의 보호 3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성 4. 전자금융거래의 사고 예방 및 조치 5. 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항에 관한 업무를 수행하여야 한다.

(4) 개인정보보호책임자(개인정보 보호법)

개인정보처리자는 개인정보 보호법에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 개인정보 보호책임자는 1. 개인정보 보호 계획의 수립 및 시행 2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제 4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 5. 개인정보 보호 교육 계획의 수립 및 시행 6. 개인정보파일의 보호 및 관리·감독 7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무를 수행하여야 한다. 개인정보 보호책임자는 그 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있으며, 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다(제31조).

(5) 개인정보관리책임자(정보통신망법)

한편, 정보통신서비스 제공자등은 정보통신망법에 따라 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자를 지정하여야 하며, 개인정보관리책임자의 자격요건과 그 밖의 지정에 필요한 사항은 대통령령으로 정한다(제27조).

3. 주요정보통신기반시설 등의 지정

(1) 주요정보통신기반시설 지정(정보통신기반보호법)

중앙행정기관의 장은 소관분야의 정보통신기반시설 중 특별히 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. 중앙행정기관의 장이 소관분야의 정보통신기반시설을 주요정보통신기반시설로 지정할 때에는 1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성 2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도 3. 다른 정보통신기반시설과의 상호연계성 4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위 5. 침해사고의 발생가능성 또는 그 복구의 용이성 등을 고려하여야 한다(정보통신기반보호법 제8조). 주요정보통신기반시설로 지정된 시설을 관리하는 관리기관의 장은 기반시설보호대책의 수립·시행, 취약점 분석·평가, 정보보호책임자 지정, 보호조치, 침해사고 통지 등의 의무를 지지만, 한편 정부는 관리기관에 대하여 주요정보통신기반시설을 보호하기 위하여 필요한 기술의 이전, 장비의 제공 그 밖의 필요한 지원을 할 수 있다.

(2) 정보보호관리체계인증(ISMS) 대상기업(정보통신망법)

미래창조과학부장관은 정보통신망법에 따라 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적인 정보보호 관리체계를 수립·운영하고 있는 자에 대하여 관리적·기술적·물리적 보호대책을 포함한 인증기준에 적합한지에 관하여 인증을 할 수 있다. 다만, 정보통신서비스 제공자로서 1.「전기통신사업법」제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자 2. 집적정보통신시설 사업자 3. 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자는 반드시 정보보호관리체계 인증을 받아야 한다. 미래창조과학부장관은 한국인터넷진흥원 또는 미래창조과

학부장관이 지정한 기관(정보보호 관리체계 인증기관)으로 하여금 인증에 관한 업무를 수행하게 할 수 있다(제47조의3).

4. 점검, 평가 및 인증제도

(1) 취약점 분석·평가(정보통신기반보호법)

관리기관의 장은 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다. 관리기관의 장이 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다. 다만, 한국인터넷진흥원, 정보공유·분석센터, 한국전자통신연구원, 정보보호전문서비스기업 등으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 한 경우에는 전담반을 구성하지 아니할 수 있다. 미래창조과학부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다(제9조).

(2) 행정망 등의 보안성 심사(전자정부법)

행정자치부장관은 전자적 대민서비스와 관련된 보안대책을 국가정보원장과 사전 협의를 거쳐 마련하여야 하고, 중앙행정기관과 그 소속 기관 및 지방자치단체의 장은 보안대책에 따라 해당 기관의 보안대책을 수립·시행하여야 한다(제24조).

국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 하고, 행정기관의 장은 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다. 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다(제56조).

(3) 정보보호 사전점검(정보통신망법)

정보통신서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다. 미래창조과학부장관은 1. 정보통신망법 또는 다른 법령에 따라 미래창조과학부장관의 인가·허가를 받거나 등록·신고를 하도록 되어 있는 사업으로서 대통령령으로 정한 정보통신서비스 또는 전기통신사업 2. 미래창조과학부장관이 사업비의 전부 또는 일부를 지원하는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 정보보호 사전점검기준에 따라 보호조치를 하도록 권고할 수 있다(제45조의2).

(4) 정보보호관리체계 인증(정보통신망법)

미래창조과학부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 정보보호 관리체계를 수립·운영하고 있는 자에 대하여 관리적·기술적·물리적 보호대책을 포함한 인증기준에 적합한지에 관하여 인증을 할 수 있다. 미래창조과학부장관은 정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있고, 한국인터넷진흥원 또는 정보보호 관리체계 인증기관으로 하여금 인증에 관한 업무를 수행하게 할 수 있다. 정보보호 관리체계의 인증을 받은 자는 인증의 내용을 표시하거나 홍보할 수 있다(제47조)

(5) 정보보호시스템 인증(국가정보화기본법)

미래창조과학부장관은 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있고, 유통 중인 정보보호시스템이 기준에 미치지 못할 경우에 정보보호시스템의 보완 및 그 밖에 필요한 사항을 권고할 수 있다(제38조). 미래창조과학부장관은 정보보호시스템의

성능과 신뢰도에 관한 기준을 정하거나, 그 기준에 맞는지의 여부를 평가 또는 인증하는 업무에 관한 세부 사항을 정할 때에는 관계기관의 장(국가정보원장)과 미리 협의하여야 한다. 이 경우 관계 기관의 장이 인증 업무에 관한 세부 사항을 정하여 미래창조과학부장관에게 통보하는 경우에는 협의를 거친 것으로 본다. 미래창조과학부장관은 정보보호시스템을 제조하거나 수입하는 자가 그 시스템이 기준에 합치되는지의 확인을 요청한 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원의 장 또는 관계 국제협약에서 정한 기준에 맞는 기관의 장에게 그 시스템을 조사 또는 시험·평가하게 할 수 있다(시행령 제35조).

(6) 개인정보보호 인증(개인정보보호법, 정보통신망법)

행정자치부장관은 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 개인정보 보호 마크의 도입·시행을 지원하기 위한 시책을 마련하여야 하고(제13조), 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 개인정보 보호법에 부합하는지 등에 관하여 인증할 수 있다. 이 경우 행정자치부장관은 대통령령으로 정하는 전문기관으로 하여금 인증에 관한 업무를 수행하게 할 수 있다(제32조의2).

한편, 방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(개인정보보호 관리체계)를 수립·운영하고 있는 자에 대하여 관리적·기술적·물리적 보호대책을 포함한 인증기준에 적합한지에 관하여 인증을 할 수 있다. 방송통신위원회는 개인정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다(제47조의3).

(7) 정보보호제품 성능평가 등 (정보보호산업진흥법)

미래창조과학부장관은 정보보호제품의 품질확보·유통촉진·이용자 보호·융합산업 활성화 등을 위하여 정보보호제품에 관한 성능평가를 실시할 수

있다. 미래창조과학부장관은 성능평가를 전문적으로 수행하기 위한 평가기관을 지정할 수 있다(정보보호산업진흥법 제17조).

정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 정보통신서비스를 이용하는 자의 안전을 위하여 미래창조과학부에 등록된 평가기관으로부터 정보보호 준비도 평가를 받을 수 있다. 정부는 정보보호 준비도 평가를 받은 기업에 대하여 평가 결과에 따라 포상 등 필요한 지원을 할 수 있다(정보보호산업진흥법 제12조).

5. 침해사고 정보의 수집 및 분석

(1) 침해사고정보 공유(정보통신기반보호법)

관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원에 그 사실을 통지하여야 한다. 이 경우 관계기관 등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다. 정부는 침해사고를 통지함으로써 피해확산의 방지에 기여한 관리기관에 예산의 범위 안에서 복구비 등 재정적 지원을 할 수 있다(정보통신기반보호법 제13조).

금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공 2. 침해사고가 발생하는 경우 실시간 경보·분석체계 운영 등의 업무를 수행하고자 하는 자는 정보통신기반보호법에 따라 정보공유·분석센터를 구축·운영할 수 있다. 정보공유·분석센터의 장은 업무종사자의 인적사항 등 대통령령이 정하는 사항을 관계중앙행정기관의 장에게 통지하여야 하며, 관계중앙행정기관의 장은 통지받은 사항을 미래창조과학부장관에게 통보하여야 한다. 정부는 정보공유·분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있다(정보통신기반보호법 제16조).

(2) 침해사고 원인분석(정보통신망법)

정보통신서비스 제공자 및 집적정보통신시설 사업자는 침해사고가 발생하면 즉시 그 사실을 미래창조과학부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다. 미래창조과학부장관이나 한국인터넷진흥원은 침해사고의 신고를 받거나 침해사고를 알게 되면 정보통신망법 제48조의2제1항 각 호에 따른 필요한 조치를 하여야 한다(정보통신망법 제48조의3).

정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다. 미래창조과학부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관 합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다. 미래창조과학부장관은 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있고, 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 민·관 합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다(정보통신망법 제48조의4).

6. 침해사고에 대한 대응

주요정보통신기반시설을 관리하는 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다. 관리기관의 장은 복구 및 보호조치를 위하여 필요한 경우 관계중앙행정기관의 장 또는 인터넷진흥원의 장에게 지원을 요청할 수 있으며, 이 경우 관계중앙행정기관의 장 또는 인터넷

진흥원의 장은 피해복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취하여야 한다(정보통신기반보호법 제14조).

정보통신기반보호위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고 대책본부를 둘 수 있다. 위원회의 위원장은 대책본부의 업무와 관련 있는 공무원의 파견을 관계 행정기관의 장에게 요청할 수 있고, 침해사고가 발생한 정보통신기반시설을 관할하는 중앙행정기관의 장과 협의하여 대책본부장을 임명하여야 한다. 대책본부장은 관계 행정기관의 장, 관리기관의 장 및 인터넷진흥원의 장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있으며, 이 경우 관계 행정기관의 장등은 특별한 사유가 없는 한 이에 응하여야 한다(정보통신기반보호법 제15조).

한편, 미래창조과학부장관은 침해사고에 적절히 대응하기 위하여 1. 침해사고에 관한 정보의 수집·전파 2. 침해사고의 예보·경보 3. 침해사고에 대한 긴급조치 4. 그 밖에 대통령령으로 정하는 침해사고 대응조치 등의 업무를 수행하여야 하며, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다. 주요정보통신서비스 제공자, 집적정보통신시설 사업자, 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자는 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 미래창조과학부장관이나 한국인터넷진흥원에 제공하여야 하며, 침해사고의 대응을 위하여 미래창조과학부장관이나 한국인터넷진흥원에서 인력의 지원을 요청하면 이에 협조할 수 있다. 미래창조과학부장관은 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있다. 한국인터넷진흥원은 수집된 정보를 분석하여 미래창조과학부장관에게 보고하여야 한다(정보통신망법 제48조의2).

7. 기술 등의 지원

관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설 보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관과 국가정보원장등 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 1. 주요정보통신기반시설 보호대책의 수립 2. 주요정보통신기반시설의 침해사고 예방 및 복구 3. 보호조치 명령·권고의 이행에 대한 기술적 지원을 요청할 수 있다.

주요 교통시설, 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설 등과 같이 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대하여 관리기관의 장이 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다(정보통신기반보호법 제7조).

8. 기술적·관리적 보호조치

관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다. 관계중앙행정기관의 장은 기술의 발전 등을 감안하여 보호지침을 주기적으로 수정·보완하여야 한다(정보통신기반보호법 제10조).

정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다. 미래창조과학부장관은 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(정보보호지침)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키

도록 권고할 수 있다. 이 경우 정보보호지침에는 1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치 2. 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치 3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치 4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치에 관한사항이 포함되어야 한다(정보통신망법 제45조).

9. 정보보호 현황의 공시

정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있다. 이 경우 「자본시장과 금융투자업에 관한 법률」 제159조에 따른 사업보고서 제출대상 법인은 같은 법 제391조에 따라 정보보호 준비도 평가 결과 등 정보보호 관련 인증 현황을 포함하여 공시할 수 있다. 정보보호 현황을 공개한 자가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항에 따른 정보보호 관리체계 인증을 받고자 하는 경우에는 납부하여야 할 수수료의 100분의 30에 해당하는 금액을 할인받을 수 있다(정보통신융합법 제13조).

10. 불법정보의 유통 금지

누구든지 정보통신망을 통하여 1. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보 2. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보 3. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보 4. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보 5. 그 밖에 범죄를 목적으로 하거나 교사 또는 방조하

는 내용의 정보를 유통하여서는 아니 된다. 방송통신위원회는 상기 제1호 및 제2호의 정보에 대하여는 방송통신심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 취급을 거부·정지 또는 제한하도록 명할 수 있다. 또한 방송통신위원회는 상기 제3호 내지 제5호의 정보에 대하여는 관계 중앙행정기관의 장의 요청이 있고, 요청을 받은 날부터 7일 이내에 방송통신심의위원회의 심의를 거친 후 시정 요구를 했음에도 해당 정보통신서비스 제공자나 게시판 관리·운영자가 시정 요구에 따르지 아니한 경우에는 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 취급을 거부·정지 또는 제한하도록 명하여야 한다(정보통신망법 제44조의7).

11. 중요정보의 국외유출 제한 및 정보보호 국제협력

정부는 국내의 산업·경제 및 과학기술 등에 관한 중요 정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스 제공자 또는 이용자에게 필요한 조치를 하도록 할 수 있다. 이 같은 중요정보의 범위에는 1. 국가안전보장과 관련된 보안정보 및 주요 정책에 관한 정보 2. 국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보가 포함된다(정보통신망법 제51조).

정부가 1. 개인정보의 국가간 이전 및 개인정보의 보호에 관련된 업무 2. 정보통신망에서의 청소년 보호를 위한 업무 3. 정보통신망의 안전성을 침해하는 행위를 방지하기 위한 업무 4. 그 밖에 정보통신서비스의 건전하고 안전한 이용에 관한 업무를 추진할 때에는 다른 국가 또는 국제기구와 상호 협력하여야 한다(정보통신망법 제62조).

미래창조과학부장관은 정보보호산업에 관한 국제적 동향을 파악하고 국제협력을 추진할 수 있으며, 정보보호산업 분야의 국제협력을 추진하기 위하여 정보보호기술 및 전문 인력의 국제교류 및 국제공동연구개발 등의 사업을 지원할 수 있다. 또한 미래창조과학부장관은 정보보호산업과 관련된 민간부문의 국제협력을 지원할 수 있다(정보보호산업진흥법 제16조).

12. 정보통신서비스 이용자 보호조치

정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다. 주요정보통신서비스 제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다. 또한 「소프트웨어산업 진흥법」 제2조에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 한국인터넷진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알려야 한다(제47조의4).

13. 이해당사자의 역할 규정

정보통신서비스 제공자는 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 이용자의 권익보호와 정보이용능력의 향상에 이바지하여야 하고, 이용자는 건전한 정보사회가 정착되도록 노력하여야 하며, 정부는 정보통신서비스 제공자단체 또는 이용자단체의 개인정보보호 및 정보통신망에서의 청소년 보호 등을 위한 활동을 지원할 수 있다(정보통신망법 제3조).

14. 정보보호 기술 개발 및 표준화 추진

미래창조과학부장관은 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 대통령령으로 정하는 바에 따라 관련 연구기관으로 하여금 연구개발·기술협력·기술이전 또는 기술지도 등의 사업을 하게 할 수 있다. 정부는 연구개발 등의 사업을 하는 연구기관에는 그 사업에 드는

비용의 전부 또는 일부를 지원할 수 있다(정보통신망법 제6조).

미래창조과학부장관은 정보통신망의 이용을 촉진하기 위하여 정보통신망에 관한 표준을 정하여 고시하고, 정보통신서비스 제공자 또는 정보통신망과 관련된 제품을 제조하거나 공급하는 자에게 그 표준을 사용하도록 권고할 수 있다(제8조).

미래창조과학부장관은 정보보호기술의 개발 및 투자를 촉진하기 위하여 1. 정보보호기술 수준의 조사 및 기반기술의 연구개발 2. 미래 성장유망분야의 정보보호 핵심 원천기술 발굴 및 개발 3. 정보보호기술에 관한 국제 공동연구 개발 및 지원 4. 정보보호기술의 상용화 및 지역의 정보보호 관련 산업의 클러스터 구축 5. 산·학·연 정보보호기술 공동연구 지원 사업 6. 정보보호기술의 거래 활성화 사업 7. 그 밖에 정보보호기술의 개발 및 투자촉진을 위하여 필요한 사업을 추진할 수 있다. 또한 미래창조과학부장관은 정보보호기술의 거래 활성화, 정보보호제품 간 호환성 확보 등을 위하여 1. 정보보호기술등에 관한 표준의 제정·개정·폐지 및 보급 2. 정보보호기술등과 관련된 국내외 표준의 조사·연구·개발 3. 국내 정보보호기술등에 관한 표준의 국제표준화를 위한 시책 마련 4. 그 밖에 정보보호기술등의 표준화에 필요한 사업을 추진할 수 있다(정보보호산업발전법 제17조).

15. 정보보호 인력양성

미래창조과학부장관은 정보보호 산업의 진흥에 필요한 전문 인력 양성을 위하여 관계 중앙행정기관의 장과 협의하여 1. 전문 인력의 수요 실태 파악 및 중·장기 수급 전망 수립 2. 전문 인력 양성기관의 지정, 설립·지원 3. 전문 인력 양성 교육프로그램의 개발 및 보급 지원 4. 정보보호 산업 관련 자격제도의 정착 및 전문 인력 수급 지원 5. 각 급 학교 및 그 밖의 교육기관에서 시행하는 정보보호 산업 관련 교육의 지원 6. 그 밖에 대통령령으로 정하는 전문 인력 양성에 필요한 시책을 수립·시행할 수 있다(정보보호산업발전법 제15조).

Ⅲ 현행 사이버위협 대응체계의 문제점 및 한계

앞 장에서 본 바와 같이 우리나라는 사이버보안 또는 사이버안전을 위해 어느 나라보다 다양한 예방 및 대응 수단을 마련해 두고 있다. 그러나 이 같은 수단들이 각각의 법령에서 경쟁적·중복적으로 도입되고 있을 뿐, 사이버 환경의 특수성을 고려한 통합적인 관리 수단이 부재하여 중복된 수단만큼이나 시너지 효과를 거두기 어려우며, 전 방위적인 사이버 공격 또는 위기가 발생한 경우에는 무용지물이 될 수 있다.

국가안보 및 테러대응이라는 관점에서 볼 때 인터넷(사이버)은 매우 취약한 루프홀(loophole)을 가지고 있는 등 오프라인과는 다른 많은 특징을 가지고 있다. 때문에 오프라인에서 오랫동안 발전·정착되어 온 많은 법이론들이 인터넷 환경에서는 부적합하거나 그대로 적용하기 어려운 경우가 많다. 따라서 사이버 공격 또는 위협에 대한 대응체계를 마련할 때에도 인터넷 및 ICT기술의 특성이 충분히 고려되어야 한다.

1. 공사 영역의 엄격한 분리

일반적으로 오프라인 환경에서는 공공시설과 민간시설, 공공영역과 민간영역, 공무원과 민간인이 뚜렷하게 구분된다. 그리고 이와 같은 경계는 쉽게 허물어뜨릴 수 없다. 사이버 환경에서도 공공부문과 민간부문, 공공시설과 민간시설, 공무원과 민간인은 명확히 구분된다. 그러나 사이버 공간에서는 공공영역과 민간영역의 경계가 오프라인에서와는 달리 쉽게 허물어질 수 있다. 즉 공공기관 또는 공공영역에서 이용되는 정보통신시스템이라도 인터넷에 연결되는 순간 누구라도 쉽게 접근이 가능하고, 역으로 공공기관 또는 공무원이 인터넷을 통해 민간인의 정보통신시스템에 접속하는 것도 어렵지 않다.

또한 정보통신시설 또는 정보통신시스템에 대한 공격은 스턱스넷(Stuxnet), EMP공격 등과 같이 예외적으로 인터넷을 통하지 않고도 이루어지는 공격이 있기는 하지만, 대부분의 사이버 공격은 인터넷을 통해 이루어진다. 공격의

대상이 공공시설이냐 민간시설이냐에 대해서 차이가 있을 뿐 인터넷을 통해서 이루어진다는 점에서는 동일하다. 이처럼 인터넷 공간에 관한 한 그것은 공공과 민간을 구분할 수 없다. 또한 디도스 공격에 이용되는 숙주 컴퓨터 역시 공공용과 민간용을 구분하지 않는다.

따라서 사이버공격 행위를 효과적으로 예방하고 신속하게 대응하기 위해서는 공공영역과 민간영역을 구분해서 각각의 영역에 설치된 정보통신시설에 대한 안전한 관리·감독도 중요하지만, 각각의 영역에서 끊임없이 시도되고 있는 사이버공격 정보(공격자, 공격방법, 공격루트, 이용되는 악성코드 등)의 통합적 관리·통제가 필요하며, 인터넷 공간에 대해서도 통합적인 관리·감독이 필요하다.

그러나 우리나라의 현행 사이버보안법제는 사이버공격에 이용되고 있는 공격정보 그 자체(공격의 원인)에 초점을 두고 대응체계를 구축하기 보다는, 공격의 대상이 되는 정보통신시설 또는 정보통신시스템과 같은 물리적인 시설의 소유자(공격의 대상)에만 초점을 두고 그 시설의 소유자가 공공기관인지 군대인지 민간인지에 따라 관리·감독 영역을 엄격하게 구분하고 있어 사이버 공격에 효과적인 대응이 어렵다. 예컨대 정보통신망법은 정보통신서비스제공자들이 소유·관리하는 민간의 정보처리시스템을 대상으로 하고 있고, 전자정부법과 국가사이버안전관리규정은 행정기관 등이 소유·관리하는 정보통신시설만을 대상으로 하며, 심지어 국가안전보장이나 경제사회전반에 피해가 우려되는 전자적 제어·관리시스템의 보호를 목적으로 제정된 정보통신기반보호법조차도 공공부문과 민간부문 그리고 국방부분으로 나누어 접근하고 있다.

2. 권한의 분산 및 대응 사각지대

공공영역과 민간영역의 엄격한 구분 못지않게 문제가 되고 있는 것이 사이버 영역에 대한 관리·감독 권한의 엄격한 분산이다. 영역별로 민간부분은 미래창조과학부가, 공공영역은 국가정보원과 행정자치부가, 국방영역은 국

방부가, 금융분야는 금융감독위원회, 의료분야는 보건복지부 등이 각기 나누어서 관리하는 체계이다. 영역별로만이 아니라 기능별로도 구분되어 있다. 불법정보에 대해서는 미래창조과학부와 방송통신위원회가, 사이버 범죄는 경찰과 검찰이, 사이버안보와 관련해서는 국가정보원이, 사이버전에 대비해서는 국방부가 권한을 수행한다. 또한 사이버 공격의 위협 수준에 따라 사이버위기의 경보수준을 정상-관심-주의-경계-심각으로 나누고 미래창조과학부와 국가정보원의 역할을 구분하기도 한다.

이와 같은 영역별 또는 기능별 권한의 분산이 잘못된 것은 아니다. 또한 권한의 집중 방지와 크로스 체크를 위해 바람직한 것이기도 하다. 그러나 앞 절에서도 살펴보았듯이 사이버공격 또는 사이버위협이 그렇게 영역별로 완벽하게 구분되기 어렵고, 어떤 사이버공격 행위가 발생하였을 때 그것이 단순 범죄행위에 그치는 것인지 테러나 전쟁 수준의 공격인지 결과를 분석해 보기 전에는 알기 어렵다는 점이다.[3] 또한 사이버경보 수준도 평상시에는 공격의 위협 정도에 따라 단계별 권한 행사가 가능할 수 있으나, 대다수 사이버공격은 공격의 주체가 누구인지 알 수 없고(민간인인지 테러분자인지 군인인지), 은밀하게 오랜 기간을 걸쳐 준비되기 때문에 공격이 있었는지 여부 자체를 모를 수도 있고(해킹 등), 수초 또는 수분 내에 순식간에 공격이 이루어져 속수무책이 수도 있다(디도스 공격 등).

따라서 사전에 사이버보안에 대한 컨트롤타워가 만들어져 있지 아니하면 사이버공격에 대한 전방위적인 대응이 어렵고 사이버안보에도 사각지대가 발생하기 쉽다. 외형상 또는 형식상으로 보면 대통령 훈령인 「국가사이버안전관리규정」에 의하여 국가정보원에게 사이버안전에 대한 컨트롤타워 역할

3) 예컨대, 프린터 메모리칩 속에 컴퓨터 바이러스를 숨겨져 있는 경우 누구의 영역인가, 테러리스트로 의심되는 자가 인터넷에서 원격조정 드론이나 장난감 헬리콥터를 구입한다면 경찰/검찰/미래부/국정원 중 누구의 관할인가, 누군가 사제 폭탄에 사용되는 제품을 구입한다면 누가 관리해야 하나....이런 문제에 경찰이 개입한다면 오히려 사찰이 확대될 수 있다. 문제는 그 사람이 어떤 일을 했느냐보다 어떤 목적으로 일을 했느냐 이다.

이 부여된 것으로 볼 수 있으나, 대통령 훈령이라는 한계 때문에 개별 법률에 우선하기 어렵고, 법률에 의해 권한이 뒷받침되지 아니하여 충분한 권한행사가 어려우며, 국가안보를 위협하는 민간영역의 다양한 사이버공격 활동에 대해서는 예방적 대응 수단 자체가 마련되어 있지 않다. 더욱이 새로운 정권이 들어설 때마다 청와대 내에 만들어지는 비전문적 조직이 사이버안전에 대해 컨트롤타워 역할을 자처하고 있어 국가정보원의 역할은 더욱 왜소해 질 수밖에 없다.

3. 정보 공유 및 활용 체계 부재

사이버 상에서는 테러의 진입장벽이 낮아 국민의 생명・재산과 국가의 안위를 위협하는 사이버공격 행위가 끊임없이 이루어지고 있다. 한수원 사건, 스노든 사건, 3.4/7.7 디도스 공격 등이 그 예라 할 수 있다. 이 같은 공격행위는 정치적 갈등이나 종교적 신념에 의한 것 일수도 있으나, 국가적 또는 경제적 이득을 취할 목적으로 한 것일 수도 있다(국가기밀 또는 산업기술 해킹 등). 사이버공격은 흔히 사이버 시스템이나 네트워크 그 자체가 공격의 대상이 되지만, 최근에는 사이버 네트워크를 이용한 온・오프라인 융합형 테러 행위도 증가하고 있다. 즉 인터넷을 이용한 테러의 공모, 준비, 지령, 실행 등이 그것이다. 이것도 광의에서 사이버공격 또는 사이버테러의 일종으로 볼 수 있다. 최근 발생한 파리테러 사건에서도 IS는 테러를 공모하는데 인터넷을 이용한 것으로 알려지고 있다.

사이버공간은 익명성이 보장되는 곳이어서 누구든지 자신을 숨기고 테러에 가담할 수 있으나, 동시에 사이버 공간은 어떤 형태로 든 항상 공격자의 흔적을 남기기도 한다. 따라서 사이버공격 정보를 잘 수집・분석하면 상당수의 사이버공격은 이를 미리 예상하거나 예방할 수 있다. 또한 공격자가 누구인지 확인하기 위해서도 사이버공격 정보의 수집・분석 및 축적은 필수적이다. 따라서 정보통신시스템을 소유・관리하는 자는 사이버공격을 실시간으로 수집・분석하여야 하고, 해당 공격정보를 CERT, ISAC, 당국과 공유하여

야 한다. 또한 정부는 이들 공격정보를 통합적으로 수집·관리하는 사이버위협종합관리·분석시스템을 운영하여야 한다.

그러나 우리나라는 정보통신망법, 정보통신기반보호법, 전자금융거래법, 클라우드 발전법 등 다수의 개별법에서 해당 중앙행정기관 등에 대해 침해사고정보의 보고의무가 규정되어 있지만, 이들 정보를 통합적으로 수집·관리하고 분석하는 종합적인 관리·분석 시스템은 마련되어 있지 아니하다. 따라서 많은 공격정보들이 분야별(섹터별)로는 수집·공유되고 있지만 국가 차원에서는 관리되고 있지는 아니하여 수집된 공격정보들이 제대로 활용되지 못하고 있다.

4. 정부기관 간 및 정부와 민간 간 협력체계 부재

1.25 인터넷 대란(2003), 7.7 디도스 공격(2009) 등과 같은 전국적인 침해사고에 신속하게 대응하기 위해서는 관련 정부기관은 물론 민간 기업이나 일반국민도 침해사고의 원인분석 및 대응을 위해 상호 협조하여 한다. 민간기업의 경우 정보통신서비스 제공자뿐만 아니라 정보통신서비스를 이용하는 일반기업의 협조 역시 필수적이라고 할 수 있다.

공격에 악용되는 컴퓨터의 대부분을 정보보안에 취약한 기업이나 개인들이 소유·관리하고 있는 경우가 많아, 그와 같은 컴퓨터를 이용하고 있는 기업이나 국민들의 협조가 없이는 악성코드의 신속한 수집·분석이 어렵고, 정보통신서비스 제공자가 그 같은 이용자의 인터넷을 차단하거나 통제하지 않고 방치하면 계속적인 공격행위를 막기 어려운 경우도 발생한다. 또한 공격에 이용된 악성코드 등의 특성을 분석하고 치료 및 예방 백신을 개발하기 위해서는 사이버보안 전문기관이나 민간기업의 도움이 필요할 경우도 있을 수 있다. 이처럼 사이버공격에 대비하고 대응하기 위해서는 정부(국가 및 지자체)-정보통신서비스제공자-정보통신서비스이용자 간의 탄탄한 협력 시스템이 필요하다.

이에 따라, 정보통신망법은 미래창조과학부장관으로 하여금 정보통신서비

스 제공자의 정보통신망에 중대한 침해사고가 발생한 경우 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관 합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있게 하고 있고, 또한 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 민·관 합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사할 수도 있게 하고 있다(제48조). 정보통신기반보호법도 정보통신기반보호위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고 대책본부를 둘 수 있게 하고 있고, 또한 대책본부장은 관계 행정기관의 장, 관리기관의 장 및 한국인터넷진흥원의 장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있게 하고 있다(제15조).

그러나 정보통신망법에 따른 원인 분석 자료의 제공 및 사업장 출입 대상은 정보통신서비스 제공자 등으로 한정되어 있어 일반 기업이나 국민에게는 미치지 아니하며, 또한 중대한 침해사고가 발생한 경우에만 가능하다. 해당 침해사고가 국가안보와 관련된 것이라도 정보통신망법상 국가정보원장은 정보통신서비스 제공자 등에게 침해사고 원인분석 자료의 보전명령이나 제출명령을 할 수 없다. 국가정보원장은 악성코드, 해킹프로그램 등을 유포하는 이메일 계정을 발견한 경우에도 현행법상 그것의 차단을 사업자에게 직접 요구할 권리가 없다. 단지 정보통신서비 이용자로서 정보통신서비스 제공자나 한국인터넷진흥원에게 신고를 할 수 있을 뿐이다. 주요정보통신기반시설의 경우에도 정보통신기반보호위원회 위원장이 대책본부장으로 국가정보원장을 임명한 경우에 한해 국가정보원장이 관계 행정기관의 장, 관리기관의 장 및 한국인터넷진흥원의 장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있다(제15조).

Ⅳ 사이버위협 대응을 위한 법제 개선 방향

우리나라의 현행 사이버보안 관련 법제는 각각의 개별법은 어느 나라 못지 않게 훌륭하다고 할 수 있으나 이들을 통합할 수 있는 기본법이 부재한데서 발생하는 문제라고 할 수 있다. 따라서 현행 사이버위협 대응체계가 안고 있는 근본적인 문제점과 한계를 극복하기 위해서는 각각의 개별법들은 그대로 두고 영역별 및 기능별 권한분산을 유지함으로써 부처 간 Check and Balance가 가능하도록 하되, 사이버안전과 관련한 기존의 컨트롤타워가 제 기능을 발휘할 수 있도록 법률적 기반을 제공함과 동시에, 컨트롤타워를 중심으로 정부(국가 및 지자체)-정보통신서비스 제공자-정보통신서비스 이용자(민간기업 등) 간에 공격정보, 분석기술, 위협동향 등의 공유와 협력이 활발히 이루어질 수 있도록 협력적 거버넌스 시스템을 도입할 필요가 있다. 이와 같은 문제인식을 바탕으로 발표자는 기본법의 제정 방향을 아래와 같이 제시하고자 한다.

1. 기본법의 명칭

현재 국회에는 「국가 사이버테러 방지에 관한 법률안」(서상기 의원 대표발의, 2013.4.9), 「사이버위협정보 공유에 관한 법률안」(이철우 의원 대표발의, 2015.5.19.), 「사이버테러 방지 및 대응에 관한 법률안」(이노근 의원 대표발의, 2015.6.24.)이 발의되어 계류 중에 있다. 서상기의원안과 이노근 의원안은 본질적인 차이가 크지 않다고 보지만, 이철우 의원안은 사이버위협정보의 공유에 맞추어져 있다. 이철우 의원안의 특이한 점은 "사이버테러"라는 용어를 사용하지 않고 "사이버위협"이라는 용어를 사용하고 있다는 점이다. 최근 미국 등 외국의 입법동향을 따른 것으로 보인다.

이철우 의원안은 현재 세계적으로도 가장 뜨거운 이슈 중 하나인 사이버위협정보의 공유에 초점을 두고 있다는 점에서 의미가 크고, 법안의 통과 가능성을 높일 수 있다는 전략적인 측면을 고려한 것으로 볼 수 있지만, 사이버위

협의 산적한 문제를 풀기위한 기본법으로서의 역할을 기대하기에는 한계가 있다. 서상기/이노근 의원안도 사이버테러에 초점을 두고 있어 법안 통과의 필요성을 역설할 수 있고 대국민 홍보적 효과가 강하다고 볼 수 있지만, 오히려 일부 내용이 다수 국민들에게 위기감과 거부감을 조장할 수 있고, 법률의 목적과 성격이 사이버테러에 한정되어버릴 수 있다는 단점이 있다.

따라서 법률의 목적 또는 목표를 사이버테러 예방 및 방지에 두기보다는 사이버안전에 초점을 두고, 법률의 명칭에서도 국가 전반의 사이버안전을 추구하는 기본법으로서의 성격을 명확히 드러내는 것이 바람직하다고 생각한다. 예컨대 사이버안전기본법,[4] 사이버보안기본법, 사이버위협의 관리 및 대응에 관한 법률 등이 타당하다고 생각한다. 일본, 유럽 등에서는 "Cyber Security"라는 용어를 그대로 사용하고 있다. "Cyber Security"는 해석상 사이버안전, 사이버보안 등으로 해석이 가능할 것이다.

2. 용어의 정의

(1) 사이버테러 vs. 사이버공격

인터넷을 이용한 공격행위에 대하여 국회 발의안에서는 "사이버테러" 또는 "사이버위협"이라는 용어를 사용하고 있고, 국가사이버안전관리규정에서는 "사이버공격"이라는 용어를 사용하고 있으며, 정보통신망법/정보통신기반보호법 등에서는 "침해사고"라는 용어를 사용하고 있다. 그러나 각각의 용어에도 불구하고 기본적인 내용에는 큰 차이가 없다.

서상기 의원안과 이노근 의원안은 사이버테러를 "해킹·컴퓨터바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 절취·훼손·왜곡 전파하는 등 모든 공격행위를 말한다"라고 정의하고 있고, 이철우 의원안은 사이버위협을 "해킹·컴퓨터

4) 현재 국가사이버안전에 관한 대통령훈령은 "국가사이버안전관리규정"이라는 용어를 사용하고 있다.

바이러스・서비스방해・전자기파 등 전자적 수단을 이용하여 정보통신망과 정보통신기기를 침입・교란・마비・파괴하거나 정보를 절취・훼손・왜곡전파할 수 있는 행위를 말한다"라고 정의하고 있다. 한편, 국가사이버안전관리규정에서는 사이버공격을 해킹・컴퓨터바이러스・논리폭탄・메일폭탄・서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입・교란・마비・파괴하거나 정보를 절취・훼손하는 일체의 공격행위를 말한다"라고 정의하고 있고, 정보통신망법은 침해사고를 "해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다"라고 정의하고 있다.

이처럼 사이버테러, 사이버공격, 침해사고가 모두 유사한 의미로 사용되고 있지만, 사이버테러 및 사이버위협이 사이버공격과 다른 것은 '정보의 왜곡전파'가 추가되었다는 점이고, 침해사고가 사이버테러, 사이버공격 및 사이버위협과 다른 점은 공격행위로 인해 발생한 결과(사태)를 의미한다는 점에서 차이가 있다. 그런데 해킹, 컴퓨터바이러스, 서비스방해, 전자기파 등 전자적 수단에 의하여 정보통신시설을 침입, 교란, 마비, 파괴하거나 정보를 절취, 훼손, 왜곡 전파하는 등의 모든 공격행위를 "테러"로 규정하는 것은 적절하지 않아 보인다. 즉 이들 정의에는 테러 수준에 이르지 아니하는 공격이나 위협도 포함되어 있으므로 사이버테러보다는 사이버공격 또는 사이버위협이라는 용어가 더 적합할 것으로 보인다. 또한 '정보의 왜곡전파'를 사이버테러 또는 사이버공격의 개념 안에 포함시키는 것도 무리로 보이므로, 이 법의 적용 대상이 되는 왜곡정보는 테러정보, 국제범죄정보, 간첩행위 등과 같이 국가안보 및 국민안전에 직접적으로 영향을 미치는 정보로 한정하여 정치사찰, 민간감시 등의 시비를 차단하여야 할 것이다.

(2) 사이버안전 vs. 사이버보안 vs. 사이버안보

이노근 의원안은 이 법의 목적을 "사이버테러 방지 및 대응에 관한 기본적

인 사항을 규정하여 국가안보를 위협하는 사이버테러를 예방하고 사이버위기가 발생한은 때에 신속하게 대처함으로써 국가의 안전보장과 질서유지에 이바지함을 목적으로 한다"고 규정하면서, 사이버안전을 "사이버테러로부터 정보통신시설과 정보를 보호하기 위하여 수행하는 관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함한다"라고 정의하고 있다.[5] 국가사이버안전관리규정도 사이버안전을 "사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다"라고 정의하고 있다. 이처럼 국내법에서는 사이버테러 또는 사이버공격으로부터의 보호활동에 대해 "사이버안전"이라는 용어를 사용하고 있다.

일본의 「사이버시큐리티기본법」에서는 사이버시큐리티를 "전자적 방식, 자기적 방식 및 기타 사람의 지각으로는 인식할 수 없는 방식(이하 이 조에서 "전자적 방식"이라 한다)으로 기록되거나 발신, 전송 또는 수신되는 정보의 누설, 멸실 또는 훼손 방지 및 기타 정보의 안전관리를 위하여 필요한 조치와 정보시스템 및 정보통신 네트워크의 안전성 및 신뢰성의 확보를 위하여 필요한 조치(정보통신 네트워크 또는 전자적 방식으로 작성된 기록과 관련된 기록매체(이하 "전자적 기록매체"라 한다)를 통한 전자계산기에 대한 부정한 활동에 의한 피해의 방지를 위하여 필요한 조치를 포함한다)가 강구되고 그 상태가 적절하게 유지·관리되고 있는 것을 말한다"라고 규정하여, 우리나라의 "사이버안전"에 해당하는 용어로 "사이버시큐리티"를 그대로 사용하고 있다.

한편, 학계나 실무 계에서는 사이버보안 또는 사이버안보라는 용어도 종종 사용하고 있다. 그러나 사이버안전은 목적 지향적이지만 사이버보안은 수단적 의미가 강해 사이버안전을 위한 하위 개념으로 이해되며, 사이버안보는

5) 이노근의원안을 서상기의원안을 기본으로 하고 있는 것으로 보이며, 따라서 서상기의원안은 이노근의원안과 목적, 정의 등이 같거나 매우 유사하다.

사이버안전과 마찬가지로 목적 지향적인 용어이지만 사이버안전보다는 개념이 좁다. 사전적 의미로 보면 안전은 “위험이 생기거나 사고가 날 염려가 없음 또는 그런 상태”를 의미하지만, 안보는 “편안히 보전됨 또는 편안히 보전함”의 의미도 있지만 흔히 “안전보장(외부의 위협이나 침략으로부터 국가와 국민의 안전보장)’을 줄여 이르는 말”로 이해되고 있다. 영어로 보면 안전은 safety로, 보안 또는 안보는 security로 번역된다. 이처럼 영어 security는 우리나라에서는 흔히 안보로 번역되지만 security의 개념에는 안전의 개념도 포함되어 있다(all the measures that are taken to protect a place, or to ensure that only people with permission enter it or leave it). 따라서 “사이버보안” 또는 “사이버안보”보다는 “사이버안전”이라는 용어가 더 적합한 것으로 생각된다.

3. 기본법의 적용범위

기본법의 적용 대상 또는 범위를 어디까지로 할 것인지에 대해서는 첨예한 논란이 예상되지만, 이 법이 사이버공격의 사각지대를 최소화하고 사이버위협에 전 방위적인 대응을 목표로 한다는 점에서 국가 및 지방자치단체, 공공기관은 물론 국방영역, 민간영역에 대해서도 적용되어야 하고, 사이버테러, 국가안보뿐만 아니라 사이버공격 또는 사이버위협 행위 전반을 커버할 수 있어야 한다.

다만, 기본법은 국가기관 간 또는 국가와 민간 영역 간 사이버공격을 예방하고 대응하기 위한 상호 협력 및 정보 공유 체계(거버넌스)의 구축과 실효적인 집행에 초점을 두어야 하고, 각 영역별 관리・감독 체계는 개별법에 따르도록 하여야 할 것이다. 또한 사이버공격에 대한 효과적인 예방 및 대응을 위해서는, 이 법을 사이버위기 또는 침해사고 발생 시에만 적용할 것이 아니라 평상시에도 기능을 발휘하도록 하여 사이버안전 관련 주체 간에 상시적으로 협력 및 정보 공유 체계가 가동・유지되도록 하여야 한다.

또한 최근에는 인터넷을 이용한 온・오프라인 융합형 테러(파리테러 등)

가 많이 발생하고 있고, 향후 테러의 양상이 테러 효과를 극대화하기 위해 온라인 테러와 동시에 오프라인 테러를 병행하여 시도할 가능성이 크므로, 인터넷, SNS, 이메일 등을 이용한 테러공모, 간첩활동 등에 대해서도 기본법의 적용 범위에 포함하여 관련 정보들이 적법한 절차를 거쳐 수집되고 통합관리되도록 하여야 할 것이다.

4. 기본법의 구체적 내용

(1) 일본 「사이버시큐리티기본법」의 주요내용

일본의 「사이버시큐리티기본법」은 제1장 총칙에서 사이버시큐리티의 기본이념을 천명하고, 주체별(국가, 지방자치단체, 중요사회기반사업자, 사이버 관련사업자, 기타사업자, 교육연구기관, 국민) 책무를 규정하고 있으며, 사이버시큐리티를 위한 정부의 법제상/재정상/세제상 조치 강구 및 사이버시큐리티를 위한 국가의 행정조직 정비 노력을 규정하고 있다.

제2장(사이버시큐리티전략)에서는 사이버시큐리티에 관한 시책을 종합적이고 효과적으로 추진하기 위하여 정부로 하여금 "사이버시큐리티전략"을 수립하여 각의의 결정을 받도록 규정하고 있다.

제3장(기본시책)에서는 행정기관, 중요사회기반사업자, 민간사업자, 교육기관, 중소기업 등이 사이버시큐리티를 위해 추진해야 할 업무 및 시책을 열거하는 한편, 특히 국가 행정기관, 중요사회기반사업자 등의 사이버시큐리티에 관한 연습 및 훈련과 국내외 관계기관과의 연계 및 연락조정에 의한 사이버시큐리티에 대한 위협에의 대응, 국가 행정기관, 독립행정법인, 특수법인, 중요사회기반사업자 등 간에 사이버시큐리티에 관한 정보 공유 시책의 강구를 강조하고 있으며, 국가는 관계부성(府省) 상호간의 연계를 강화하는 동시에, 국가, 지방공공단체, 중요사회기반사업자, 사이버 관련사업자 등의 다양한 주체가 상호 연계하여 사이버시큐리티에 관한 시책에 대처할 수 있도록 필요한 시책을 강구하도록 규정하고 있다.

제4장(사이버시큐리티전략본부)에서는 사이버시큐리티에 관한 시책을 추진하기 위한 추진기구로 내각에 사이버시큐리티 전략본부를 두고, 전략본부장은 내각관방방관이 되고, 부본부장은 국무대신 중에서 충원하며, 전략본부원으로는 국가공안위원회 위원장, 총무대신, 외무대신, 경제산업대신, 방위대신, 그 밖에 내각총리대신이 지정 또는 임명한 국무대신과 외부전문가로 구성하도록 규정하고 있다.

(2) 미국 2012년 사이버안전법(안)

「2012 사이버안전법안(Cybersecurity Act of 2012)」은 미국에서 지금까지 발의되거나 제정된 법률 중에서 사이버보안과 관련한 가장 포괄적이고 일반적인 법률안이다. 정식 명칭은 「미합중국 사이버 및 통신인프라 안전 및 회복능력 제고 법안(A bill to enhance the security and resiliency of the cyber and communications infrastructure of the United States)」이다. 제목을 통해서도 알 수 있듯이 이 법안은 주로 민간부문에 의해서 소유・관리되고 있는 경우가 대부분인 미국내 주요 기반시설의 사이버안전을 향상시키기 위해 공공부문과 민간부문간에 튼튼한 파트너십을 확립하는 것을 목적으로 한다. 동 법안은 오바마(Obama) 대통령과 민주당의 강력한 지지를 받았으나, 자유권침해 등의 논란으로 상원에서 52-46으로 부결됐다.[6)]

이 법안은 해커나 외국정부의 사이버공격으로부터 미국의 주요기반시설을 강력하게 보호하고자 하는 것으로, 그 배경에는 사이버 공격이 현실적이고도 급박한 위험으로 존재하고 있다는 인식에서부터 출발하고 있다. 미국은 사이버 공격이 미국의 경제와 미국인의 생활방식에 심각한 피해를 줄 뿐만 아니라, 미국의 국가안보에도 영향을 줄 수 있고, 사이버 공격이 소위 "진주만 공격"이나 "카트리나 피해"보다 더 큰 피해를 줄 수 있다고 생각한다. 이에 따

6) 미국에서는 매년 이와 관련한 새로운 법안이 발의되고 있으나 아직 법률로 성사된 것은 없다.

라 동 법안은 아래와 같은 내용을 담고 있다.

첫째, 국가 사이버안전위원회의 설립이다. 국방부, 법무부, 상무부, 보안기관, 그밖의 연방기관 등으로 구성된 국가사이버안전위원회(National Cybersecurity Council)를 설립한다. 위원회는 미국에 대한 가장 크고 임박한 사이버 리스크를 발견하기 위하여 리스크 평가 기능을 수행한다.

둘째, 국토안보부(DSH)의 기능 재정립이다. 국토안보부는 주요기반시설 보유 및 관리자, 주요기반시설파트너십자문회의(Critical Infrastructure Partnership Advisory Council), 그밖의 연방기관과 민간부문과 협의하여 i) 어떤 분야가 가장 급박한 리스크에 직면해 있는지를 결정하기 위한 최고 수준의 사이버보안 리스크를 평가해야 하고, ii) 주요기반시설의 지정을 위한 절차를 마련해야 하며, iii) 사이버보안 성과 평가를 위한 조건을 확인・개발하고, iv) 사이버 공격에 대한 대응 및 복구계획을 시행해야 한다. 또한, 사이버 위험(risks) 및 위협(threats)의 통지와 주요기반시설에 영향을 미치는 중대한 사이버 사고의 보고를 포함하여 주요기반시설의 안전을 위한 요구조건을 수립해야 한다.

셋째, 「연방정보보안관리법(FISMA)」을 개정하여 연방기관들이 단순히 법을 준수하는 문화에서 안전을 실천하는 문화로(from a culture of compliance to a culture of security) 풍토를 바꾸도록 국토안보부에 사이버안전 리스크의 계속적인 모니터링과 리스크 보고를 효율화 할 수 있는 권한을 부여하고 있다. 또한 연방 기관들을 위한 사이버안전의 요구 조건도 개선된다.

넷째, 「국토안보법(HSA)」을 개정하여 사이버안전을 위한 기존 국토안보부의 모든 인적・물적 자원을 국가 사이버 안전 및 통신 센터(National Center for Cybersecurity and Communications)로 통합한다. 아울러 연방 정보인프라 복구능력의 확보과 보호를 위한 노력의 관리, 정보인프라의 보호를 위한 민간 영역의 노력 지원, 정보인프라에 대한 가장 중대한 리스크의 우선순위 확정, 프라이버시 보호 확보 등을 포함한 센터의 임무를 규정한다.

사이버안전을 위한 연방정부기관의 책무를 규정하고 있다. 국토안보부는

사이버안전에 관한 지원 및 인식제고 프로그램을 시행해야 하고, 국토안보부와 상무부는 사이버안전 분야에서 일하는 능력 있는 개인을 발굴하고 개발해서 채용할 수 있는 프로그램을 설치해야 하며, 국가과학재단은 기초적인 사이버보안 연구·개발 분야의 혁신을 자극하고 사이버보안 전문가를 채용하고 연수시킬 프로그램을 설치해야 한다. 인사처는 연방 공무원들에게 요구되는 사이버안전 능력과 준비 상태를 평가하고, 연방 공무원과 계약자들을 위한 사이버안전 인식제고 및 교육 프로그램을 수립하여야 한다. 교육부는 초등학교 및 그 상급학교, 직업학교, 기술학교 등의 학생들을 대상으로 사이버안전 이슈를 다루는 표준 커리큘럼을 개발하여야 한다.

법안은 민간 기업이나 단체도 정보시스템을 보호하기 위하여 사이버위협(threat) 정보를 적법하게 공개하고 제공받을 수 있도록 권한을 부여하고 있다. 또한 사이버 위협 정보의 분배, 수집, 교환을 위한 사이버안전정보교환소(cybersecurity exchanges)를 지정하기 위한 절차도 마련해 두고 있다. 비연방 기관들도 사이버안전정보교환소에 적법하게 수집한 사이버안전 위협정보를 공개할 수 있다. 또한 선의방어원칙(a good faith defense)을 포함하여 사이버보안 모니터링 활동에 참여하고 있는 기관들을 위한 법적 보호정치도 마련해 두고 있다.

국토안보부와 국방부는 매년 의회에 행정기관 및 국방분야 정보통신망과 관련한 주요 사이버 사고에 대해 보고하여야 하고, 법무부와 FBI는 사이버범죄에 대한 수사 및 기소에 대해 매년 의회에 보고하여야 한다.

마지막으로, 국무부장관은 국제적인 사이버 이슈에 대한 외교적 노력을 위하여 국무부 고위공무원을 지명할 수 있고, 사이버범죄와 관련한 중요한 글로벌 이슈, 트렌드 등에 대하여 평가하고 그 결과를 의회에 보고해야 하며, 사이버범죄와의 전쟁을 위해 고안된 해외 지원 프로그램의 우선순위를 정해야 한다.

(3) 사이버테러 방지 및 대응에 관한 법률안 등

이노근 의원안은 제1장 총칙에서 사이버테러 예방을 위한 책임기관의 책

무와 사이버테러 방지 및 대응을 위한 민·관 협의체의 구성·운영 등에 대해서 규정하고 있고, 제2장에서는 사이버테러 방지 및 위기관리 추진체계로 국가정보원장 소속의 사이버안전전략회의 및 사이버안전센터의 설치와 사이버테러 방지 및 대응 기본계획의 수립·시행 등에 관해서 규정하고 있다.

제3장에서는 사이버테러 방지 및 위기관리를 위한 정부, 국가정보원, 중앙행정기관, 책임기관 등의 구체적인 활동을 규정함과 동시에, 사이버위협정보의 효율적인 관리 및 활용을 위한 사이버위협정보통합공유체계의 구축·운영에 대하여 규정하고 있다. 마지막으로 제4장에서는 사이버테러 방지 및 대응을 위한 연구개발, 산업육성, 인력양성, 교육홍보, 국제협력, 책임기관 지원 등에 대해서 규정하고 있다.

서상기의원안도 이노근 의원안과 대부분 내용이 유사하며, 이철우 의원안은 사이버위협정보 공유체계 구축과 사이버위협정보 보유기관의 사이버위협정보 수집 및 공유 의무를 중심으로 규정하고 있다.

(4) 기본법의 구체적 내용

기본법의 내용은 개별법의 내용과 중복 또는 충돌되지 않아야 하며, 국정원의 권한을 신설하거나 강화하기보다는 국정원의 고유기능이 발휘될 수 있도록 하는데 초점을 두어야 하며, 주체별 협력 체계를 구축하는데 무게를 두어야 한다.

첫째, 사이버안전을 위한 국가, 지자체, 공공기관, 정보통신서비스 제공자, 정보통신서비스 이용자, 일반 국민 등의 역할과 책임을 명확히 제시하여야 한다.

둘째, 범국가, 범정부 차원의 사이버안전계획이 수립·시행될 수 있도록 정부의 사이버안전 기본계획 및 시행계획의 수립·시행 체계를 수립하여야 한다. 기본계획과 시행계획은 사이버안전대책회의(또는 국무회의)의 심의를 거쳐 국회에 보고하고, 정부는 시행계획의 결과를 국회에 보호하도록 하여야 한다.

셋째, 사이버안전에 관한 중요사항을 심의·조정하기 위하여 국무총리를 의장으로 하는 "사이버안전전략회의"를 두고, 전략회의의 효율적 운영을 위하여 "사이버안전대책회의"를 두며, 사이버안전에 대한 종합적이고 체계적인 예방과 대책을 위해 국가정보원에 "사이버안전센터"를 둔다.

넷째, 중앙행정기관, 지방자치단체, 공공기관, 그밖에 대통령령으로 정하는 자는 사이버공격 정보를 실시간 탐지·분석하여 즉시 대응 조치를 할 수 있도록 보안관제센터를 설치·운영하게 한다.

다섯째, 사이버공격 및 침해사고 정보의 보고 의무자를 중앙행정기관, 지방자치단체, 공공기관, 보안관제센터, 수사기관 외에, 한국인터넷진흥원, 국가예산을 지원받는 정보공유분석센터(ISAC) 등과 같은 민간영역의 사이버공격정보 보유기관으로까지 확대하고, 수집된 정보의 분석결과를 일정한 범위 내에서 일정한 대상에 대하여 공개할 수 있도록 한다.

여섯째, 침해사고 또는 사이버공격에 대하여는 소관 중앙행정기관의 장이 조사하는 것을 원칙으로 하되, 국가안보 및 국민경제에 중대한 영향을 미칠 수 있다고 판단되는 침해사고로써 소관 중앙행정기관의 장 또는 해당 정보통신시설의 관리·운영자의 요청이 있는 경우에는 국가정보원장이 직접 또는 공동으로 사고를 조사할 수 있도록 한다.

일곱째, 온·오프라인 융합형 테러 등에 대응하기 위하여 SNS, 메신저, 화상대화, 이메일 등을 통한 테러정보 등의 수집·관리 및 공유 체계를 수립하고, 사이버테러리스트 등의 출입국관리기록, 금융거래정보 및 통신사실 확인 자료의 제공을 관계기관 및 단체에 요청할 수 있는 근거를 마련하여야 한다. 다만, 해당 법률에서 정한 바에 따르도록 한다.

여덟째, 사이버공격 또는 침해사고 발생시 침해사고 분석 및 대응을 위한 보안회사, 정보통신서비스제공자, 정보통신서비스이용자, 언론기관, 대학, 연구기관 등의 협력의무를 규정하고, 국정원장, 수사기관, 관련연구기관 등에게 악성코드의 유포처에 대한 차단 및 보안조치를 한국인터넷진흥원(미래부)에게 요청 또는 권고할 수 있는 권한을 부여하여야 한다.

끝으로, 사이버공격에 대한 대응훈련, 사이버위기경보, 기술지원, 연구개발, 인력양성, 국제협력, 교육·홍보 등에 대해서 규정한다.

05

사이버안보법정책논집

제5장 국제법상 사이버공격의 전쟁적용성

사이버공격과 자위권

오 승 진*

목 차

Ⅰ 서 론

오늘날 국가들이 적국의 컴퓨터 시스템에 침입하거나 정보를 수집하는 프로그램을 개발하거는 사례가 늘고 있다.[1] 더 나아가 적국의 교통, 통신, 은행, 무기 체계 등을 통제하는 컴퓨터 시스템에 접속하여 컴퓨터 시스템의 작동을 멈추게 하거나 오작동을 일으킴으로써 물리적인 피해를 야기하거나 사람의 생명을 위협하는 활동도 한다. 통신, 운수, 전력, 수리, 전기, 가스, 석유, 은행 및 재무 시스템에 컴퓨터 시스템은 중요한 국가의 기간산업이다. 그러므로 이러한 시스템에 대한 공격은 군사적인 목표물에 대한 직접적인 공격 못지않은 중대한 결과를 야기할 수 있다. 이러한 국가들의 활동은 사이버전쟁(cyber

* 단국대학교 법과대학 교수

1) Arie J. Schaap, "Cyberwafare Operations: Development and Use under International Law", 64 A.F.L. Rev (2009), 123.

warfare), 사이버공격(cyber attack), 사이버작전(cyber operation) 등으로 다양하게 불린다.

대부분의 국가들은 사이버공격을 수행하거나 사이버작전을 수행하는 부서 또는 부대를 운용한다. 중국은 사이버작전을 통하여 타국의 정보를 빼내거나 지적 재산권을 침해하는 것으로 알려져 있다. 나아가 중국은 쿠바와의 협정을 통하여 미국의 인터넷 활동과 특히 미국 국방부의 인터넷을 감시하는 것으로 알려져 있다.[2] 중국의 사이버 전략사령부는 약 130,000명으로 구성되어 있으며 주로 신호정보와 방어정보체계에 주력하고 있다고 알려져 있다.[3] 중국의 사이버 부대는 2007년부터 2009년까지 미국의 록히드 마틴사의 컴퓨터에 침입하여 F-35 전투기에 대한 정보를 빼냈다는 의심을 받는다.[4] 2010년 6월경에는 우라늄을 농축하는 이란의 고속원심분리기의 통제시스템에 Stuxnet 바이러스가 침투하여 이란의 원심분리기에 오작동을 일으킨 바가 있는데, 이 바이러스는 개인이 아닌 집단이나 국가 등이 만들어 유포한 것으로 의심되고 있다.[5]

이와 같이 국가들이 다양한 모습으로 사이버활동을 하거나 사이버공격 등 피해를 입는 것이 현실이므로 국내법 또는 국제법적으로 사이버활동을 규제할 필요성이 있지만 법적인 규제는 아직 거의 존재하지 않는다. 국제법전문가들이 사이버전에 적용될 국제법원칙 등을 정리한 매뉴얼인 “사이버전에 적용될 국제법에 관한 탈린 매뉴얼(Tallin Manual on the International Law Applicable to Cyber Warfare)”이 있으나 이는 구속력이 없는 문서이다. 유럽이사회가 채택한 “사이버 범죄에 관한 협약(Convention on Cybercrime)”은 단지 사기, 아동포르노, 저작권침해 등 사이버범죄에 대응하기 위한 다자조약이다.[6] 다만, 이 조약이 사이버전이나 사이버공격에 대응

2) Gary D. Solis, Cyber Warfare, 219 Mil. L. Rev. 1, p. 4.
3) Ibid., p. 5.
4) Ibid.
5) Ibid., pp. 44-45.

하기 위한 것은 아니다.

사이버활동과 관련하여 사용되는 용어들은 다양하게 정의되고 있다. 첫째, 사이버공간(cyber space)의 개념이다. 사이버 공간은 "인터넷, 정보통신네트워크, 컴퓨터 시스템 등을 포함하는 상호의존적인 정보기술기반으로 이루어진 정보환경 안에 존재하는 전지구적 영역",[7] "물리적인 지형과 상관없이 컴퓨터와 통신을 통한 인간의 상호연결",[8] "상호연결된 시스템 및 관련 물리적 시설을 통하여 정보를 저장, 수정, 교환하기 위하여 컴퓨터 및 기타 전자적 장치를 사용하는 영역"[9] 등으로 정의된다. 사이버공간의 정의에는 특별한 어려움이 없다.

둘째, 사이버전쟁(cyber warfare)의 개념이다. Richard Clarke는 사이버전(cyber war)을 "국가가 다른 국가의 컴퓨터나 네트워크를 파괴하거나 장애를 일으키기 위하여 침투하는 것"이라고 정의한다.[10] 이 정의에 의하면 비국가 행위자의 사이버공격은 사이버전의 개념에서 제외된다. Michael Hayden은 사이버전을 "다른 국가의 컴퓨터 네트워크를 무력화하거나 파괴하려는 시도"라고 정의한다.[11] 미국 국방부는 "사이버 작전(cyber operations)"을 군사적 목적이나 효과를 달성하기 위하여 사이버공간에서 또는 이를 이용하여 사이버 능력을 이용하는 것이라고 정의한다.[12] 그리고 미국 국방부는 "컴퓨터 네트워크 공격"을 컴퓨터 네트워크를 이용하여 컴퓨터 및 컴퓨터 네트워크 안에 있는 정보, 컴퓨터 또는 네트워크 자체를 손상, 퇴화, 파괴하는 행위"라고 정의한다. 2001년 미 의회에 대한 CRS 보고서는 사이버전쟁이 사이버공간에

6) Michael Gervais, "Cyber Attacks and the Laws of War", 1 J.L.& Cyber Warfare 8 (2012), p. 19.
7) Schaap, supra note 1, p. 125.
8) Ibid.
9) Ibid.
10) Oona A. Hathaway et al, "The Law of Cyber Attack", 100 Cal.L. Rev. (2012), p. 823.
11) Ibid.
12) Ibid.

서 정보 및 컴퓨터 네트워크를 공격하거나 이를 방어하거나 또는 적국의 이러한 능력을 방해하는 등 다양한 목적을 갖는다고 설명한다.[13]

상하이협력기구(The Shanghai Cooperation Organization)는[14] "정보전(information war)를 "사회와 국가를 혼란스럽게 하거나 적국의 이익을 위하여 행위하도록 하는 대규모의 심리적인 선전"이라고 정의하면서 "다른 국가의 사회, 정치, 경제적 시스템과 정신, 도덕 및 문화적 영역에 해로운 정보를 유포"하는 것을 정보안전에 대한 주요한 위협으로 언급하고 있다.[15] 상하이협력기구의 정의는 사이버상의 위험을 정보전이라는 개념으로 가장 넓게 정의하고 있다.[16] 사이버전쟁에 대한 다양한 정의는 사이버활동 중에서 무엇을 위협으로 볼 것인가에 대한 견해의 차이에서 기인한다.

셋째, 사이버공격(cyber attack)이라는 개념도 있는데, 일반적으로 "정치적 또는 국가안보의 목적으로 컴퓨터 네트워크의 기능을 저해하기 위한 활동"이라고 정의된다.[17] 이러한 정의에 따르면 적극적인 공격, 그리고 방어를 위하여 적국의 컴퓨터에 대하여 취하는 방어활동은 모두 사이버 공격에 해당하게 된다. 다만, 소극적인 예방조치는 사이버 공격에 해당하지 아니한다. 이 정의에 따르면 폭탄 등을 이용하여 물리적으로 컴퓨터 네트워크를 파괴하는 행위도 사이버 공격에 해당한다.[18] 개인이 정치적 또는 국가안보의 목적으로 사이버상의 범죄활동을 하는 경우에 사이버공격에 해당할 수 있으나 사이버에서 사기 등의 범죄를 저지르는 것은 사이버 범죄에 해당하며 사이버공격의 범주에서 제외된다.

참고로 미국 육군은 사이버공격을 "해를 끼치거나 사회적, 이념적, 종교적,

13) Ibid.
14) 상하이협력기구는 중국, 러시아, 이란, 인도, 파키스탄 등으로 구성된 안보협력기구이다.
15) Onna A. Hathaway, et al. supra note 10, p. 825.
16) Ibid. p. 825.
17) OOna A. Hathaway, p. 826.
18) OOna A. Hathawa, p. 827.

정치적인 목적으로 또는 그러한 목적으로 사람을 위협하기 위하여 컴퓨터 및 네트워크에 대하여 하는 고의적인 방해나 위협적인 활동"이라고 정의한다.[19] 미국 합동참모본부는 사이버 공격을 "적국의 중요한 사이버 시스템, 자산 또는 기능을 방해하거나 파괴하기 위하여 컴퓨터 또는 관련 네트워크나 시스템을 이용한 적대적인 행위"로 정의한다.[20]

사이버전쟁은 사이버 정보수집(cyber espionage)와 구분된다. 국가들은 군사적인 목적을 위하여 일상적으로 타국의 네트워크에서 정보를 수집하거나 분석하며, 이러한 작업은 타국의 컴퓨터나 네트워크 또는 그 속의 정보를 방해, 파괴하지 아니한다.[21] 이러한 행위는 국내법상 범죄가 될 수도 있지만 적극적으로 컴퓨터나 네트워크에 장애를 일으키거나 이를 파괴하는 활동과 구분된다.

국제사회는 무력의 행사의 적법성에 관한 국제법(Jus Ad Bellum), 무력행사의 수단과 방법에 관한 국제법(Jus In Bello)를 발전시켜 왔으나 사이버전쟁이나 공격에 관하여는 특별한 규범을 마련하지 못하고 있다. 이 글은 기존의 국제법적인 틀 안에서 사이버전 또는 사이버공격이 어떠한 법적인 규제를 받을 수 있는지 여부를 검토한다. 첫째는 사이버공격이 무력사용을 금지하는 유엔헌장 제2조 4항을 위반하는가 하는가 여부이다. 둘째는 사이버공격이 유엔헌장 제51조의 규정에 따라 자위권의 행사를 정당화하는 무력공격에 해당하는가 여부이다. 마지막으로는 사이버공격에도 무력충돌법이 적용되는가 여부이다. 이에 대한 분석을 위하여 사이버전쟁 또는 사이버공격을 위하여 사용되는 수단을 살펴본다.

19) Shaun Roberts, "Cyber wars: Applying Conventional Law of War to Cyber Warfare and Non-State Actors", 41 N.Ky. L. rev. (2014), p. 539.
20) Oona A. Hathaway, p. 824.
21) Gervais, supra note 6, p. 23.

Ⅱ 사이버공격의 유형

1. Dos(Denial of Service) 공격

Dos 공격은 네트워크에 과도하게 접속을 하여 네트워크에 장애를 일으키거나 완전히 작동을 멈추도록 하는 공격을 말한다.[22] 그리하여 네트워크의 이용자가 정상적으로 네트워크를 이용할 수 없게 된다. Dos 공격은 비교적 적은 비용으로 실행될 수 있다는 장점이 있다. 분산 D Dos(DDos) 공격은 바이러스에 감염된 많은 수의 컴퓨터나 시스템이 하나의 시스템을 공격하여 과부하를 유도하는 것을 말한다. DDos 공격은 많은 컴퓨터와 시스템을 통하여 이루어지므로 이를 막는 것이 쉽지 않다.

2. 악성 프로그램

악성 프로그램은 컴퓨터의 정상적인 기능을 방해하거나 원거리에서 당해 컴퓨터나 시스템을 조종하도록 한다.[23] 악성 프로그램은 컴퓨터를 작동불능하게 만들거나 파일을 삭제하거나 파괴한다. 바이러스, 웜, 토로이 목마 등이 이에 해당한다. 바이러스는 컴퓨터의 장애를 일으키는 코드로, 프로그램이나 파일에 첨부되어 다른 컴퓨터로 전파될 수 있다. 사용자가 악성프로그램을 실행하거나 열면 컴퓨터가 이에 감염된다. 웜은 컴퓨터나 네트워크의 장애를 일으키는 프로그램으로 사람의 도움이 없이 파일이나 정보이동수단을 통하여 전파될 수 있다는 특징이 있다. 웜은 시스템에서 스스로 복제할 수 있는 능력이 있으므로 복제, 전파되며, 시스템의 메모리를 소진하여 컴퓨터에 장애를 일으킨다. 트로이 목마는 프로그램이나 데이터에 포함되어 지정된 장애를 일으킨다. 사용자가 합법적인 것처럼 보이는 소프트웨어나 파일을 열면 컴퓨터가 감염되어 시스템상의 파일이나 정보를 삭제한다. 나아가 공격자가

22) Arie J. Shaap, supra note 1, p. 134.
23) Ibid.

시스템이나 컴퓨터를 통제하거나 정보를 빼내는 것이 가능해진다. 그리고 여러 악성 프로그램을 결합하여 컴퓨터나 네트워크를 마비시키거나 공격할 수도 있다.

3. 논리폭탄

논리폭탄은 특정한 조건이 갖추어 지거나 정해진 시간에 실행되는 악성 코드이다.[24] 이것이 작동되면 컴퓨터를 마비시키거나 데이터를 삭제하고 Dos 공격을 야기한다.

4. IP 기만

IP 기만은 IP 주소 사기라고도 불린다. 허위로 만들어진 사이트가 합법적인 사이트를 가장하여 사이트를 방문한 이용자의 정보를 빼내는 것을 말한다.[25]

5. 디지털 조작

디지털 조작은 컴퓨터 프로그램을 이용하여 디지털 이미지를 변경하는 것을 말한다.[26] 기술의 발달로 인하여 사진, 영상, 음성 등을 실시간으로 합성, 조작하여 이를 유포하는 것이 가능하다.

Ⅲ 무력사용금지원칙과 사이버공격

1. 무력사용금지의 원칙

국제평화와 안전은 2차 세계대전 이후 국제공동체의 가장 중요한 목표가 되었다. 국제사회는 이를 위하여 무력사용금지의 원칙을 유엔헌장에 도입하

24) Ibid, p. 137.
25) Ibid.
26) Ibid.

여 전면적으로 국가들의 무력사용을 금지하였다. 즉, 모든 유엔회원국은 유엔헌장 제2조 4항에 따라 국제관계에서 타국의 영토보전 또는 정치적 독립에 반하거나 유엔의 목적에 반하는 어떠한 방식으로도 무력(힘)의 위협이나 무력사용을 삼가야 한다. 전면적인 무력사용금지의 원칙은 2차 세계대전 이전에는 상상하기 어려운 것이었다. 무력의 사용은 헌장의 규정에 따라 예외적으로 인정되는 경우를 제외하고는 어떤 경우에도 전면적으로 금지된다.

다만, 헌장 7장에 따라 안전보장이사회가 국제평화와 안전을 위하여 무력의 사용을 허가하는 경우, 헌장 제51조에 따라 무력공격을 받은 국가가 자위권을 행사하는 경우에 한하여 무력사용이 적법하게 된다. 금지되는 것은 군사적인 힘의 사용, 즉, 무력의 사용이다. 유엔헌장의 기초 당시에 헌장의 목적에 부합하지 않는 경제적인 힘의 사용도 금지하고자 하는 안은 수용되지 아니하였다.[27] 국가들에 의하여 금지되는 "힘(force)"는 군사적인 힘, 즉, 무력의 사용만을 의미하는 것으로 이해되었으며, 이것이 다수의 견해이다.[28] 그러므로 헌장 제2조 4항에 의하여 금지되는 것은 무력의 사용이며, 일반적으로 국제관계에서 타국에 대하여 정치적 또는 경제적인 힘 또는 압력을 행사하는 것은 허용되는 것으로 해석된다.

아래의 자위권의 행사에서 보듯이 무력사용과 무력공격은 "규모와 효과"면에서 구분되므로 모든 형태의 무력사용이 무력공격에 해당하는 것은 아니다. ICJ는 무력공격이 정규군에 의한 국경침범과 무장대나 비정규군, 용병 등에 의하여도 행해질 수 있다고 본다.[29] 그러나 ICJ는 반란군에게 무기 및 훈련 등 원조를 하는 것은 무력사용금지에 위반하지만 무력공격에 해당하지 않는다고 보았다.[30] 이에 따르면 무력공격이 아닌 무력사용의 피해자인 국

27) Gervais, supra note 6, p. 27.
28) 정인섭, 『신국제법 강의』 (박영사, 2015), 1077쪽.
29) Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), Merits (1986), para 195.
30) Ibid.

가는 헌장 제51조에 따른 자위권을 행사할 권리가 인정되지 않으며, 단지 비무력적인 대응조치 등을 이용할 수 있다.

사이버공격이나 사이버활동은 매우 다양한 모습을 띤다. 다른 작전과 독립된 것일 수도 있고, 군사적 공격의 일환으로 행해질 수도 있다. 사이버공격의 결과도 매우 다양할 수 있다. 약간의 불편, 재산이나 물건의 파괴, 사망으로 이어질 수도 있다. 그러므로 사이버공격이나 사이버활동만으로 이것이 무력사용이나 무력공격에 해당한다고 판단하는 것은 지나치다.[31]

2. 무력사용금지와 사이버공격

사이버공격이 무력사용금지의 원칙을 위반할 수 있는가? 사이버공격이 국제법상 금지되는 무력사용에 해당하거나 헌장 제51조에 따라 자위권을 정당화하는 무력공격에 해당하는지 여부에 관하여는 다양한 견해가 존재한다. 뒤에서 살피는 바와 같이 사이버공격이 그 규모와 효과 면에서 일정한 정도에 이르면 무력공격에 해당하며, 자위권의 행사를 정당화할 수 있다. 사이버 공격이 사람의 상해나 사망 또는 물건에 대한 일정한 손해나 파괴를 야기하면 자위권을 행사할 수 있는 것이다. 다만, 중요한 기간 산업에 대한 장애를 일으키거나 사회적, 경제적 또는 정부의 기능에 장애를 일으킬 수 있는 사이버 작전이나 공격이 그 규모나 효과 면에서 일정한 정도에 이르지 아니한 경우에는 무력공격의 개념에 해당하지 않으며, 따라서 이에 대하여는 자위권의 행사도 허용되지 아니할 것이다.

사이버공격이 규모와 효과 면에서 그다지 무겁지 아니하여 헌장 제2조 4항이 금지하는 무력사용에는 해당하지만 헌장 제51조의 무력공격에는 해당하지 않는 경우가 있을 수 있다. 사이버공격이 무력공격에 해당하는 경우가 오히려 예외적인 현상일 것이다. 무력공격에 미치지 못하는 사이버공격에 대하여 국가들은 어떠한 대응을 할 수 있는가가 문제된다. 이에 관하여는 대응

31) Gervais, supra note 6, p. 28.

조치가 가능한 것으로 보인다. 대응조치는 위법행위로 인하여 피해를 입은 국가가 유책국을 상대로 그 의무이행을 강제하기 위하여 상응하는 의무불이행으로 대응하는 것을 말한다.[32] ICJ는 Nicaragua 사건에서 무력공격에 미치지 못하는 무력사용에 대하여 대응조치를 취할 수 있다고 판단하였다.[33] 다만, 대응조치의 내용은 자국이 입은 피해에 비례해야 한다.

사이버작전에 무력의 사용에 미치지 못한다고 하여 그러한 행위가 모두 국제법상 적법한 것은 아니다. 국가는 타국의 국내문제에 직접적 또는 간접적으로 간섭할 수 없으므로[34] 이론적으로는 국가가 지속적으로 타국에 대하여 사이버작전을 행하는 경우에 이것이 불간섭의 의무를 위반할 수 있기 때문이다. 니카라과 사건에서 ICJ는 강제력을 사용하는 간섭은 위법하다고 하였는데,[35] 사이버작전은 일반적으로 강제력을 사용한다고 볼 수 없으므로 단순한 사이버상의 정보수집이나 침투는 불간섭의무의 위반이라고 보기 어려운 면이 있다.

Ⅳ 자위권과 사이버공격

1. 자위권 행사의 요건 – 무력공격이 발생한 경우

무력공격을 받은 국가는 이를 격퇴하기 위하여 헌장 제51조에 따라 적법하게 무력을 행사할 수 있는데, 이를 자위권이라고 한다. 관습국제법상 자위권이 원용된 대표적인 사례는 Caroline 사건이다.[36] 이 사건의 내용은 다음과 같다. 1837년경 일단의 미국인들이 선박 Caroline호를 이용하여 영국의 식민지이던 캐나다를 지원하고 있었다.[37] 영국인들이 이를 이유로 미국 내

32) Article 49, Draft of State Responsibility.
33) para. 64.
34) Nicaragua case, supra note 29, para. 205.
35) Ibid, para. 205.
36) Malcolm N. Shaw, International Law 4th edition (Cambridge University Press, 1997), p. 787.

의 위 선박을 공격하였다. 영국은 위 행위를 자위권의 행사라고 주장하였는데, 미국은 자위권의 행사가 적법하기 위한 요건으로 자위권의 필요성은 급박하고, 압도적이며, 다른 수단을 선택할 여지가 없으며, 생각할 여유가 없을 경우에 인정된다고 주장하였다.[38] 이러한 미국의 입장은 그 후 자위권행사의 적법성에 관한 요건으로 받아들여졌다.

ICJ는 가장 무거운 형태의 무력행사인 "무력공격(armed attack)과 그보다 낮은 수준의 무력사용을 구분한다.[39] 유엔헌장 제51조의 규정에 따라 국제법상 국가의 자위권발동을 가능하게 하는 무력공격은 가장 무거운 형태의 무력행사인 것이다. 일반적으로 생명 또는 재산의 파괴를 낳거나 낳을 수 있는 소규모의 포격, 해상 및 공중으로부터의 공격은 무력공격에 해당한다. 다만, 무력행사를 시위하기 위하여 무인지경에 한 번의 포격이나 미사일 공격을 한 경우에 무력행사금지의 원칙을 위반한 것이기는 하지만 무력공격에 해당하지 않을 것이다.[40]

자위권의 행사는 그 수단과 방법에서 무력공격을 격퇴하는 정도로 제한된다. ICJ는 자위권의 행사는 필요성과 비례성의 원칙에 의하여 제한을 받는다고 판시하였다.[41] 자위권은 무력공격을 격퇴하는데 필요해야하며, 그 정도에 비례해야 한다. ICJ는 Oil Platforms 사건에서 무력공격에 비례하지 아니한 자위권의 행사는 위법하다고 판시하였다.[42] ICJ는 이 사건에서 자위권의 행사가 적법하기 위한 필요성의 원칙은 엄격하며 객관적이며, 국가의 재량의 여지가 없다고 판시하였다.[43] 그러므로 무력공격을 받은 국가는 공격

37) Ibid.
38) Ibid.
39) Nicaragua case, supra note 29, para. 195.
40) Gervais, supra note 6, p. 37.
41) Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J Reports 1996, para. 41.
42) Oil Platforms (Iran v. United States), Judgment, I.C.J. Reports 2003, para. 77.
43) Ibid. para. 73.

을 격퇴하기 위하여 무력공격에 비례하고 격퇴를 위하여 필요한 정도의 무력만 사용할 수 있다.

자위권의 행사를 정당화하는 무력공격은 반드시 국가에 의한 것일 필요는 없으며, 테러단체나 기타의 무장단체, 즉, 비국가 행위자에 의한 무력공격도 자위권의 행사를 정당화할 수 있다. 이에 관하여 다소 논란이 없는 것은 아니다. 예를 들어, ICJ는 Nicaragua 사건에서 국가만이 타국에 대하여 무력공격을 할 수 있는 것처럼 판시한 바가 있다.[44] ICJ는 Construction Wall 사건에서도 자위권을 정의하면서 국가가 타국을 무력공격하는 경우에 자위권을 행사할 수 있다고 판시하여[45] 국가만이 무력공격을 할 수 있다는 취지를 밝히고 있다. 그러나 9/11 이후에 테러단체 등이 국가에 대하여 무력공격을 할 수 있다는 점이 일반적으로 받아들여지고 있다.[46]

무력의 행사가 무력공격에 해당하는가 여부를 판단함에 있어서 사용된 무기의 종류는 중요하지 않다. ICJ는 헌장 제2조 4항 및 51조의 요건과 관련하여 어떠한 형태의 무기의 사용도 무력의 행사에 해당할 수 있다고 보았다.[47] 유엔안전보장이사회는 납치된 비행기가 무기로 사용된 9/11 사건과 관련하여 미국이 자위권을 행사할 수 있다고 보았다.

2. 사이버공격은 무력공격에 해당하는가?

자위권의 행사요건인 무력공격에 사이버공격도 포함되는가에 관하여 3가지 입장이 대립된다. 수단을 중시하는 견해, 목표물을 중시하는 견해, 효과를 중시하는 견해가 그것이다.

첫째, 무력행사의 수단을 중시하여 사이버공격은 물리적인 특성을 가진 전통적인 무력행사의 수단이 아니므로 사이버공격은 일반적으로 무력행사에

44) Nicaragua case, supar note 29, para. 195.
45) Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, para. 139.
46) Antonio Cassese, International Law (Oxford University Press, 2005), p. 355.
47) Legality of Nuclear Weapons, supra note 41, para. 39.

해당하지 않는다는 견해이다.[48] 유엔헌장 제41조는 안전보장이사회의 조치에 관하여 규정하면서 무력을 사용하지 아니하는 안전보장이사회의 조치로 전신, 무선통신의 전부 또는 일부의 단절을 규정하고 있는데, 이에 따르면 통신의 장애를 초래하는 사이버공격은 무력행사에 해당하지 않는다고 주장한다.[49] 나토조약 제4조는 사이버공격이 발생한 경우에 회원국 사이의 협의를 요하도록 하고 있다. 그러나 나토조약 제5조에 따르면 무력공격에 대하여는 회원국 상호간에 원조의무가 발생한다. 나토조약은 사이버공격과 무력공격을 구분하는 것이다. 이 견해는 군사적 무기를 구분하기 쉬우므로 적용이 쉽다는 장점이 있다. 그러나 사이버공격은 전통적인 군사적 무기를 사용하지 않고서도 치명적인 결과를 가할 수 있다는 특징이 있으므로 이러한 견해는 그다지 지지를 받지 못하고 있다.

둘째, 공격의 목표물을 중시하여 은행, 통신, 교통 등 국가의 중요한 컴퓨터 시스템을 공격하는 사이버공격을 무력공격으로 정의하는 견해가 있다.[50] 이 견해는 중요한 컴퓨터 시스템에 대한 공격을 무력공격으로 봄으로써 자위권의 행사를 용이하게 하는 이점이 있다. 그러나 사이버공격 자체가 무차별적이고 공격자의 통제를 벗어나는 경우가 있으므로 중요한 컴퓨터 시스템에 대한 공격이 의도적이지 않은 경우에도 자위권의 행사를 정당화하는 한계가 있다. 이 견해에 따르면 사이버충돌이 쉽게 무력충돌로 이어질 가능성이 있다.

셋째, 사이버공격의 결과를 중시하여, 사이버공격의 영향이 전통적인 무기에 의한 무력행사와 유사하면 무력행사에 해당한다는 견해가 있다. 이에 따르면 재산 또는 생명에 대한 피해가 발생해야 한다.[51] 이 견해는 사이버공격

48) Shuan Roberts, “Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors”, 41 N.Ky.L.Rev. 535 (2014), p. 554.
49) Ibid.
50) Ibid.
51) Michael Gervais, supra note 6, p. 31.

을 기존의 국제법의 틀 안에서 이해할 수 있다는 장점이 있는데, 현재 다수의 견해이다. 이 견해의 한계는 대부분의 사이버공격이 직접적으로 물리적인 피해나 사망의 결과를 일으키지 않는다는 점이다. 예를 들어, 사이버공격으로 응급 서비스가 마비된 경우에 직접적으로는 사망이라는 결과가 발생하지 않지만 간접적으로 사람이 사망할 수도 있다. 사이버공격의 결과를 어떻게 평가할 것인가에 관하여는 피해 자체만을 고려하거나 사이버공격과 최종적인 결과 사이의 관련성을 고려하는 등 다양한 방법이 있다. 이 견해에서는 어떠한 형태의 영향이 자위권의 행사를 정당화하는가의 질문이 중요하다. 예를 들어, 교통통제시스템에 대한 공격, 발전소의 시스템에 대한 공격, 증권시장에 대한 공격 등이 있는 경우에 어느 경우에 자위권의 행사가 가능한가 하는 의문이 떠오른다. 모든 경우에 크고 작은 인명 또는 재산상의 피해가 발생할 가능성이 있으므로 어느 단계에서 무력공격이 있는 것인가 판단하기 쉬운 것은 아니다.

사이버공격이 자위권의 행사를 정당화하는지 여부는 사이버공격이 전통적인 무력사용의 결과와 유사한가 여부에 따라 판단해야 한다고 본다. Michael N. Schmitt도 사이버공격이 무력행사에 해당하는가 여부는 사이버공격의 결과에 비추어 판단해야 한다고 주장한다.[52] 이에 따르면 사이버공격이 전통적인 공격의 결과와 유사한가 여부에 따라 무력행사에 해당하는지 여부를 판단한다. 그는 사이버공격의 결과를 평가함에 있어서 심각성(피해의 종류와 정도), 즉각성(공격 이후에 어느 정도 빠르게 피해가 현실화하는가), 직접성(공격과 피해의 인과관계의 시간), 침해성(공격이 피해국의 영토를 침범하는 정도), 계량성(피해가 계량화되는 정도), 합법성(전체적으로 사이버활동의 영역에서 무력공격을 구성하는 사이버공격이 예외인 사실에 부여되는 무게감) 등 6가지 요소를 고려한다.[53]

52) Ibid, pp. 31-32.
53) Ibid.

Daniel Silver의 견해도 위와 유사하지만 그는 사이버공격이 무력공격에 해당하는가 여부는 피해의 심각성만을 기준으로 하여 판단되어야 한다고 주장한다. 그에 따르면 사이버공격은 예상되는 결과가 신체상의 피해 또는 재산상의 손해를 야기하는 경우, 그리고 예상되는 결과의 심각성이 무력공격으로 인한 결과와 유사한 경우에만 자위권의 행사를 정당화한다. 이에 따르면 항공기의 관제시스템에 대한 사이버공격으로 비행기를 추락시키는 것은 생명 및 재산에 대한 피해로 이어질 것이 예상되므로 무력공격에 해당하지만 단순히 웹사이트에 대한 사이버공격이나 중요한 컴퓨터 시스템에 대한 접속은 생명이나 재산에 대한 피해로 이어지지 아니하는 한 무력공격에 해당하지 아니한다. 이에 반하여 상당한 정도로 재산을 파괴하거나 사람의 생명에 피해를 입히는 사이버공격은 무력공격에 해당하며, 자위권의 행사를 정당화할 수 있다.

3. 필요성 및 비례성의 원칙과 사이버공격

앞서 살펴본 바와 같이 자위권의 행사는 필요성 및 비례성의 원칙에 의하여 제한된다. 그러므로 사이버공격이 그 규모와 효과에서 상당하여 자위권의 행사를 정당화하는 경우에도 이는 필요성 및 비례성의 원칙에 의하여 제한된다. 필요성의 원칙에 따르면 무력의 사용은 최후의 수단이어야 하며, 외교적인 교섭 등 평화적인 수단에 의하여 목적을 달성할 수 있는 경우에는 무력행사는 허용되지 않는다. 그러므로 사이버공격을 막을 수 있는 다른 적절한 수단이 있는 경우에는 자위권을 행사하는 것은 허용되지 않는다. 비례성의 원칙에 의하면 피해국이 실제로 입은 손해나 급박한 위험에 비하여 과도한 무력의 행사는 허용되지 않는다. 그러나 비례성의 원칙이 동종의 대응을 해야 한다는 의미는 아니므로 사이버공격에 대하여 전통적인 무력을 사용하는 것은 허용된다. 이와 같이, 사이버공격에 대한 자위권의 행사로 필요성 및 비례성의 원칙을 넘어 과도하게 무력을 사용하는 것은 허용되지 않는다. 다만, 사이버공격에 대한 자위권의 행사에 필요성 및 비례성의 원칙을 적용하는 것은

생각만큼 쉽지 않다.

4. 비국가 행위자의 사이버공격

국가의 국제위법행위는 국가책임을 유발한다.[54] 국가책임이 성립하려면 당해 행위를 국가에 귀속시킬 수 있어야 한다. 국가기관의 행위와 국가기관의 권한을 넘은 행위는 당연히 국가의 행위가 된다. ICJ는 "무력충돌의 당사자는 군대의 구성원의 모든 행위에 대하여 책임을 부담한다"고 판시하였다.[55] 새 정부를 구성하는 데 성공한 반란단체의 행위는 국가에 귀속된다.[56] 많은 국가들이 군대 안에 사이버부대를 창설하고 있다. 사이버공격의 경로를 파악하는 것이 용이한 일은 아니지만 사이버공격의 피해국이 가해국의 사이버부대의 사이버공격을 입증할 수 있다면 피해국은 가해국에 대하여 국제책임을 추궁할 수 있을 것이다. 그러한 사이버공격이 헌장 제51조의 무력공격에 해당하는 상황에서 피해국은 자위권을 행사할 수 있게 된다.

사이버공간의 특성상 애국적 동기 또는 특정한 이데올로기를 가진 개인이나 테러단체 등 비국가 행위자가 정부와 상관없이 타국에 대하여 사이버공격을 할 가능성이 없지 않다. 나아가 비국가 행위자가 본국이 아닌 제3국에서 타국을 상대로 사이버공격을 하는 경우도 상정해 볼 수 있다. 이 경우에 이들이 소재하거나 활동하는 국가는 어떠한 책임을 부담하는지, 나아가 이러한 개인이나 테러단체에 대하여 자위권을 행사할 수 있는지가 문제된다.

원칙적으로 개인이나 민간단체의 행위는 원칙적으로 국제법상 국가의 행위로 귀속되지 않는다. 그러므로 개인이나 민간단체가 타국에 대하여 사이버공격을 하는 경우에 당해 개인이나 민간단체가 소재하거나 활동하는 수용국이 이에 대하여 책임을 부담할 이유는 없는 것이다. 다만, 비국가 행위자도

54) Article 1, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
55) Armed Activities on the Territory of the Congo, (Democratic Rep. Congo v. Uganda), 2005 I.C.J. 116, 216.
56) 정인섭, 전게서, 393-397쪽 참조.

타국에 대하여 무력공격을 할 수 있으며, 이때 무력공격을 받은 국가는 당해 테러단체 등 비국가 행위자에 대하여 자위권을 행사할 수 있을 것이다. 유엔 안전보장이사회는 9/11 이후 결의 1368을 통하여 테러단체에 대하여 자위권을 행사할 수 있다는 견해를 표명하였다.[57]

테러단체에 대하여도 자위권을 행사할 수 있다고 보는 경우에 당해 테러단체를 수용하고 있는 국가에 대하여도 자위권의 행사로 무력을 행사할 수 있는가 하는 의문이 제기된다. ICJ는 Corfu Channel 사건에서 국가의 영토주권은 국제관계의 근본적인 기초이며, 국제법상 모든 국가는 자신의 영토가 타국의 권리를 침해하는 행위에 이용되지 않도록 할 의무가 있다고 판시하였다.[58] 그러므로 이러한 범위 내에서 국가가 자국의 관할권 내에 존재하거나 활동하는 개인 또는 테러단체가 타국에 대한 사이버공격을 하거나 할 예정이라는 사실을 인식하거나 예상하고 있다면 이에 근거하여 당해 국가의 국가책임이 발생할 여지도 있다.

국제법의 이론에 의하면 개인이나 테러단체 등 비국가 행위자의 행위는 일정한 요건을 갖추면 당해 개인이나 테러단체를 수용하는 국가에게 귀속될 수 있다. 어떠한 상황에서 비국가 행위자의 행위를 국가에 귀속시킬 수 있는가에 관하여 실효적 통제 및 전반적 통제의 두 가지 입장이 대립한다. ICJ는 Nicaragua 사건에서 국가가 비국가 행위자의 행위를 실효적으로 통제하면 당해 비국가 행위자의 행위가 국가에 귀속된다고 판단하였다.[59] 이 사건에서는 니카라과 정부에 대항하는 콘트라 반군의 행위에 대하여 미국이 책임을 부담하는가가 쟁점이 되었는데, ICJ는 비국가 행위자의 행위에 대하여 국가가 국제책임을 부담하기 위해서는 당해 행위에 대한 국가의 실효적인 통제가 있어야 한다고 보았다.[60]

57) S.C. Res. 1368, U.N. Doc. S/Res/1368(Sept 12, 2001)
58) Corfu Channel case, Judgment of April 9th, 1949:P I.C.J. Reports 1949, p. 22.
59) Nicaragua case, para. 115.

반면에 전반적 통제의 기준에 따르면 국가가 비국가 행위자의 행위를 전반적으로 통제하기만 하면 비국가 행위자의 행위가 국가에 귀속된다.[61] 전반적 통제의 기준에서는 국가가 비국가 행위자에 대하여 장비의 지원, 자금지원, 훈련, 어느 정도의 지휘, 감독 등 약한 정도의 통제만 있어도 국가는 비국가 행위자의 행위에 대하여 국가책임을 부담하게 된다.

국가가 비국가 행위자의 행위를 사후적으로 승인하거나 묵인하는 경우에도 당해 국가가 책임을 부담한다. 국가책임에 관한 초안은 국가가 비국가 행위자의 행위를 자신의 것으로 인정하거나 받아들이는 경우에 국가책임을 부담한다고 규정하고 있다.[62] ICJ는 Diplomatic and Consular Staff in Tehran 사건에서 이란이 비국가 행위자의 인질 억류를 승인하였으므로 이란이 미국에 대하여 책임을 부담한다고 판시하였다.

이상에서 살핀 바에 따르면 국가는 비국가 행위자의 사이버공격에 대하여 실효적 또는 전반적인 통제를 하거나 사후적으로 이를 국가의 행위로 받아들이는 경우에 비국가 행위자의 행위에 대하여 국가책임을 부담하게 될 것이다.

9/11 이후 비국가 행위자의 행위에 대한 국가의 책임은 다소 무거워지는 것으로 보인다. 이를 사이버공격과 관련하여 본다면, 국가는 비국가 행위자가 타국에 대하여 사이버 공격을 하지 않도록 적절한 조치를 취해야 한다는 것을 의미한다. 국가가 이러한 의무를 소홀히 하는 경우에 피해국이 자위권을 행사할 가능성이 있는 것이다.[63] 예를 들면, 안전보장이사회 결의 1368은 9/11 사건의 범죄자를 원조하거나 지원한 자는 물론 이들에게 피난처를 제공하는 자들도 책임을 부담한다고 명시하고 있다. 이러한 입장은 국가가 비국가 행위자에 대하여 실효적 통제 또는 전반적 통제를 하거나 비국가 행

60) Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Bosnia and Herzegovina v. Serbia and Montenegro, I.C.J. Reports 43, para. 406.
61) Prosecutor v. Tadic, Case No. IT-94-1-T (July 14, 2007), para. 145.
62) Article 11, Draft Articles on State Responsibility.
63) Gervais, supra note 6, p. 47.

위자의 행위를 승인한 경우에만 국가책임을 부담한다는 견해에서 조금 더 나아간 것이다. 물론, 아직까지 이러한 입장이 일반적으로 받아들여지고 있는 것은 아니다. 그럼에도 불구하고 사이버공격이 은밀하게 이루어진다는 점을 고려하면 이와 같은 견해는 국가들에게 많은 부담을 주게 될 것이다.[64]

개인이나 테러단체 등의 행위가 수용국에게 귀속되어 수용국의 국가책임이 발생하는 경우에도 피해국이 수용국에 대하여 자위권을 행사할 수 있는가 여부는 별도의 문제일 수가 있다. 이에 관하여는 수용국이 중립적인 지위를 상실하였으므로 무력공격이 가능하다는 견해, 개입권에 의하여 수용국에 대한 무력행사가 정당화된다는 견해, 긴급피난의 이론에 따라 무력행사가 가능하다는 견해 등이 존재한다.[65] 개인이나 테러단체의 행위가 수용국에 귀속되면 피해국은 이들의 수용국에 대하여도 자위권을 행사할 수 있다는 것이 다수의 견해로 보인다.

V 사이버전쟁과 무력충돌법

1. 서론

국가가 무력공격을 받은 경우에 이를 격퇴하는데 필요한 범위 내에서 자위권을 행사할 수 있다. 이 경우에도 무력충돌법상의 원칙은 준수되어야 한다. 무력충돌법에 따르면 무력충돌의 과정에서 필요성, 비례성, 구분의 원칙, 중립성의 원칙 등이 준수되어야 한다. 사이버공격만으로 무력충돌이 발생하는 경우는 드물지만 전쟁에서 하나의 수단으로 사이버공격을 하거나 전통적인 무력공격을 준비하는 과정에서 사이버공격이 이용되는 사례는 있을 수 있다. 그런데 사이버공격 자체만으로는 네트워크에 대한 일시적인 장애만으로 초래하는 경우가 많고, 직접적으로 심각하거나 파괴적인 결과가 발생하지 않는

64) Gervais, supra note 6, p. 48.
65) 정인섭, 신국제법 강의 (박영사, 2015), 1123쪽.

경우가 많으므로 사이버공격이 비례성의 원칙을 준수하였는지 판단하는 것이 쉽지 않다. 사이버공격과 관련하여 전투원, 적대행위에 직접적으로 참가하는 민간인, 계속적으로 전투의 기능을 수행하는 민간인과 보호받는 민간인을 구분하는 것도 쉽지 않다. 사이버공격의 원천을 속이는 것도 그다지 어렵지 않으므로 중립성의 원칙을 지키는 것도 어려울 수 있다.

2. 필요성의 원칙

무력충돌법상 필요성의 원칙에 따르면 공격은 군사적인 목적을 달상하기 위하여 필요해야 한다. 제네바협약 추가의정서 제52조에 따르면 공격의 목표물을 엄격히 군사목표물에 한정되며, 물건에 대한 군사목표물은 그 성질, 위치, 목적, 용도상 군사적 행동에 유효한 기여를 하고, 당시의 상황으로 볼 때 그 파괴, 포획 또는 무용화가 명백한 군사적 이익을 제공하는 물건으로 한정된다. 사이버공격에서도 필요성의 원칙은 준수되어야 한다. 만일 사이버공격이 군사적 목적을 달성하지 못하는 것이라면 필요성의 원칙을 위반한 것이 된다.

다만, 목표물이 명백히 군사적 이익을 제공하는지 여부를 판단하는 것은 매우 어렵다. 대부분의 사이버공격에서는 공격을 할 당시에는 그 간접적인 효과를 예측하기 어렵다.[66]

전통적인 무력충돌에서도 공통적으로 등장하는 문제로 사후적으로 명백한 군사적 이익을 판단하는 것은 용이하여도 사이버 공격자가 사전에 이를 예측하는 것은 어렵다. 사이버 공격자가 필요성의 원칙을 충족하였는지 여부는 개별적으로 판단해야 할 문제이다.

3. 비례성의 원칙

무력충돌법상 비례성의 원칙에 따르면 “우발적인 민간인 생명의 손실, 민

66) Gervais, supra note 6, p. 72.

간인에 대한 상해, 민간물자에 대한 손상, 또는 그 복합적 결과를 야기할 우려가 있는 공격으로서 예상되는 구체적이고 직접적인 군사적 이익에 비하여 과도한 공격"은[67] 금지된다. 그러므로 군사적인 의사결정을 하는 사람은 예상되는 민간인 손실, 민간 시설에 대한 파괴와 공격으로 달성되는 군사적 이익을 검토하여야 한다.

그러나 일반적으로 사이버공격의 직접적인 효과는 일시적이며 치명적이지 않으므로 사이버공격이 비례성의 원칙이 충족되었는지 판단하는 것은 쉽지 않다. 예를 들면 인터넷의 연결을 일시적으로 방해하는 사이버공격은 일반적으로 불편한 정도에 그치지만 병원이 인터넷을 이용하지 못하면 환자의 생명이 위험해질 수도 있다. 사이버공격으로 인한 피해는 재래식 무기를 이용한 공격보다 훨씬 그 결과를 예측하기 어렵다.

4. 구별의 원칙

무력충돌의 당사국은 항시 민간주민과 전투원, 민간물자와 군사목표물을 구별하며, 그들의 작전은 군사목표물에 대하여만 행해지도록 해야 한다.[68] 그러므로 군지휘관은 목표물을 정확하게 공격할 수 있는 무기를 사용해야 하며, 이를 이용하여 민간목표물과 군사목표물을 구별해야 한다. 전투원은 합법적으로 적대행위에 참가할 수 있으며, 합법적인 공격의 대상이 된다. 전투원은 국가의 통제 아래에 있는 모든 군대, 단체 등으로 구성된다. 전투원은 어느 정도 조직되거나 지휘체계를 필요로 한다.

마찬가지로 통제가 불가능하거나 예상할 수 없는 사이버공격, 민간목표물과 군사목표물을 구별할 수 없는 사이버공격은 금지된다. 민간인의 생존에 필수불가별한 물건에 대한 공격도 금지된다. 이러한 논리에 따르면 사이버공격으로 군사용 비행장의 관제시스템을 마비시키는 것은 허용되지만 민간은

67) 1949년 제네바협약에 대한 추가 및 국제적 무력충돌의 희생자 보호에 관한 의정서(제1 추가의정서), 제51조 5호.
68) 제네바협약 제1 추가의정서 48조.

행, 병원, 박물관 등의 컴퓨터나 네트워크에 장애를 일으키는 것은 허용되지 아니할 것이다. 문제는 대부분의 군사용 네트워크가 민간 네트워크를 이용하므로 민간 네트워크에 대한 공격이 군사적인 이익을 가질 수 있다는 점이다.

무력충돌법에 따르면 전투원, 적대행위에 직접적으로 참가하는 민간인,[69] 계속적으로 전투 기능을 수행하는 민간인이 합법적인 공격의 대상이 된다. 민간인이 사이버공격에 참가하거나 계속적으로 사이버공격을 수행하면 합법적인 공격의 대상이 되는가 여부가 문제된다. 일반적으로 무기를 설계하는 사람은 직접적으로 적대행위에 참여하는 사람으로 보기 어렵다. 그러나 사이버공격에 정기적으로 참여하는 민간인은 직접적인 적대적 행위에 참가하는 것으로 보는 견해가 강하다. 사이버 공격은 신속하고 은밀하게 이루어지므로 피해국이 사이버공격의 경로를 파악하기까지 상당한 시간이 걸릴 수 있다. 개인이 사이버공격을 하는 동안에 적법한 공격의 목표물이 될 수 있지만 그 개인이 더 이상 적대적인 행위를 하지 않으면 무력충돌법에 따라 보호되는 민간인의 지위를 회복하게 된다.

무력충돌의 당사자가 민간인을 이용하여 전투를 수행할 경우에는 민간인을 합법적인 공격의 대상으로 만들게 되므로 구별의 원칙이 무의미하게 된다. 그런데, 국가들은 사이버공격에서 더욱 민간인을 이용할 가능성이 높다. 민간인은 공무원이 갖지 못한 전문적인 기술을 가질 가능성이 높으며,[70] 민간인을 이용함으로써 사이버공격의 주체를 숨길 수 있다.[71]

5. 중립의 원칙

국가는 무력충돌에 대하여 중립을 선언할 수 있다. 중립국은 교전에 참여하지 않거나 자신의 영토가 군사적 목적으로 사용되는 것을 허용하지 아니하는 한 보호된다. 헤이그협약에 따르면 중립국은 중립국으로서 권리와 적대행

69) 제네바협약 제1 추가의정서 51조 3호.
70) Oona A. Hathaway, supra note 10, p. 854.
71) Ibid.

위에 참여하지 아니할 의무가 있으며, 교전당사국은 중립국의 중립을 존중할 의무가 있다.

사이버공격은 중립국에서 오는 것처럼 보이거나 실제로 중립국에서 올 수 있다. 일부의 견해는 중립국이 자신의 통신시설을 교전국이 이용하지 못하도록 할 의무가 있는 것은 아니지만 교전국이 중립국 내에 그러한 시설을 설치하는 것을 돕거나 허용해서는 아니 된다고 주장한다. 다른 견해는 중립국이 자국의 영토에서 기인하는 사이버공격을 막지 않거나 막을 의사가 없는 경우에는 합법적인 공격의 대상이 될 수 있다고 본다. 이들의 견해에 따르면 중립국은 스스로 사이버공격을 하지 아니할 의무가 있을 뿐만 아니라 자신의 영토가 타국의 권리를 침해하는데 이용되는 것을 방지할 의무가 있다.

타국에 있는 컴퓨터, 일명 좀비 컴퓨터를 이용하여 제3국에 사이버공격을 하는 경우에 당해 컴퓨터의 소유자는 물론 그 컴퓨터가 존재하는 국가는 이러한 사실을 알기 어렵다. 사이버공격에 자국 내의 컴퓨터가 이용되는 경우에 당해 국가는 이러한 사실을 알기 어려우며, 스스로 중립의 원칙을 위반하고 있다는 사실도 알기 어렵다. 공격이 어디에서 기인하는가 여부는 중립의 원칙을 위반하였는지 여부를 판단하는데 매우 중요하지만 이에 대한 판단이 사실상 매우 어렵다.

Ⅵ 결 론

국가들이 사이버공격에 취약하다는 점은 분명하게 드러난다. 국가의 중요한 산업에 대한 사이버공격은 점차적으로 그 범위를 넓혀 가고 있다. 사이버공격의 위험이 급속도로 높아지고 있음에 반하여 그에 대한 법적인 대응은 아직 미흡하다.[72] 오늘날의 무력사용금지의 원칙이나 자위권에 관한 국제법은 물리적인 무력사용과 무력공격의 개념에 기초한 것으로 사이버공격을 규

72) Hathaway, supra note 10, p. 885.

제하기에는 대단히 부적합한 것이 사실이다. 그러므로 사이버공격을 직접적으로 규제하기 위한 법적 장치가 필요한 시점이다. 사이버공격을 규제하기 위한 국제법 규제가 기존의 국제법과 완전히 다른 것일 수 는 없다. 기존의 무력사용금지원칙 및 자위권의 개념 안에서 일부 사이버공격의 특성을 고려해야 할 것이다. 사이버공격을 직접적으로 규제하기 위한 국제법적 장치가 별도로 존재하지 아니하는 상태에서는 기존의 국제법적 질서 안에서 사이버공격을 이해할 수밖에 없을 것이다.

제6장 사이버공격과 사이버안전보장을 위한 대응법제

사이버공격과 통합방위법의 공법적 문제

황 창 근*

목 차

Ⅰ 들어가는 글

통합방위법(United Defense Act)은 적의 침투·도발이나 그 위협에 대응하기 위하여 국가 총력전의 개념에서 국가방위요소를 통합·운용하기 위한 필요한 사항을 규정함을 목적으로 하고 있다(제1조). 이 법은 1997. 1. 13. 제정되었는데,[1] 그 이전에는 1995. 1. 1. 제정된 「통합방위지침」(대통령훈령 제26호)이 같은 역할을 하고 있었다. 이 훈령은 3급비밀로 분류되어 있어서 일반에게 공개된 법령은 아니었다.

통합방위법이 제정된 이유는 3가지 정도로 요약할 수 있는데, 첫째 당시 대통령훈령인 통합방위지침은 3급비밀로서 비공개된 상태였기 때문에 민관군의 제반 국가방위요소의 통합의 근거를 공개할 필요가 있었고, 둘째 통합

* 홍익대학교 법과대학 교수

1) 통합방위법안의 제정 연구에 대하여는 장병옥외, (가칭)통합방위기본법 일반법률(안) 연구, KIDA, 1996. 참조할 것

방위는 민관군 및 향토예비군, 민방위대원 등 국가의 제반 방위요소를 통합하여 운영함에 있어서 기본권 제한요소가 있음에도 불구하고 대통령훈령으로 제한하는 것은 문제가 있으므로 법률상 근거가 필요하고, 통합방위작전에 있어서의 관할구역안의 지휘·통제권의 일원화를 보장하기 위한 법적 근거가 필요하였으며, 셋째 1996. 9. 18. 이후 수행한 강릉 대침투사건[2]의 작전상 교훈으로 통합방위작전의 실효성을 보장하기 위함이 그것이다.[3]

통합방위법의 기본 구조를 보면, 통합방위와 통합방위사태를 기본개념으로 하여 통합방위사태의 선포, 통합방위작전의 훈련 및 수행, 통합방위정책의 수립 및 통합방위기구의 설치 및 운영, 국가중요시설 및 취약시설의 관리 등으로 구성되어 있다.

이 논문은 통합방위법을 중심으로 기본내용을 분석한 다음, 적에 의한 사이버공격이 있는 경우 통합방위법을 적용할 수 있는지의 관점에서 통합방위법상 통합방위의 개념, 통합방위사태, 통합방위작전, 제반 방호작용 등을 살펴보고자 한다. 따라서 사이버공격과 관련한 개념이나 법제에 대하여는 기존의 논의로 대체하고 상세한 내용은 생략하기로 한다.

Ⅱ 통합방위법의 주요 내용

1. 통합방위법의 입법 목적

1997년 제정 당시는 강릉 잠수함 침투가 있는 직후로, 이를 계기로 대간첩작전의 효율적 수행을 도모하기 위하여 통합방위 관련기구의 설치 및 민관군 방위요소의 통합적 운용을 위한 법적 근거로 도입되었다. 당시에는 모법

2) 1996. 9.18. 강릉 해안가에 발견된 북한 잠수함 사건으로서 그해 11. 5.까지 49일간 소탕작전이 수행된 사건이다. 당시 군은 진돗개1을 발령하고 강원도 전역에 통합방위태세 '을종'을 선포하여 예비군을 동원하고 통행금지를 단행하였다. 이 작전에서 1명 생포, 13명 사살, 11명 살해된 채 발견.

3) 국회 국방위원회, 통합방위법안 심사보고서, 1996.12. 4면

의 근거 없이 '통합방위지침'(대통령훈령 제26호)으로 대간첩작전이 이루어지고 있었다.

통합방위법의 헌법적 근거로는 국가안보 또는 질서유지를 예상할 수 있는데, 통합방위법은 평시에서 적의 침투로부터 국가를 보위하기 위하여 국가방위요소를 통합하여 운영하는 법적 근거를 제공한 것으로서, 헌법상 국가안보를 위한 입법이고 적에 의한 테러 등에 대응하기 위한 질서유지의 성격도 함께 가지는 것으로 보인다.

2. 통합방위법의 법적 성격 및 지위

(1) 국가안보법

통합방위법은 민관군의 국가방위요소[4]를 통합적으로 운영하기 위한 국가안전보장법의 성격을 가진다. 국가안보를 위하여는 다양한 법제 중에서 특별히 통합방위법이 가지고 있는 역할과 필요성에 대한 이해가 필요하다. 국가안보는 1차적으로 군의 임무라고 할 것인데, 민관군의 경우에도 국방의 의무를 전제로 하여 국가안보 임무를 수행할 의무가 있다고 할 것이므로 이와 같은 제반 방위요소를 통합하여 국가방위의 실효성을 제고하기 위하여 이 법률을 제정한 것으로 보인다. 이 법의 목적을 규정한 제1조에서 '국가 총력전'이라는 개념을 사용하고 있는 것이 그러한 이유이다. 국가안보법으로서 통합방위법은 군 이외에 다른 행정기관, 민간과의 통합, 협력 등의 행정응원법으로

4) 제2조(정의)
2. "국가방위요소"란 통합방위작전의 수행에 필요한 다음 각 목의 방위전력(防衛戰力) 또는 그 지원 요소를 말한다.
가. 「국군조직법」 제2조에 따른 국군
나. 국민안전처·경찰청 및 그 소속 기관과 「제주특별자치도 설치 및 국제자유도시 조성을 위한 특별법」에 따른 자치경찰기구
다. 국가기관 및 지방자치단체(가목과 나목의 경우는 제외한다)
라. 「예비군법」 제1조에 따른 예비군
마. 「민방위기본법」 제17조에 따른 민방위대
바. 제6조에 따라 통합방위협의회를 두는 직장

서 의미가 있다.

국가안보법은 먼저 조직법과 작용법의 성격에 따라 ① 조직법 성격으로 국군조직법, 군인사법, 병역법, 예비군법, 민방위법 등이 있고, ② 작용법 성격으로 국가보안법, 통합방위법, 방위사업법, 군사기밀보호법, 군형법, 군사법원법, 「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」 등이 있다.

국가안보법 중 사이버안보와 관련하여서는 정보통신기반 보호법, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법이라 함), 「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」, 국가사이버안전관리규정(대통령훈령) 등이 있다.

(2) 경찰법

통합방위사태는 '적'의 침투나 도발, 위협으로부터 방위하기 위한 것이지만, 이는 전면전에 이르지 아니한 상태에서의 적 도발에 대비하여 치안유지를 위한 목적도 있는바 특히 병종사태의 경우에는 지방경찰청장의 지휘·통제 하에 통합방위작전을 수행하여 단기간 내에 치안을 회복하도록 하고 있으므로 치안유지 목적의 경찰행정의 성격도 함께 가지고 있다고 할 것이다.

통합방위작전 또는 경계태세가 발령이 되면 일반인의 출입을 금지·제한하거나 그 통제구역으로부터 퇴거할 것을 명할 수 있고(제16조), 시·도지사 등은 통합방위사태가 선포된 때에는 인명·신체에 대한 위해를 방지하기 위하여 즉지 작전지역에 있는 주민이나 체류중인 사람에 대한 대피명령을 할 수 있으며(제17조), 군경합동검문소의 운용(제18조) 및 불심검문(제15조 제5항, 동시행령 제26조)을 규정하고 있다. 이러한 내용은 국가안보 측면의 기본권 제한과 동시에 일반적인 경찰작용의 성격도 가지는 것으로 보인다. 특히 군경합동검문소의 경우에는 예방경찰작용의 근거인 동시에 군의 민간인에 대한 기본권 제한의 근거가 되기도 한다.

(3) 국가긴급권제도 내지 국가위기관리법제와의 관계

통합방위법은 적의 침투, 도발 또는 그 위협 등 국가위기시 발령된다는 점

에서 그리고 통합방위사태로 규정한 갑종사태, 을종사태, 병종사태 등은 헌법이 규정하고 있는 계엄 등의 국가긴급권제도와 유사한 점이 발견되어 그 관계를 살펴볼 필요가 있다. 대한민국 헌법에서는 대통령이 발하는 1) 내우・외환・천재・지변 또는 중대한 재정・경제상의 위기에 있어서 국가의 안전보장 또는 공공의 안녕질서를 유지하기 위하여 긴급한 조치가 필요하고 국회의 집회를 기다릴 여유가 없을 때에 한하여 최소한으로 필요한 재정・경제상의 처분 또는 이에 관하여 발하는 법률의 효력을 가지는 명령(제76조 제1항), 2) 국가의 안위에 관계되는 중대한 교전상태에 있어서 국가를 보위하기 위하여 긴급한 조치가 필요하고 국회의 집회가 불가능한 때에 한하여 발하는 법률의 효력을 가지는 명령(제76조 제2항), 3) 전시・사변 또는 이에 준하는 국가비상사태에 있어서 병력으로써 군사상의 필요에 응하거나 공공의 안녕질서를 유지할 필요가 있을 때에는 법률이 정하는 바에 의하여 발하는 계엄령(제77조)을 들 수 있다. 위 국가긴급권 제도의 발령 상황을 보면 크게 다른 것 같지 않지만, 그 긴급권제도의 규범형식은 헌법이 자체적으로 인정한 법률대위명령이나 처분, 계엄법에 근거한 계엄령으로 엄격히 규정하고 있고, 일반 법률에 의하여 국가긴급권제도의 형성이나 시행을 예정하고 있지 아니하다. 그런 점에서 보면 통합방위사태에 직면하여 통합방위훈련 등의 제반 작용을 행하는 근거인 법률은 헌법상 국가긴급권제도의 시행 단계에 이르지 아니하는 것임을 알 수 있다. 최초 법률의 제정 당시에는 갑종비상사태를 계엄선포사태를 전제로 하고 있어서 우려가 있었으나,[5] 당시 국방부장관은 계엄시의 기본권 제한, 사법권, 행정권의 제한은 있을 수 없음을 분명히 하고 있다.

한편, 통합방위법은 국가위기관리법제의 하나이다. 통합방위사태는 국가위기사태의 일종인 것이다. 국가위기사태에 대응하기 위한 법령으로는 계엄법, 비상대비자원관리법, 징발법, 병역법, 예비군설치법, 통합방위법, 재난

5) "갑종사태"란 대규모의 적의 침투, 도발 또는 이에 준하는 국가비상사태로서 계엄법에 의한 계엄을 선포하고 계엄사령관의 지휘・통제 하에 통합방위작전을 수행하여야 할 사태를 말한다.

및 안전관리 기본법, 자연재해대책법, 민방위기본법, 소방기본법, 국민보호와 공공안전을 위한 테러방지법, 국방부위기관리규정, 국가대테러활동지침 등이 있다. 국가위기의 개념은 체계적으로 구축된 것이 아니라 그 때 그 때 사정에 따라 제정된 것으로서 각 법령간에 체계적합성을 갖추지 못하고 있어서 통합된 법령을 제정하여 조직, 자원, 조치 및 기능 등에 관한 기준과 원칙을 정할 필요가 있다는 주장도 있다.[6][7]

3. 통합방위의 개념

통합방위의 상황 요건에 대하여 "적의 침투·도발이나 그 위협"에 대응하는 것으로 명문으로 규정하고 있다(제2조 제1호). 최초 제안한 법률안에서는 '적의 침투·도발이나 그 위협' 이외에 '우발상황'까지 포함하고 있었으나 제정당시에 요건의 광범위성을 우려하여 '우발상황'은 삭제하고 제정하였다.[8] 특히 '위협'에 대하여는 제정당시부터 그 요건이 지나치게 광범위하다는 지적이 있었다. 이에 대하여 당시 국방부장관은 위협이라는 것은 일반적인 위협이 아니라 '적의 침투·도발'과 직접 관련이 있는 것으로 한정하는 것이라고 답변하고 있다.[9]

여기서 "침투"란 적이 특정 임무를 수행하기 위하여 대한민국 영역을 침범한 상태를 말하고, "도발"이란 적이 특정 임무를 수행하기 위하여 대한민국 국민 또는 영역에 위해를 가하는 모든 행위를 말하며, "위협"이란 대한민국을 침투·도발할 것으로 예상되는 적의 침투·도발 능력과 기도가 드러난 상태를 말한다. 그리고 "방호"란 적의 각종 도발과 위협으로부터 인원·시설 및 장비의 피해를 방지하고 모든 기능을 정상적으로 유지할 수 있도록 보호

6) 주성빈·최응렬, "국가 통합위기관리체계의 구축방안에 관한 연구", 한국경호경비학회 제34호, 2013, 302면
7) 19대 국회당시 한기호 의원이 '국가위기관리기본법안'을 대표발의한 바 있다(2012. 11. 20).
8) 통합방위법안 제2조 제1호
9) 국회 국방위원회, 통합방위법안 심사보고서, 12면.

하는 작전 활동을 말한다(이상 제2조).

4. 통합방위사태와 통합방위작전

통합방위사태란 적의 침투·도발이나 그 위협에 대응하여 각 단계별로 구분하여 선포하는 사태를 말하고, 현행법상 갑종사태, 을종사태, 병종사태로 구분한다. 그리고 이와 별도로 군부대의 장 및 경찰관서의 장은 적의 침투·도발이나 그 위협이 예상될 경우 통합방위작전을 준비하기 위하여 경계태세를 발령할 수 있는 것으로 규정하고 있다(제11조). 경계태세는 다시 3급, 2급, 1급으로 구분하고 있다(동시행령 제22조). 통합방위작전이란 통합방위사태가 선포된 지역에서 제15조에 따라 통합방위본부장, 지역군사령관, 함대사령관 또는 지방경찰청장(이하 "작전지휘관"이라 한다)이 국가방위요소를 통합하여 지휘·통제하는 방위작전을 말한다.

[통합방위사태 및 경계태세의 분류]

구분	정의
갑종사태	갑종사태란 일정한 조직체계를 갖춘 적의 대규모 병력 침투 또는 대량살상무기(大量殺傷武器) 공격 등의 도발로 발생한 비상사태로서 통합방위본부장 또는 지역군사령관의 지휘·통제 하에 통합방위작전을 수행하여야 할 사태를 말한다.
을종사태	을종사태란 일부 또는 여러 지역에서 적이 침투·도발하여 단기간 내에 치안이 회복되기 어려워 지역군사령관의 지휘·통제 하에 통합방위작전을 수행하여야 할 사태를 말한다.
병종사태	병종사태란 적의 침투·도발 위협이 예상되거나 소규모의 적이 침투하였을 때에 지방경찰청장, 지역군사령관 또는 함대사령관의 지휘·통제 하에 통합방위작전을 수행하여 단기간 내에 치안이 회복될 수 있는 사태를 말한다.
경계태세	적의 침투·도발이나 그 위협이 예상될 경우 통합방위작전을 준비하기 위하여 관할 군부대장 등이 발령하는 태세

5. 통합방위법의 행정체계

(1) 통합방위정책 및 작전 수행

통합방위업무는 정책수립과 작전수행으로 크게 나눌 수 있다. 통합방위정책의 심의권한은 국무총리가 의장이 되는 중앙 통합방위협의회에게 있고, 그 통합방위정책의 수립·조정 권한은 통합방위본부(합동참모본부)가 가지고 있다. 통합방위본부는 통합방위 정책의 수립·조정, 통합방위 대비태세의 확인·감독, 통합방위작전 상황의 종합 분석 및 대비책의 수립, 통합방위작전, 훈련지침 및 계획의 수립과 그 시행의 조정·통제, 통합방위 관계기관 간의 업무 협조 및 사업 집행사항의 협의·조정 등의 사무를 분장한다(제8조 제3항). 따라서 통합방위정책의 소관기관은 통합방위본부 업무를 수행하는 합동참모본부에게 있다고 할 것이다. 통합방위협의회는 중앙 통합방위협의회(의장 국무총리), 지역 통합방위협의회, 직장 통합방위협의회로 구분되며 지역 통합방위협의회는 시·도협의회, 시군구 통합방위협의회로 구분된다.

통합방위작전은 지방경찰청장, 지역군사령관 또는 함대사령관이 관할구역에 따라 통합방위사태가 선포된 때에는 이를 신속하게 수행하고, 다만, 을종사태가 선포된 경우에는 지역군사령관이 통합방위작전을 수행하고, 갑종사태가 선포된 경우에는 통합방위본부장 또는 지역군사령관이 통합방위작전을 수행한다(제11조).

(2) 지방자치단체의 통합방위업무의 성격

통합방위법은 민관군의 제반 국가방위요소를 통합 운용하기 위한 체제이므로 지방자치단체도 위와 같이 통합방위기구인 통합방위협의회를 구성하여 운영하고 있는데, 이 업무의 성격이 국가사무인지 자치사무인지 법적 성격이 문제가 된다. 국가사무인지 자치사무인지 구별 실익은 관리주체, 지방의회의 관여, 조례제정,[10] 비용부담, 사무수행의 자율성과 국가의 감독, 감독기관의

10) 통합방위법시행령은 지역협의회의 구성 등에 관한 조례기준안을 제정하여 제시하고

감사, 국가배상법상 배상책임자 등에서 차이가 난다.[11] 지방자치법에 의하면 지방자치단체의 사무를 예시하고 있는 제9조에서는 지역민방위 및 지방소방에 관한 사무(제6호)를 규정하고 있지만 통합방위사무는 규정하고 있지 아니하고, 한편 지방자치단체는 국방 등 국가존립에 관한 사무는 처리할 수 없는 것을 원칙으로 하고 다만 법률에서 달리 규정하면 처리할 수 있는 것으로 규정되어 있다(제11조 제1호). 통합방위의 목적은 제1조에서 보는 바와 같이 현행법상 '적의 침투·도발 및 그 위협'에 대응하기 위한 것이므로 국방사무(병종사태의 경우에는 치안사무)에 해당되고, 이와 같은 국방사무는 통합방위법이라는 예외 법률에 의한 국가사무 처리에 해당된다고 할 것이다.[12]

6. 통합방위법의 주요 행정작용과 그 효력

(1) 각급 행정청의 구속

통합방위법은 적의 침투·도발이나 그 위협 시에 적용되는 법률로서, 국가의 방위요소를 통합하여 운용하기 위하여 제정된 법으로서 국가방위요소인 국군, 국민안전처, 경찰, 국가기관 및 지방자치단체, 예비군, 민방위대, 통합방위협의회를 두는 직장이 수범대상이 된다. 즉 다양한 국가기관의 방위요소를 통합하여 운영하기 위한 것이므로 근본적으로 각급 행정청을 구속하는 법규로서 성격을 가진다.

통합방위법은 일응 통합방위사태 시의 작전 수행을 위한 체계를 구성한 것이므로 관계 행정기관만을 구속하는 것으로 이해할 수 있지만, 동법에 의하여 동원되는 예비군, 민방위대원 등 민관군 제반 방위요소에 효력이 모두 미친다고 할 것이다. 앞서 본 바와 같이 각 통합방위사태에 대응한 작전수행시

있다(제8조). 이에 따라 각 지방자치단체는 일명 '통합방위협의회 구성 및 운영 등에 관한 조례'를 제정 시행하고 있다.

11) 박균성, 행정법강의, 제9판, 2012, 1016면

12) 통합방위에 대한 사무를 지방자치법상 지방자치단체의 사무(제9조)로 개정하여야 한다는 견해가 있다. 정원영, 지방자치의 통합방위, 한국국방연구원, 2000, 95면

강제적인 동원 등의 기본권제한이 불가피하게 따르는 것이므로 단순한 행정청의 내부 조직규범으로만 해석할 수 없다고 할 것이다. 따라서 기본권제한 법률유보로서의 엄격한 검토가 필요한 법체계라고 할 것이다.

(2) 국민의 기본권 제한 입법

통합방위사태 또는 경계태세가 발령이 되면 그 부수적인 효과로 일반 국민에게 영향을 미치는 다양한 공권력작용이 나타나게 된다. 통합방위사태 또는 경계태세는 그 자체적으로 국민의 기본권을 제한하거나 행정, 사법상의 권한을 제한하는 등의 조치를 수반하는 것은 아니다. 그런 의미에서 헌법 또는 계엄법상 계엄과는 거리가 멀다. 그러나 통합방위작전의 수행을 위하여 다양한 방법으로 공권력이 발동되고 그 범위내에서 국민의 기본권이 제한되게 된다. 그런 의미에서 통합방위사태 또는 통합방위작전시 국민의 기본권을 제한하기 위하여 법률의 근거를 요하게 되는 것이다. 통제구역에의 출입 금지 등(제16조), 대피명령(제17조), 검문소의 운용(제18조), 신고의무(제19조) 등이 그러한 예이다.

(3) 통합방위법의 효력(범위)

통합방위법의 효력의 범위가 평시에만 미치는 것인지 전시에도 미치는 것인지 분명한 규정이 없다. 법률의 효력은 명문의 규정이 없는 한 평시이든 전시[13] 이든 달라질 것이 없는 것이고, 전시에 법률의 효력을 제한하기 위하여는 별도의 법률을 제정하는 것이 보통이다. 이를 전시 대비 법령이라고 한다. 만일 전시 대비 법령에서 통합방위법의 적용을 배제하는 규정이 없는 한 이 법은 전시에도 적용되는 것으로 해석하는 것이 타당하다. 학설에 의하더라도 통합방위법은 적의 침투, 도발은 전시위기인 동시에 평시의 국지도발을 포함하는

13) 전시의 개념은 국제법적으로 이해할 수 있지만, 우리나라 현행법이 규정하고 있는 전시의 개념은 다음과 같다. “전시”란 상대국이나 교전단체에 대하여 선전포고나 대적(對敵)행위를 한 때부터 그 상대국이나 교전단체와 휴전협정이 성립된 때까지의 기간을 말하고(군형법 제2조 제6호), “사변”이란 전시에 준하는 동란(動亂)상태로서 전국 또는 지역별로 계엄이 선포된 기간을 말한다(군형법 제2조 제7호)

개념이라고 할 것이어서 전시와 평시에 모두 적용된다고 보고 있다.[14]

Ⅲ 사이버공격 대비 통합방위법의 주요 쟁점

1. 논점의 제기

통합방위법은 적의 침투나 도발로부터 국가를 보위하기 위한 국가안보법의 성격을 가지고 있으며, 그를 위하여 제반 국가방위요소를 통합하는 총력전의 개념에서 고안된 법률이다. 한편 전통적인 적의 침투나 도발은 물리적인 것을 전제로 하고 있고, 물리적인 침투나 도발은 지상이나 해상, 공중 등 일정 지역을 전제로 한 개념이다. 그에 따라 통합방위법 상의 통합방위사태와 통합방위작전은 물리적인 지역을 전제로 하여 구성되어 있다. 따라서 최근 빈발하고 있고 향후 중요한 침투방법으로 예상되는 사이버공격을 통합방위법과 어떤 방식으로 연계할 것인가의 문제는 통합방위법의 원래의 입법목적 뿐만 아니라 장차 적의 침투, 도발의 양상을 함께 고려하여야 하는 다층적인 쟁점을 가지고 있다.

우선, 사이버공격에 의한 적의 침투, 도발 및 위협의 방식을 통합방위법상 적의 침투, 도발 등으로 볼 것인지, 둘째 만일 사이버공격을 적의 침투, 도발의 공격양상에 포함할 경우 현재의 통합방위훈련 및 통제방식이 적합한 것인지 그리고 적합하지 않다면 어떤 방식으로 개편하여야 하는지, 셋째 입법방식으로 사이버공격이 적의 침투, 도발의 새로운 방법으로 예상되는 경우 국가총력전을 규정한 현행 통합방위법을 중심으로 이를 논할 것인지 아니면 사이버 버전의 새로운 '사이버 통합방위법'을 제정할 것인가 하는 점 등이 논의되어야 한다.

14) 류상일・정찬권・김태진, "국가위기관리 법령 분석 및 시사점", 한국위기관리논집 제11권 제4호, 2015.4, 11면 ; 김충묵・김창수, "군사행정법상 읍면동 통합방위제도의 개선방안", 국가법연구, 제9권 제1호, 2013, 137면

2. 사이버공격은 적의 침투·도발 및 그 위협에 해당되는지

(1) 국가위기사태의 개념 비교

국가위기사태는 전시와 평시, 자연재난과 사회재난, 국가비상사태·계엄·민방위사태·통합방위사태 등 다양한 측면에서 논의되어 상호 중복이나 공백이 발생되고, 해당 사태에 적용되는 법률도 상이하여 그 법률의 적용범위를 정하는 것도 쉽지 않다. 해당 법률에 따라 소관 중앙행정기관도 달라 행정에 있어 충돌과 공백도 발생될 수 있다. 또한 전시와 관련하여 전시에 적용되는 전시법령과 평시법령의 적용과 상호간 연계도 분명하지 않아 혼란이 발생된다.[15]

통합방위사태의 대상인 '적의 침투·도발 및 그 위협'과 사이버공격, 사이버테러 또는 국가재난사태의 개념 사이에 그 구분이 명확하지 아니하다. 각자 용법의 목적이 다르기는 하지만 나타나는 현상이나 결과 차원에서 본다면 그 구분이 반드시 분명한 것이 아니다.

국가사이버안전관리규정(대통령훈령)에 의하면 사이버공격과 사이버위기를 규정하고 있다. 사이버공격은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말하고, 사이버위기란 이와 같이 사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 말한다고 규정하고 있다(국가사이버안전관리규정 제2조). 한편 사이버테러란 통상적으로 정부나 시민을 위협하는 목적으로 사이

15) 우리나라 국가위기관리법령의 문제점을 다음과 같이 분석하고 있다. 첫째 용어규정에서 법령별 위기개념이 상이하고, 둘째 위기적용상 전시법령과 평시법령이 연계되어 있지 아니하며, 셋째 단계별 위기관리 활동의 연계가 부족하고, 넷째 위기관리체계가 분산되어 있다는 것이다. 류상일·정찬권·김태진, 전게논문, 21-24면

버 툴(tool)을 이용하여 에너지, 수송, 공공시설 등 주요 국가 기반시설을 중지시키려고 하는 행위를 말한다.[16]

이처럼 사이버공격이나 사이버테러가 적에 의하여 이루어진 경우에 이를 통합방위의 대상인 '적의 침투·도발 및 그 위협'으로 볼 수도 있는 것이고, 사이버공격과 사이버테러의 구분도 분명하지 아니하며, 나아가 「재난 및 안전관리 기본법」에 의하면 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비를 사회재난의 한 종류로 정의하고 있기 때문에(제3조 제1호 나목) 사이버테러도 국가재난에 해당될 수도 있다.[17]

또한, 이 적의 침투, 도발 또는 위협이라는 상황은 국가위기관리의 개념과 관련하여 해석할 수도 있다. 「국가위기관리 기본지침」(대통령훈령)에 의하면 국가위기를 국가의 주권, 국가의 핵심요소(정치, 경제, 사회, 문화체계), 국가가 지향하는 핵심가치에 위해가 가해질 가능성이 있거나 가해지고 있는 상태라고 정의하고 있고, 국가위기를 전통적 안보분야(북한관련 위기, 외부관련 위기, 내부 위기), 재난 분야(자연재난, 인적 재난), 국가핵심기반 분야(에너지, 식용수, 보건의료, 금융, 수송, 사이버)로 구분하고 있다.

(2) 사이버공격에 의한 적의 침투나 도발, 위협이 인정되는지

통합방위법상 적의 침투, 도발 및 그 위협이라는 요건은 3가지의 개념요소로 구성되어 있다. 첫째 주체요소로서 적(敵)에 의한 것이어야 하고, 둘째 행위요소로서 침투, 도발 및 위협이 있어야 하며, 셋째 장소요소로서 적의 침투, 도발 및 위협이 일정한 지역을 전제로 한다는 점이다. 따라서 사이버공격을 통합방위법상 적의 침투, 도발 및 위협에 해당되는지 판단하기 위하여는 이러한 개념요소별 검토를 요한다.

첫째, 사이버공격이 적(敵)에 의한 것이어야 한다. 적(敵)이란 사전적으로

16) 곽병선, "사이버테러 대응을 위한 법체계 검토", 법학연구 제59집, 한국법학회, 2015, 1면.
17) 윤해성 등, 사이버안전체계 구축에 관한 연구, 한국형사정책연구원, 2010, 264면

'서로 싸우거나 해치고자 하는 상대'[18]를 말하는데, 법률상 분명한 정의규정은 없다. 다만 형법에서는 제2장 외환의 죄에서 '적국' 및 '준적국'이라는 용어를 사용하고 있는데, 적국이란 적 중에서 '국가의 형태를 띤 적'을 대상으로 하는 것이다.[19] 준적국을 규정한 제102조에서 대한민국에 적대하는 외국 또는 외국인의 단체는 적국으로 간주한다고 하여 국가가 아닌 단체의 경우에도 외환의 죄를 적용토록 하고 있다. 적국의 개념에 대하여는 대한민국과 국제법상 선전포고를 하고 전쟁을 수행하는 국가에 국한된다는 견해와 사실상 전쟁을 수행하는 국가를 의미한다고 견해의 대립이 있다.[20] 그렇다면 통합방위법상의 적의 개념과 형법상 적국, 준적국의 개념은 실질적으로 차이를 발견하기 어렵다고 보인다. 따라서 통합방위법상의 적이란 개념에는 적국, 준적국을 포함하여 우리나라와 싸우거나 해치고자 하는 상대방이면 모두 포함되는 개념이라고 할 것이다.

둘째, 행위요소로서 적의 침투·도발 및 그 위협에 사이버공격을 포함할 수 있는가 하는 점이다. 통합방위법상 침투란 대한민국 영역을 침범한 상태를 말하고, 도발이란 대한민국 국민 또는 영역에 위해를 가하는 모든 행위를 말하는 것이며, 위협이란 그와 같은 침투·도발 능력과 기도가 드러난 상태를 말한다고 규정하고 있다. 적어도 위협의 경우에는 침투나 도발의 능력과 기도가 드러난 상태라면 물리적인 것 이외에 사이버상의 위협도 충분히 해석상 가능하다고 할 것이므로, 침투나 도발의 경우에도 사이버상의 침투나 도발이 인정될 것인가 하는 점이다. 학설의 대립이 있다. 적극설은 통합방위법이 물리적인 침투나 도발로 전제하지 않고 있으며 사이버공격이 기반시설에 대하여 이루어지는 경우 대한민국의 영역을 침범한 것으로 볼 수 있으며 방호활동도 물리적인 것뿐만 아니라 사이버상의 작전활동 등을 포함하여야 한

18) 네이버사전
19) 제93조 여적죄, 제94조 모병이적죄, 제95조 시설제공이적죄, 제96조 시설파괴이적죄, 제97조 물건제공이적죄, 제98조 간첩죄, 제99조 일반이적죄가 그것이다.
20) 박재윤 편집대표, 주석형법-형법각칙(1), 제4판, 2006, 89면

다는 것이다.[21] 이에 대하여 소극설은 단순한 해커에 의한 사이버공격과 국제법상 적에 의한 사이버공격을 구분하기 어렵고,[22] 통합방위법은 물리적 공격을 전제로 하는 것인데 이를 수반하지 않은 사이버공격은 포함하지 않은 것으로 보아야 한다는 것이다.[23] 최근 사이버공격에 대한 국제법적 논의가 활발한데, 탈린메뉴얼[24]에 의하면 무력충돌 상황에서 수행된 사이버작전은 무력충돌법을 따르게 되고, 사이버공격은 공격적인지 방어적인지 관계없이 사상자 또는 물적 손해 내지 파괴를 야기할 것이 합리적으로 예상되는 사이버작전으로서 공격에 해당되는 것으로 보고 있다. 즉 공격은 상대방에 대한 폭력을 의미하고 폭력의 존재 여부에 대한 판단은 폭력적 결과의 의미에서 고려되어야 하고 그 행위가 폭력적인지 여부는 중요하지 않다고 보고 있다.[25] 또한 사이버공격이 규모와 효과가 물리적 공격에 의한 무력사용의 수준에 준할 때는 이를 무력사용에 해당되는 것으로 본다.[26]

셋째, 통합방위사태와 통합방위작전은 지역적 개념을 전제로 하고 있다는 점을 들 수 있다. 적의 침투·도발 또는 그 위협이 있는 경우에 각 단계별 통합방위사태를 선포하게 되고 그에 따라 통합방위작전을 수행하게 되는데, 통합방위작전은 '통합방위사태가 선포된 지역'이라는 물리적 범위내에서 작전이 수행되고 있다. 그런데 사이버공격은 특정인의 컴퓨터나 전산시스템을 목표로 하거나 해킹을 시도하는 것으로서 그 특성상 특정지역으로 한정하여

21) 정준현, "국가사이버안전법제의 방향에 관한 연구", 법학논총 제39권 제4호, 299면
22) 정준현, 전게논문, 300면 ;
23) 김재광, "진화하는 사이버안보 위협과 법제적 대응방안", 인터넷법제포럼 제3차 월례회의, 자료집, 2016. 7. 20. 31면
24) 탈린매뉴얼(Tallinn Manual)은 사이버전쟁과 사이버 분쟁에 관한 95개 규칙이 정리된 국제법안을 말한다. 탈린이란 에스토니아 수도를 말하는데, 2007년 탈린에서 발생한 사이버공격 이후 NATO 산하 사이버방어센터가 사이버전쟁에 대한 연구를 하게 된 것에서 유래한다.
25) Michael N. Schmitt, 한국전자통신연구원 부설연구소(번역), 성재호, 김민호(감수), 「사이버전쟁에 적용가능한 국제법: 탈린매뉴얼」, 글과 생각, 2014, 117면, 158-159면.
26) 이정석·이수진, "북한 사이버공격에 대한 국제법적 검토를 바탕으로 한 국방 사이버전 수행 발전방향", 보안공학연구논문지, 제12권 제4호, 2015, 324면

침투 또는 도발이 존재하는 것으로 해석하기 어려운 점에서 지역적 범위를 정하여 상정한 통합방위사태나 통합방위작전의 개념은 적합하지 않은 것으로 보인다. 이에 따라 사이버공격으로 침투나 도발이 있는 경우에는 통합방위사태 중 어느 단계를 선택하여야 할지 사실상 어려울 것이고, 그렇다면 가장 범위가 넓은 갑종사태를 선택할 여지가 많을지도 모른다. 그러나 갑종사태는 사실상 국가비상사태에 준하는 대규모의 도발이나 침투가 벌어진 상황이기 때문에 국가나 사회가 받은 영향이 지대하므로 남용이나 악용은 금지된다는 점에서 모든 사이버공격에 적용하기는 곤란하다고 할 것이다.

(3) 소결

적의 침투·도발 또는 위협으로부터 발생되는 상황은 국가의 제반 방위요소를 통합하여 운영하여야 할 상황이라는 점에서, 그 침투나 도발을 반드시 물리적인 침투나 도발로 한정하여서는 안된다. 그와 같은 해석은 국가안보의 공백을 초래할 수도 있기 때문이다. 위에서 본 바와 같이 적에 의한 사이버공격이라면 사이버상의 침투나 도발, 위협이 있는 경우에 그것이 폭력적인 방법으로 행해진 것이 아니라고 하더라도 그 결과가 '폭력'적이라면 사이버공격에 해당된다고 보는만큼 적의 침투나 도발, 위협에 해당되는 것으로 보는 것이 타당한 것이다. 통합방위법의 제정자는 적의 침투나 도발의 유형을 굳이 물리적인 것인지 여부에 의하여 구분한 것이 아니라 일체의 물리적인 침투 등을 상정한 것으로 보인다. 다만 통합방위법 제정당시에는 현재와 같은 사이버공격이라는 침투수단의 중요성을 충분히 인식하지 못하였던 것이 아닌가 생각된다. 다시 말하면 입법의 불비 내지 공백이지 이를 두고 사이버공격을 배제한 것으로 이해하기는 곤란한 것이다(제한적 적극설).

그러나, 적의 침투 등에 사이버공격이 포함된다고 적극설을 취한다고 하여 바로 통합방위법을 적용할 수 있다는 것으로 연결할 수 없다. 통합방위법이 적의 침투·도발 또는 위협이라는 비상사태에 대비하기 위하여 만들어지고 일정 부분 행정기관은 물론이고 국민의 기본권을 제한하고 있는 사정을 고려

하여 본다면 통합방위법상 통합방위의 대상요건에 대한 해석, 적용은 법치행정원리상 확대해석이나 유추해석이 허용되어서는 곤란하다. 즉 이 법은 통합방위사태의 선포 및 그 작전 수행상 국민의 기본권이 직접적으로 제한되고, 특별한 경우에는 형사처벌 규정[27]까지 있으므로 엄격한 요건 구성이 필요하다고 할 것이다. 이를테면 적의 침투・도발 및 그 위협에 사이버공격을 명문으로 포함하고,[28] 사이버공격에 대응한 유효적절한 수단과 방법이 강구되어야 하는 것이다.

3. 통합방위법은 적의 사이버공격에 대비한 법률인가

(1) 사이버공격에 대한 대비 법제

북한의 사이버공격의 사례 및 양상에 대하여는 여기서 따로 논의하지 아니하고,[29] 법제에 대하여 보면 일반법은 존재하지 아니하고 분야별 또는 적용대상별로 개별법률들이 마련되어 있으나 법률간에 법체계 정합성 측면에서 문제점이 발견되며, 사물인터넷을 통한 융합서비스에서의 사이버공격에 대한 법제적 대응이 필요하다고 하고 있다.[30] 비교법적으로 보면 일본의 사이버시큐리티기본법의 제정, 미국의 국가사이버안보보호법의 제정 등의 움직임이 있다. 이에 대하여 19대 국회에서 수차례 입법안이 제출되었으며, 20대국회에도 유사한 내용의 가칭 '국가 사이버안보에 관한 법률안'이 제출되고 있으며,[31] 국가정보원도 가칭 국가사이버안보기본법을 제정 추진중에 있다고 한다.[32]

27) 제24조(벌칙)
① 제16조제1항의 출입 금지・제한 또는 퇴거명령을 위반한 사람은 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
② 제17조제1항의 대피명령을 위반한 사람은 300만원 이하의 벌금에 처한다.

28) <개정안> 제2조 1. "통합방위"란 적의 침투・도발이나 그 위협(사이버공격을 포함한다)에 대응하기 위하여 각종 국가방위요소를 통합하고 지휘체계를 일원화하여 국가를 방위하는 것을 말한다.

29) 자세한 내용은 김재광, 전게 발표자료, 8면 이하. 참조할 것

30) 김재광, 전게 발표자료, 24면.

31) 이철우 의원 대표발의(의안번호 2000032 2016-05-30 발의)

32) 중앙일보, "국정원, 사이버안보법 정부 입법 추진", 2016. 8. 3. 보도기사

국가 또는 사회 공동체의 존속과 유지의 기반이 되는 것이 안보정책이고, 그 사이버 버전이 사이버안보정책 내지 사이버안보법제라고 할 것이다. 사이버안보 또는 사이버보안, 사이버안전의 용어는 개념적으로 혼용되고 있다. 보안과 안보의 관계는 대체로 유사한 개념으로 보이지만 안보가 국가적・공공적 의미가 강조됨에 비하여, 보안은 상대적으로 민간 분야의 적용 내지 미시적 의미가 강하다고 할 것이며, 안전은 보안과 안보를 모두 포함하는 개념으로 이해할 수 있다. 따라서 사이버안보의 의미는 국가안보의 사이버 버전으로 이해하는 것이 타당하다. 그렇다면, 사이버안보법・정책의 범위는 행정 및 공공 부문에 적용되는 사이버 안전 관련 체계를 핵심으로 한다고 할 것이다. 다만 현행법체계에서 사이버안보에 일반적으로 적용되는 일반법 또는 기본법이 제정되어 있지 아니하고 각 분야별로 다양한 법령이 마련되어 시행되고 있다. 예컨대 정보통신망법, 정보통신기반 보호법, 전자정부법, 국가사이버안전규정, 군사기밀보호법 등이 대표적인 법령에 해당된다고 할 것이다.

(2) 적에 의한 사이버공격시 통합방위법의 적용 가능성

기술한 바와 같이 북한 등 적의 사이버공격도 적의 침투, 도발 또는 그 위협이 있는 경우에 해당된다고 볼 것이니, 통합방위사태의 발령 요건에 해당된다고 보인다. 그러나 실제 적에 의한 사이버공격 발생시 통합방위사태를 발령할 수 있을지는 해결하여야 할 과제가 많이 있다.

첫째, 기술한 바와 같이 통합방위사태 또는 통합방위작전을 수행하기가 사실상 어렵다는 점을 지적하고자 한다. 통합방위사태는 특정 지역을 기반으로 해당 지역군사령관의 지휘 통제하에 작전을 수행하는 것이기 때문이다. 즉 갑종사태에 해당하는 상황이 발생하였을 때 또는 둘 이상의 특별시・광역시・특별자치시・도・특별자치도(이하 “시・도”라 한다)에 걸쳐 을종사태에 해당하는 상황이 발생하였을 때는 국방부장관이 국무총리를 거쳐 대통령에게 통합방위사태의 선포를 건의하여야 하고, 둘 이상의 시・도에 걸쳐 병종사태에 해당하는 상황이 발생하였을 때는 행정자치부장관 또는 국방부장관

이 국무총리를 거쳐 대통령에게 통합방위사태의 선포를 건의하여야 한다(제12조 제2항). 또한 통합방위작전은 해당 통합방위사태가 선포된 지역을 중심으로 관할구역을 정하여 작전지휘관이 통합방위작전을 수행하도록 하고 있다(제15조). 이와 같이 통합방위사태의 선포나 작전은 지역적 범위를 전제로 하고 있는 점을 보면 사이버공격을 받는 지역적 범위를 정하여 통합방위사태를 선포하는 것이 사실상 어렵다는 것을 보여준다. 그리고 무엇보다도 사이버공격시 지역적 범위를 정하여 비상사태를 선포하고 작전을 수행하는 것은 사이버공격의 특성상 맞지 않다.

둘째, 사이버공격에 대응한 적절한 방호작용을 갖추고 있지 못하다. 현행법상 통제구역 등의 출입제한(제16조), 대피명령(제17조), 검문소의 운용(제18조), 신고의무(제19조), 통합방위훈련(제20조)을 하도록 규정되어 있는데, 이와 같은 훈련은 모두 물리적인 침투나 도발 등을 전제로 한 것으로 보이므로, 사이버공격이 이루어진 때의 방호방식으로는 적합하지 못하다. 따라서 사이버공격으로부터 국가안전을 보장하기 위한 다양한 정책수단을 개발할 필요가 있다. 기존의 정보통신망법이나 정보통신기반보호법 등에 유사한 내용이 규정되어 있고 특히 국가사이버안전관리규정에는 사이버위기라는 개념하에 사이버위기 대응훈련등이 규정되어 있어서 통합방위법 개선시에 충분히 참고할 수 있을 것이다.

4. 적의 사이버공격에 대비한 통합방위법제의 입법방법론

입법론은, 현행 통합방위법을 전면적으로 개정하는 방안과 통합방위법에 대응한 사이버버전 즉 (가칭) 사이버 통합방위법을 제정하는 방안 2가지로 논의할 수 있다.

(1) 통합방위법 개정 방식

사이버공격이 통합방위 대상요건에 포함된다고 하면, 사이버공격시 어떤 방식으로 통합방위사태를 선포하고 작전을 수행하고 기타 관련 작용을 구성

하여야 할 것인지 문제가 된다. 이 방안의 장점은 적의 침투, 도발 및 위협을 사이버공격까지 포함하여 일원적으로 규정, 처리한다는 것이고, 단점은 기존의 통합방위법이 물리적인 공격과 지역적 범위를 전제로 다양한 훈련과 방호방식을 고안한 것이므로 사이버공격에 전혀 어울리지 않는다는 점이고, 사이버공격에 대한 새로운 통합방위사태, 작전등을 고안하여야 한다는 어려움이 있고 결국 사이버공격에 대한 사태, 작전 등은 완전히 별개의 것이라는 점에서 완전한 단일법이라고 하기는 어려운 것이 아닌가 생각된다. 만일 단일법으로 구성할 경우에 염두해 두어야 할 내용인 통합방위사태, 통합방위작전, 관련 실효성 있는 방호작용에서 고민할 내용은 다음과 같다.

1) 통합방위사태의 구성

현행 통합방위사태는 갑종, 을종, 병종을 막론하고 지역을 전제로 하고 있으며, 물리적인 도발이나 침투의 경우에는 지역적 범위를 설정하는 것이 효과적인 것이므로 지역적 범위를 전제로 하는 현행 통합방위사태의 구분은 타당하다고 할 것이다. 그러면 적에 의한 사이버공격으로 도발 또는 침투하는 경우는 사이버공격의 특성상 지역적 범위를 설정하는 것이 어려우므로 전국적인 단위를 전제로 한 별도의 통합방위사태를 설정하는 것이 필요하다고 할 것이다. 이를테면 '사이버 통합방위사태'와 같은 것이다.

2) 통합방위작전의 구성

통합방위작전도 통합방위사태의 지역적 범위를 전제로 하여 관할구역을 지상, 해상, 공중으로 나누고 있고, 지방경찰청장·지역군사령관 또는 함대사령관 등이 통합방위작전을 수행하도록 되어 있다(제15조). 위와 같이 사이버공격에 의한 통합방위사태의 경우에는 작전지휘관을 따로 구성하는 것이 타당하다. 작전의 관할구역도 현재와 같은 지상, 해상, 공중의 3개 구역에 사이버공간을 추가하여 총 4개의 관할구역으로 만들고, 관련 작전지휘관도 별도로 구성할 필요가 있는 것이다.

3) 기타 사이버공격에 대비한 방호작용

가. 사이버공간에서의 기본권 제한의 특성

현행법상의 통제구역의 출입금지, 불심검문, 검문소 운영, 신고의무 등을 사이버공간으로 적용하여 보면, 특정 사이트에의 접속금지, 사이버 불심검문(필터링 등)의 방호작용을 예상해 볼 수 있다. 국민의 기본권 제한에 있어서 전통적인 질서유지 차원의 행동의 자유의 규제에 대하여는 헌법상 적법절차 원리 등의 적용을 통한 기본권제한법리가 확립되어 있다. 문제는 사이버공간에서 기본권 제한에 대하여는 사이버공간의 출입이나 이용이 단순한 행동의 자유 측면이 아니라 표현의 자유에 대한 제한으로 이해된다는 점에서 기본권 제한이 훨씬 민감한 문제라는 점이다. 정보통신망법 제44조의7을 근거로 한 불법정보에 대한 인터넷심의제도와 어떻게 차별을 둘 것인지, 심의절차는 어떻게 구성하고 누가 주도할 것인지 등 국가안보법 이외에도 사이버공간의 규제 관점에서 다른 접근이 필요한 것이다.

기타 실효성 있는 사이버상 방호작용으로 고려되어야 할 수단과 방법으로는 다음과 같은 기존의 법령 내용을 참고할 수 있을 것으로 본다.

나. 국가사이버안전관리규정

제9조의2(사이버위기 대응 훈련) ① 중앙행정기관, 지방자치단체 및 공공기관의 장은 소관 정보통신망을 대상으로 매년 정기적으로 사이버위기 대응 훈련을 실시하여야 한다.

② 국가정보원장은 국가 차원의 사이버위기 발생에 대비하여 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 대상으로 사이버위기 대응 통합훈련을 실시할 수 있다. 이 경우 국가정보원장은 특별한 사유가 없으면 사전에 훈련 일정 등을 해당 기관의 장에게 통보하여야 한다.

③ 국가정보원장은 제2항의 훈련 결과 필요하다고 판단하는 경우에는 중앙행정기관, 지방자치단체 및 공공기관의 장에게 필요한 시정조치를 요청할 수 있다. 이 경우 해당 기관의 장은 특별한 사유가 없는 한 그 요청에 따라야 한다.[본조신설 2012.1.2]

제10조(사이버공격과 관련한 정보의 협력) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을

국가안보실장 및 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가안보실장 및 국가정보원장에게 통보하여야 한다. 〈개정 2013.9.2.〉

② 국가정보원장은 제1항의 규정에 의하여 관련 정보를 제공받은 경우에는 대응에 필요한 조치를 강구하고 그 결과를 정보를 제공한 해당기관의 장에게 통지한다.

제10조의2(보안관제센터의 설치·운영) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 설치·운영하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 다른 중앙행정기관(국가정보원을 포함한다)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다.

② 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다.

③ 보안관제센터를 설치·운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다.

④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 미래창조과학부장관이 지정하는 보안관제전문업체의 인원을 파견받아 보안관제업무를 수행하도록 할 수 있다. 이 경우 보안관제전문업체의 지정·관리 등에 필요한 사항은 미래창조과학부장관이 국가정보원장과 협의하여 정한다. 〈개정 2013.5.24.〉

⑤ 제1항의 보안관제센터의 설치·운영 및 제2항의 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.

제11조(경보 발령) ① 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를 발령할 수 있다. 다만, 민간분야에 대하여는 미래창조과학부장관이 경보를 발령하고, 국방분야에 대하여는 국방부장관이 경보를 발령하며, 국가정보원장, 미래창조과학부장관 및 국방부장관은 국가차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 발령 전에 상호 교환하여야 한다. 〈개정 2008.8.18, 2013.5.24., 2013.9.2〉

② 제1항의 규정에 의하여 경보를 발령하였을 때에는 관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장에게 이를 신속히 전파하고 적절한 조치를 취하여야 한다.

③ 국가정보원장은 사이버공격이 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우에는 국가안보실장과 협의하여 심각 수준의 경보를 발령할 수 있다. 〈개정 2008.8.18., 2013.5.24〉

④ 국가정보원장은 제1항의 규정에 의한 경보 발령에 필요한 정보를 관계 중앙행정기관의 장에게 요청할 수 있다. 이 경우 관계 중앙행정기관의 장은 특별한 사유가

없는 한 이에 협조하여야 한다.

제12조(사고통보 및 복구) ① 중앙행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체없이 그 사실을 국가안보실장 및 국가정보원장에게 통보하여야 한다. 〈개정 2013.9.2.〉
② 지방자치단체의 장 및 공공기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 지체 없이 국가안보실장, 국가정보원장 및 관계 중앙행정기관의 장에게 통보하여야 한다. 〈개정 2013.9.2.〉
③ 국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 제1항 및 제2항의 규정에 의한 통보를 받은 때에는 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있으며, 요청받은 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제13조(사고조사 및 처리) ① 국가정보원장은 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 해당 기관의 장이 자체적으로 조사하게 할 수 있으며, 이 경우 해당 기관의 장은 사고개요 및 조치내용 등 관련 사항을 국가정보원장에게 통보하여야 한다.
② 국가정보원장은 제1항의 규정에 의하여 조사한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다.
③ 국가정보원장은 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우에는 관계 중앙행정기관의 장과 협의하여 범정부적 사이버위기 대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다. 〈개정 2010.4.16.〉
④ 사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위하여 대책본부 내에 합동조사팀 등 필요한 하부기구를 둘 수 있다. 이 경우 하부기구의 구성·운영 등에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다. 〈신설 2010.4.16.〉
⑤ 국가정보원장은 제4항에 따른 사고조사 및 피해복구 등의 조치를 위하여 관계 중앙행정기관의 장에게 필요한 인력·장비 및 관련 자료의 지원을 요청할 수 있다. 〈개정 2010.4.16.〉
⑥ 국가정보원장은 사이버공격에 의한 피해 및 대책본부의 대응 상황을 국가안보실장에게 통보하고, 국가안보실장은 이를 종합하여 대통령에게 보고한다. 〈신설 2013.9.2〉

다. 정보통신기반 보호법

정보통신기반보호법에 의하면 제4장에서 주요정보통신기반시설의 보호 및 침해사고의 대응 규정을 두고 있는데, 그 내용을 도입하면 가능하다고 보

인다.[33] 이 중에서 특히 보호조치 명령(제11조), 침해행위 등의 금지(제12조), 복구조치(제14조) 등은 통합방위법 개선시에 충분히 도입이 가능한 내용이다.

제11조(보호조치 명령 등) 관계중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다.

1. 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책을 분석하여 별도의 보호조치가 필요하다고 인정하는 경우
2. 제5조의2제3항에 따라 통보된 주요정보통신기반시설보호대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.

1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작・파괴・은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스・논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

제13조(침해사고의 통지) ① 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란・마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다. 〈개정 2013.3.23.〉

② 정부는 제1항의 규정에 의하여 침해사고를 통지함으로써 피해확산의 방지에 기여한 관리기관에 예산의 범위안에서 복구비 등 재정적 지원을 할 수 있다.

제14조(복구조치) ① 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

33) [정보통신기반 보호법] 제4장 주요정보통신기반시설의 보호 및 침해사고의 대응 제10조 보호지침, 제11조 보호조치 명령 등, 제12조 주요정보통신기반시설 침해행위 등의 금지, 제13조 침해사고의 통지, 제14조 복구조치, 제15조 대책본부의 구성등, 제16조 정보공유・분석센터

② 관리기관의 장은 제1항의 규정에 의한 복구 및 보호조치를 위하여 필요한 경우 관계중앙행정기관의 장 또는 인터넷진흥원의 장에게 지원을 요청할 수 있다. 다만, 제7조제2항의 규정에 해당하는 경우에는 그러하지 아니하다. 〈개정 2013.3.23.〉
③ 관계중앙행정기관의 장 또는 인터넷진흥원의 장은 제2항의 규정에 의한 지원요청을 받은 때에는 피해복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취하여야 한다. 〈개정 2013.3.23.〉

라. 정보통신망법

제46조의2(집적정보통신시설 사업자의 긴급대응) ① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. 〈개정 2009.4.22., 2013.3.23.〉
1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에서 발생한 이상현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우
2. 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우
3. 중대한 침해사고가 발생하여 미래창조과학부장관이나 한국인터넷진흥원이 요청하는 경우

② 집적정보통신시설 사업자는 제1항에 따라 해당 서비스의 제공을 중단하는 경우에는 중단사유, 발생일시, 기간 및 내용 등을 구체적으로 밝혀 시설이용자에게 즉시 알려야 한다.
③ 집적정보통신시설 사업자는 중단사유가 없어지면 즉시 해당 서비스의 제공을 재개하여야 한다.

제48조의2(침해사고의 대응 등) ① 미래창조과학부장관은 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다. 〈개정 2009.4.22., 2013.3.23.〉
1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 대통령령으로 정하는 침해사고 대응조치

② 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 미래창조과학부장관이나 한국인터넷진흥원에 제공하여야 한다. 〈개정 2009.4.22., 2013.3.23.〉
1. 주요정보통신서비스 제공자
2. 집적정보통신시설 사업자
3. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자

③ 한국인터넷진흥원은 제2항에 따른 정보를 분석하여 미래창조과학부장관에게 보고하여야 한다. 〈개정 2009.4.22., 2013.3.23.〉
④ 미래창조과학부장관은 제2항에 따라 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있다. 〈개정 2013.3.23.〉
⑤ 미래창조과학부장관이나 한국인터넷진흥원은 제2항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다. 〈개정 2009.4.22., 2013.3.23.〉
⑥ 미래창조과학부장관이나 한국인터넷진흥원은 침해사고의 대응을 위하여 필요하면 제2항 각 호의 어느 하나에 해당하는 자에게 인력지원을 요청할 수 있다. 〈개정 2009.4.22., 2013.3.23.〉

제48조의3(침해사고의 신고 등) ① 다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 미래창조과학부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다. 〈개정 2009.4.22., 2013.3.23.〉
1. 정보통신서비스 제공자
2. 집적정보통신시설 사업자
② 미래창조과학부장관이나 한국인터넷진흥원은 제1항에 따라 침해사고의 신고를 받거나 침해사고를 알게 되면 제48조의2제1항 각 호에 따른 필요한 조치를 하여야 한다. 〈개정 2009.4.22., 2013.3.23.〉

제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다.
② 미래창조과학부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다. 〈개정 2013.3.23.〉
③ 미래창조과학부장관은 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다. 〈개정 2013.3.23.〉
④ 미래창조과학부장관은 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다. 〈개정 2013.3.23.〉
⑤ 미래창조과학부장관이나 민·관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는

사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다. 〈개정 2013.3.23.〉

⑥ 제2항에 따른 민·관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.

(2) 사이버 버전의 통합방위법 제정 방식

기술한 바와 같이 통합방위법은 물리적 공격, 지역적 침범 등을 전제로 제정된 것이므로 통합방위사태, 통합방위작전 등의 개념 설정은 완전히 새로운 법의 제정으로 보인다. 그런 점에서 보면 사실상 새로운 통합방위법의 제정으로 볼 수도 있다.

최근 논의되는 국가사이버안보법제의 제정 논의는 이러한 관점에서 볼 수 있다.[34] 여러 가지 입법론이 제기되고, 그 규율범위도 다양하게 전개되고 있어 일률적으로 이것이 사이버 버전의 통합방위법이라고 할 수는 없겠지만, 적어도 통합방위법의 사이버 버전에 해당될 것으로 보려면 통합방위법이 규정하고 있는 정도의 사태의 정의, 대응작전, 국가통합방위요소의 통합 등 국가총력전의 관점에서 적절하게 구성되어 있는지 여부가 검토되어야 할 것이다. 구체적인 내용 구성은 앞서 본 통합방위법의 개정 요소와 다를 바 없다고 생각된다.

5. 적에 의한 사이버공격 대비 국가안보법의 소관 행정기관의 구성 문제

사이버공격에 대한 소관 행정기관은 누구로 볼 수 있는가? 이는 사이버안보 또는 사이버안전에 관한 현행 법령과 통합방위법상의 규정을 함께 해석하여야 하는 문제이다.

통합방위법에 의하면 통합방위작전은 통합방위사태가 선포된 지역에서 통합방위본부장(합동참모의장), 지역군사령관, 함대사령관 또는 지방경찰청장

34) 국가사이버안전법제의 입법론에 대하여는 정준현, 전게논문, 참조할 것.

(이하 작전지휘관이라 함)이 지휘·통제하도록 규정하고 있으므로(제2조 제4호), 결국 해당 작전지휘관이 속한 중앙행정기관이 통합방위업무의 중앙행정기관이 될 것이고 그 외에도 통합방위기구로 통합방위협의회를 중앙, 지역, 직장에 두도록 하고 있다. 따라서 통합방위법상 통합방위의 행정체계는 통합방위본부장을 중심으로 하여 각군, 경찰, 지방자치단체가 유지하는 것으로 하고 있다.

국가사이버안전관리규정에 의하면 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정하고, 국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의 설치하도록 하는 등 국가사이버안전에 관한 사항은 국가정보원장의 주도로 이루어지고 있다(제5조, 제6조).

기존의 사이버안보 관련 규정에 의하면 다양한 해석이 가능한데, 이것이 단순한 사이버공격인지 적에 의한 사이버공격인지, 통합방위법상 통합방위사태에 준하는 사이버 방위사태인지 여부, 전시 내지 준전시 등을 상정한 사태인지 등 다양한 요소를 고려하여야 하고, 한편으로는 사이버공격이 적에 의한 것인지 단순한 해커에 의한 것인지 공격 대상이 국가안보에 관한 것인지 다른 목적인지 등의 구분이 쉽지 않은 점도 고려되어야 한다.

만일, 적에 의한 사이버공격이 발생된 경우에 현행 통합방위법에 준하는 '사이버 방위사태'를 두게 된다면 위에서 본 바와 같은 통합방위법상의 통합방위작전이 수행되고 그 해당 작전지휘관은 사이버안전에 정통한 기관으로 설정하는 것이 타당하다고 할 것이다.

Ⅳ 마치는 글

1995년 최초의 통합방위지침이 제정될 당시에는 오늘날과 같은 사이버공간을 바탕으로 한 사이버공격 내지 사이버침투가 일반화되지 않은 상태였고, 오로지 육해공 지역을 통한 적의 침투나 도발이 중요한 때였다. 그런 상황에

서 제정된 통합방위법은 당연히 물리적인 공격 내지 무력에 대응한 국가총력전의 체계와 작전을 염두해 둘 수밖에 없는 것이다.

그런데, 오늘날 전쟁은 물리적 무기를 사용한 무력의 충돌에 그치는 것이 아니라 사이버전으로 변화될 가능성이 커지고 있다. 만일 3차 세계대전이 발발된다면 사이버전쟁이 주도한다는 것이 그런 예이다.

이러한 때 적에 의한 사이버공격에 유효적절한 대응, 즉 민관군의 통합된 대응을 위한 통합방위법의 적용이 절실히 요청되고 있다. 기술한 바와 같이 현행 통합방위법은 입법취지가 일체의 적의 침투 등에 대응하기 위한 국가총력전을 목표로 하고 있지만, 법률유보원칙상 사이버공격의 포함여부, 통합방위사태 및 작전의 개념, 사이버공격에 대한 사이버전(cyber戰) 등 대응방식의 구체화, 관계인의 기본권제한 등의 내용이 구체화되어야 하는 것이다.

특히, 위와 같이 논리적으로 본다면 사이버공격을 적의 침투나 도발로 보는 것은 가능하지만, 이를 통합방위법의 우산 아래에서 논의를 계속하는 것이 타당한지 여부에 대하여 고민을 할 필요가 있다. 특히 사이버공격은 물리적 공격과 달리 장소적 제한이 없고, 공격자가 적인지 여부를 알 수 없다고 보면 기존의 물리적 공격에 대응한 통합방위법의 입법취지를 달성하기는 곤란한 것이 아닌가 생각한다. 그런 점에서 통합방위법의 사이버버전의 내용을 가지는 경우에 이를 어떤 방식으로 입법할 것인가 하는 점인데, 완전히 새로운 법률로 만들 것인지, 아니면 통합방위법을 전면적으로 개편할 것인지 장단점을 보고 선택하여야 한다. 기존의 군사작전의 내용, 평시에서의 사이버안전체계, 특히 군사이버사령부의 존재목적과 설립취지 등이 종합적으로 고려되어야 한다.

위험분배에 따른 사이버 안보 관련 법제와 관련기관의 역할에 대한 고찰*

오 일 석**

목 차

Ⅰ 서 론

정보통신기술의 발달로 탄생한 사이버 공간은 비공간성, 비시간성, 익명성 등 불확실성에 기초하고 있는바, 해킹, 웜·바이러스 유포, 논리폭탄 등 과학기술의 발전이 의도하지 않았던 새로운 사이버 위험이 상존하면서 증가하고 있다. 더구나 최근 외교·안보의 핵심 정보를 다루는 정부 고위 공무원 등

* 이 발표문은, 발표자가 기존에 발표한 위험분배의 관점에 기초한 정보통신기반보호법 개선 방안, 『법학논집』(이화여자대학교 법학연구소, 2014. 9) 제19권 제1호, ; 사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안에 대한 고찰, 『법학연구』(인하대학교 법학연구소, 2014. 6) 제17집 제2호 등을 기초로 통합방위법 재난 및 안전관리 기본법과 사이버 보안의 관계 및 사이버 보안 관련 기관의 역할에 대한 부분을 첨가하여 정리한 것이다.

** 고려대학교 법학연구원 책임연구원

90여명이 북한의 해킹 공격을 받아 이 가운데 56명은 이메일 비밀번호가 유출된 사건은 사이버 위험의 심각성을 다시금 알려주고 있다.[1] 한편 경찰청 사이버수사과는 "인터파크해킹 사건에 사용된 인터넷 프로토콜(IP) 주소, 악성코드를 분석한 결과 북한 정찰총국 해커들의 소행으로 판단된다"고 발표했다.[2] 이와 같이 해킹, 바이러스 유포 등 사이버 위험은 국가안보에 위협을 야기함은 물론 경제적 불이익과 사회적 불편을 가중 시키고 있다.

한편 위험은 법적으로 "장래의 불확실한 사건으로 인하여 불이익이 발생할 개연성 또는 실제로 발생한 불이익"으로 정의되기도 한다.[3] 이러한 법적 의미의 위험은 위험과 관련된 활동에 참여한 사람들 사이에서 공평하게 분배되어야 한다. 더구나 위험과 관련된 활동이나 영업으로 이익을 얻고 있는 참여자가 있다면, 위험은 이들 사이에서 보다 합리적으로 분배되어야 한다. 이러한 원칙에 기초하여 위험은 당사자 사이에서 자유롭게 합의에 의하여 분배되기도 하고, 법률에 의하여 강제적으로 분배될 수도 있다.

한편 사이버 위험은, 과학기술의 발전이 의도하지 않았던 현대적 위험으로, 컴퓨터와 네트워크로 연결된 사이버 공간을 이용하여 해킹, 웜·바이러스 유포, 논리폭탄 등과 같은 사이버 공격이나 전자적 침해행위로 등으로 인하여 불이익이 발생할 개연성 또는 실제로 발생한 불이익으로 정의될 수 있다. 사이버 위험은 사이버 공간이 존재하는 한 상존하는 것이므로 사이버 공간을 이용하는 모든 사람들 사이에서 적절하게 분배되어야 한다. 그런데 사이버 위험은 그 발생 여부, 책임의 원인과 피해의 범위가 불명확하기 때문에, 사이버 공간을 이용하는 모든 사람들에게 분배되도록 하는 것은 곤란하다.

따라서 사이버 공간을 이용하는 일상적인 삶의 안정을 유지하고, 사이버

1) KBS 뉴스(2015. 8. 1), 北 안보 공무원 90명 해킹 56명 비번 유출(http://news.kbs.co.kr/news/view.do?ncd=3322000&ref=A, 최종방문 2016. 8. 7)
2) 전자신문(2016. 7. 29), 인터파크 해킹 북한 지목, 협박메일에 "총적으로 쥐어짜면.." 결정적 단서(http://www.etnews.com/20160729000045, 최종방문 2016. 8. 7)
3) 권영준, "위험배분의 관점에서 본 사정변경의 원칙", 『민사법학』(한국민사법학회, 2010. 12), 제51호, 225면 참조.

위험으로부터 발생하는 국가적 안전보장체계를 수립하기 위해서 입법자는 사이버 위험이 국가·공공부문에서 우선적으로 분배되어 감내될 수 있도록 하여야 한다. 이에 따라 입법자는 정보통신기반보호법, 국가사이버안전관리규정, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등을 통하여 사이버 위험을 분배하고 있다.

한편 입법자는 재난에 대한 대응체계를 수립함은 물론 적(敵)의 침투·도발이나 그 위협에 대응하기 위한 통합방위에 대책을 수립하기 위한 법제 또한 정립하였다. 이와 같은 재난관리법이나 통합방위법 등의 법제와 그에 따른 각 기관들 또한 재난이나 통합방위에 따른 역할을 수행함에 있어 사이버 위험 대응에 어느 정도의 역할을 수행하고 있다. 그렇지만 이들 법제는 재난대응이나 통합방위와 관련하여 사이버 위험에 기여하고 있는바, 이들 법제를 통한 사이버 보안과 관련한 입법적 개입정도를 위험분배의 관점에 따라 검토할 필요가 있다. 이를 위하여 이하에서는 사이버 위험의 분배와 정부의 개입, 입법적 개입의 정도와 한계를 우선 살펴보고자 한다. 이를 기반으로 재난과 사이버 위험의 분배, 통합방위와 사이버 위험의 분배를 살펴본 다음, 관련 기관들의 역할에 대하여 검토해 보고자 한다.

Ⅱ 사이버 위험의 분배와 정부의 개입

1. 계약에 의한 당사자 사이의 위험분배[4)]

위험은 상해, 손해 또는 손실의 가능성, 또는 상해, 손해 또는 손실에 대한 책임이라고 한다.[5)] 위험은 불확실성으로 인하여 손실이 발생할 가능성이라고 하기도 한다.[6)] 계약 당사자들은 재화의 교환이나 서비스의 제공뿐만 아니

4) 이 부분은 오일석, 『원유·가스 개발계약에서의 계약설계에 관한 연구』(고려대학교 대학원 박사학위논문, 2012), 40-44면을 요약, 정리, 보완한 것이다.
5) Black's Law Dictionary(Second Package Edition 2001), pp.616-17.
6) 황창용, "민간투자사업에 있어서 법령변경에 따른 위험과 그 배분-우리나라와 영국의

라 새로운 가치를 창조하기 위하여 계약을 체결한다.[7] 그러나 계약 당사자들은 계약 목적을 달성하는데 있어, 예상하였거나 또는 예상할 수 없는 위험에 직면하게 된다.

따라서 계약 당사자는 계약에 기초한 상호간의 관계 설정을 통하여 합리적으로 계약과 관련된 위험을 분배하고자 한다. 또한 당사자는 위험을 분배하는 과정에서 협상력과 교섭력을 강화하여 자신에게 유리하게 위험이 분배되도록 계약을 설계한다. 이와 같이 당사자 사이의 위험분배는 계약 목적 달성을 위해 계약의 전과정에서 발생하거나 내재되어 있는 위험을 당사자 사이에서 합리적으로 배분 또는 회피하는 것을 말한다. 합리적인 위험분배를 위하여 당사자는 위험 원인의 제거, 실사(實査)의 강화를 통한 위험의 감소, 법률, 계약 및 보험을 통한 위험의 이전, 위험에 대한 내부관리 등에 대해 검토하여야 한다.[8] 또한 계약 당사자는 주요 계약조항에서 그 위험에 대응하고 극복하는 방법을 구체적으로 규정함으로써 합리적인 위험분배를 달성할 수 있다.

계약 당사자들은 계약의 전과정에서 발생하거나 내재되어 있는 위험을 분배함에 있어, 원칙적으로 위험을 통제・인수할 수 있고, 위험 통제를 통하여 우월한 경제적 이익을 향유할 수 있는 자에게 위험이 분배되도록 하여야 한다.[9] 따라서 가장 최소 비용으로 위험을 회피할 수 있는 당사자가 누구인지,

민간투자사업을 중심으로-", 『원광법학』(원광대학교 법학연구소, 2010. 12), 제26권 제4호, 423면.

7) George Triantis, "The Evolution of Contract Remedies (and Why Do Contracts Professors Teach Remedies First?)", 60 University of Toronto Law Review, 643, 645 (2010).

8) Patrick Mead, "Current Trends in Risk Allocation in Construction Projects and their Implications for Industry Participants", 23 Construction Law Journal, 23, 29 (2007).

9) Vincent Hooker, "Major Oil and Gad Project-the Real Risks to EPC Contractors and Owners", 26 Construction Law Journal, 98, 106 (2010). 그러나 이러한 위험분배의 원칙이 실무에 그대로 적용되는 것은 아니다. 왜냐하면 실무에서는 위험을 가장 잘 관리할 수 있는 당사자에게 위험이 분배되지는 않으며, 공식적인 위험평가가 시행되는 것도 아니고, 위험 관련 계약조항은 모델계약과는 상이하고 다양하며, 위험을 관리하는 것이 불가능한 수급인 및 컨설턴트에게 위험이 이전되는 경우도 있으며, 위험이 입찰자들에게 비용이 되지 않을 수도 있고, 위험이 효과적으로 분배되었더라면 비용절

위험에 상대적으로 민감하지 않는 당사자가 누구인지, 위험이 구체화되는 경우 최소한 비용으로 위험을 감내할 수 있는 당사자가 누구인지 등을 기준으로 효율적인 위험부담자를 식별하여야 한다.[10] 이 경우 당사자들은 위험에 대한 통제의 정도, 위험에 대한 익숙함, 보상 필요성, 수급인 혹은 보험자에 대한 위험의 전가 가능성 여부, 위험의 이전에 대한 가치 등에 따라 위험분배에 대하여 결정하여야 한다.[11]

2. 사이버 보안에 대한 시장실패와 정부의 개입

(1) 사이버 보안에 대한 시장실패

사이버 위험은 컴퓨터와 네트워크로 연결된 사이버 공간을 이용한 해킹, 웜・바이러스 유포, 논리폭탄 등과 같은 사이버 공격이나 전자적 침해행위로 등으로 인하여 불이익이 발생할 개연성 또는 실제로 발생한 불이익으로 정의될 수 있다. 사이버 위험은 과학기술의 발전이 의도하지 않았던 현대적 위험 가운데 하나이다. 이와 같은 사이버 위험을 방지하고 대응하기 위한 사이버 보안 활동은 사이버 공간을 이용하는 모든 사람들의 편익을 증진시킨다. 따라서 사이버 공간을 이용하는 모든 사람들은 사이버 위험에 대한 위험분배에 참여하여야 한다. 왜냐하면 사이버 공간에 대한 참여로 편익을 향유하기 때문에 그에 해당하는 위험을 분배받아 감수하는 것이 형평의 원리에 부합하기 때문이다.

이에 따라 사이버 공간을 이용하는 사람들은 일정한 사이버 보안 관련 활동을 실행하여야 한다. 사이버 공간을 이용하는 모든 사람들이 사이버 보안

감 효과가 발생할 수도 있었을 터인데 그렇게 되지 않으며, 위험분배의 변경에 대한 합의는 당사자 이외에는 알려지지도 않고, 위험분배 변경의 결과로 인하여 분쟁과 소송이 증가되고 있기 때문이다.

10) George Triantis, “Unforeseen Contingencies. Risk Allocation in Contracts” in Boudewijn Bouckaert and Gerrit De Geest (eds), 『Encyclopaedia of Law and Economics』(Edward Elgar, 2000) Vol Ⅲ, 100.

11) Vincent Hooker, 위의 글(주 12), pp.106, 107.

관련 활동을 실행하는 경우, 사이버 위험을 절대적으로 차단할 수는 없겠지만, 상당 수준 감소시킬 수는 있다. 따라서 사이버 공간을 이용하는 모든 당사자들은 자신들이 통제할 수 있는 범위 내에서 사이버 위험에 대한 위험분배에 참여하고, 사이버 보안 관련 활동을 실행하거나 관련된 비용을 부담하여야 한다.

이와 같이 사이버 공간을 이용하는 모든 사람들이 사이버 보안 활동을 지속적으로 실행하거나 관련된 비용을 부담한다면 사이버 위험이 발생할 가능성은 감소될 수 있다. 이러한 사이버 보안 활동은 사이버 공격이나 전자적 침해해위 등이 감행되어 사이버 위험이 발생할 가능성이 감소시킴으로써 모든 컴퓨터나 네트워크 사용자들에게 편익을 가져다준다.

그렇지만 사이버 보안 활동을 수행하지 않은 개인이나 기업에 대하여, 사이버 보안 활동을 수행한 개인이나 기업이 사이버 위험의 발생에 대한 책임을 물을 수 없다. 왜냐하면, 사이버 공간을 이용한 모든 당사자들이 상호 계약관계를 맺고 있는 것은 아니며, 만일 이들 사이에서 계약을 통해 사이버 위험을 분배하였다 하더러도, 사이버 위험은, 과학기술의 발전으로 인한 의도하지 않은 새로운 위험으로 그 결과를 즉시 알 수 없는 경우가 대부분이고 원인규명도 명확하게 할 수 없는 경우가 많기 때문에 사이버 보안 활동을 수행하지 않는 개인이나 기업에 대하여 책임을 부담시키기 곤란하기 때문이다. 결국 사이버 보안 활동을 강화한 개인이나 기업은 이러한 활동을 통하여 구체적이고 실질적인 편익을 향유하는 것은 아니다.[12] 왜냐하면 이와 같은 사이버 보안 활동을 수행하지 않는 개인이나 기업들로 인하여 사이버 위험은 제거되지 않고 더욱 증가될 것이기 때문이다.

사이버 보안 활동이나 조치를 실행할 능력이 있는 개인이나 기업이 있다하더라도, 다른 기업들이 이러한 활동이나 조치를 실행하지 않음으로 인하여,

12) Hal R. Varian, “System Reliability and Free Riding.”, 『Proceedings of the First Workshop on Economics and Information Security』(University of California, Berkeley, 2002년 5월 16일-17일).

사이버 위험의 경감이라고 하는 구체적이고 실질적인 편익을 누리는 것이 없으므로, 사이버 보안을 위한 활동이나 조치를 실행하려고 하지 않을 것이다. 사이버 공간을 이용하는 모든 사람들이 이와 동일한 동인을 갖기 때문에, 모든 사람들이 서로 다른 사람들에게 편익이 되는 사이버 보안 활동이나 조치를 실행하였더라면 얻을 수 있었던 사이버 위험의 감소라는 구체적이고 실질적인 편익을 아무도 향유하지 못하게 된다.[13] 그러므로 사이버 보안은, 사이버 공간을 이용하는 모든 사람들의 사이버 보안 관련 활동에 의하여 영향을 받기 때문에, "공공재(public good)"로 인식되어, 시장 실패적 요소가 내재된 것으로 평가되고 있다.[14]

한편 사이버 보안을 실행한 개인이나 기업은 자신들에 대한 사이버 위험이 감소되는 편익은 일정부분 향유한다. 예를 들어, 사이버 보안 활동이나 조치로 사이버 공격으로부터 사적인 정보나 중요한 문서 등이 유출되거나 위·변조되는 위험을 방지 또는 감소시킬 수 있다. 비록, 사이버 보안이 공공재로 인식되기 때문에 시장 실패적 요소를 가지고 있지만, 이와 같은 편익을 일정한 수준까지 향유할 수 있다면, 개인이나 기업들은 사이버 보안 활동이나 조치를 실행하고자 할 것이다. 그러나 개인이나 기업들은, 사이버 보안을 위해 지출하여야 할 비용은 막대한 반면에 자신들의 편익 증가는 미미한 대신 공공의 편익만 증가한다면, 사이버 보안 활동이나 조치를 실행하려고 하지 않을 것이다. 이와는 반대로 사이버 보안에 따른 비용은 적지만, 자신들의 편익이 크다면, 개인이나 기업은 비용대비 편익에 있어 최적 수준의 사이버 보안 조치를 실행하고자 할 것이다.

13) Benjamina Powell, "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", 1 Journal of Law, Economics and Policy, 497, 498-499 (2005).

14) Ross Anderson, "Why Information Security is Hard-An Economic Perspective", 『Proceedings of the 17th Annual Computer Security Applications Conference』, (New Orleans, LA, 2001, https://www.acsac.org/2001/papers/110.pdf, 최종방문 2016년 8월 7일).

그러나 최적 수준의 사이버 보안을 식별하는 것은 곤란하다. 왜냐하면 현실적으로 사이버 보안과 관련된 개인적 또는 사회적 비용과 그로 인한 편익을 파악하는 것은 곤란하기 때문이다. 아울러 사이버 보안을 위해 비용을 아무리 투입한다 하여도, 완벽한 사이버 보안을 달성할 수는 없다. 기업의 경우, 해당 기업의 정책결정자들은 투자대비 효용에 대한 명확한 근거 없이 사이버 안보에 대해 투자하는 것을 주저하게 된다.[15] 민간 기업들은 한정된 예산의 범위 내에서 모든 IT 분야의 서비스 제공은 물론 보안과 관련된 활동도 수행하여야 하므로, 투자대비 효과에 대한 분석 없이 사이버 안보에 대해 일정한 예산을 투입하려고 하지도 않는다.

나아가 사이버 보안과 관련하여 최적 수준의 투자대비 효용을 판단하기 위한 신뢰할 수 있는 데이터를 확보하는 것 또한 현실적으로 매우 곤란하다. 신뢰할 수 있는 투자대비 효용 데이터는 사이버 위험의 빈도, 사이버 위험의 비용 및 이를 감소시키기 위한 방법의 효용성 등에 관한 데이터에 기초하여야 하는데,[16] 이를 담보하는 것이 곤란하다. 우선 기업들이 사이버 위험으로 발생한 피해를 인식하지 못한 경우도 많고, 사이버 공격이나 전자적 침해행위 등으로 인한 피해를 인식하였다 하더라도 보고하지 않는 경향이 있기 때문이다.[17] 기업들의 입장에서는 사이버 공격이나 전자적 침해행위에 대한

15) Simon Moffatt, “Information Security: Why Bother?”, Infosec Island(2012, 12, 9), http://www.infosecisland.com/blogview/22774-Information-Security-Why-Bother.html, 최종방문 2016년 8월 7일)

16) Melanie J. Teplinsky, “Fiddling on the Roof: Recent Developments in Cybersecurity”, 2 American University Law Review 226, 307 (2013).

17) Dmitri Alperovitch, Revealed Operation Shady Rat (McAfee White Paper, 2011), p.2 (http://www.mcafee.com/us/resources/white-papers/wp-operation- shady-rat.pdf, 최종방문, 2016년 8월 7일); Nicole Perlroth, “Nissan Is Latest Company to Get Hacked”, New York Times Bits Blog (Apr. 24, 2012, available at, http://bits.blogs.nytimes.com/2012/04/24/nissan-is-latest-company- to-get-hacked/, 최종방문 2016년 8월 7일); Tom Kellermann, Panel 1: The Promise and Peril of Being Interconnected, Interoperable, and Intelligent at the American University Law Review Symposium: America the Virtual: Security, Privacy, and Interoperability in an Interconnected World (Oct. 25, 2012, available at http://www.aulawreview.com/index.php?view

피해의 보고로 법령 위반, 소비자의 대응, 다른 기업들에 대한 경쟁력 약화, 비용 증가, 평판 악화 등을 두려워한다.[18] 결국 기업들에 대한 신뢰할 수 있는 사이버 위험 관련 정보를 획득하기 곤란하기 때문에, 이를 수치화하여 측정하는 것은 곤란하다. 또한 사이버 위험의 원인이 되는 사이버 공격이나 전자적 침해행위 등과 관련된 유형·무형의 비용에 대한 신뢰할 수 있는 정보 또한 부재한 상황이다. 왜냐하면 사이버 공격이나 전자적 침해행위 등으로 인한 기회비용의 상실, 평판악화로 인한 비용 증대, 소비자 신뢰의 상실, 지적재산권의 상실, 소비자 개인정보의 유출 등으로 인한 비용은 측정하기 곤란하기 때문이다.[19]

(2) 입법을 통한 정부의 개입과 위험분배의 확장

민간 자율에 의한 사이버 위험의 위험분배와 그에 따른 사이버 보안 관련 활동은 한계에 봉착할 수밖에 없다. 따라서 사이버 보안을 강화하기 위해서는 국가가 개입하여 어느 정도 강제적인 사이버 위험에 대한 위험분배를 결정하고, 적합한 보안 수준 등을 지정함으로써 국가 전체적인 사이버 대응 수준을 향상시켜야 한다.[20] 특히 민간 기업들이 전력, 통신, 도로, 항공 등 국가의 핵심시설과 관련되어 있는 경우, 국가에 의한 사이버 위험분배의 개입은 필수불가결하다. 우리의 경우 이러한 핵심시설들은 공공기관에 의하여 운영되고 있는 경우가 대부분인바, 국가의 개입을 통한 사이버 위험에 대한 위험분배가 더욱 요구된다. 왜냐하면 이러한 국가 핵심시설의 운영 및 유지와 관련된 위험

=vidlink&catid=278:symposium-2012&id=155:promise-and-peril-of-interconnectivity&option=com_vidlinks&Itemid=150, 최종방문 2016년 8월 7일).

18) Siobhan Gorman & Shara Tibken, “Security ‘Tokens’ Take Hit”, Wall Street Journal (June 7, 2011, available at http://online.wsj.com/news/articles/SB10001424052702304906004576369990616694366, 최종방문, 2016년 8월 7일)

19) Ross Anderson et al, “Measuring the Cost of Cybercrime(June 26, 2012, available at http://cseweb.ucsd.edu/~%20savage/papers/WEIS2012.pdf, 최종방문 2016년 8월 7일)

20) 그러나 국가의 개입은 사이버 보안에 대한 시장실패를 가중시킬 뿐이며, 민간영역에서 사이버 보안에 대한 시장실패의 실질적 증거가 없는바 사이버 보안을 민간자율에 맡겨야 한다는 견해도 있다. Benjamina Powell, 위의 글(주 16), pp.507-508.

을 이미 국가·공공 분야에서 감수할 것으로 분배하고 있기 때문이다.

정부는 시장 실패적 요소를 내재하고 있는 사이버 보안과 관련된 위험을 입법적 수단을 통하여 이해관계인 또는 국가와 사회로 배분하여야 한다. 우리 입법자들은 국가의 핵심 기능을 운영하는 정보통신기반시설에 대한 사이버 위험에 대하여는 「정보통신기반보호법」을 통해, 또한 국가·공공 분야에서 발생하는 사이버 위험에 대해서는 「국가사이버안전관리규정」을 통해, 민간분야의 사이버 보안 및 개인정보 보호와 관련한 위험에 대해서는 「정보통신망이용촉진 및 정보보호 등에 관한 법률」 등을 통하여 규정하고 있다. 아울러 「개인정보 보호법」, 「전자금융거래법」, 「정보보호 산업 진흥에 관한 법률」 등을 통하여 사이버 위험에 대하여 규정하고 있다.

이와 같은 사이버 보안 관련 입법을 통하여 입법자는 기본적으로 국가·공공 분야의 사이버 위험은 국가정보원이, 국방 분야의 사이버 위험에 대하여는 국방부가, 민간 분양의 사이버 위험에 대하여는 미래창조과학부가, 금융분야에 대하여는 금융위원회가 주도하여 사이버 위험에 대응하도록 규정하고 있다.

Ⅲ 위험분배를 위한 입법의 개입 정도와 사이버 안보 관련 법제

1. 입법의 개입 정도와 한계

입법(regulation)[21]은 여러 가지 의미를 가지고 있지만, 원칙적으로 법적

21) 입법은 보통 legislation으로 번역할 수 있다. 입법은 실질적으로는 국가기관을 통한 일반적·추상적 법규범의 정립을, 형식적으로는 의회가 입법절차에 따라 법률의 형식을 갖춘 법을 제정하는 것을 의미하는 것으로, 입법은 사회구성원의 다양한 의사를 입법기관이 수렴하여 이를 법규범으로 변화시켜가는 추상적이고 동태적인 과정을 의미한다(국회 법제실, 법제실무-개정 증보판(2015. 1) 10면 참조). 이러한 의미에서 여기서는 regulation도 입법으로 번역하기로 한다. 한편, 법제란 일반적으로 법률안을 작성하는 행위를 말하는 것으로 입법 아이디어를 정제된 용어로 표현하여 궁극적으로 입법자의 입법 목적을 달성할 수 있도록 법률적 언어체계로 구성하는 일련의

수단을 이용하여 사회 경제적인 정책적 목적의 달성을 실현하는 것으로 볼 수 있다. 여기서 법적 수단이라는 의미는 정부가 제재조치를 동원하여 개인이나 단체로 하여금 규정된 행위준칙에 합치되는 행동을 하도록 강제하는 것을 말한다. 특히 국가는 영리활동을 수행하는 회사에 대하여 공정한 경쟁은 물론 소비자와 근로자의 복리 증진을 위해 특정 가격을 준수하고, 특정 물품을 공급하며, 특정 시장에서 영업행위를 하고 생산에 있어 특정 기술을 사용하며 최저임금을 제공하여야 하는 등의 조치를 강제할 수 있다. 이러한 조치에 위반하는 경우 정부는 벌금, 위반의 공시, 징역, 이행강제명령, 특정 행위의 금지, 영업활동의 변경 또는 금지 등의 재제조치를 가할 수 있다.

현대 자본주의 사회에서 부족한 자원은 시장 메커니즘을 통하여 조정됨으로써 부족한 자원의 분배가 최적화되는 것이 원칙이다. 그러나 자원분배의 최적화는 특정 상황과 조건을 전제로 하는 것으로 현실에서 발생하기 곤란하며 이론적으로만 가능할 수 있다. 이와 같이 현실에서 자원분배의 최적화를 달성하기 곤란하다는 사실을 시장실패라고 한다.

시장실패가 존재하는 곳에서 자원 분배의 효율성을 달성하기 위한 하나의 방법은 입법을 통한 정부의 개입이다. 그런데 이러한 입법을 위해서는 입법의 거래비용과 정보비용이 발생한다. 그럼에도 불구하고, 입법은 시장실패에 대한 대처에 있어 상대적으로 보다 효과적인 수단이 된다. 예를 들어 공공복리의 증진을 위해 필요한 공공시설을 설립함에 있어, 정부는 공정한 가격과 정당한 보상 비율을 정립하기 위하여 거래비용을 지출하지만, 공정한 가격과 정당한 보상은 위 공공시설의 설립과 관련하여 발생한 갈등을 조정하고 경감시킴으로써 사회적 복리를 증진시킬 수 있다. 이와 같은 사회적 입법(social regulation)[22]은 당사자들이 협상을 통하여 문제를 해결하는 것보다 환경오

기술적 과정을 의미한다. 다시 말해 법제는 입법과정 중에서 법률안을 실제적으로 입안・작성하는 행위를 말한다.

22) 사회적 입법(social regulation)은 환경, 직업적 보건과 안전, 소비자 보호 및 노동 등의 분야에서 합의를 도출하는 것을 목적으로 하는 입법이다. 예를 들어 환경적으로 유해한 물질의 제거, 공장이나 작업장에서의 안전 관리, 제품에 대한 표시・광고 정

염이나 직장에서의 사고 등과 같은 일정 분야에 있어 발생하는 문제의 해결에 보다 효율적인 수단이 될 수 있다. 비록 입법자들이 사회적 입법과 관련한 완전한 정보를 획득할 수는 없지만, 입법에 의한 개입으로 인한 한계비용과 증가되는 사회적 한계효용이 일치하는 지점을 판단하기 위한 보다 많은 정보를 결합할 것이다.

그러나 입법이 공공복리의 증진에 기여한다고 하기 위해서는 입법자들이 공공복리를 위해 행동하거나 정치적 의사결정과정이 효율적으로 운영되고 있다는 사실이 전제되어야 함은 물론, 입법의 비용과 효용에 대한 정보 또한 용이하게 접근할 수 있다는 것이 전제되어야 한다. 예를 들어, 입법적 개입이 없는 상황에서 공공 서비스를 제공하는 독점 기업이 있다고 가정해 보자. 이 회사는 서로 다른 소비자 집단에 대하여 차별적 가격을 부과하고 있는바, 농촌 지역이나 비용이 많이 소요되는 소비자들에게는 서비스를 제공하지 않음으로써 비정상적인 이익을 취득하고 있다. 이는 자원 분배에 있어 비효율을 양산하고 있다. 만일 이 회사에 대한 입법적 개입이 없다고 한다면 자원분배의 비효율에 따른 비용은 무한대로 확대될 수 있다. 그러나 입법적 개입이 강화될수록 자원배분의 비효율은 감소하여 소비자들의 복리 손실을 경감시킬 것이다. 결국 이러한 시장에 대한 입법적 개입은 소비자 집단의 비용을 경감시키는 결과를 가져와 복리의 증진을 촉진한다. 이와 같이 입법은 사회 전반의 자원이 효율적으로 분배될 때까지 가격을 하락시키고, 생산을 증가시킨다.

그러나 사회에 대한 입법적 개입이 증가할수록 개입 비용(intervention cost) 또한 증가한다. 그러므로 입법자는 효율적 가격이 결정되기 전까지, 기업이 직면한 비용과 수요에 대한 정보를 가지고 있어야 한다. 한편 기업들에게는 입법적 개입에 따라 시간, 노력 및 자원을 투입하여 입법을 준수하여

보제공의무, 특정 물품이나 서비스 제공의 금지, 종교, 성별, 피부색, 국적에 따른 차별의 금지 등을 규율한다.

야 하는 준수비용(compliance cost)이 발생한다. 즉 기업들은 입법을 준수하기 위하여 행정 조치의 정립, 내부적 절차의 정립 등에 따른 비용과 손실을 부담하여야 한다. 아울러 기업 활동에 대한 감독과 같은 입법에 따른 집행과 관련한 비용도 발생한다.

한편 기업들 또한 입법자에게 관련된 정보를 누락시키거나 위장하기도 하는 등 전략적으로 행동하기 때문에 입법적 개입으로 인한 사회적 비용이 발생할 수도 있다. 입법적 개입으로 인한 이와 같은 비용과 손실의 증가로 이익이 감소하는 경우 기업은 생산 비용을 절감하거나 새로운 제품이나 생산기술을 개발하려고 하지 않을 것이다. 입법적 개입으로 정부 정책에 대한 예측 가능성과 신뢰성이 상실되는 경우, 정부 위험에 따른 보험료가 상승하고, 투자가 감소하고 경제성장률이 둔화될 수도 있다.

비록, 입법자가 이러한 비용을 인식하여 가격, 이익 또는 가격과 이익의 조화 등 여러 가지 정책적 사항을 선택할 수도 있지만, 입법적 개입은 예상하지 못한 결과의 발생에 직면하는 비용을 야기할 수도 있다. 따라서 입법자는 입법적 개입의 정도를 심도 있게 고려하여야 한다. 결국 입법적 개입의 최적화 수준은 입법적 개입의 증가 수준과 비효율적인 기업행동의 경감 사이에서 이루어지는 자원분배의 균형점에 있다. 이를 위하여 입법자는 시장에 대해 허가권, 특허권 등 배타적 권리를 부여할 수도 있고, 시장에 직접 개입하여 국가로 하여금 공공시설 등을 직접 운영하는 공기업을 설립할 수도 있다. 물론 이러한 입법 정책적 수단들은 입법적 개입 비용을 야기함은 물론 효율성도 다르고, 의도한 입법 목적과 전혀 다른 결과를 발생시킬 수도 있다. 또한 입법적 개입과 관련한 여러 수단의 선택은 더 많은 정보의 요구, 행정적 비용은 물론, 관리책임, 부패 위험 등 사회에 대하여 새로운 부담을 야기할 수도 있다.

결국 시장실패가 존재하는 곳에 자원배분의 효율성을 달성하기 위한 방법으로 입법적 개입이 요구되는데, 이 경우 입법자는 입법적 개입에 따른 비용의 증가와 입법으로 인한 시장참여자들의 비효율적 행동 경감으로 발생한 복리 증진의 균형점에서 입법의 정도를 결정하여야 한다.

2. 사이버 위험과 최적 대응 정책[23]

사이버 위험은 국가안보와 공공질서는 물론 개인의 일상을 위협하는 위험으로 사이버 공간이 존재하는 한 상존하는 위험이다. 따라서 정책 결정자는 사이버 위험에 대응하기 위한 다양한 방법 가운데, 사이버 위험을 최소화하거나 제거할 수 있는 가장 효율적이고 적절한 대책을 선별하여야 한다. 이와 관련하여 미국 국토안보부는 위험과 관련한 경제성 평가에 기초하여 보안 접근법을 개발하였고[24] 이를 사이버 보안에도 적용하였다.[25]

사이버 위험 관리 측면에서 볼 때, 사이버 위험(Risk)은 위협(Threat)과 취약성(Vulnerability) 및 결과발생(Consequence)의 곱으로 평가될 수 있다.[26] 이 평가기준에 의하면, 위협, 취약성, 결과발생을 감소시키면 위험은 감소하며, 이중 하나라도 완전히 제거하면 위험은 발생하지 않는다. 그런데 위협, 취약성, 결과발생을 제거하여 사이버 보안을 강화하는 것은 관련된 비용의 증대를 야기하게 된다. 따라서 정책결정자는 비용과 안보 가치의 사이에서 최적 균형점을 찾아야 한다. 결국 정책결정자는 위험의 제거 또는 감소에 소요되는 비용과 사이버 보안 강화로 증대되는 사회적 복리의 비교를 통하여 가장 효율적인 정책 수단을 선택할 수밖에 없다.[27]

23) 이 부분은 오일석・김소정, 사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안에 대한 고찰, 『법학연구』(인하대학교 법학연구소, 2014. 6. 30), 제17집 제2호, pp.143-144면을 요약, 정리, 보완한 것이다.

24) Department of Homeland Security, National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency(2013).

25) Michael Chertoff, "Foreword to Cybersecurity Symposium: National Leadership, Individual Responsibility", 4 Journal of National Security Law and Policy, 1, 3 (2010).

26) Paul Rosenzweig, "Cybersecurity and Public Goods: The Public/Private Partnership," Hoover Institution・Stanford University, 2, 7 (2011). (available at http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf, 최종방문 2016년 8월 7일).

27) Steven R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line", 4 Journal of National Security Law and Policy, 27, 35 (2010).

위협을 제거하기 위해서는 공격 원점에 대한 타격이 가장 확실한 수단이 될 수 있으나, 이는 공격원점에 대한 명백하고 확실한 증거, 타격의 동가치성 등 사이버 전쟁 수행과 관련한 문제점 때문에 곤란하다.[28] 그러므로 그 위협을 탐지하고 모니터링하여 예방하는 것이 보다 현실적 대안이다.

또한 취약성을 제거하기 위한 가장 최선의 방법은 컴퓨터와 네트워크를 이용하지 않는 것이다. 이러한 방법으로 사이버 위험은 완전히 제거될 것이지만, 이 경우 현대 사회의 생존과 유지가 곤란하여 사회적 비용의 증가가 보다 더 크게 발생한다. 따라서 취약성 감소를 위하여 컴퓨터와 네트워크에 대한 취약성 분석 평가 및 관리 체계를 구축하고 일정 시점마다 평가하는 것이 필요하다.

결과 발생의 방지나 예방과 관련해서는, 특히 주요정보통신기반시설에 대한 사이버 공격이나 전자적 침해행위로 인한 결과가 심각하기 때문에, 국가차원의 주요정보통신기반시설 보호 체계를 보다 효과적으로 운영할 필요가 있다. 또한 국가·공공기관에 대하여는 내부망과 외부망을 분리하여 위협을 차단함으로써 결과발생을 최소화할 수 있다. 이러한 의미에서 보안기관이 중심이 되어 실시한 우리의 망 분리 정책은 매우 적절하다. 아울러 사이버 보안 시스템의 운영, 인력 운영현황 등에 대하여도 주기적으로 점검할 필요가 있다.

결국 사이버 위협을 탐지하고 모니터링하며, 취약성 분석 평가 및 관리체계를 구축하고, 주요정보통신기반시설에 대한 보안 체계를 강화하며, 결과발생의 방지나 예방을 통하여 사이버 위험을 방지 또는 최소화시킬 수 있다. 이와 같은 사이버 위험을 방지 또는 최소화시키기 위한 정책 실현을 위해, 특히 정보통신기반보호법과 국가사이버안전관리규정은 사이버 위험에 관하여 위험분배를 입법적으로 구현하고 있다.

28) 그러나 결과발생이나 위협의 감소를 위하여 대응 타격의 개발(developing counter-strike capabilities)과 적극적 방어(active defense)를 강조하는 견해도 있다. Jay P. Kesan and Carol M. Hayes, “Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace”, 25 Harvard Journal of Law and Technology, 429, 474-485 (2012).

3. 재난과 사이버 위험

(1) 사이버 보안과 사이버 안전

현대적 위험이 국가에 대해 미치는 위험 상황을 국가위기로 정의할 수 있으며, 이는 일반적으로 국가의 주권, 정치, 경제, 사회, 문화 체계 등 국가를 구성하는 핵심요소나 가치에 중대한 위해가 가해질 수 있거나 가해지고 있는 상태를 의미한다.[29] 국가위기는 국민위기, 영토 및 주권위기, 국가핵심기반위기로 구분될 수 있다. 여기서 국민위기는 국민생활위기와 재난위기로 나누어 볼 수 있으며, 영토 및 주권위기는 전통적 안보위기로 분류할 수 있고, 국가핵심기반위기는 국가핵심기반의 안전보장을 위협하는 것으로 국가부문과 민간부문으로 나누어 볼 수 있다.[30] 이렇게 볼 때, 안보는 안전을 포함하는 개념으로, 영토와 주권을 수호함은 물론 국가기능의 유지와 확보를 기반으로 국민보호를 실현하는 것이다. 이러한 국가위기 가운데 국민 생활의 위기와 재난에 대응하는 것을 안전으로, 이를 제외한, 나머지, 즉, 영토 및 주권의 보전과 국가 핵심기능에 대한 위기 대응을 보안이라고 할 수 있다.

이러한 안보 개념 하에서, 사이버 위험으로부터 사이버 공간에서의 영토와 주권을 수호하고, 국가기능의 유지와 확보를 바탕으로 국민의 자유와 권리를 보호하는 것을 사이버 안보라고 할 것이다. 이러한 사이버 안보 개념은 사이버 안전과 사이버 보안이라는 개념을 포함한다. 이 경우 사이버 위험으로부터, 국민 개인의 컴퓨터나 네트워크 및 관련 재산권을 보호하는 것은 사이버 안전(cyber safety)의 개념에 포섭된다고 할 것이다. 이에 대응하여, 핵심 국가기능의 유지와 국가 주권 수호를 위하여 정보통신기반시설과 국가·공공기관의 컴퓨터시스템과 네트워크를 보호하고 국가차원의 전략과 정책을 기획하여

29) 이희훈, "집회시 경찰권 행사의 법적 근거와 한계: 객관적 수권조항을 중심으로", 『경찰학연구』 제8권 제3호(경찰대학, 2008), 91면.
30) 이재은, "포괄적 안보 개념 하에서의 국가 위기관리 법제화의 의의와 내용 분석", 『한국위기관리논집』, 제2권 제2호(위기관리이론과실천, 2006. 12), 20면 참조.

국민의 자유와 권리를 보호하는 것은 사이버 보안(cyber security)의 영역이라고 할 것이다.[31]

(2) 재난과 사이버 위험의 대응

각종 재해로부터 국민의 생명, 신체 및 재산을 예방하고 보호하기 위한 일련의 구제행위를 재난관리라고 한다.[32] 한편 재난 및 안전관리 기본법에서는 재난관리를 재난의 예방, 대비, 대응 및 복구를 위하여 하는 모든 활동으로 정의하고 있다. 이는 헌법 제34조가 규정하고 있는 국가의 국민에 대한 보호의무에 기초하고 있다. 즉 헌법 제34조는 '국가는 재해를 예방하고 그 위험으로부터 국민을 보호하기 위하여 노력하여야 한다.'고 명시하여 재난을 예방하고 재난으로부터 국민을 보호하여야 할 의무가 국가에 있음을 명시하고 있다.

우리나라의 재난관리체계는 자연재난에 대한 관리로부터 시작되어,[33] 1990년대 성수대교 붕괴, 대구지하철공사장 폭발, 삼풍백화점 붕괴 등 각종 대형사고의 발생을 계기로 1995년 5월 24일 재난관리법이 제정되어 7월 18일 공포・시행됨에 따라 대형 복합재난 관리를 위한 조직상의 국가재난관리체계, 재난예방, 수습처리 및 긴급구조 등에 대한 종합적이고 체계적인 운영의 기틀이 마련되었다.[34] 이후 2004년 6월 1일 행정자치부 소속 외청으

31) 이와 같은 사이버 안보와 사이버 안전 및 사이버 보안 개념은 필자가 앞에서 살펴본 안보 개념 즉 포괄적 안보 개념에 기초하여 도출을 시도한 것이다. 그러나 사이버 안보, 사이버 안전, 사이버 보안의 개념은 아직까지 정확한 개념 규정이 곤란한 부분으로 남아 있으며, 혼재되어 사용되고 있다. 이는 특히 영어 'Security'가 문맥에 따라 안전, 안보, 보안으로 번역될 수 있기 때문에 기인하는 측면도 있다. 사이버 안보, 사이버 안전, 사이버 보안 등의 용어에 대한 보다 자세한 논의에 대해서는 정필운, "사이버 보안이란 개념 사용의 유용성과 한계", 『연세의료・과학기술과 법』, 제2권 제2호(연세대학교 법학연구원 의료・과학기술과 법센터, 2011. 8); 정완, "한미 사이버 보안 법제 동향에 관한 고찰", 『경희법학』 제48권 제3호(경희법학연구소, 2013. 9); 박노형, "미국 사이버 안전에 관한 법 제정 동향과 시사점", 『법제연구』 제46호(한국법제연구원, 2014. 5.) 참조.

32) 김태환, 『재난관리론』, 국립방재교육연구원(2009), 38면 참조.

33) 김은성, 안혁근, 『중앙정부와 지방정부 재난안전관리의 효과적 협력방안 연구』, 한국행정연구원(2009), 133면 참조.

로 소방방재청이 신설되었고, 행정자치부 안전정책관이 신설되었으며, 2008년 2월 29일 국토해양부 소속 외청으로 해양경찰청이 개편되었고, 행정안전부 재난안전실이 신설되었다. 2013년 3월 23일에 위 재난안전실은 안전행정부 안전관리본부로 확대 개편되었고, 위 해양경찰청은 해양수산부 소속 외청으로 해양경찰청으로 개편되었다. 한편 2014년 세월호 사건 이후 재난안전체계에 대한 전반적인 개편에 관한 사회적인 요구를 수용하여, 2014년 11월 7일 정부조직법 개정안(국민안전처 신설 내용)이 국회를 통과함에 따라 2014년 11월 19일 국민안전처가 출범하게 되었다.

여기서 재난이라 함은 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것을 말한다. 이러한 재난은 자연재난과 사회재난으로 나누어 볼 수 있다. 자연재난이라 함은 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 낙뢰, 가뭄, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해을 말한다.[35] 사회재난이란 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방사고·환경오염사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병 예방법」에 따른 가축전염병의 확산 등으로 인한 피해 등을 말한다.[36]

이와 같이 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비 등과 같은 사회적 재난은 사이버 공격으로 인한 국가주요정보통신기반시스템에 대한 피해와 매우 유사한 것으로 보인다. 그렇지만 「재난 및 안전관리 기본법」에서 말하는 재난은 기본적으로 에너지·통신·교통·금융·의료·수도 등 국가기반체계에 대한 물리적 피해를 상정하고 있다. 아울러 이러한 국가기반체계에 대한 피해발생의 원인을 따로 정하고 있지 않고 있다.

34) 전주(前註)
35) 「재난 및 안전관리 기본법」 제3조제1항 가목.
36) 「재난 및 안전관리 기본법」 제3조제1항 나목.

한편 「정보통신기반보호법」은 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 등 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 하고 있다.[37] 즉 이 법에 의할 때, 피해의 발생 유형이 전자적침해행위로 한정되어 있으며, 그 피해 대상도 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 등 정보통신기반시스템으로 한정되어 있다.

한편 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 정보통신망으로 규정하면서, 정보통신서비스 제공자로 하여금 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 취하도록 하고 있다.[38] 나아가 이 법은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 침해사고라고 하고 있다.

그러므로 정보통신망을 이용하여 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 주요정보통신기반시설에 대하여 피해를 발생시키거나, 정보통신망 또는 이와 관련된 정보시스템을 공격하여 피해가 발생하는 경우를 사회적 재난으로 개념 포섭하여 「재난 및 안전관리 기본법」을 우선 적용하는 것은 곤란하다.

37) 정보통신기반보호법 제1조.
38) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조제1항 참조.

(3) 검토

재난은 국민 생활의 안전과 밀접한 관련을 가지고 있다. 사이버 위험으로부터, 국민 개인의 컴퓨터나 네트워크 및 관련 재산권을 보호하는 것은 사이버 안전(cyber safety)의 개념에 포섭된다고 할 것이다. 이에 대응하여, 핵심 국가 기능의 유지와 국가 주권 수호를 위하여 정보통신기반시설과 국가·공공기관의 컴퓨터시스템과 네트워크를 보호하고 국가차원의 전략과 정책을 기획하여 국민의 자유와 권리를 보호하는 것은 사이버 보안(cyber security)의 영역이라고 할 것이다.

이러한 의미에서 볼 때, 재난관리법은 사이버 안전과 어느 정도 관련성을 가지고 있다. 따라서 정보통신망을 이용하여 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하여 피해가 발생하는 경우를 사회적 안전과 관련된 문제로 파악하여 재난관리법을 적용해 볼 수도 있을 것이다.

그렇지만 입법자는 이러한 사이버 안전의 문제는 이미 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 통하여 구체적으로 규정하고 있다. 나아가 에너지·통신·교통·금융·의료·수도 등 주요정보통신기반시설에 대한 사이버 공격에 대해서는 국가안보 문제로 인식하여 정보통신기반보호법을 통해 상세하게 규정하고 있다. 이와 같은 침해사고로 인하여 발생하는 피해 또는 국가 주요 정보시스템에 대한 위험의 분배는 이미 정보통신기반보호법이나 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 통해 규정되고 있다. 결국 사이버 공격으로 인한 물리적 피해는 물론 사이버 공간의 피해에 대한 국가안전보장 차원의 대응을 위하여 정보통신기반보호법, 국가사이버안전관리규정으로 대응하고 있는 것이다. 이러한 국가적 위기에 대하여는 재난 및 안전관리 기본법 보다는 위 법제에 따른 대응체계를 통하여서만이 탄력적 대응이 가능하다. 왜냐하면 재난관리법을 통하여 사회적 재난의 하나로써 사이버 위험에 대응할 수 있다고 하더라도, 이는 사회적 재난으로부터 국민의 생활의 안전을 확보하는 데 보다 중점을 두고 있는바, 해킹, 바이러스

등 사이버 위험으로부터 국가핵심기능의 유지와 관리, 국가 주권 수호를 위하여 국가·공공기관의 컴퓨터와 네트워크 보안에 주력하는 데에는 한계가 있기 때문이다.

결국 「재난 및 안전관리기본법」은 해킹, 바이러스 등에 의한 사이버 공격으로부터 발생하는 위험을 분배하기 보다는 국가기반체계에 대한 물리적 위험분배와 대응체계를 중점적으로 규정하고 있기 때문에, 사이버 공격에 대응하기 위한 규범으로 확장하는 데에는 한계가 있다. 다만, 천재지변이나 대규모 정전사태에 따른 통신시스템에 대한 국가적 마비 사태 등 물리적 원인과 피해에 대한 대책으로서 재난대응체계의 발동은 가능할 것이다.

4. 통합 방위와 사이버 위험

(1) 사이버 공격과 국제 전쟁법

사이버 전쟁은 특정 국가 또는 이에 준하는 집단이, 다른 국가의 컴퓨터 시스템이나 네트워크 등에 대하여 무력사용이나 전투에 이를 정도로 심각한 사이버 공격을 감행하여, 생명, 신체, 재산에 대한 실질적인 피해를 야기함으로써, 국가 차원의 대응 활동이 요구되는 안보 위협 상황이라고 정의할 수 있다. 아울러 이러한 무력적 사이버 전쟁에 대한 자위권 차원의 사이버 공격 또는 무력적 공격을 실행하는 경우에는 전쟁법의 일반 원칙에 따라야 한다.

그러나 이러한 사이버 전쟁에 사용된 사이버 공격의 무력공격과의 동가치성, 무력행사에 대한 입증곤란, 특정 국가에 대한 책임귀속의 곤란 등으로, 사이버 전쟁으로 개념 포섭할 수 있는 사이버 공격에 대하여, 자위권 차원의 사이버 전쟁이나 무력적 공격으로 대응하는 것은 현실적으로 곤란하다. 나아가 무력적 공격과 연계되거나 그 일부로 행하여진 것이 아닌 사이버 공격에 대하여 전쟁법의 원칙에 따라 자위적 사이버 전쟁으로 대응하는 것은 더욱 곤란하다.

결국 사이버 공격이 무력공격으로 간주되어 사이버 전쟁이 성립하기 위해

서는 정치적 혹은 국가안보적 차원에서 (조직적으로) 감행되어 신체적, 재산적 손해를 발생시킴으로써 국가안보와 관련된 심각한 결과를 가져와야 한다. 따라서 단순한 사이버 공격에 대하여 무력공격으로 간주하고 공격의 주체와 목적, 결과를 고려함이 없이 사이버 전쟁으로 개념 규정하는 것은 자제되어야 한다. 단순한 사이버 공격을 기화로 무력사용의 정당성을 도출하여 전쟁을 조장할 수도 있기 때문이다.

한편 미국은 사이버 공격에 대하여 재래식 무기를 사용하는 것을 효과적인 정책수단의 하나로 적극적으로 고려하고 있는 것으로 보인다. 그러나 사이버 공격이 전쟁 활동으로 간주되는 경우 이에 대응하여 재래식 무기(kinetic force)를 사용하는 국가는 명백성(distinction), 인도성(humanity), 필요성(necessity) 및 비례성(proportionality) 등 전쟁법의 원칙을 존중하여야 한다. 이러한 측면에서 볼 때, 사이버 공격에 대한 재래식 무기 사용의 공격은 사이버 공격으로 인한 피해와 심각하게 불일치함은 물론 비례성에 적합하지도 않기 때문에 적절하지 못하다. 사이버 전쟁도 전쟁으로서의 요소를 가지고 있으므로, 사이버 전쟁을 통하여 무력전쟁으로의 확전 가능성을 배제할 수 없다. 특정 국가가 사이버 공격에 따른 무력공격의 존재와 피해의 정도를 자의적으로 결정하여, 사이버 전쟁 및 무력적 공격으로 대응수단을 남용할 가능성이 있기 때문에, 사이버 전쟁에 대한 재래식무기로의 대응은 매우 자제되어야 한다.

(2) 사이버 공격에 대한 국내 전쟁 법규의 적용

1) 사이버 작전

사이버 전쟁도 '전쟁'을 내포하고 있는바, 국가적 행위, 무력행사, 침략행위 등과 같은 개념이 적용되어야 하므로, 사이버 전쟁을 수행하려는 경우 각국은 전쟁 수행과 관련된 국내 절차와 법규를 준수하여야 한다. 전쟁 수행을 위하여 당사국은 내부적으로 전쟁 승인 절차를 거치고 선전포고를 행하는 것이 보통이다. 한편 미 의회는 미국에 대한 사이버 공격에 대한 주기적 혹은

체계적 정보에 관여하지 않으려고 하는바,[39] 사이버 전쟁에 대하여 침묵하게 되었는데, 이는 결국 사이버 전쟁에 대하여 대통령에게 전속적인 권한을 부여하는 결과를 초래할 수 있게 되기 때문에,[40] 적극적 방어 개념으로서의 사이버 전쟁을 제한하여야 한다는 주장이 제기된 바 있다.[41]

이러한 의미에서 볼 때, 국내 전쟁법 절차를 통한 사이버 전쟁에 대한 통제를 회피하는 수단으로 사이버 작전이라는 개념을 사용하는 것으로 보인다. 사이버 작전을 군사적 목적이나 효과를 달성하기 위하여 사이버 공간에서 또는 이를 이용하여 사이버 능력을 이용하는 것이라고 정의하여 사이버 전쟁과 구분되는 개념으로 사용할 경우, 사이버 작전의 수행은 전쟁 수행과 직접적으로 관련한 활동이 아니므로 의회나 기타 다른 기관의 전쟁과 관련된 절차적 수단을 회피할 수 있다. 미국 국방부는 물론 NATO의 탈린 매뉴얼에서 사이버 작전에 대한 개념을 강조하고 사용하고 있는 것도 이러한 내부적 견제와 통제 절차를 회피하고자 하는 의도가 있는 것으로 보인다.

2) 사이버 전쟁의 국내법적 한계

한편 우리 헌법 제5조 제1항은 침략전쟁을 부인하고 있다. 그런데 사이버 전쟁으로 대응할 수 있는지 여부가 불분명한 정도의 사이버 공격에 대하여 적극적인 사이버 전쟁으로 대응하는 경우, 침략전쟁으로 간주되어 헌법에 정면으로 배치될 수도 있다. 또한 헌법 제73조에 따라 대통령은 선전포고권을 가지고 있으며, 헌법 제60조 제2항에 따라 국회는 선전포고에 대하여 동의권을 가지고 있다. 따라서 사이버 전쟁을 수행하기 위해서는 대통령이 선전포고를 하고 국회의 동의를 받아야 한다. 이 경우 상대국의 무력공격에 해당

39) Commission on Offensive Information Warfare, National Research Council of the National Academies, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities, William A. Owens et al. eds., 1, 80 (2009).(available at http://www3.nd.edu/~cpence/eewt/Owens2009.pdf, last visited July 7, 2016, 이하 “NRC 보고서”라 함), p.233.

40) NRC 보고서, p.236.

41) Stephen Dycus, Congress's Role in Cyber Warfare, 4 Journal of National Security Law & Policy, 155, 163 (2010).

하는 사이버 공격에 대하여 명백하고 확실한 증거로 해당국에 대하여 선전포고 하여야 한다는 상당한 부담이 존재한다. 아울러 외교단절, 경제제재, 국제사법재판소 등에 대한 제소 등 다른 분쟁해결 방안들을 거친 다음 사이버 전쟁으로 나아가야 하는데 이 경우 신속 급변하는 무력적 사이버 공격에 대한 탄력적이고 적극적 대응에 한계를 가지게 된다. 더구나 사이버 공격을 이유로 선전포고를 하는 경우 상대방이 무력공격으로 나선다면 물리적 전쟁으로의 확전 가능성이 상존하는 문제점이 있다.

나아가 사이버 공격에 의한 사이버 안보 위기 상황은 언제든지 발생할 수 있음에도 불구하고 사이버 전쟁으로 대응하기 위해 전쟁 절차를 밟는다면 국민생활에 불안감을 조성함은 물론 그 준비에 상당한 비용이 투입되고, 대외신인도가 하락하여 국내 경제에 악영향을 미칠 수 있다. 또한 사이버 전쟁과 관련한 교전수칙 등이 명확하게 정립되지 않은바, 사이버 공격에 군이 나서서 대응하는 것은 확전가능성을 증대시켜 국민의 피로도 증대, 시장 불안정성을 초래하게 될 것이다. 결국 사이버 공격에 대한 대응은 중요한 국가 안보 문제로 국가 안보업무를 담당하는 기관에서 지속적으로 수행하여야 할 것이다.

한편 미국에 대한 무력공격에 해당하는 사이버 공격으로 미국이 사이버 전쟁을 개시하는 경우, 우리도 한미방위조약에 따라 자동적으로 사이버 전쟁을 수행하여야 하는데, 이 경우 남북대치상황에서 자칫 사이버 전쟁이 무력전쟁으로 확전될 가능성이 있다는 사실도 심각하게 고려되어야 한다.

(3) 사이버 위험 대응을 위한 통합방위법 적용의 한계

정보통신과학기술의 발달로 탄생한 사이버 공간은 비공간성, 비시간성, 익명성 등 불확실성에 기초하고 있다. 이러한 사이버 공간에서는 해킹, 웜·바이러스 유포, 논리폭탄 등 과학기술의 발전이 의도하지 않았던 새로운 사이버 위험이 증가하고 있다. 이러한 사이버 위험은 국민위기, 영토 및 주권위기, 국가핵심기반위기에 모두 관련이 되어 있는바, 국가안보 차원에서의 대응이 우선적으로 고려되어야 한다. 왜냐하면 사이버 위험은 개인정보 유출,

사이버 범죄, 사회공학적 기법에 의한 금융 피해 등 국민 생활에 대해 방해와 피해를 야기할 수 있으며, 방송, 통신, 도로, 항만, 에너지, 항공 등 국가 핵심 기반에 대한 위기는 물론, 심각한 경우 사이버 공격이나 사이버 작전과 같은 국가 주권에 대한 위기를 초래할 수 있기 때문이다.

우리 헌법은 제5조에서 침략적 전쟁을 부인하면서 국군으로 하여금 국가의 안전보장과 국토방위의 신성한 의무를 수행할 것을 사명으로 규정하고 있다. 이러한 헌법 규정에 따라 적의 침투·도발이나 그 위협 또는 우발상황에 있어서 통합방위사태를 선포하고 국가총력전의 개념에 입각하여 민·관·군·경과 향토예비군 및 민방위대등을 통합·운용하는 등 효율적으로 대응하기 위하여 필요한 사항을 정하기 위하여 통합방위법이 제정되었다.[42] 통합방위법은 적(敵)의 침투·도발이나 그 위협에 대응하기 위하여 국가 총력전(總力戰)의 개념을 바탕으로 국가방위요소를 통합·운용하기 위한 통합방위대책을 수립·시행하기 위하여 필요한 사항을 규정함을 목적으로 하고 있다. 따라서 통합방위법은 평상시 국가방위에 대한 규범체계가 아니라, 적의 침투나 도발이나 그 위협 등 전시 및 이에 준하는 상황에 대하여 국가 총력전 차원에서 그 대응 체계를 정립하고 관련된 위험을 분배하고 있다. 이러한 사실은 이 법에서 통합방위에 대하여 적의 침투·도발이나 그 위협에 대응하기 위하여 각종 국가방위요소를 통합하고 지휘체계를 일원화하여 국가를 방위하는 것이라고 정의하고 있는 것에서도 알 수 있다.

앞에서 살펴본 바와 같이, 통합방위법은 적(敵)의 침투·도발이나 그 위협에 대응하기 위하여 국가 총력전(總力戰)의 개념을 바탕으로 국가방위요소를 통합·운용하기 위한 통합방위 대책을 수립·시행하기 위하여 필요한 사항을 규정함을 목적으로 하고 있는바, 사이버 공격에 대하여 통합방위법을 기준으로 대응하는 것은 사이버 전쟁을 기본 전제로 하여야 한다. 다시 말해 사이버 공격에 대한 통합방위법이 적용되기 위해서는 사이버 공격이 무력전

42) 통합방위법안(150347, 1996. 11), 제안이유 참조.

쟁의 과정이나 직전의 전단계에서 사용됨으로써 국가 총력전의 개념에 기초하여 방위 대책이 필요한 경우로 한정되어야 한다. 그런데 사이버 전쟁과 관련하여 무력사용과의 동가치성, 그 입증의 곤란 및 국내법적 절차에 따른 한계 등을 고려할 때, 사이버 공격에 대한 적절한 대응방법으로 통합방위법에 따른 체계를 적용하는 것은 상당히 곤란하다.

결국 통합방위법은 영토·국민·주권의 수호라는 전통적 안보 개념에 기초하여 국가 총력전의 개념을 전제하고 있는바, 컴퓨터 네트워크를 통한 국가 핵심기능의 유지, 관리, 복구를 위한 사이버 보안과는 다소 거리가 있다고 할 수 있다.

Ⅳ 사이버 위험 관련 법제에 따른 관련 기관 역할 검토

1. 국가안보실

(1) 국가의 기관, 행정청 및 보좌기관

국가의 기관은 그 행위의 결과 즉 권리·의무가 귀속되는 국가의 행위가 되는 모든 조직 안에 있는 단위 기관의 장이 다 포함된다. 정부조직법에 규정된 대통령과 대통령비서실장, 국가안보실장, 대통령경호실장, 국가정보원장이나 국무총리와 국무조정실장, 국무총리비서실장, 각 처장, 각부 장관과 그 및에 설치된 청의 장은 물론 개별법에 의하여 설치된 합의제 행정기관인 위원회 또는 그 위원회의 장을 포함한다. 또한 그 하부조직인 특별지방행정기관과 부속기관 등 소속기관의 장도 제한된 범위 안에서 독자적으로 예산을 집행하며 사무를 처리할 수 있으므로 국가기관에 포함된다.[43]

그런데 행정청이라 함은 국민 등 외부에 대하여 행정에 관한 의사를 결정하여 표시하는 단위를 말하며 법률상 처분청이라고 표현하기도 한다.[44] 한

43) 김명식, 『행정조직법』, 법우사(2014. 4), 55면 참조.
44) 김명식, 앞의 책, 52-53면 참조.

편 행정조직은 외부에 담당 직위가 표시되는 행정청과 내부적으로 그 업무를 나누어 수행하는 행정기관으로 구성되는데, 법령상으로는 이를 업격히 구분하지 않고 행정청과 행정기관을 합하여 (넓은 의미의) 행정기관이라고 하고, 행정청을 행정기관의 장이라고 표현하기도 한다.[45]

그러나 같은 조직 단위 안에서 행정청의 업무를 돕는 보좌기관이나 보조기관, 자문기관의 장은 독자적으로 의사표시를 할 권한이 없으므로 행정청으로 보기 어렵다.

(2) 국가안보실의 법적 성격

정부조직법 제15조는 국가안보에 관한 대통령의 직무를 보좌하기 위하여 국가안보실을 둔다고 규정하고 있다. 아울러 국가안보실에 실장 1명을 두되, 실장은 장관급 정무직으로 한다고 규정하고 있다. 이와 관련하여 국가안보실 직제(시행 2015.4.3. 대통령령 제26182호, 2015.4.3., 일부개정)가 시행되고 있다. 이 직제 대통령령은 국가 국가안보실의 조직과 직무범위, 그 밖에 필요한 사항을 규정함을 목적으로 하고 있다. 결국 국가안보실은 대통령의 국가안보에 관한 직무를 보좌하기 위한 보좌기관이다.[46] 이러한 사실은 국가안보실 직제에서 "국가안보실은 국가안보에 관한 대통령의 직무를 보좌한다".[47]고 규정하고 있는 것을 통하여도 확인할 수 있다.

(3) 보좌기관의 기능과 역할

보좌기관은 행정기관이 그 기능을 원활하게 수행할 수 있도록 그 기관장이나 보조기관을 보좌함으로써 행정기관의 목적달성에 공헌하는 기관을 말한다. 보좌기관은 전문적 지식을 활용하여 정책의 기획, 계획의 입안, 연구·조사, 심사·평가 및 홍보와 행정개선 등에 관하여 행정기관의 장이나 그 보좌기관을 보좌한다.[48]

45) 김명식, 앞의 책, 59면 참조.
46) 김명식, 앞의 책, 135면 참조.
47) 국가안보실 직제 제2조 참조.

한편 정부조직법은 제6조제1항에서 “행정기관은 법령으로 정하는 바에 따라 그 소관사무의 일부를 보조기관 또는 하급행정기관에 위임하거나 다른 행정기관·지방자치단체 또는 그 기관에 위탁 또는 위임할 수 있다. 이 경우 위임 또는 위탁을 받은 기관은 특히 필요한 경우에는 법령으로 정하는 바에 따라 위임 또는 위탁을 받은 사무의 일부를 보조기관 또는 하급행정기관에 재위임할 수 있다.”고 규정하고 있다. 이 규정을 통하여 볼 때 보좌기관은 권한의 위임을 받을 수 없도록 되어 있는데 보좌기관은 독립적인 사무를 분장하는 것이 아니라 보좌하는 기관의 성격상 당연한 것이다.[49] 그러므로 보좌기관은 특정 권한을 위임받아 행사하는 집행적 기능을 수행할 수 없으므로 정책을 기획, 입안하거나 결정할 수 없다. 나아가 정책의 기획, 계획의 입안, 연구·조사, 심사·평가 및 홍보와 행정개선 등의 기능은 정책을 집행할 수 있는 기관을 통하여 수행되어 왔다.[50]

(4) 소결 : 보좌기관인 국가안보실의 업무의 한계

결국 국가안보실은 정책 수행기능은 없는 대통령의 보좌기관이기 때문에 국가 사이버 안보 정책의 기획, 계획, 입안, 조사 등의 업무를 수행할 수는 없다. 이러한 업무는 대통령 소속기관으로서 해당 업무에 대한 정책 수행기관이 국가정보원을 통하여 실행되어야 한다. 다만 국가안보실은 국가정보원을 통하여 정책적으로 수립된 국가 사이버 안보 정책의 기획, 계획, 입안, 조사 등에 대하여 대통령을 보좌하는 차원에서 의견을 제시하거나 관련 부처와의 협의 등을 도출하는 등의 보좌활동을 수행할 수 있을 것이다.

2. 합동참모본부(사이버사령부)

앞에서 살펴본 바와 같이 통합방위법은 전시 또는 이에 준하는 사태를 상

48) 김명식, 앞의 책, 64면 참조.
49) 김종성, “국의 보조·보좌기관 구분에 대한 비판적 검토”. 한국행정학보 제41권 제3호(2007. 가을), 180-181면 참조.
50) 김종성, 앞의 논문, 184면 참조.

정하여 총력전의 개념으로 방위태세 차원에서 국가적 대응역량을 규정하고 있으므로, 사이버 위험에 대하여 적용하는 것은 곤란하다. 사이버 공격이나 사이버 위협 등 모든 사이버 위험에 대하여 통합방위법을 적용하는 순간 위 사이버 공격에 대한 전쟁법 적용에 따르는 문제점이 수반되어 적절한 대응을 할 수 없기 때문이다.

사이버 전쟁을 위해서는 특정 국가의 군대 조직이나 단체에 의한 사이버 안보 위협이 무력분쟁을 야기할 정도의 무력의 사용과 동일한 가치를 가지고 조직적으로 이루어졌다는 사실이 명백하고 확실한 증거로서 입증되어야 한다. 또한 사이버 전쟁에 대응하여 자위권 행사의 방법으로 사이버 전쟁이나 작전을 수행하고자 하는 경우, 그러한 사이버 전쟁이나 작전이 필요성과 비례성 원칙에 부합함을 입증하여야 한다. 그러나 이러한 입증은 매우 곤란하다. 예를 들어 3. 20 인터넷 사태, 농협전산망 해킹 사태 등은 국가안보를 위협할 목적의 사이버 공격이지만, 민간인 사망 등 생명이나 신체에 대한 심각한 결과가 발생한 것은 아니므로 무력공격을 사용한 사이버 전쟁으로 보기 어려운 측면이 있다. 이러한 사태에 대한 대응은 사이버 전쟁이 아닌 사이버 공격, 위협 및 테러 대응의 일환으로 평상시에 지속적으로 수행되어야 할 국가안보 활동의 하나로 인식되어야 한다. 따라서 앞에서 지적한 바와 같이 국가안보를 위협하는 사이버 위기 상황은 국가보안 업무를 담당하는 기관에서 평상시에 지속적으로 대응하여야 한다.

아울러 사이버 공격에 대하여 합동참모본부 등이 사이버 전쟁이나 작전을 수행하는 경우 상대국이 무력공격으로 간주하여 사이버 전쟁으로 대응할 수 있는 빌미를 제공함은 물론 무력전쟁으로 확전될 가능성이 있다. 따라서 합동참모본부의 사이버 작전은 방어에 주력하여야 하며, 군 정보네트워크에 대한 평상시의 지속적인 감시·관제와 같은 소극적 대응과 훈련을 통해 사이버 공격에 대응하여야 한다.

3. 국민안전처

앞에서 살펴본 바와 같이 사이버 공격으로 인한 물리적 피해는 물론 사이버 공간의 피해에 대한 국가안전보장 차원의 대응을 위하여 정보통신기반보호법, 국가사이버안전관리규정으로 대응하고 있다. 다만 천재지변이나 대규모 정전사태에 따른 통신시스템에 대한 국가적 마비 사태 등 물리적 원인과 피해에 대한 대책으로서 재난대응체계의 발동은 가능할 것이다. 이러한 재난 관련 대책에 따라 국민안전처는 통신 인프라 시설에 대한 물리적 복구에 역량을 집중할 것이다.

한편 국민안전처의 연혁을 살펴보면, 1940년대 내무부 치안국 소방과에서 출발하여 1970년대까지 해양경찰대, 민방위본부 및 소방국을 거쳐, 1990년대에 해양경찰청과 민방위 재난통제본부로 확대되었다가, 2000년대 들어 소방방재청이 신설되고 해양경찰청와 안전행정부 안전관리본부로 확대 개편되었다. 이후 2014년 세월호 사건을 계기로 국민안전처가 설립되어 장관급기구로 격상되었으며, 기획조정실, 안전정책실, 재난관리실, 특수재난실, 중앙소방본부, 해양경비안전본부 등으로 구성되었다. 한편 특수재난실은 특수재난지원과, 민관협동지원과, 조사분석관으로 구성되어 있으며, 정보통신과 관련하여 특수재난지원과에 IT협업담당관 2명을 두고 있다.

이와 같은 조직 연혁과 편제에서 알 수 있듯이 국민안전처는 사이버 안전과 관련하여 사이버 공격에 대한 대응보다는 물리적 복구와 대응에 치중하고 있는 것으로 보인다. 아울러 사이버 공격을 포함한 각종 정보통신 관련 사고와 관련하여 2명의 IT협업담당관을 두고 있는데, 급격하게 증가하고 있는 사이버 공격, 사이버 범죄 등에 따른 사회적 재난과 관련된 업무를 감당하기에는 매우 부족하다고 할 수 있다.

국민안전처는 사이버 공격에 대응하기 위한 실질적인 조치나 대책을 조정하거나 기술적 지원을 제공하기 보다는, 물리적 피해에 대한 관련 기관 사이의 대응 등에 관한 협력을 독려하고 있는 수준에 그치고 있다고 보인다. 따라

서 국민안전처는 「재난 및 안전관리 기본법」을 근거로 사이버 공격에 대한 대응에 있어 특정 역할을 주도하기보다는, 정보통신기반보호법이나 국가사이버안전관리규정에 따라 사이버 공격에 대한 대응에 있어 기술적 우위를 점하고 있으며, 관련 기관들 사이의 활동을 조정 및 총괄할 수 있는 국가 보안 업무를 담당하고 있는 기관의 관련 활동에 협력하는 것이 보다 효율적인 것으로 보인다.

V 결 론

과학기술의 진보가 전혀 의도하지 않았던 현대적 위험 가운데 하나인 사이버 위험은, 사이버 공간이 존재하는 한 상존하는 것으로 위험이 있는 곳에 책임이 있다는 원칙에 따라 모든 사이버 이용자들에게 적절하게 분배되어야 한다. 그러나 사이버 위험은 위험의 결과를 즉시 알 수 없고, 원인규명을 명확하게 할 수 없는 경우가 많기 때문에 이용자들 사이에서 계약에 의하여 분배되기 곤란하다. 또한 사이버 보안에 대한 무임승차의 동인 및 투자대비 효용에 대한 명백한 자료와 데이터가 부재하여 민간 자율에 의한 사이버 위험 분배는 한계에 봉착할 수밖에 없다.

따라서 국가가 개입하여 어느 정도 강제적인 사이버 위험분배를 결정하고, 적합한 보안 수준 등을 지정함으로써 국가 전체적인 사이버 위험 방지와 대응 수준을 향상 시켜야 한다. 한편 사이버 위험은 재난이나 통합방위와도 일면 관련이 있지만, 재난관리는 사회적 재난으로부터 국민의 안전을 보호하는 데 중점을 두고 있으며, 통합방위는 영토·국민·주권의 수호라는 전통적 안보 개념에 기초하여 국가 총력전의 개념을 전제로 하고 있다는 점에서, 해킹, 바이러스 공격 등 사이버 위험으로부터 국가 핵심 기능을 유지하고 관리하며 국가 주권을 수호하기 위하여 국가·공공 기관의 컴퓨터와 네트워크를 보호하는 사이버 보안과는 다소 거리가 있다.

한편 사이버 보안 관련 기관의 역할을 살펴보면, 국가안보실은 정책 수행

기능은 없는 대통령의 보좌기관이기 때문에 국가 사이버 안보 정책의 기획, 계획, 입안, 조사 등의 업무를 수행하는데 일정한 한계가 있음을 알 수 있다. 사이버 공격에 대하여 합동참모본부 등이 사이버 전쟁이나 작전을 수행하는 경우 상대국이 무력공격으로 간주하여 사이버 전쟁으로 대응할 수 있는 빌미를 제공함은 물론 무력전쟁으로 확전될 가능성이 있다. 따라서 합동참모본부의 사이버 작전은 방어에 주력하여야 하며, 군 정보네트워크에 대한 평상시의 지속적인 감시·관제와 같은 소극적 대응과 훈련을 통해 사이버 공격에 대응하여야 한다. 또한 국민안전처는 사이버 공격에 대응하기 위한 실질적인 조치나 대책을 조정하거나 기술적 지원을 제공하기 보다는, 물리적 피해에 대한 관련 기관 사이의 대응 등에 관한 협력을 독려하고 있는 것으로 보인다. 따라서 국민안전처는 「재난 및 안전관리 기본법」을 근거로 사이버 공격에 대한 대응에 있어 특정 역할을 주도하기보다는, 정보통신기반보호법이나 국가사이버안전관리규정에 따라 사이버 공격에 대한 대응에 있어 기술적 우위를 점하고 있으며, 관련 기관들 사이의 활동을 조정 및 총괄할 수 있는 국가 보안업무를 담당하고 있는 기관의 관련 활동에 협력하는 것이 보다 효율적인 것으로 보인다.

사이버 위험에 대하여 재난관리 차원의 대응이나 통합방위 차원의 사이버 전쟁이 아닌 최적 정책수단의 선택이 필요하다. 이를 위해서는 사이버 공격 위험에 관한 평가에 기초한 정책 수단을 발굴할 필요가 있다. 사이버 공격 위험 평가에 기반한 사이버 위험 감소를 위해서는 위협이나 취약성의 감소나 제거는 물론 결과 발생의 방지가 핵심적으로 요구되는바, 평상시 국가 안보 활동을 강화함으로써 이를 차단하거나 감시하고 예방함은 물론 탄력적으로 대응하는 것이 중요하다.

이와 같이 평상시 국가안보 활동의 하나로 사이버 공격에 효율적으로 대응하기 위해서는 평상시 국가·공공기관에 대한 사이버 안보 업무를 담당하는 국가정보원의 관련 활동을 강화할 필요가 있다. 특히 사이버 안보의 핵심시설인 정보통신기반에 대한 보호 활동이 보다 적극적으로 수행되도록 하여야

할 것이다. 이를 위해서는 국가사이버안전관리규정에 기초한 사이버 안보에 대한 기본 법률이 제정되어야할 것이다. 아울러 사이버 안보와 관련된 연구개발에 대한 지원과 정책적 뒷받침을 강화하여야 한다.

그러나 국가정보원을 중심으로 한 사이버 안보 활동에 관해서는 민주적 통제절차가 강화되어야 할 것이다. 즉, 국회에의 보고, 승인, 감독 등 국회통제절차를 강화함으로써, 사이버 안보 활동이 국민적 지지 하에, 중요한 국가적 과제로서 지속적으로 추진되도록 하여야 할 것이다.

국가 사이버안보 강화를 위한 현행법제도 문제점과 개선과제 검토

김 희 정*

목 차

Ⅰ 서

최근의 사이버 위협은 단순 정보절취를 넘어 국민생활과 직결되는 사회기반시설의 안전까지 위협하고 있으며, 우리의 경제와 국가안보를 저해하는 가장 심각한 위협 중의 하나로 대두되고 있다. 실제 우리나라는 2009년 7.7 디도스 공격 이후, 2011년 4월 농협전산망파괴, 2012년 6월 언론사 전산망 파괴, 2013년 3월 3.20 사이버테러, 같은 해 6월 6.25 사이버 공격 등 사이버 공격으로 큰 피해를 입은 바 있다. 특히, 국가 및 공공기관을 대상으로 한 사이버 테러는 매년 수만건 씩 발생해 2010년부터 2014년까지 최근 5년간 약 7만 6천여건의 사고가 발생한 것으로 나타났다.

* 성균관대학교 연구원, 법학박사

그리고 대검찰청에 따르면, 올해 북한 해킹조직으로 추정되는 단체에 의해 1~6월 정부 외교·안보 부처 공무원과 전문가 등 90명을 대상으로 이메일 해킹 시도를 해 56명의 계정 비밀번호가 노출됐다고 한다. 또 최근 인터파크가 해킹으로 회원 1,030만명의 개인정보를 유출되는 사건이 발생했다.

이렇듯 빈번한 사이버테러에도 불구하고 여전히 사이버 테러 발생 시 효율적인 대응은커녕 컨트롤 타워의 부재, 법률 부재로 인한 각 부처간 책임 떠넘기기와 업무지휘 혼선 등으로 국민의 빈축을 사고 있다. 시·공간을 초월해 공공·민간 영역 구분 없이 동시 다발적으로 발생하는 사이버 위협에 대처하기 위해서는 사이버 위협정보를 공유·분석하고 협력해 사이버 위협을 조기에 탐지하고 전파할 수 있는 체계의 구축이 필요하다. 특히, 우리나라에서 발생된 많은 사이버 테러가 북한의 소행인 것으로 밝혀졌고, 피해액과 피해 수준도 높아 북한의 사이버 공격에 대비할 수 있는 법제가 마련되어야 함은 이미 오랜 시간 논의되고 주장되어 왔다. 하지만 사이버테러방지법과 같은 법이 국회에서 수년간 통과되지 못하고 있어 북한 뿐 아니라 외국의 사이버공격에 국가적 대응체계가 마련되지 못하고 있는 것이 현실이다.

그리고 사이버안보를 위한 사이버 공격에 대한 법적 개념이 명확하게 정의되지 못하고 있고 입법목적과 사이버 공격의 유형에 따라 소관부서도 제각각이라 앞서 언급한 바와 같이 효율적 대응이 어렵다.

이에 본 발표에서는 기존의 사이버공격의 유형과 지능정보화시대에 따른 새로운 사이버 공격을 예측해보고 국내 사이버안보와 관련된 법제도를 분석하여 효율적으로 사이버 공격에 대비하여 국가 사이버안보를 강화할 수 있는 개선과제를 검토하도록 한다.

Ⅱ 사이버안보와 사이버공격과의 관계

1. 사이버 안보의 개념

최근 몇 년간 사이버테러가 많이 발생함에 따라 사이버안보에 대한 관심이

증가하였고 사이버안보에 대한 관심과 함께 사이버안보에 대한 개념에 대한 관심도 증가하였다. 사이버안보라는 용어에 대해 법률상 명확한 정의는 아직 없다. 다만, 대통령훈령인 「국가사이버안전관리규정」에 사이버안전이라는 용어를 사용하고 있으며, 사이버안전이란 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성・무결성・가용성 등 안정성을 유지하는 상태로 정의하고 있다(제2조 제3호). 사이버안보 또는 사이버보안이라는 개념과 별도로 사이버안전이라는 개념이 사용된 배경은, 훈령 제정 당시 참여정부가 사이버보안이라는 용어가 아닌 새로운 용어를 찾았고, 그 결과 사이버안전이라는 새로운 개념이 등장하게 되었다.[1)]

즉, 사이버안보란 사이버상의 위험으로부터 정보의 기밀성・무결성・이용가능성 등을 유지 및 확보하기 위하여 모든 형태의 사이버공격으로부터 정보시스템과 정보통신망을 보호하는 일체의 행위로 정의할 수 있다.[2)]

2. 사이버안보 관련 개념 정리

사이버공격이란 국가사이버안전관리규정에서 정의하고 있는 바에 의하면, 해킹・컴퓨터바이러스・논리폭탄・메일폭탄・서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입・교란・마비・파괴하거나 정보를 절취・훼손하는 일체의 공격행위를 의미한다(제2조 제2호) 그리고 이미 많은 연구에서 사이버테러, 사이버전쟁, 사이버 범죄를 혼용해서 쓰고 있으며, 각 연구마다 개념을 구별하고 정의하고 있지만 개념을 구별하는 실익에 대해서는 명확하게 정의내리고 있지 않고 있다.

(1) 사이버테러의 개념

사이버테러란 용어는 사이버(Cyber)와 테러리즘(Terrorism)의 합성어이다. 테러는 대체로 정치적 목적을 달성하기 위해 정부나 대중 또는 개인에

1) 정필운, 사이버보안이란 개념의 사용의 유용성 및 한계, 의료・과학기술과 법, 2011, 9면.
2) 정필운, 앞의 논문 9-10면.

게 위해를 가하거나 예측할 수 없는 폭력을 사용하는 조직적 행위를 뜻한다.[3] 사이버테러는 사이버공간에서 사이버적 수단을 이용하여 이루어지는 테러리즘의 한 형태를 의미하며, 기존의 테러처럼 물리적 폭력이 아닌 해킹, 바이러스 유포 등의 형태를 나타낸다.

외국에서는 사이버테러에는 정보공격, 기반시설 공격, 기술적 조장, 기금마련 및 홍보로 분류한다. 정보공격이란 사이버테러리스트들이 전자파일, 컴퓨터 시스템, 다양한 자료의 내용물을 파괴하거나 변경하는 것을 의미하며, 기반시설 공격이란 사이버테러리스트들이 실제 하드웨어, 운영플랫폼, 컴퓨터 관련 프로그래밍을 파괴하거나 와해하도록 설계되어 있다. 기술적 조장은 테러리스트 공격 계획을 전송하고 공격을 시작하거나 전통적 테러 및 사이버테러리즘을 용이하게 하기 위하여 사이버 커뮤니케이션을 이용한다. 마지막으로 기금마련 및 홍보는 폭력적인 정치적 행동을 지지하는 단체를 발전시키기 위한 목적으로 기금을 마련하거나 폭력 성향이 있는 이념을 홍보하기 위하여 인터넷을 이용한다.

한국에서는 주로 수단 또는 수법의 피해를 중심으로 분류하고 있다.

경찰청 사이버 테러대응센터는 정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스 유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용하여 컴퓨터시스템과 정보통신망을 공격하는 행위를 사이버 테러형 범죄로 분류하고, 이를 해킹(단순침입, 사용자 도용, 파일 등 삭제와 자료유출, 폭탄메일)과 악성프로그램으로 구분한다.[4]

국가정보원은 국가안전 보장 또는 국가이익에 큰 피해를 유발할 우려가 있는 다음의 사이버공격으로서 국가정보원장이 별도로 분류한 것을 "안보위해공격"으로 규정하고 있다. 국가정보원 사이버안전센터의 안보위해공격 유형분류를 살펴보면 다음의 표와 같다. 이와 같이 기존의 한국의 사이버테러는

3) 김흥석, 사이버테러와 국가안보, 저스티스 제121호, 한국법학원, 2010, 324면.
4) http://wwww.netan.go.kr

정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스 유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용하여 컴퓨터시스템과 정보통신망을 공격하는 행위로 나누거나 국가안전보장 또는 국가이익에 큰 피해를 유발할 우려가 있는 사이버공격으로 크게 분류할 수 있다.

[국가정보원 사이버안전센터 안보위해 공격 유형 분류]

유형	내용
국가기밀에 속하는 문서·자재·시설·지역 등을 대상으로 한 공격	국가정보원법 제3조 및 보안업무규정에 따른 국가기밀에 속하는 문서·자재·시설·지역 및 이를 관리하는 인원을 대상으로 한 사이버공격
반국가단체, 국제범죄조직 및 테러단체에 의한 공격	국가보안법 제2조에 따른 반국가단체, 국가정보원법 제3조에 따른 국제범죄조직 및 테러단체에 의하여 수행되는 사이버공격
국가안전보장 관련 주요정보통신기반시설을 대상으로 한 공격	'정보통신기반 보호법' 제7조 제2항에 따른 국가안전보장 관련 주요정보통신기반시설 및 이를 관리하는 인원을 대상으로 한 사이버공격
국가핵심기술을 대상으로 한 공격	'산업기술의 유출방지 및 보호에 관한 법률' 제9조에 따른 국가핵심기술 및 이를 취급하는 인원을 대상으로 한 사이버공격

(2) 사이버전쟁의 개념

사이버전쟁이란 국가와 국가 간에 사이버 공간상에서 벌어지는 일련의 전쟁 과정으로 자국의 특정 이익을 위해 타국을 대상으로 적대적 행위를 가하는 것을 말한다.[5] 사이버전쟁은 국가 간에 이루어지는 적대적 행위가 인터넷과 같은 사이버공간에서 정보기술을 이용하여 이루어지는 행위라고 볼 수 있다. 이와 같이 사이버전쟁은 국가 또는 국가를 대표하는 요원이 자국의 이익을 위해 인터넷 등 사이버공간에서 정보기술을 이용하여 타국을 대상으로 적대적 행위를 가가고 이에 대해 상대 국가가 사이버 공간에서 정보기술을 통해 공격을 방어하는 것을 의미[6]하는데 이러한 사이버전쟁은 전쟁법상 군사력의 사용이 가능할 것이다.

5) 조성권, 네트전쟁과 정보기관의 새로운 역할, 국제문제조사연구소, 2001, 4면.
6) 김흥식,앞의 논문, 322면.

(3) 사이버범죄의 개념

사이버범죄는 협의의 의미로는 컴퓨터시스템의 보안과 컴퓨터시스템에서 처리하는 데이터를 대상으로 하는 컴퓨터 사용의 위법행위, 광의의 의미로는 컴퓨터시스템 또는 네트워크와 관련된 모든 위법행위를 의미하는데, 이러한 위법행위로는 컴퓨터시스템이나 네트워크를 사용하여 정보를 빼오거나, 다른 사람에게 제공하거나, 배포하는 행위를 포함한다. 이러한 사이버범죄의 정의 외에도 정보통신공간, 사이버공간과 관련하여 일어하는 모든 범죄행위[7], 사이버공간에서 발행하는 범죄[8], 인터넷 사이트와 그것들을 서로 연계시키는 컴퓨터 네트워크를 수단으로 하여 특정 네티즌이나 사이트, 또는 네트워크 그 자체를 대상으로 하는 범죄 및 일탈[9], 개인 혹은 조직화된 단체가 사이버 공간에서 시간과 장소에 관계없이 개인과 단체들에 대하여 정치성을 내포하지 않고 경제적 이익과 관련된 행위 또는 반사회적·문화적 행위를 범하는 경우[10]로 정의되고 있다.

(4) 사이버테러, 사이버전쟁, 사이버범죄의 관계성

앞서 언급한 바와 같이 사이버테러, 사이버전쟁 그리고 사이버범죄를 명확히 구분하기는 쉽지 않다. 또 사이버테러, 사이버전쟁, 사이버범죄의 특성상 공격의 주체를 파악하기 어려우며, 공격의 목적 또한 정확하고 신속하게 파악하기 어려운 특성이 있다. 이러한 문제에도 불구하고 사이버테러, 사이버전쟁, 사이버범죄를 구분하는 실익은 각각의 정의에 따라 각기 다른 법률요건을 구성하고 소관부서도 달라 질 수 있기 때문이다.

사이버전쟁은 국가간에 발생하는 사이버상의 공격이라면 사이버범죄는 보통 개인 간에 사이버 상에서 발생하는 공격이다. 하지만 사이버테러는 개인 간 또는 국가간에 발생되는 사이버공격의 중간에 속하는 것으로 볼 수 있다.

7) 백광훈, 사이버테러리즘에 관한 연구, 한국형사정책연구원, 2001, 52면.
8) 신종범죄론, 사법연수원, 2009, 23면.
9) 이민식, 사이버공간에서의 범죄피해, 한국형사정책연구원, 2000, 29면.
10) 이태윤, 새로운 전쟁, 21세기 국제 테러지름, 2004, 198면.

그러므로 사이버범죄가 범위가 가장 큰 공격으로 볼 수 있으며 사이버 전쟁이 가장 좁은 범위의 사이버공격으로 생각할 수 있다.

즉, 사이버전쟁과 사이버테러 그리고 사이버범죄는 해킹, 바이러스 유포, 대량정보전송, 서비스 거부공격 등을 통한 컴퓨터 시스템 또는 네트워크에 대한 전자적 침해행위를 수단으로 하여 사이버공간에서 이루어지는 공격이라는 점에서 공통점이 있다. 하지만 사이버전쟁은 보통 국가기관 또는 기관을 대표하는 국가요원에 의해 국가적 이익을 위해 상대 국가에 대한 공격을 의미한다. 반면에 사이버범죄는 개인, 단체 또는 국가가 대부분 개인적 목적에 의해 개인적 피해 또는 단체나 조직의 피해를 목적으로 가하는 공격을 의미한다고 볼 수 있다. 이 둘의 중간 영역에 있는 사이버테러는 좀 더 복잡하다. 사이버테러는 개인, 국가 또는 테러집단에 의해 개인적, 정치적, 사회적, 종교적, 민족적, 군사적, 국가적 의도 등으로 국가안보, 사회안전 침해 또는 위협을 하는 공격을 의미한다. 문제는 사이버테러를 어느 범위까지 볼 수 있느냐에 따라 국가 안보를 위한 국가안전 사무의 수행기관들의 역할 또한 정의될 수 있을 것이라 생각된다. 사이버테러를 사이버전쟁으로까지 확대해서 본다면, 오프라인상의 평시상태에서 군사작전으로 사이버공격에 대응할 수 있는지가 문제가 될 수 있다.

형사정책연구원의 연구보고서의 분류기준에 따르면 사이버전은 국가의 공격으로 주요정보통신기반시설, 군사시설, 기반시설을 공격하여 국가기능 및 전쟁수행력을 파괴를 목적으로 하며 공격 근원지를 국외로 본다. 사이버테러의 경우는 국가나 테러단체가 주요정보통신기반시설, 군사시설, 기반시설을 공격하여 사회기능 마비 및 공포를 목적으로 공격 근원지는 국내 또는 국외이다.[11] 형사정책연구원의 연구보고서의 분류기준을 보더라도 사이버전과 사이버테러 모두 정보통신기반시설을 대상으로 하고 있고, 공격 근원지도 모

11) 윤해성, 강석구, 박영우, 김민호, 권현영, 김도승, 김기범, 사이버안전체계 구축에 관한 연구, 형사정책연구원, 2010, 57면.

두 국외, 공격 수법이나 공격대상도 거의 비슷하여 구별의 실익이 크지 않다고 할 수 있다.

3. 사이버공격의 유형

(1) 기존의 공격 유형

사이버공격의 전통적 유형은 해킹, 악성코드 유포, 서비스거부 공격 등이 있다. 해킹은 네트워크, 시스템, 응용프로그램, 데이터 기타 정보자원 등에 인가받지 않은 자가 의도적으로 혹은 물리적으로 불법 접근하는 행위를 말하며, 악성코드 유포 공격은 컴퓨터바이러스, 웜, 트로이목마, 백도어, 봇(BOT), 스파이웨어 등 악성코드가 사용자의 동의 없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 컴퓨터를 오작동 시키고 네트워크를 마비시키는 행위를 말하고, 서비스 거부 공격은 시스템에 과도한 부하를 유발하여 정상적인 서비스를 차단하거나 성능을 저하시키는 행위를 말한다. 그 외 기타 공격 유형은 위의 악성코드 공격, 서비스 거부 공격, 비인가 접근 공격 등의 요소를 복합적으로 이용하는 공격행위를 말한다. 그리고 미국 국립표준기술연구소의 「컴퓨터 보안사고 처리 가이드 초안」에 의한 보안사고 유형에 비인가자 접근, 강탈, 협박 부적절한 이용 등도 포함되어 있다.[12]

(2) 사이버공격의 진화

초기 사이버공격은 대부분 데스크탑 컴퓨터를 이용하여 인터넷에 접속하는 방법으로 이루어졌다면 현재는 무선 와이파이를 통해 스마트폰 등과 같은 모바일 장비로 인터넷 연결이 가능해 시공간을 초월한 공격이 가능해졌다. 이런 기술의 발달에 따라 기존의 사이버공격에 비해 피해의 범위가 광범위해지고 범죄수단 또한 진화하고 있는 것이 현실이다.

특히, 해킹의 방법도 변화되고 있다. 기존에는 특정 시간에 타인이나 회사의

12) 정준현・지성우, 국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구-애국자법과 국토안보법을 중심으로, 미국헌법연구, 미국헌법학회, 2009, 221면.

컴퓨터에 침입하여 영업비밀이나 개인정보 등을 훔쳐가는 형태였으나 최근에는 APT(지능형지속위협)의 방법으로 메일이나 웹문서 등을 통해 악성코드를 해킹 상대방에 심은 뒤 오랜 기간 잠복해 정보를 빼낸다.[13] APT(Advanced Persistent Threat)공격은 침투, 검색, 수집 및 유출의 4단계로 실행되는데[14] 특정 대상을 정해놓고 짧게는 수 개월에서 길게는 수 년까지 장기간에 걸쳐 은밀하게 공격을 감행한다.

이뿐 아니라 과거 비밀번호를 해킹해 상대방 통장에서 돈을 인출하던 기존 방법과 달리 상대방 컴퓨터 메모리에 상주하는 악성코드를 설치한 후, 피해자가 정상적인 은행거래를 할 때 데이터를 조작하여 받는 계좌와 금액까지 변경할 수 해킹, 즉 메모리 해킹이 주로 발생되고 있다.[15]

또 최근에는 무료쿠폰, 모바일 청첩장, 택배사에서 보내온 문자, 경찰청 또는 검찰청 사칭 문자 등을 내용으로 하는 문자메세지[16]를 불특정 대상에게 보내고 상대방이 인터넷 주소를 클릭하면 악성코드가 상대방 스마트폰에 설

13) 아이뉴스24 2016년 7월 28일자 인터파크 해킹은 북한 소행?…“면죄부 안돼” 기사 참조

14) APT 공격의 특징은 첫째, 침투단계에서는 공격자들은 표적의 대상에 대한 관찰과 아울러 목표시스템으로부터 침투를 위해 내부 임직원이 실수나 부주의로 링크를 클릭하거나 첨부파일을 열게끔 사회공학적 기법을 접목하거나 제로데이 취약점을 이용하기도 한다. 둘째, 검색단계에서는 보안탐지를 회피하도록 설계된 검색프로세스를 이용한 은밀한 정보수집이 이루어지게 된다. 셋째, 수집 단계에서 보호되지 않은 시스템에 저장된 데이터는 즉시 공격자에게 노출될 뿐 아니라 조직 내의 데이터오ㅑㅏ 명령어를 수집하기 위해 표적 시스템이나 네트워크 액세스 포인트에 루트킷이 은밀하게 설치되어 오랜기간 지속적으로 정보를 수집하게 된다. 마지막단계는 제어로서 불법 침입자들은 표적 시스템의 제어권을 장악하여 각종 기밀 데이터를 유출하며, 소프트웨어 및 하드웨어 시스템에 손상을 입히고 경우에 따라서는 원격 시동이나 소프트웨어 및 아드웨어 시스템에 손상을 입하고 또는 원격 시동이나 소프트웨어 및 하드웨어 시스템의 자동 종료를 야기하여 국가주요시설의 마비를 결과할 수도 있게 된다.; 정준현, 국가사이버 안보를 위한 법제 현황과 개선방향, 한국국가정보학회 학술대회, 2011, 85-86면.

15) 권양섭, 사이버범죄 처벌규정의 문제점과 대응방안, 법학연구 제53호 ,한국법학회, 2014, 187면.

16) 도로 교통법 위반 사건 기소내용 본문확인, 택배가 부재중으로 반송되었습니다. 주소지 확인요망~, 법원 등기 발송하였으나 전달 불가하였습니다. 조회요망 등의 문자를 발송한다.

치되어 상대방도 모르는 사이에 소액결제가 이루어지도록 하는 스미싱으로 인한 피해가 늘고 있다. 스미싱이란 문자메시지(SMS)와 피싱(Phishing)의 합성어로 기존의 피싱과 비슷하지만 스마트폰 이용자의 급증으로 새로운 형태로 변화된 사이버공격으로 볼 수 있다. 이외에도 사물인터넷 시대의 도래로 사물인터넷을 통한 사이버공격이 가능하다.

사물인터넷은 기기의 최소화, 경량화에 따른 보안이 취약하며, 여러 가지 기술이 통합되어 특정 서비스를 제공하기 때문에 각 요소 기술 자체의 보안 취약성과 연동 시 새로운 보안 취약성이 발생할 가능성이 매우 높다. 그러므로 사이버테러 또는 범죄 단체들이 사물인터넷을 공격할 가능성 또한 매우 높다. 실제 미국에서는 베이비 카메라가 많이 보급되어 있는데 많은 베이비 카메라가 보안에 취약한 것으로 조사되었다. 약 78달러에 팔리는 필립스의 베이비 모니터(모델명: In.Sight B120)는 암호화되지 않은 정보가 인터넷에 곧바로 연결되었고, 이렇게 되면 해커가 원격으로 카메라를 조종하거나 설정을 바꿀 수 있을 뿐 아니라 온라인으로 영상도 시청할 수 있게 된다.

사물인터넷시대와 더불어 지능정보화시대로 접어들고 있는 현시점에서 사물인터넷뿐 아니라 드론, 자율주행자동차, 지능형로봇 등도 사이버공격의 대상이 될 수 있다.

드론과 자율주행자동차도 사물인터넷과 마찬가지로 여러 가지 기술이 통합되어 있고 각 요소 기술 자체의 보안 취약성이 문제 될 수 있을 뿐 아니라 연동시 새로운 보안 취약성이 발생할 가능성이 매우 높다. 자율주행자동차의 경우 대상에 따라 '자동차 대 자동차'의 V2V(Vehicle to Vehicle)와 '자동차 대 시설'의 V2I(Vehicle to Infrastructure), '자동차 대 사람'의 V2P(Vehicle to Personal)로 나뉠 수 있는데, 가령 바로 앞 차 너머의 상황이나 신호를 위반하고 교차로로 질주하는 차의 존재를 미리 알려주는 등 각 통신 주체끼리 실시간으로 끊임없이 정보를 주고받는 식으로 이용된다. 이때 보안의 취약성에 따른 해킹 등의 사이버 공격이 발생되면 심각한 피해와 국가적 혼란을 야기시킬 수 있다. 드론과 지능형 로봇도 마찬가지이다. 지능형

로봇은 물류 및 배송서비스, 의료서비스, 인공지능 로봇, 군사용 로봇 등 다양한 분야에서 이용되는데 지능형 로봇의 경우 개인정보는 주로 로봇의 메모리에 저장되거나 소프트뱅크의 페퍼와 같이 클라우드에 저장되어 공유-업데이트 되므로 개인정보의 생성 및 수집부터 유통 및 관리, 활용에 이르기까지 안전한 관리와 보안 시스템이 요구된다. 기존의 해킹은 단순한 금전적 피해만을 야기했다면 지능형 로봇에 대한 해킹은 인체와 생명의 안전까지 위협할 수 있으므로 문제의 심각성이 크다고 할 수 있다.

Ⅲ 사이버안보와 현행법·제도의 현황과 문제점

1. 국내의 사이버안보 관련 법안의 현황

(1) 사이버안보를 위한 법안의 변화와 노력

19대 국회에서 2013년 서상기, 하태경 의원 등이 사이버안보와 관련된 법안을 발의하였다. 2013년 서상기 의원에 의해 발의된 「국가 사이버테러 방지에 관한 법률(안)」의 제안이유는 사이버위기 발생 가능성을 조기에 차단하여, 위기 발생시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 하는 것을 입법목적으로 하고 있다. 이 법률안의 특징은 국가정보원 중심의 사이버테러 방지체계를 구성하고 악성프로그램에 대한 조치, 기술이전, 국제협력, 포상, 벌칙 등 현행 국가사이버안전관리규정에서 다루지 않는 사항을 다수 추가하여 규율했다는 점이다.

2013년 하태경 의원에 의해 발의된 「국가 사이버안전 관리에 관한 법률(안)」은 사이버안전을 확보하며 국가의 안전보장과 국민의 이익에 이바지하는 것을 입법의 목적으로 한다. 이 법률안의 특징으로는 정책심의를 국무총리 소속 회의에서 수행하고 실행은 국가정보원을 중심으로 수행한다는 점이다. 이외에도 2013년 정청래 의원, 2014년 변재일 의원에 의해 발의된 정보통신기반보호법이 있다. 이 법안들은 앞서 소개한 법률안과는 달리 미래부가

사이버안보 컨트롤 타워 역할을 맡는 내용을 핵심으로 하고 있다. 이 법률안들은 국정원을 컨트롤타워로 하는것에 대한 반대, 인터넷이용자의 권리를 과도하게 침해한다는 이유 등으로 19대 국회 임기만료로 자동 폐기되었다.

이철우 의원은 20대 국회가 시작하자 「국가 사이버안보에 관한 법률안」을 재차 발의하였고, 이 법안은 △사이버안보 주요 사항 심의를 위한 대통령 소속 '국가사이버안보정책조정회의' 설치 △국가 차원의 종합적이고 체계적인 업무 수행을 위해 국정원장 소속 '국가사이버안보센터' 구성 △국정원장이 사이버안보 기본계획을 수립하고 이에 따라 시행계획을 작성해 책임기관의 장에게 배포하는 등의 내용을 담고 있다.

(2) 사이버안보와 관련된 현행법의 검토

1) 국내 입법 동향

현행 사이버안보와 관련된 법은 매우 산발적으로 규정되어 있어 일원화된 법률로 규정하여 법적 안정성과 효율적 대응체계를 갖춰야 할 필요가 있다.

현행법상 사이버공격의 대응에 대한 법률로는 형법, 정보통신기반보호법, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 국가정보화기본법, 전자정부법, 전자서명법 등이 있다. 특히, 국가사이버위기 대응체계와 관련해서는 "국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적"으로 발하여진 대통령 훈령인 국가사이버안전관리규정이 있다.

2) 정보통신망 이용촉진 및 정보보호에 관한 법률

「정보통신망 이용촉진 및 정보보호에 관한 법률」(이하 정보통신망법)은 정보통신망의 건전하고 안전한 이용을 촉진하고 정보통신서비스 이용자의 개인정보를 보호하기 위하여 제정되었으며, 사이버보안의 예방조치에 관한 여러 규정을 두고 있다.

정보통신망법은 정보통신서비스 제공자는 정보통신서비스의 제공에 사용

되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다고 규정하고 있다. 정보통신망법은 누구든지 정보통신망에 접근하여 권한 없이, 권한을 초과하여 침입하는 행위를 금지하고 있으며, 침입행위에 대한 형사처벌 규정을 두고 있다.

또 정보통신망법 제45조는 정보통신망의 안정성 확보를 위해 정보통신서비스 제공자에게 일정한 보호조치의무를 부과하고 있다. 즉, 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치, 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치, 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치, 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치를 하도록 규정하고 있다. 이는 EU나 미국과 비슷한 수준의 보안 위협의 조치로, 물리적·기술적 조치에 대한 정보통신서비스 제공자의 의무 규정을 다루고 있다고 볼 수 있다. 또한 제52조에서 인터넷 진흥원을 설립하여 정보통신망의 이용 및 보호를 위한 홍보 및 교육·훈련, 정보보호 산업 정책 지원 및 관련 기술 개발과 인력양성, 분쟁조정위원회의 운영 지원과 개인정보침해 신고센터의 운영, 정보통신망 침해사고의 처리·원인분석 및 대응체계 운영 등을 하도록 하고 있다.

이외에 악성프로그램의 유포 등 침해행위를 금지하면서 침해사고 대응을 위한 방송통신위원회의 대응조치 및 원인분석을 위한 규정도 두고 있다.

3) 정보통신기반보호법

정보통신기반보호법은 전자적 침해행위로부터 주요 정보통신 기반시설을 보호하기 위하여 제정되었으며, 국가안전보장, 행정, 국방, 금융, 통신, 운송, 에너지 등의 업무와 관련된 전자적 제어 및 관리 시스템 및 정보통신망 이용촉진 및 정보보호에 관한 법률상의 정보통신망에 대한 해킹, 컴퓨터바이러스, 논리메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의한 사이버 공격

을 금지하고 있다.

정보통신기반보호법에서는 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위, 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위, 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위를 주요정보통신기반시설 침해 금지 행위로 규정하고 형사처벌 규정을 두고 있다.

동법은 주요정보통신기반시설을 보호하기 위해 '정보통신기반보호위원회'를 설치하고(제3조), 정보통신기반시설을 관리하는 장에게 보호대책수립의 무를 부과(제5조)하고 있다. 또한 주요정보통신기반시설의 보호 및 침해사고의 대응을 위한 지침제정 의무를 부여(제10조)하고 있고, 동시설에 침해행위가 있을 경우 일정한 보호조치 명령을 내릴 수 있는 권한을 부여(제11조)하고 있다.

4) 형법

정보통신망 교란, 파괴 및 사이버전쟁과 관련하여 사이버상의 공격 행위에 적용할 수 있는 형법상 구성요건을 분석해보면, "손상·은식·기타방법으로 효용 해함", "손괴·불통·기타방법으로 방해", "전복·매몰·추락·파괴", "손괴·허위정보입력·부정입력·기타방법 정보처리에 장애를 발생", "허위정보입력·부정명령입력·무권한정보입력·변경하여 정보처리를 하게함"등으로 분류할 수 있다. 이러한 구성요건은 사이버상에서 이루어져 많은 피해를 발생시킬 수 있는데 이러한 행위로 인해 국가기관의 기능을 정지하거나(형법 제87조), 군용시설 또는 기타 물건을 파괴(형법 제96조), 공무소 사용서류 또는 전자기록 및 특수매체기록을 손상·은닉·기타방법으로 효용을

해함(형법 제141조 제1항), 교량을 손괴 또는 불통하거나 기타 방법으로 자동차・항공기 등을 전복・매몰・추락・파괴(형법 제187조), 교통방해 상해・사망(형법 제188조), 컴퓨터등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무 방해(형법 제314조 제2항), 전자기록 등 특수매체 기록을 취거・은닉 또는 손괴하여 타인의 권리행사 방해(형법 제323조), 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력・변경하여 정보처리를 하게 함으로써 재산상 이익취득하거나 권한없이 정보를 입력・변경하여 정보처리를 하게 함으로써 재산상 이익취득하거나 제3자로 취득(형법 제347조의2), 전자기록 등 특수매체기록을 손괴 또는 은닉 기타 방법으로 기효용을 해함(형법 제366조) 등이 있다.

이러한 행위 태양은 국가적 법익, 사회적 법익, 개인적 법익을 침해하는 경우로 나눌 수 있으며, 국가적 법익과 관련된 경우는 형법 제87조, 형법 제97조 등이며, 사회적 법익과 관련된 경우는 형법 제141조 제1항, 형법 제185조, 형법 제186조, 형법 제187조, 형법 제188조 등이며, 개인적 법익과 관련된 경우는 형법 제314조 제2항, 형법 제323조, 형법 제347조의 2, 형법 제366조 등이다.

또한 사이버상에서 국가의 의사와 상관없이 외국과 전투행위를 벌이고 이것이 무력에 의한 조직적 공격이라면 외국사전행위(형법 제111조)가 성립될 수 있으며, 사이버 테러 또는 사이버전쟁을 위한 특정・다수인이 계속적인 의사연락하에 단체를 조직하거나 이에 가입하였다면 범죄단체조직・가입죄(형법 제114조)가 성립될 수 있다.[17]

그 밖에 사이버 상에서 발생되는 비밀침해는 형법 제316조의 비밀침해죄

17) 윤해성, 사이버테러의 동향과 대응방안에 관한 연구, 형사정책연구원, 2012년, 247-249면.

에 해당할 수 있으나, 형법상의 비밀침해죄는 '봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸'을 대상으로 하므로, 비밀번호 등에 의해 보호 조치[18]를 해놓은 전자기록이어야 하며, 기록으로서의 성질상 저장매체에 저장된 것이어야 한다. 또한 그 내용을 지득한 경우에만 적용을 받기 때문에 전산망에 침입만 했을 뿐, 특정 정보를 알아낼 의도가 없었거나, 지득한 사실이 없다면, 형법상의 비밀침해죄는 성립되지 않는다.[19] 이 경우 전자통신망상의 정보통신비밀침해죄는 보호조치한 것에 한정되지 않으며, 저장한 것은 물론 '처리중이거나 전송 중인 비밀'도 포함하여 그 내용을 지득할 것을 요하지 않아 처벌가능하다.

5) 국가사이버안전관리규정

국가 사이버안전관리규정은 국가사이버안전에 관한 조직체계 및 운영에 관한 내용을 규정하고 있고 사이버안전업무를 수행하는 기관과의 협력을 강화하여, 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 사이버테러 범죄에 대응에 총괄하는 대통령 훈령이다.

동 훈령에는 국가사이버안전정책 및 관리(제5조), 국가사이버안전전략회의(제6조)가 규정되어 있는데, 이것은 국가정보원이 중심이 되어 사이버안전에 관한 국가의 기본정책을 결정하도록 하고 있다. 특히, 동 훈령 제8조에 국가정보원 소속하에 국가사이버안전센터를 두도록 규정하여, 동 센터에서 국가사이버안전정책의 수립 등 근본적인 사이버전략, 정보수집, 분석, 전파를 하도록 규정하고 있으며, 중앙행정기관의 장의 임무로서 사이버안전대책

18) 비밀로 한 특수매체 기록의 내용을 권한 없는 자가 권한 있는 자의 진정한 비밀을 이용하여 비밀을 지득한 경우 본죄에 해당하는가와 관련해서는 자신의 컴퓨터 계정에로의 타인의 불법적 접근을 막기 위한 비밀번호 자체만 가지고 본죄의 '봉함 기타 비밀장치'의 개념에 포함시킬 수 없으므로 본죄에 해당하지 않는다는 부정설과 본죄에 해당된다는 긍정설이 대립하고 있다. 입법취지를 생각했을 때, 긍정설이 타당하다고 본다.

19) 김일수・서보학, 형법각론, 227면.

수립・시행・훈련・사고통보 및 복구를 규정하고, 국가정보원장에 의한 사고조사 및 처리를 규정하고 있다.

6) 산업통상자원부 개인정보보호지침

사이버안보를 위한 법적 의무규정은 산업통상자원부 개인정보보호지침에서도 발견할 수 있다.

개인정보처리자는 정보통신망을 통한 개인정보처리시스템 및 개인정보를 보유하고 있는 업무용 컴퓨터에 불법적인 접근 및 침해사고 방지를 위해 시스템을 설치・운영하도록 규정하고 있다. 즉, 개인정보처리시스템에 대한 접속권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하도록 하고 있다. 또한 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다. 그리고 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 필요한 보호조치를 취하여야 한다. 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터만을 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있도록 규정하고 있다.

그리고 동 지침 제74조에서 개인정보처리자는 악성 프로그램 등을 방지・치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치・운영하여야 하며, 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시해야하며, 악성 프로그램 관련 경보가 발령된 경우 또는 사용중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트

공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하도록 규정하고 있다.

2. 국내의 사이버안보 관련 현행법과 법안의 문제점

국내에서 발생된 여러 사이버테러 사건을 분석해보면 몇 가지 문제점을 발견할 수 있다.

첫째, 북한의 사이버 테러 공격이 이미 현실화 되었고 은행 업무의 마비 수준이 아닌 앞으로 원자력・전력・가스・항공・교통 등 SCADA망으로 공격을 확대될 것이라는 예측이 불가능 한 일이 아니라는 점이다. 반면에 국가기관은 이러한 공격을 사전에 탐지하지 못하고 대응하지 못하고 있다. 사이버테러의 대부분은 사건 발생 직후에 인지하고 있는데, 이는 국가가 사이버테러에 대한 위협을 체계적으로 측정하지 못하고 있다는 것을 단적으로 보여주는 것이다. 이에 사이버공격에 대응하기 위한 독립된 통합법체계의 구축이 필요하다.

둘째, 공격의 귀속의 문제와 관련하여 수사기관이 중요한 역할을 한다는 점이다. 사건발생 초기에는 국정원, 방통위, 경찰청, 대검찰청 등 관련기관이 모두 참여하였지만, 사건의 귀속은 수사기관의 역할로 경찰과 검찰에서 범죄수사라는 수단을 통해서 공격의 주체를 북한, 중국 등으로 특정하였다. 이에 초기 대응과 관련하여 귀속의 책임과 역할을 부여할 법제도적인 체계정비를 강구할 필요가 있다.

셋째, 대부분의 사이버공격이 해외 서버를 이용하고 있다. 이에 사이버 테러 대응은 장기적으로 국제협력 체계를 구축하고 시스템화 해야 한다.

넷째, 사이버공격에 대한 법정형에 대한 정비가 필요하다. 외국에 비해 사이버공격에 대한 관대한 판결, 사이버공격의 심각성과 피해정도에 따른 엄중한 처벌을 위한 처벌조항이 없기 때문에 이와 관련한 처벌규정을 신설함은 물론, 물적 피해에 대한 형량을 더욱 강화할 필요가 있다. 또 형법, 정보통신망법, 정보통신기반보호법에서 사이버비밀침해, 사이버업무방해, 사이버업무방해, 사이버 자료훼손죄 등에 대해 각각 산발적으로 처벌 규정이 마련되어

있는데, 정보통신망법과 같은 특별법에 의해 처벌하기 보다는 형법전에 규정함으로써 구성요건적 지위를 높일 필요가 있다.[20]

다섯째, 사이버공격에 대비한 사이버 수사 전문인력 양성과 전문 증거분석 기구의 설립이 필요하다.

Ⅳ 우리나라 사이버안보 법·정책적 개선과제

1. 관계부처·기관 역할의 법적 근거 마련

우리나라는 사이버안보 상의 문제에 대한 관계부처 및 기관 역할에 대한 명확한 법적 근거가 정비되어 있지 않아 제도상의 문제가 항상 제기되어 왔다. 국가 사이버안보 종합대책에 의한 추진체계에서 청와대가 컨트롤 타워를 담당하고 국가정보원이 실무를 총괄한다고 정하였으나 현행법상 이를 뒷받침하기에 다소 부족한 점이 있다. 현재 사이버위협의 문제에 관해 국가정보원의 주요 규범으로 적용되는 「국가사이버안전관리규정」은 대통령훈령으로서 행정기관 내부에만 효력이 있고, 그 적용범위를 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망으로 있어 민간부문의 정보통신망과 정보통신기반시설은 제외하고 있어 실무 총괄의 근거로는 한계가 있다는 지적이 있다.[21] 즉, 사이버안보와 관련된 법령의 정비가 미진함에 따라 집행력이 미약하고 대국민 효력을 발휘하기에 한계가 있다는 것이다. 그러므로 법률상 관계부처·기관이 수행하는 사이버안보 활동의 법적 근거를 명확히 정하여 효과적인 사이버 위협에 대응하고 효율적인 사이버안보 마스터플랜을 수립할 수 있을 것으로 생각된다.

20) 권양섭, 앞의논문, 188면.
21) 권양섭, 앞의 논문, 189면; 김태계, 사이버테러 범죄 대응에 관한 제도적 문제점과 대책, 법과 정책연구 제 14권 제3호, 한국법정책학회, 2014, 1367면; 곽병선, 사이버테러 대응을 위한 법체계 검토, 법학연구 제59권, 한국법학회, 2015, 15면; 김재광, 진화하는 사이버안보 위협과 법제적 대응방안, 인터넷법제도포럼 발표문, 2016, 25면.

2. 정보공유 체계의 정립의 필요

현재 사이버안보를 총괄하는 법률이 없고 부문별로 정보보호를 정한 법률들이 산재하여 정보공유 체계가 불완전하다. 현행 법령 규정상 정보공유체계가 공공부문과 민간부문의 체계가 별개이며, 정보통신기반시설의 체계는 이와는 또 별개의 문제이다. 「국가사이버안전관리규정」에 의하면 공공부문의 경우 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체 없이 그 사실을 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출・훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가정보원장에게 통보하여야 한다. 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지・분석하여 즉시 대응 조치를 할 수 있는 보안관제센터를 설치・운영하여야 한다. 다만, 보안관제센터를 설치・운영하지 못하는 경우에는 국가정보원 등 다른 중앙행정기관의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치・운영하는 보안관제센터에 그 업무를 위탁할 수 있다. 보안관제센터를 설치・운영하는 기관의 장은 수집・탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다. 하지만 민간부문의 경우 「정보통신망법」에 의해 주요정보통신서비스 제공자, 집적정보통신시설 사업자, 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자는 침해사고 관련 정보를 미래창조과학부나 인터넷진흥원에 신고하도록 규정되어 있다. 또 주요정보통신기반시설의 경우 「정보통신기반보호법」에 따라 주요정보통신기반시설 관리기관의 장은 침해사고가 발생하여 소관 주요 정보통신기반시설이 교란・마미 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 그 사실을 통지해야 한다. 그리고 금융・통신 등 분야별 정보통신기반시설을 보호하기 위하여 취약점 및 침해요인과 그 대응방에 관한 정보제공, 침해사실

의 실시간 경보·분석체계 운영을 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다. 이와 같이 부문별로 정보공유체계를 관장하는 기관이 다르고, 공공부문과 민간부문 및 주요정보통신기반 시설의 정보공유체계가 일원화되어 있지 않아 정보가 원활히 교류되지 않을 소지가 많다. 따라서 공공기관간, 민간기업간, 그리고 공공과 민간 모두 정보공유가 원활이 이루어 질 수 있도록 부문별 구분없이 정보수집·분석을 책임질수 있는 정보공유 체계를 수집하고 정보공유의 활성화를 제도적으로 보장할 필요가 계속해서 제기되어 왔다. 그러므로 새로운 법안에는 사이버 공격의 탐지 및 대응과 관련한 책임기관의 역할, 사이버 안보 유관기관간, 민관간 사이버위협정보의 공유에 관한 조직 및 협의체 구성에 관한 내용[22]이 포함되어야 할 것이다.

계속해서 발생되고 있는 사이버위협 및 테러에 효과적으로 대응하기 위해서는 민·관간의 정보의 공유는 필수적이고 이에 관련된 정보공유 및 분석에 관한 입법도 매우 필요하다. 다만, 사실이나 개인 프라이버시 침해의 문제를 효과적으로 해결할 수 있는 입법이 추진 될 필요가 있겠다.

3. 사이버안보를 위한 합동 대응 확립

현행 법령에 의하면 사고대응을 위한 합동대응 시 공공부문과 민간부문의 체계가 별개이고, 정보통신기반시설의 체계는 이와 또 별개로 구성되어 있다.

정부는 우리나라의 사이버 공간의 보호를 위해 국가 사이버안보 강화 방안을 마련하여 시행하고 있다. 사이버안보 역량 강화, 핵심기술 개발 및 인력양성, 국제공조 확대, 업무수행체계 정비, 컨트롤 타워 강화 등 범정부 차원의 대책을 바탕으로 사이버안보 강화를 위한 다방면의 노력을 다하고 있다. 현재 정부는 국가안보실 중심으로 사이버안보비서관을 신설하고 국가사이버안전센터를 통해 민·관·군의 사이버위협 합동대응팀을 운영하고 있다. 「국가

22) 김재광, 앞의 발표문, 33면.

사이버안전관리규정」에 의해 국가정보원장은 국가 차원의 사이버 위협에 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반을 설치·운영할 수 있으며, 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우에는 관계 중앙행정 기관의 장과 협의하여 범정부적 사이버위기 대책본부를 구성·운영할 수 있다. 한편, 미래창조과학부는 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 민·관 합동조사단을 구성하여 그 침해사고의 원인을 분석한다. 이와 별개로 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생된 경우에는 정보통신기반보호위원회의 위원장이 이에 필요한 응급대책, 기술 지원 및 피해복구 등을 위한 정보통신기반 침해사고 대책본부를 둘 수 있다.

이렇듯 우리나라에서 사이버테러 등 사고가 발생하면 공공부문은 국가정보원 주도의 민·관·군 합동 대응반이 꾸려지며, 민간부문은 미래창조부가 주도하는 민·관합동조사단, 주요정보통신기반시설은 정보통신기반보호위원회가 주도하는 정보통신기반침해사고대백본수가 합동 대응하게 된다. 하지만 현행 우리나라 사이버 침해대응에 관한 규정이 각 개별 법령으로 산재되어 침해사고 규정 및 단일화된 추진체계가 미비하여, 신속하고 효율적인 침해대응 체계 구축이 어려운 문제가 있다. 이미 최근 몇 년간 수차례의 해킹 사건이나 디도스 공격으로 인해 사이버안보의 공공·민간의 구분은 불필요하고 이에 따른 대응은 효과가 떨어지는 것을 겪어왔다. 또 ICT, IoT 시대에는 더욱 공공·민간의 구분이 불필요해졌다고 할 수 있다. 그러므로 산재되어 있는 법령의 일관성과 통일성을 구축하고 사이버안보조직체계의 명확한 정립이 하루빨리 이루어져야 할 것이며 이에 따른 적절한 법체계가 규정되어야 할 것이다.

4. 처벌규정의 정비와 양형의 문제

사이버테러나 범죄에 대해 우리나라는 특별법을 제정해 대부분 대응해 왔다. 대부분의 사이버공격에 의한 테러 또는 범죄를 형법보다는 정보통신망법 등과 같은 특별법에 의해 처벌되고 있다. 사이버범죄는 IT 기술과 과학기술의 발달에 따라 진화하고 있어 형법이 적극적으로 대응하기 어렵기 때문에 특별법이 효과적으로 대응하수 있지만 형법전에 사이버범죄를 규정함으로써 구성요건적 지위를 높일 필요가 있다는 주장도 있다.[23] 즉, 형법으로 포섭 가능한 사이버범죄들은 형법에 규정하는 것이 특별법 난립으로 인하여 발생하는 여러 문제들을 해결하고, 사이버범죄에 보다 효과적으로 대응할 수 있다는 주장이다. 하지만 형법이 IT 기술과 과학기술의 발전에 따른 사이버테러나 범죄를 모두 즉각적으로 대등하기 힘든 어려움이 있으므로 사이버테러와 범죄를 총체적으로 규율할 수 있는 일반법적 성격의 특별법은 필요하다.

예를 들면, 사이버명예훼손, 사이버비밀침해, 사이버자료훼손 등은 기존 형법 조문에 부가하여 조문화하고 형법상 컴퓨터사용사기죄의 행위 객체를 재산상의 이익에서 재물도 추가함으로써 안정적인 범죄적 지위를 확보할 수 있겠다. 이외의 사물인터넷이나 자율주행자동차, 드론 또는 지능형 로봇 등에서 발생하는 새로운 유형의 사이버공격의 피해에 대해서는 일반법적 성격의 특별법 예를 들어 현행 정보통신망법 등을 통해 신속하게 대응할 필요가 있다.

현재 사이버테러 범죄의 양형을 살펴보면, 정보통신망법상의 해킹, 컴퓨터 바이러스, 논리폭탄, 디도스 공격, 메일폭탄에 대해 최고 7년 이하의 징역 또는 7천만원 이하의 벌금에 처하도록 처벌 규정을 개정하여 더욱 엄격하게 처벌한다. 또 정보통신기반보호법상에는 침해행위의 대상이 정보통신기반인 관계로 그 형량이 10년 이하의 징역 또는 1억원 이하의 벌금으로 규정되어 있다.[24] 하지만 미국의 경우 「애국법」에 의하면 사이버테러 범죄를 범하는

23) 권양섭, 앞의 논문 188면.

인터넷 해커 초범에게도 징역 10년, 상습범에게는 징역 20년의 중형을 선고할 수 있도록 규정하고 있고, 특히 「사이버보안 강화법」에는 공격자가 고의 또는 부주의로 법률을 위반하여 심각한 신체적 상해를 유발하거나 시도한 경우 20년 이하의 징역에 처하고 사망에 이르게 하면 무기 징역에 처할 수 있도록 하고 있는데[25] 우리 법에 비해 엄격하게 처벌하고 있음을 알 수 있다. 정보통신망법은 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포한 경우, 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입, 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하는 경우보다 가중 처벌한다. 하지만 사이버테러 범죄로 인해 발생된 신체적 피해 즉, 상해나 사망에 대해서는 미국과 같이 처벌하는 규정이 미비한 것이 현실이므로 이에 관한 법률이 추가될 필요가 있다. 예컨대, V2V나 V2I 자율주행자동차를 다수 해킹하여 도로를 마비시킨다거나 사고를 고의로 발생시킨다면 형법 제185조의 일반교통방해죄, 제187조 기차등의 전복등, 제188조 교통방해치사상죄, 제190조 미수죄 등으로 처벌 가능성은 있다. 하지만 사이버테러 범죄로 인한 사고일 경우 일반 사고보다 더 엄격히 처벌할 필요가 있다.

또 사이버테러범죄로 인해 실형을 받은 수를 비교해보면 2012년 기준 형사재판에서 판결을 선고받은 총 인원 287,883명이고 그중 실형 선고를 받은 인원수는 41,889명으로 실명 선고율이 14.66%에 비해 사이버테러범죄의 대부분을 차지하고 있는 정보통신망법의 법률 위반죄에 관한 판결 선고인원은 1,753명 중 실형을 선고받은 인원은 59명[26]으로 실형 선고율이 3%에

24) 김태계, 앞의논문, 2014, 1352면.
25) 이연수외 3, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구", 국가정보연구 제1권 제2호, 한국국가정보학회, 2009, 97면.
26) 대법원, 2013년 사법연감, 884면

불과해 일반범죄에 비해 실형선고율로 매우 저조한 것을 볼 수 있다. 일반범죄에 사이버테러범죄가 피해의 범위와 심각성이 매우 큰것에 비해 처벌 수위와 처벌율이 매우 낮아 이에 대한 대책이 필요하다. 특히, 최근 인터파크 해킹 사건, SK, 한진 등 국내 대기업을 대상으로 발생한 공격, 2013년 방송사와 금융기관 등을 상대로 한 3·20 사이버테러 등 북한 소행의 사이버테러범죄에 대해서는 단 1명의 범죄자도 구속되거나 처벌한 전례가 없어 이에 대한 장래의 수사나 형사처벌에 대해서도 문제가 될 수 있다. 사이버테러범죄에 대한 법정 형량을 현행규정보다 상향조정해야 하며, 또한 사이버테러범죄로 인한 상해나 사망의 결과가 발생한 경우 결과적가중범에 대한 처벌규정을 신설함은 물론이고 물리적 피해에 대한 형량을 더욱 강화할 필요가 있다.

5. 사이버 수사 전문인력 양성과 전문기관 설치

사이버공격에 대비하여 입법적 공백을 최소화하고, 신속한 증거수집을 위한 제도적 장치를 마련해야 할 뿐 아니라 전문적인 기술을 이용한 사이버공격에 대응하기 위한 전문인력 양성이 시급하다. 최근 보도에 따르면, 북한의 주요 대남공작은 모두 정찰총국이 주도하고, 정찰총국 산하의 여러 연구소와 해커부대에는 과학영재학교인 금성1·2 중학교에서 집중교육을 받고 선발된 과학 영재들이 총참모부 산하 지휘자동화대학인 미림대학 등에서 사이버전사로 양성된 사이버 요원들이 집중적으로 배치된 것이라고 한다.[27] 현재 사이버 수사는 경찰청의 사이버테러대응센터, 전국지방경찰청 사이버범죄수사대, 경찰서 단위의 사이버범죄수사팀에서 전담하고 있다. 하지만 전문인력은 턱없이 부족한 상황인데, 지방경찰청에서는 전문인력이 배치되어 있다하더라도 일선 경찰서 단위는 사이버수사팀만 존재할 뿐 전문인력이 거의 전무한 실정이다.[28] 이에 외국이나 북한과 같이 대학에서 법학적 지식과 IT 기술

27) 문화일보 8월 1일자 기사, "北, 안보해킹부터 쇼핑몰 공격까지... 전방위'사이버 테러'
28) 권양섭, 앞의 논문 190면.

을 겸비한 융합형 인재를 양성하고 경찰과 국정원과 같은 기관에서 적극적으로 전문인력을 채용하여 전문성을 키워나갈 필요가 있다.

사이버테러 범죄와 관련된 증거는 무체정보성, 변조의 용이성, 원본과 구별 불가능성, 대량성, 전문성이라는 특성을 가지고 있어 기존의 유체증거물을 전제로 한 엄격한 강제처분 법정주의의 정의와 한정된 증거수집방법 만으로는 체계적으로 대응하기 힘들다.[29] 이런 사이버공격의 전문 인력의 수사와 관련하여 증거확보를 위한 디지털포렌식에 관한 법령과 디지털증거분석을 위한 연구소 설립을 위한 법령제정도 필요하다고 생각한다.

Ⅴ 결 론

지금까지 사이버안보와 관련하여 사이버테러, 사이버전쟁, 사이버범죄의 개념과 유형을 정리해보고 사이버안보와 관련한 현행법을 검토하면서 문제점과 개선방향을 제시해보았다. 가장 최근 언론에 보도된 북한소행의 사이버테러는 인터파크 해킹사건이었다. 언론 보도에 따르면, 북한은 대상을 가리지 않고 전방위 '사이버테러'를 행하고 있는데 북한 관련 정보를 다루는 외교·안보 부처 공무원의 이메일이나 스마트폰 해킹을 시도하는 것은 물론, 국민 생활과 밀접한 보건·산업 시설에 대한 사이버 공격까지 서슴지 않고 있다고 한다. 사물인터넷 시대를 넘어 지능정보화사회로 넘어가고 있는 현실에서 인공지능, 자율주행자동차, 드론, 로봇 등으로 사이버공격의 범위는 확대될 것은 당연한 일이다.

기술의 발달과 함께 사이버공격의 범위와 피해정도는 점차 커지고 있는 반면, 현행법의 사이버공격에 대한 보안, 대응, 처벌 등에 관한 규정이 산재되어 있어 즉각적이고 효과적인 대응이 힘든 것이 현실이다. 이에 사이버공격에 효과적으로 대응할 수 있는 전문 총괄기구가 설치되어야 하며, 위기경보,

29) 김태계, 앞의 논문 34면.

사후대응조치, 정보공유, 합동대응 등을 통합적으로 규정할 법률의 제정이 필요하다.

사이버공격에 대한 수사나 처벌에 관해서는 현행 형법에 의해 사이버테러 범죄에 대한 처벌 규정에 큰 흠결이 없어 보이나 사이버공간을 수단으로 하는 전통적 범죄는 형법개정을 통해 형법에서 규율하도록 하고 산재되어 있는 사이버 범죄처벌규정을 정비할 필요는 있겠다. 또한 사이버테러 범죄에 대한 양형에 대한 문제는 좀 더 고민해 볼 필요가 있으며, 처벌규정에 대한 정비도 중요하지만 효과적인 사이버 수사를 위한 수사절차상의 제도 보완도 필요하다.

[참고문헌]

정필운, 사이버보안이란 개념의 사용의 유용성 및 한계, 의료・과학기술과 법, 2011
김홍석, 사이버테러와 국가안보, 저스티스 제121호, 한국법학원, 2010
조성권, 네트전쟁과 정보기관의 새로운 역할, 국제문제조사연구소, 2001
김홍식, 사이버테러와 국가안보, 저스티스, 2010
백광훈, 사이버테러리즘에 관한 연구, 한국형사정책연구원, 2001
신종범죄론, 사법연수원, 2009
이민식, 사이버공간에서의 범죄피해, 한국형사정책연구원, 2000
이태윤, 새로운 전쟁, 21세기 국제 테러지름, 2004
윤해성, 강석구, 박영우, 김민호, 권현영, 김도승, 김기범, 사이버안전체계 구축에 관한 연구, 형사정책연구원, 2010
정준현・지성우, 국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구-애국자법과 국토안보법을 중심으로, 미국헌법연구, 미국헌법학회, 2009
정준현, 국가사이버 안보를 위한 법제 현황과 개선방향, 한국국가정보학회 학술대회, 2011
권양섭, 사이버범죄 처벌규정의 문제점과 대응방안, 법학연구, 제53호 2014
윤해성, 사이버테러의 동향과 대응방안에 관한 연구, 형사정책연구원, 2012
김태계, 사이버테러 범죄 대응에 관한 제도적 문제점과 대책, 법과 정책연구 제14권 제3호, 한국법정책학회, 2014
곽병선, 사이버테러 대응을 위한 법체계 검토, 법학연구 제59권, 한국법학회, 2015
김재광, 진화하는 사이버안보 위협과 법제적 대응방안, 인터넷법제도포럼 발표문, 2016
이연수 외 3, 주요국의 사이버안전관련 법・조직체계 비교 및 발전방안 연구, 국가정보연구 제1권 제2호, 한국국가정보학회, 2009
김일수・서보학, 형법각론, 227면
대법원, 2013년 사법연감
문화일보 “北, 안보해킹부터 쇼핑몰 공격까지... 전방위‘사이버 테러’, 8월 1일

사이버위협에 대응한 국가사이버안보법의 제정 필요성 및 고려요소

이 성 엽*

목 차

Ⅰ 서 론

종래 국가는 소위 야경국가(night watch state)로서 국가의 역할은 외교, 국방, 치안 등과 같이 국민의 재산, 신체, 생명의 보호를 하는 것이었다. 그러나 자본주의 위기를 거친 국가는 복지국가(welfare state)를 표방하여 생존배려 급부 등 국민의 최소한의 경제적, 사회적 삶의 보장하는 것을 목적으로 하고 있다.

인터넷혁명의 시대의 국가의 역할은 종래와 다르면서도 유사한 측면이 있다. 인터넷(Internet)은 네트워크의 네트워크로서 모든 사람과 사물이 사이버 공간에서 경계 없이 연결된다는 의미이다.[1] 이러한 인터넷혁명 시대에 국

* 법학박사, 서강대 ICT 법경제연구소 부소장/초빙교수
1) 최근 사물과 사물을 연결하는 사물통신이 Internet of things 즉, IoT로 불리면서

가의 역할은 우선 진흥 및 촉진국가이다. 인터넷 네트워크 구축, 산업 및 경제의 성장, 기업 활동의 지원 등의 역할이 중요해지는 것이다. 그 외 종래 야경국가와 유사한 사이버 야경 국가의 역할도 요구된다. 인터넷을 비롯한 사이버 공간에서 일어나는 사이버 공격의 방어, 정보보안, 개인정보 보호, 정보자유의 보호가 중요한 국가의 역할이 되는 것이다. 국민의 안전을 지키는 것은 그것이 물리적 공간이든 사이버 공간이든 국가의 가장 기본적 역할이라고 할 것이다.

그런데 한국에서는 이러한 사이버 야경국가 역할이 특히 중요하다고 할 수 있다. 그 이유는 첫째, 한국이 세계 최고수준의 인터넷 네트워크와 스마트폰 이용자수로 인해 사이버공격 및 위험에 지속적으로 노출되고 있다는 것이다. 둘째, 다른 국가와 달리 지속적인 남북 대치 상황으로 인한 사이버 공격 위협이 있다는 것이다.[2] 셋째, 사이버 위협정도는 높은데 비해 사이버위협, 정보보안에 대한 인식이 부족하다는 것이다. 보안에 대한 투자는 불요불급한 투자로 생각하는 경향과 보안사고 발생한 후에 사후 대처하려는 경향이 강하다는 것이다.

이하에서는 사이버 위협의 내용을 살펴보고 사이버위협에 대응하기 위한 법체계로서 국가사이버안보법 제정의 필요성과 법제정시 주요 고려사항을 살펴보고자 한다.

지능정보화 시대 핵심 기술로 각광 받고 있다.

2) 다음 두가지가 북한소행으로 추정되는 대표적인 사이버 공격사례이다.1) 3・20 방송・금융전산망 해킹(2013.3.20): KBS・MBC・YTN 및 농협・신한은행 등 주요 방송・금융기관의 전산망에 동시다발적으로 악성코드가 유포돼 서버・PC・ATM 등 총 4만 8748대 데이터가 삭제됨. 2) 한국수력원자력(한수원) 문서유출 (2014.12.15): 불상의 방법으로 한국수력원자력 조직도, 설계도면 등 6차례에 걸쳐 85건을 유출해 네이버 블로그 등에 게시하고 금전을 요구. 북한(중국 요녕성) 공격 추정. 이상의 사이버공격의 실태에 대해서는 김재광, 진화하는 사이버안보 위협과 법제적 대응방안, 제4차 산업혁명 물결, 「ICT 법제 개선방안 토론회 발표자료」, 2016. 7. 8, 1면-10면 참조.

Ⅱ 사이버위협의 내용과 특성

1. 사이버공격, 위협의 개념

사이버공격이나 사이버위협의 개념은 실정법상 용어가 아니기 때문에 이를 어떻게 설정할 것인지가 문제될 수 있다. 다음 3가지 법에 유사한 개념이 있다. 첫째, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법) 제48조상 "정보통신망 침해행위"인데 이는 ① 정당한 접근권한 또는 허용된 접근권한을 넘은 정보통신망 침입행위, ② 악성프로그램의 전달.유포, ③ 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하는 등의 정보통신망 장애 발생행위를 의미한다. 둘째, 정보통신기반보호법상 "전자적 침해행위"이다. 이는 정보통신기반시설[3]을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다(정보통신기반보호법 제2조 제2호). 셋째, 「악성프로그램 확산방지 등에 관한 법률(안)」상 개념이다. 이에 따르면 악성프로그램이란 정당한 사유 없이 컴퓨터·데이터 또는 컴퓨터에 설치된 프로그램을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 컴퓨터프로그램(특정한 결과를 얻기 위하여 컴퓨터 내에서 직접 또는 간접으로 사용되는 일련의 지시·명령으로 표현된 전자적 정보)이다. 감염이란 컴퓨터에 악성프로그램이 설치되어 해당 컴퓨터가 전자적 침해행위에 이용될 수 있는 상태를 말한다. 동법은 최근 컴퓨터, PDA, 스마트폰 등 다양한 정보처리장치를 통해 언제 어디서나 인터넷에 접속할 수 있는 IT 환경이 구축되면서, 일반 이용자컴퓨터를 대상으로 한 악성프로그램이 확산·증대되고 있으며, 특히, 악성프로그램에 감염된 이른바

3) 정보통신기반시설이란 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 의미한다(정보통신망법 제2조 제1호).

'좀비PC'가 DDoS(분산 서비스 거부) 공격 등 침해사고에 악용되고 있어 일반 이용자 컴퓨터를 보호할 수 있는 법체계 확립이 필요하다는 문제의식에서 입법이 시도되었다.[4] 즉, 현행 정보보호 법제는 네트워크(망) 또는 정보통신기반 보호를 중점으로 하고 있어 이용자 컴퓨터의 보호 및 실효성 있는 침해사고 예방 및 대응에 한계가 있다는 문제의식으로 입법을 추진했으나 입법이 이루어지지 않았다.[5]

결론적으로 사이버공격, 사이버위협의 개념은 정보통신망법상 침해사고의 개념을 참조하는 것이 적절해 보인다. 즉, 사이버공격은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다고 할 수 있다(정보통신망법 제2조 제7호).

다음 사이버공격(cyber-attack), 사이버테러(cyber-terror), 사이버위협(cyber-threat), 사이버위기(cyber-crisis)의 구별이 문제인데, 기본적으로 사이버공격, 사이버테러는 원인행위, 사이버 위협 내지 위기는 결과로 이해할 수 있으며, 사이버테러는 사이버공격보다 광범위한 수단과 목표를 지닌 것으로 이해할 수 있고 사이버위기도 사이버위협보다는 광범위한 피해를 초래할 수 있는 상황으로 이해할 수 있다.

2. 사이버위협의 내용

1) 해킹(Hacking)

해킹이란 컴퓨터 네트워크의 취약한 보안망에 불법적으로 접근하거나 정보시스템에 유해한 영향을 끼치는 행위로 해킹방법으로는 ① 비밀번호 도용 ② 시스템 보안상의 빈틈 활용 ③ 트로이 목마 이용 ④ 제3의 신뢰인 이용

4) 보다 상세한 내용은 후술한다.
5) 한정연, 악성프로그램 확산방지 등에 관한 법률(안)의 주요내용 및 발전방향에 관한 소고, 「INTERNET & SECURITY FOCUS」, December 2014, 18면-41면. 입법이 좌절된 것은 일부 야당, 시민단체의 통신검열, 프라이버시 침해 우려가 그 이유가 되었다.

⑤ 침입 흔적 인멸 등이 있다. 대표적인 해킹 사례로는 2009년 7월 청와대와 미국 재무부 사이트 해킹, 2011년 4월 농협 전산망 해킹, 2013년 3월 언론사 및 금융기관 전산망 해킹, 2015년 10월 우리 정부 외교·안보라인 주요 인사 수십 명의 스마트폰 해킹이 있다.

2) 컴퓨터 바이러스(computer virus)

컴퓨터 바이러스는 컴퓨터 프로그램의 일종으로 사용자 몰래 스스로 복제하여 다른 프로그램을 감염시키고, 결과적으로 정상적인 프로그램이나 다른 데이터 파일 등을 파괴하는 악성 프로그램을 말한다. 특히 웜(worm) 바이러스 프로그램은 다른 유용한 프로그램들과 달리 자기복제를 하며, 컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 악성프로그램이며, 트로이 목마(Trojan horse)는 자료삭제, 정보탈취 등 사이버테러를 목적으로 사용되는 악성 프로그램이다.

3) 논리폭탄(logic bomb)

논리폭탄은 해커나 크래커가 프로그램 코드의 일부를 조작해 이것이 소프트웨어의 어떤 부위에 숨어 있다가 특정 조건에 달했을 경우 실행되도록 하는 것으로 컴퓨터 범죄의 하나이다. 즉, 논리폭탄이라는 용어 그대로 프로그램에 어떤 조건이 주어져 숨어 있던 논리에 만족되는 순간 폭탄처럼 자료나 소프트웨어를 파괴하여 자동으로 잘못된 결과가 나타나게 하는 것이다.

4) 메일폭탄(mail bomb)

메일폭탄이란 특정한 사람이나 특정한 시스템에 피해를 줄 목적으로 한꺼번에 또는 지속적으로 대용량의 전자우편을 보내는 것이다.

5) 서비스 거부(Denial of Service attack)

서비스 거부는 해킹 수법의 하나로 해커들이 특정 컴퓨터에 침투해 자료를 삭제하거나 훔쳐가는 것이 아니라 대량의 접속을 유발해 해당 컴퓨터를 마비시키는 수법이다. 특정 컴퓨터에 침투해 자료를 삭제하거나 훔쳐가는 것이

아니라 목표 서버가 다른 정당한 신호를 받지 못하게 방해하는 작용을 말한다.

6) 분산서비스 거부 공격(Distributed Denial of Service)

분산 서비스 거부 공격은 해킹 방식의 하나로서 여러 대의 공격자를 분산 배치하여 동시에 '서비스 거부 공격(Denial of Service attack: DoS)'을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 것이다. 해커가 사전에 악성프로그램을 유포하여 이른바 좀비PC를 만든 다음 악성프로그램에 감염된 좀비PC를 일제히 동작하게 하여 특정사이트나 시스템을 공격하는 방식이다. 공격 시나리오를 전체적으로 살펴보면, 컴퓨터를 해킹하여 사용자 몰래 악성프로그램을 설치해 놓거나 이메일 등을 통해 악성프로그램 유포하여 좀비PC를 만든 다음, 좀비PC로 하여금 공격 대상 서버에 대량의 신호 또는 데이터를 전송하여 서버의 정상적인 서비스를 마비시켜 해당 기관의 고유 업무를 방해하도록 하는 진화된 해킹 공격 방법이라고 할 수 있다.[6]

3. 사이버위협의 특성

1) 적용비용으로 막대한 경제적 피해 야기

사이버공격의 비용은 많지 않지만 인터넷 네트워크의 특성상 침해사고의 규모는 엄청난 것이 보통이다. KAIST가 추정한 2013년 3월 북한의 제3차 핵 실험 이후 북한의 사이버테러로 인한 직·간접적 피해액은 8,600억원 가량이며, 금융권의 피해액은 이와 비슷한 약 8,500억원 수준이다.[7]

2) 피해의 확산속도 및 침해규모의 심각성– 국가전체에 대한 심각한 위협

물리적 테러와 달리 사이버공격은 순식간에 정부, 기업, 개인에게 동시다발적인 피해를 야기 시킬 수 있다. 특히, 원자력발전소, 금융시스템 등 사회간접자본에 대한 공격은 국가사회의 기본적 시스템을 마비시킬 가능성이 있다.

6) 이상 사이버위협의 기술적 설명 내용은 네이버 지식백과, 컴퓨터인터넷IT용어대사전, 2011. 1. 20., 일진사등을 참고하여 정리한 것임.
7) 금융위원회 공식블로그(http://fssblog.com/220651281286. 2016.12.18. 접속)

3) 공격원인 및 흔적 발생의 곤란

DDoS 공격자는 대부분 상대적으로 해킹등에 미온적인 중국 등을 이용하기 때문에 역추적이 쉽지 않고, 공격에 사용되는 좀비PC 역시 서버도 있지만 대부분 보안에 취약한 Windows기반의 가정용 PC이며 더구나 DHCP[8]를 이용하기 때문에 IP를 알아도 역추적하거나 처리하기가 쉽지 않은 것이 현실이다.

4) 위협 제거의 한계, 상존하는 위험 관리의 필요성

보안을 아무리 강화한다고 하더라도 침해가능성이 존재한다. 왜냐하면 끊임없이 새로운 침해공격 수단이 개발되기 때문이다. 따라서 사전 예방은 물론 물론 사후 신속한 대응체계의 완비의 필요성이 존재하는 것이다.

Ⅲ 사이버위협에 대한 법제도적 대응의 필요성과 이슈

1. 주요국가의 대응방안

1) 미국

미국의 국가 사이버안전에 관한 최초의 법률은 1987년 제정되어 1990년대 중반까지 시행되었던 「컴퓨터보안법(Computer Science Act)」이다. 이 법은 연방정부의 컴퓨터시스템 내의 기밀정보(sensitive information)의 보안 및 프라이버시 보호 등의 기능을 하였다. 2001년 9·11 테러 이후 부시대통령은 국토안보부(Department of Homeland Security)를 신설하였고 그 권한을 근거지우는 「국토안보법(Homeland Security Act)」을 입법하였다. 국토안보부는 종래 FBI에 속해있던 국가기반시설보호센터(NIPC) 뿐만 아니

8) dynamic host configuration protocol의 약어. 윈도 NT를 기본으로 하는 근거리망(LAN)에 접속하는 컴퓨터에 IP 주소를 할당하는 마이크로소프트 사의 기술. 컴퓨터가 네트워크에 접속하면 DHCP 서버가 자신의 목록에서 IP 주소를 선택하여 할당해주는 것을 말한다(네이버 지식백과, 컴퓨터인터넷IT용어대사전, 2011. 1. 20, 일진사).

라 상무부의 CIAO 등 기존 부서들을 통합한 부서로서 물리적인 국토, 기반시설 보호 뿐만 아니라 사이버 보안의 총괄 조정업무를 담당하게 되었다.[9)]

2015년에는 「사이버안보법(Cyber Security Act of 2015, CSA)」을 제정하여 16개 정보기관을 관장하는 국가정보실과 국토안보부 등이 공공과 민간 간 정보공유 절차를 마련하였다. 이 법의 주용 내용은 다음 네 가지 정도로 볼 수 있다. 첫째, 민・관 사이버보안 정보공유체계 구축(Sharing centralized in the DHS)이다. 국가정보국장, 국토안보부장관, 국방부장관 및 법무부장관은 연방기관과 비연방기관(민간기관, 주・지방정부 등 포함) 간 사이버위협지표 및 방어조치에 관한 정보 공유 절차 구축 및 가이드라인을 마련하였다. 국토안보부와 법무부는 공유 받은 정보를 특정 연방기관(상무부, 국방부, 에너지부, 국토안보부, 법무부, 재무부 및 국가정보국)과 자동화된 방식으로 실시간 공유할 수 있도록 정책・절차 수립・공표하였다. 둘째, 민간기업의 책임제한(Liability protections require sharing “in accordance” with CISA)이다. 즉, 민간기관이 사이버보안 목적으로 정보시스템 및 정보를 ① 모니터링 및 ② 방어조치를 취하고, ③ 정보를 공유할 수 있는 법적 근거를 마련하였다. 이 경우 민간 기관이 이 법에 따라 사이버위협지표와 방어조치를 모니터링, 공유・제공받는 행위는 소송의 원인(cause of action)이 되지 못하도록 규정하고, 반독점법에 따른 책임을 면제하는 등의 보호규정을 마련한 것이다. 셋째, 개인정보 삭제의무(Requirement to remove information known to be unrelated personal information)이다. 즉, 정보 공유 전에 사이버보안 위협과 직접적 관련이 없는 특정 개인을 식별할 수 있는 정보 또는 특정인의 개인정보 포함 여부를 심사하여 삭제하는 절차를 확보하도록 하였다. 넷째, 정보의 사용제한(Limited use of shared information by federal and state governments)이다. 연방기관은 ‘사이버보안 목적’을 위해 사이버보안 위협

9) 권현준 외, 『사이버 보안법제 선진화 방안 연구』, 방송통신위원회 연구보고서, 2011, 12, 10면-44면.

이나 취약점을 확인하는 용도로만 공유 받은 사이버보안 정보를 사용하도록 제한을 받는다. 다만, 생명 또는 신체・재산상의 중대한 위해가 되는 특정한 위협 등 특정 범죄 관련한 법 집행 목적 등의 경우에는 일부 예외가 인정된다. 한편, 동법에 따라 국토안보부에 설립된 국가사이버보안 정보공유센터(NCCIC, National Cybersecurity and Communications Integration Center)에 사이버보안 위협지표 및 방어조치 정보, 사이버보안 위험과 사고 관련 정보 공유 기능이 부여 되었다.[10]

미국 사이버안보의 특성은 크게 네 가지로 나눌 수 있다. 첫째, 국토안보부에 사이버안보에 관한 권한 및 책임을 부여하고 있다는 점이다. 국토안보법(HSA)은 국가기반보호를 위한 관리를 담당하는 행정부처를 국토안보부(DHS)라는 이름으로 두고, 물리적 국가기반 뿐만 아니라 사이버보안도 국가기반으로서 보호하도록 하는 역할 및 책임을 부여하고 있다. 둘째, 대통령 직속의 사이버 안보자문관 및 자문위원회를 두고 있다는 점이다. 대통령의 소속에 사이버 보안자문관을 두고 연방정부의 개별 부서차원에서 행하기 어려운 부처 간 권한 배분, 범정부적・통합적 사이버보안 정책 마련 및 운영 등의 업무를 담당하도록 하였다. 셋째, 사이버안보에서 민관 협력을 강조하고 있다는 것이다. 예를 들어, 민간기업의 협조 없이는 사이버 위협정보의 분석에 사용되는 첨단기술 개발이 어렵다는 점을 인정하고 있다, 끝으로 사이버안보에서 소비자의 프라이버시 보호를 강조하고 있다. 예를 들어, 사이버 위협에 대비한 정보 공유시에도 소비자의 프라이버시 보호를 위한 장치를 고민하고 있는데 개인정보 유출시 30일 이내에 통지를 의무화하고 공유된 정보는 정보공개법에 따른 비공개대상으로 하는 방안 등이 그 사례라고 할 수 있다.

10) John Evangelakos, Brent J. McIntosh, Jennifer L. Sutton, Corey Omer and Laura S. Duncan, SULLIVAN & CROMWELL LLP, 「The Cybersecurity Act of 2015」, December 22, 2015, pp. 1-13.

2) 일본

2014년 11월 6일 일본 중의원 본회의에서는 사이버공격 대응에 관한 국가의 책무 등을 정한 「사이버보안기본법」이 통과되었다. 동법은 사이버보안에 관한 대응전략을 국가차원에서 종합적이고 효과적으로 추진하는 것을 목적으로 하며, 사이버보안에 대한 기본이념과 전략 및 국가의 책임을 정의하고 있다. 사이버 보안이 '정보시스템 및 정보통신망의 안전성 및 신뢰성 확보를 위해 필요한 조치를 강구하고 그 상태가 적절하게 유지관리 되는 것'이라고 정의하고 있고 정부 행정부처 및 산하기관들의 사이버보안 원칙준수와 함께 기간망사업자들 역시 사이버보안 전략 수립과 관련된 자발적인 노력을 촉구하고 있다. 사이버보안기본법에서는 현재 정부의 사이버보안 전략을 담당하고 있는 '정보보안정책회의'를 격상시켜 범부처를 대상으로 한 사이버보안 정책의 사령탑역할을 수행하기 위한 조직으로써 내각 산하에 「사이버보안전략본부」를 설치하도록 규정하고 있다. 내각관방장관이 본부장 역할을 하고 사무국 역할은 종래의 정보시큐리티 센터를 내각 사이버시큐리티센터로 개편하여 동 센터가 수행하도록 하였다.[11] 「사이버보안전략본부」는 사이버위협정보 수집, 사이버안보 사고조사, 행정기관 대책 평가 등 의 업무를 수행한다. 종래 정보보안정책회의는 총무성, 경제산업성, 국방성, 경찰청 등의 각 부처에서 파견된 인사들을 중심으로 구성되었으나, 법적 권한의 제약과 전문인력의 부족으로 인해 역할과 기능상의 한계를 노출하였다. 이에 따라 사이버보안전략본부에서는 민간보안전문가들을 기간제로 임용하기로 결정하고 또한, 국가안전보장회의(NSC)와 IT종합전략본부의 의견을 토대로 사이버보안전략안을 작성하고 지방자치단체들과 협력체제를 구축하였다.[12]

11) 내각 관방장관은 우리의 행정자치부 장관에 해당하는데, 종전에도 관방장관이 사무국 역할을 해왔으나 위원회 기구인 정보보안정책회의가 사이버보안전략본부로 확대 강화된 것이다.

12) KISA, 심층보고서-일본 정부의 사이버보안 강화 전략 분석, 「INTERNET & SECURITY bimonthly」, 2014 Vol.3, 5면-21면, 정보통신산업진흥원, -일본, 사이버보안기본법채택, 「정보통신방송해외정보(CONEX)」, 2014.11, 1면-3면 참조.

2. 법제도 대응방안의 이슈

1) 민간과 공공부문의 분리 내지 융합

공공부문은 공익의 원리가 지배하고 정부기관 등 공공기관에 대해서는 법치행정의 원리, 특별행정법관계가 적용되는 등 공공부문은 민간부문과 다른 특유의 이념과 조직형태를 가진다. 또한 공공부문은 국가의 방어나 국민에 대한 급부제공에서 필수적 역할을 하므로 이에 대한 사이버공격 시 그 파급효과나 피해가 훨씬 클 가능성이 있다. 반면 민간부문은 자율과 시장의 원리가 지배하고 기본권의 보장과 사적자치원칙이 적용된다는 측면에서 공공부문과는 상이하다고 할 수 있다. 다만, 민간 부문의 경우에도 대기업에 대한 사이버공격 시에는 피해가 적지 않고 인터넷네트워크로 연결된 사회에서 피해의 전파가 신속, 광범위할 가능성이 존재한다.

이에 민간과 공공부문을 통합하여 규율할 것인지 아니면 별도의 규율을 할 것인지 여부는 분리 및 통합에 따른 비용편익을 기준으로 할 필요가 있다. 분리에 따른 비용은 광범위하고 심각한 공격 시 이에 따른 통합적 대응 능력 부족으로 피해규모 증가, 통합조정의 곤란으로 인한 행정비용의 증가라고 할 수 있고 분리에 따른 편익은 민간부문의 자율성, 프라이버시의 보호 강화 가능성이 있다는 점이다. 한편 통합에 따른 비용은 민간부문의 자율성, 프라이버시 침해 가능성, 통합에 따른 기관 간 의사소통의 어려움 문제라고 할 수 있고 통합에 따른 편익은 전 국가적 사이버위협 대응에 유리하며, 특히 공공과 민간에 대한 동시 사이버공격시 대응에 효율적이며 사이버보안 자원의 집중 및 동원에 유리 하다는 것이다.

결국 공공과 민간을 구분하지 않는 광범위하고 신속한 사이버공격의 성격을 고려하면 통합형을 우선시 하는 것이 타당할 수 있으나 다만, 프라이버시 보호의 문제 등 민간의 자율성을 여하히 존중하면서 공공부문과의 통합을 이룰 것인지에 대한 고민이 필요하다고 할 수 있다.

한국의 경우 공공·민간 부문이 각각 분리, 독자 대응하고 있어 광범위한

사이버공격 위협에 대한 효율적 대처가 어려운 점이 있다. 공공 부문의 사이버 보안업무는 국가정보원이 대통령 훈령인 「국가사이버안전관리규정」에 따라 담당하고 있으나, 국회・법원・헌법재판소 등 입법・사법 기관들과 민간 분야는 대통령훈령 적용범위에서 제외되어 있는 상황이다. 민간 부문은 미래창조과학부가 정보통신망법 등을 근거로 하여 사이버공격 예방 및 대응을 위한 업무를 담당하고 있으나 법률 미비로 사이버공격 징후를 실시간 탐지・차단하거나 신속한 사고 대응에 한계를 보이고 있다.

2) 집중형과 분산형 체계의 선택과 양자의 조화 문제

집중형은 특정한 부서나 조직이 총괄적인 계획, 관리, 집행, 평가에 대한 권한과 책임을 지는 구조임에 반해 분산형은 분야별 부서나 조직이 해당 분야의 관리, 집행에 대한 권한과 책임을 지는 구조이다. 집중형과 분산형 체계의 선택기준은 업무의 특성이 효율성, 통일성을 요하는 것인지 아니면 다양성, 자율성을 필요로 하는 것인지 여부, 업무의 특성이 신속한 의사결정과 집행이 필요한 것인지, 아니면 참여와 토론이 필요한 것인지 여부, 업무의 특성이 위기대처와 관련된 것인지 아니면 평시적 업무를 대상으로 하는 것인지 여부 등이라고 할 수 있다.

다음 어떤 사안이 집중화 내지 집권화의 요인이 되는 것이 살펴보면 다음과 같다. 이 요인의 반대상황이 분산화 내지 분권화의 요인이라고 할 수 있다. 조직의 규모가 작으면 집권화 요인이 되며, 역사가 짧은 신설 조직일수록 집권화 되기 쉽다. 조직의 운영이 특정한 개인의 리더십에 크게 의존할 때 그 조직은 집권화 되기 쉬우며, 어떠한 조직이고 간에 그 조직이 위기에 직면하게 되면 집권화를 초래한다. 또한 상급자가 하급자로 하여금 획일적으로 행동하기를 원할 때 집권화는 촉진되며, 하급자(기관)가 능력면에 있어서 상급자(기관)보다 뒤떨어질 경우 또는 상급자(기관)가 하급자(기관)의 능력을 불신하는 경우에도 집권화가 촉진된다.[13]

13) (http://terms.naver.com/entry.nhn?docId=78005&cid=42155&categoryId=42155, 2016.12.18.접속), 이종수, 『행정학 사전』, 대영문화사, 2009.1.

결국 사이버안보의 집중형과 분산형의 선택도 유사한 기준을 적용할 수 있다. 사이버안보의 업무특성이 효율성, 통일성을 요하는 것인지 아니면 다양성, 자율성을 필요로 하는 것인지 여부, 사이버안보의 업무 특성이 신속한 의사결정과 집행이 필요한 것인지, 아니면 참여와 토론이 필요한 것인지 여부, 사이버안보의 업무 특성이 위기대처와 관련된 것인지 아니면 평시적 업무를 대상으로 하는 것인지 여부이다.

사이버안보업무의 경우 전반적으로 효율성, 통일성이 요구되고 신속한 의사결정과 집행이 필요함은 물론 위기대처와 관련되어 있다는 점에서 집중형이 분산형 보다는 적절한 선택일 가능성이 높다. 다만, 사회 각 분야의 물리적 보안을 소관분야별로 각 부서가 담당하고 있는 점을 고려할 때 사이버안보에 대해서도 분산형의 적절한 가미가 필요하다고 할 것이다.

3) 한국의 사이버안보의 체계의 내용과 평가

한국의 사이버안보의 총괄체계는 대통령 산하에 국가안보실(사이버안보비서관[14]), 국가사이버안전전략회의(의장: 국정원장, 위원: 차관), 대통령비서실(미래전략수석)로 구성되어 있다. 이와 함께 국가사이버안전센터(국정원)가 있으며, 이 산하에 민・관・군 사이버위협 합동대응팀이 구성되어 있다. 민・관・군 사이버위협 합동대응팀은 일상적 상황에서는 분산관리 방식을 적용해 민(미래창조과학부)・관(국가정보원)・군(국방부) 분야별로 역할을 분산한다. 그러나 국가안보 사안과 관련해서는 국정원이 총괄하는 중앙통제 방식을 적용하고 있고 최근에는 국정원・미래부・방통위・국방부・안행부・금융위 등 관계부처가 참여하고, 국정원을 중심으로 한 민・관・군 합동대응체계로 운영되고 있다.[15]

14) 2015.4월 한수원 해킹 등을 계기로 국가안보실내에 사이버보안비서관이 신설되었다. 미국의 백악관내 Cyber security coordinator와 유사하다고 할 수 있다.

15) 정준현, “국가 사이버안보를 위한 법제 현황과 개선방향”, 디지털 시대와 국가 정보발전, 「국가정보학회 동계학술회의 발표자료」, 2011.11.30, 박영철외, 『사이버보안체계 강화를 위한 정보보호법제 비교법연구』, 한국인터넷진흥원, 2015.12, 11면-51면 참조.

미래창조과학부는 주요 정보통신기반 보호시설 보호 대책 이행점검, 보호지원 주요 정보통신기반시설 지정 권고, 기반보호실무위원회 운영, 민간 정보보호 및 산업을 총괄하며 행정자치부는 개인정보보호 체계 구축, 국가기관 사이버침해 대응(정부통합전자센터: NCIA), 사이버 침해대응센터 운영을 맡고 있고, 국가정보원은 주요 정보통신기반 보호시설 보호 대책 이행점검, 보호지원 주요 정보통신기반시설 지정 권고, 국가사이버안전전략회의 및 국가사이버안전센터 운영, 정보보안 업무를 총괄한다. 또한, 국방부는 국방 분야의 사이버안전을 담당하고 방송통신위원회는 정보통신서비스 제공자 등이 운영하는 정보통신망의 안정적 운영, 침해사고 대응, 개인정보보호 등의 업무를 분장하고 금융위원회는 사이버보안과 관련해 전기통신금융사기 피해방지, 금융분야 주요 정보통신기반시설 보호, 금융분야 국가기반체계 보호를 담당하고 개인정보보호위원회는 개인정보보호 기본계획 및 관련 정책 수립을 담당한다.[16)]

한국의 사이버안보 체계는 민간영역은 미래창조과학부, 국방영역은 국방부, 공공부문은 행정자치부, 국가정보원으로 분산되어 있는 것처럼 보이나 다시 국가정보원이 사이버안전센터, 국가사이버안전전략회의를 통해 총괄기능을 수행하는 집중형 구조를 취하고 있다. 다만, 대통령 국가안보실 및 소속 사이버안보비서관이 사이버안보의 정점에 위치하는 집중형 의사결정 체제를 취하고 있다. 전반적으로 control 타워로서 청와대 국가안보실(사이버보안비서관)에 집권화된 거버넌스에다가 민, 관, 군별로 소관 부처가 책임을 지면서 다시 국가정보원이 일부 통합적 조정권한을 지닌 분산형 거버넌스가 복합된 구조로 평가된다. 집중형과 분산형의 적절한 조화가 이루어지고 있는 것으로 보여 거버넌스 자체에는 큰 문제가 없으나 합의제 형태의 최고 사이버안보 의사결정 기관이 미비한 점, 국가정보원의 역할 한계가 애매한 점이 개

16) 이상의 한국의 사이버안보대응체계는 권현준외, 앞의 글, 174면-193면, 이연수외, 주요국의 사이버안전 관련 법・조직체계 비교 및 발전방안 연구, 「국가정보연구」 제1권 2호, 2008, 56면-63면 참조.

선여지가 있는 점이라고 할 수 있다.

4) 사이버 위협정보의 공유와 프라이버시 보호의 문제

사이버 위협정보의 공유와 프라이버시 보호와 관련 미국의 아이폰 잠금 해제 사례를 살펴보고자 한다. 2015년 12월 2일 캘리포니아주 샌버나디노에서 발생한 총기테러로 14명이 사망하였고 이에 미 연방수사국(FBI)은 테러범이 사용하던 아이폰5c를 입수해 자체 해킹을 시도했으나 실패하였다. 캘리포니아주 연방지방법원은 테러범의 아이폰 잠금장치를 해제할 것을 애플측에 명령했으나 애플은 법원의 명령을 거부하고 법원의 명령에 대해 애플의 최고경영자(CEO) 팀 쿡은 "우리의 아이들과 가족 등 공공의 안전은 매우 중요하다고 생각하지만 개인정보를 보호하는 것 역시 더할 나위 없이 소중하다"며 "(법원의 명령을 따르는 것은) 국민을 심각한 위험에 빠뜨릴 수 있다"하면서 명령을 거부하였다. 공화당 소속 톰 코튼 상원의원은 "애플이 미국인들의 안전보다 테러범들의 사생활 보호를 더 우선순위에 올렸다"고 일침을 가했다.[17]

기술한바 같이 미국은 사이버보안에서 프라이버시를 강조하는 차원에서 개인정보 삭제의무와 정보의 목적외 사용제한을 규정하고 있다. 결국 이 문제는 사이버안보를 포함하는 국가안보와 프라이버시라는 가치의 충돌을 어떻게 해결하여야 할 것인지에 대한 문제이다. 즉, 국가입장에서는 국민의 생명, 재산을 보호하여야 하는 의무와 국민의 기본권을 보호하여야 하는 의무간의 충돌이고 국민입장에서 프라이버시권이라는 기본권과 생명, 신체, 재산의 자유 등 자유권간 권리의 충돌이라고 할 수 있다. 원칙적으로 이 문제는 어느 한편이 절대적 우열을 가릴 수 있는 문제가 아닌바, 우선적으로 법률유보의 원칙, 비례의 원칙[18]에 입각한 입법 및 정책집행이 요구된다고 할 것이다.

17) 방송통신위원회 블로그(http://blog.naver.com/kcc1335/220883850773, 2016.12.18. 접속), 에너지경제 2016.2.25.일자 기사 참조(http://www.ekn.kr/news/article.html?no=203140. 2016.12.18. 접속).

18) 우리 헌법상 근거는 헌법 제37조 제2항이다. 동조에 따르면 국민의 모든 자유와 권리

Ⅳ 사이버위협에 대한 국가사이버안보법 제정의 방향

1. 공공과 민간을 아우르는 통합 기본법 체계 확립

정부와 민간이 함께 협력하여 국가차원에서 체계적이고 일원화된 사이버 공격 예방·대응 업무를 수행하기 위해 통합법 제정이 필요하다고 할 것이다. 다만, 원칙적으로 기본법이 먼저 제정되고 이후 개별법등이 제정되는 것이 원칙이나 기본법이라는 성격으로 사후 제정되는 경우 개별적으로 존재하는 법률과의 관계를 명확히 하는 것이 타당하다. 즉, 구법, 신법 관계로 보아 신법우선 원칙이 적용될 가능성이 있고 만약 특별법, 일반법 관계로 보는 경우 특별법 우선의 원칙을 적용할 수 있을 것이다. 필요한 경우 개별법 조항중 적용을 배제하고 기본법을 적용할 필요가 있는 경우를 부칙에 명시하는 것을 고려할 수 있다.[19]

2. 집중형과 분산형의 적절한 조화를 추구하는 거버넌스 구축

기존 국가정보원, 미래창조과학부가 중심이 된 집중형 사이버안보 관리체계에서 관련 부처에 관리책임을 이전하는 분산형 사이버안보 관리체계를 구축을 검토하되, 다만, 통합적 의사결정을 위한 국가사이버안보위원회나 위기발생시 대책본부등 일부 사항에 대해서는 집중형 관리체계를 도입하는 것이 필요하다. 또한 대통령 국가안보실, 국정원, 그외 소관 부처의 역할 구분 및 한계를 명확화 할 필요가 있고 대통령 국가안보실 소속의 합의제 형태의 사이버 안보 최고의사결정기관의 신설을 고려할 필요가 있다. 또한, 사이버안보 계획 수립, 시행, 평가 과정에서 국정원과 소관 부처의 역할을 명확화하고

는 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다.

19) 개인정보보호법의 경우 정보통신망법, 신용정보법이 존재한 상황에서 제정되면서 그 성격을 두고 기본법, 일반법인지 논란이 있었다. 이에 따라 동일 내용이 양법에 존재하는 경우 기본법으로 보는 경우 신법우선에 따라 개인정보보호법이, 일반법으로 보는 경우 특별법 우선 원칙에 따라 기존법이 적용되는 차이가 있다.

소규모의 사이버위협과 대규모 국가적 위협을 구분하여 대응기관을 구분하는 방향의 검토가 필요하다.

3. 예방적 침해 대응, 유기적, 협조적 침해 대응 원칙의 강조

최근 발생하고 있는 침해사고의 특징은 동시다발적인 공격, 공공·민간영역을 구분하지 않는 무차별적 공격으로 단시간에 피해가 급속도로 확산되고 회복할 수 없는 손해가 발생하며, DDoS 공격과 같이 이용자의 PC를 공격의 객체이자 주체로 활용하기도 한다는 것이다. 따라서 침해사고 전에 이를 막기 위한 사전적 예방이 매우 중요하므로, 사이버 위협정보의 공유, 사이버안보 계획 수립, 사이버안보 기술개발, 인력양성, 국제공조의 원칙을 명시하는 것이 바람직할 것이다. 다음 사이버 보안 침해자에 대한 대응을 위해서는 국가 및 공공기관, 정보통신서비스제공자, 이용자 모두가 반드시 유기적으로 협조할 필요가 있다. 특히 대규모 침해에 대해서는 민, 관, 군의 역량을 결집하고 조정하는 조직을 구성하여 대응할 필요가 있다고 할 것이다.

4. 사이버보안과 기본권의 이익형량의 원칙

본질적으로 사이버 보안정책은 국민의 재산권 등 각종 기본권과 상충하는 것을 피할 수 없다. 사이버보안을 강화할수록 국민의 기본권이 제한되는 것이 불가피하므로, 입법자와 정책집행자는 사이버보안과 국민의 기본권 보호를 이익형량하여 균형점을 찾아 양자가 조화될 수 있도록 입법하고 정책을 집행하여야 한다.

이와 관련 사이버안보에 대한 개인정보보호법의 적용 제외가 문제될 수 있다. 현행 개인정보보호법은 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보의 경우에는 개인정보보호법 제3장(개인정보의 처리), 제4장(개인정보의 안전한 관리), 제5장(정보주체의 권리 보장), 제6장(개인정보 분쟁조정위원회), 제7장(개인정보 단체소송)의 규정이 적용되지 않도록 하고 있다(개인정보보호법 제58조 제1항 제2호). 이에 따라 주

요 개인 정보보호 관련 규정은 사이버안보 활동에 적용되지 않을 가능성이 높다. 또한 개인정보보호법은 공공기관의 장이 개인정보파일을 운용하는 경우에는 행정자치부장관에게 등록하도록 요구하는데(개인정보보호법 제32조 제1항), 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일등의 경우 등록이 면제되어 있어 사이버안보를 포함하는 국가 안전에 관한 사항을 기록한 개인정보파일을 운용하더라도 행정자치부장관에게 등록할 필요가 없다고 할 수 있다.[20]

다만, 사이버안보의 개념이 국가안보나 국가안전과 동일 개념인지에 대해서는 논란이 있을 수 있다. 즉, 단순한 사이버공격과 국가안보를 위협하는 사이버공격을 구분하여 전자의 경우 개인정보보호법의 규정의 적용이 가능하다는 입론이 가능하다. 그러나 현행법의 해석으로는 로 사이버안보와 관련해서는 개인정보보호법제의 작동가능성이 희박한 상황으로 평가되어 사이버안보와 개인정보보호의 긴장이 예상된다. 양자의 긴장을 조화하고 균형을 위한 기준으로는 덜 침해적인 개인정보 침해수단의 강구(The lesser technological privacy intrusive principle), 개인정보처리자의 책임성의 원칙(The principle of accountability), 투명성의 원칙(The principle of transparency), 비례의 원칙(The principle of proportionality), 효과성의 원칙(The principle of effectiveness), 공정성의 원칙(The principles of fairness)등이 고려될 수 있다.[21] 보다 구체적으로는 사이버안보에 관한 개인정보보호법의 적용여부 및 적용가능한 조항에 대한 검토를 통하여 이를 사이버안보입법안에 반영하는 방안을 검토할 필요가 있다고 할 것이다.

20) 상세내용은 최경진, 사이버안보와 개인정보보호법령의 상관성, 「嘉泉法學」 제8권 제4호, 2015.12.31. 참조.

21) Kevin Aqullina, Public security versus privacy in technology law: A balancing act?, 「Computer Law & Security Review」, Volume 26, Issue 2, March 2010.

5. 국민의 참여보장의 원칙

사이버 보안정책 수립, 집행의 결정과정은 정부가 독점해서는 안 되며, 사업자와 국민이 반드시 참여하는 것이 바람직하다. 이는 사이버 보안정책이 자칫 정부의 검열 또는 정보감시로 이어지지 않도록 하기 위해서도 매우 중요하다. 이와 관련 사이버보안 위원회 구성시 자문위원회 형태등 민간의 참여, 사이버안보 계획 수립시 민간의견 청취, 사이버안보 전문기업 육성등 민간 전문인력 양성에도 관심을 기울여야 할 것이다.

V 결 론

사이버위협 내지 사이버테러로부터 국민의 안전과 국가의 안전을 담보하여야 할 국가적 책무는 아무리 강조하여도 지나침이 없다고 할 것이며, 특히, 분단 상황에 있는 우리의 경우 더욱 중요성이 강조될 수밖에 없다. 또한, 사이버위협으로부터 안전한 신뢰기반의 지식정보사회의 구현이 IT 강국으로서 우리의 산업적 성장과 국민의 삶의 질의 향상의 기초자산이 되는 것이라는 점도 분명하다.

그럼에도 불구하고 한국의 현행 사이버보안 법체계는 관련된 법령도 다양할 뿐만 아니라 관련 규정도 여기 저기 산재되어 있는 문제점을 갖고 있으며, 추진체계와 관련하여 통일적인 조직을 갖추지 못하고 있는 것이 현실이다. '사이버 보안기본법'을 기본법이자 일반법으로 새롭게 제정하여 동법 속에 추진체계를 정비하고 기본계획과 시행계획 등 계획수립, 사전적 예방정책과 사후적 예방정책을 명시적으로 규율하는 것이 필요하다고 할 수 있다.

다만, 이 경우에도 사이버보안 강조가 프라이버시 등 국민의 기본권 침해, 민간의 자율성 저하로 이어지지 않도록 투명하고 엄격한 절차를 통한 정보공유, 민간참여, 민간역량 강화에도 소홀하지 않도록 할 필요가 있다고 할 것이다.

[참고문헌]

권현준외, 『사이버 보안법제 선진화 방안 연구』, 방송통신위원회 연구보고서, 2011.12.

김재광, 진화하는 사이버안보 위협과 법제적 대응방안, 제4차 산업혁명 물결, 「ICT 법제 개선 방안 토론회 발표자료」, 2016. 7. 8,

박영철외, 『사이버보안체계 강화를 위한 정보보호법제 비교법연구』, 한국인터넷진흥원, 2015.12.

이연수외, 주요국의 사이버안전 관련 법·조직체계 비교 및 발전방안 연구, 「국가정보연구」 제1권 2호, 2008.

정보통신산업진흥원, 일본-사이버보안기본법채택, 「정보통신방송해외정보(CONEX)」, 2014.11.

정준현, "국가 사이버안보를 위한 법제 현황과 개선방향", 디지털 시대와 국가정보 발전, 「국가정보학회 동계학술회의 발표자료」, 2011.11.30.

최경진, 사이버안보와 개인정보보호법령의 상관성, 「嘉泉法學」 제8권 제4호, 2015.12.31.

한정연, 악성프로그램 확산방지 등에 관한 법률(안)」의 주요내용 및 발전방향에 관한 소고, 「INTERNET & SECURITY FOCUS」, December 2014.

KISA, 심층보고서-일본 정부의 사이버보안 강화 전략 분석, 「INTERNET & SECURITY bimonthly」, 2014. Vol.3.

John Evangelakos, Brent J. McIntosh, Jennifer L. Sutton, Corey Omer and Laura S. Duncan, SULLIVAN & CROMWELL LLP, 「The Cybersecurity Act of 2015」, December 22.

Kevin Aqullina, Public security versus privacy in technology law: A balancing act?, 「Computer Law & Security Review」, Volume 26, Issue 2, March 2010.

제7장 최근 주요국의 사이버안보 입법동향과 시사점

북미의 사이버안보 입법동향과 시사점

- 미국과 캐나다를 중심으로 -

조 정 은*

목 차

Ⅰ 들어가는 글

2001년 9월 11일, 미국 뉴욕에서 발생한 테러는 전 세계를 공포에 휩싸이게 했으며, 국제사회가 테러에 대하여 대응하는 방식을 완전히 바꿔놓는 계기가 되었다. 9.11 테러 이전에는 많은 국가들이 정보기관으로 하여금 테러 조직에 대하여 정보를 수집하게 하고, 테러 관련자들의 자국 입국을 막는 등의 방식으로 테러에 대비하였다. 미국 정부는 9.11 테러 이후 이러한 테러 대응 방식이 불충분한 것으로 판단하고, 반테러(Anti-Terror)의 개념을 도입하였다. 반테러란 테러 조직이 테러 공격을 감행할 때까지 감시하다 대응하는 것이 아니라, 테러조직으로 변할 가능성이 높거나 테러 조직에 비전투적 지원을 하는 사람들에 대한 감시를 강화하여 애초부터 테러가 발생하지

* 건국대학교 박사

못하도록 하는 전략을 말한다. 미국이 이러한 개념을 소개했을 때 반대하던 다른 국가들도 자국에 비슷한 테러가 발생한 이후에는 미국과 마찬가지로 반테러 개념을 도입하였다.[1)]

이와 더불어 사이버공간 역시 테러의 위협에서 자유롭지 못하게 되었다. 왜냐하면 과학기술의 발전으로 현실공간과 사이버공간의 간극이 좁아졌고, 현실 공간에서 다루어져 왔던 이슈들이 사이버공간에서도 다루어지기 시작했기 때문이다. 따라서 안정적인 사회의 구현을 위해서 주요 기반 시설을 비롯한 정부 기관, 은행, 언론 기관 등의 핵심적인 인프라 시스템을 사이버공격으로부터 방어 및 보호해야 할 필요가 생겼다. 특히, 국내외를 막론하고 해킹 등에 의해서 군사 분야를 비롯한 정부의 중요 정보들이 침해 또는 탈취 되는 것을 우려해야 하는 상황이 되었다. 이에 따라 EU, OECD 등 주요 국제기구와 미국, 일본 등 여러 나라들이 국가 사이버안보 전략(national cyber security strategy)을 수립하여 사이버안보에 관한 입법을 위해 노력하여 왔다. 우리 정부도 이러한 세계적 흐름에 동참하여 「국가 사이버안보 기본법(안)」을 통과시키기 위해 노력 중이다. 그러나 일각에서는 「국가 사이버안보 기본법(안)」이 정보기관에게 너무나 많은 권한을 주어 인권이 침해될 소지가 크다고 반대하고 있다.[2)] 따라서 우리나라보다 먼저 사이버테러에 대하여 적극적으로 대처하기 위해 관련 법제를 정비해 온 국가들의 사례를 살펴보고 그 시사점을 도출해내는 것은 앞으로 우리 법제의 발전에 큰 의미가 있다고 할 것이다. 이하에서는 미국과 캐나다의 국가사이버안전관리 체계와 관련 법제의 동향에 대해서 살펴보도록 하겠다.

1) 2004년 3월 11일 스페인 마드리드 테러, 2005년 7월 7일 런던 연쇄 테러 등이 일어난 뒤에 이들 국가 모두가 '반테러' 개념을 도입하였다. 특히 2005년 런던 연쇄 테러 이후 실시된 국제 반테러 작전 '오버트(Operation Overt)' 역시 이러한 개념을 바탕으로 영국을 비롯한 여러 국가들이 참여하여 여러 건의 연쇄 테러를 사전에 예방할 수 있었다.

2) 6개 시민단체 국가 사이버안보 기본법 제정(안)에 대한 의견서, 2016.10.10, http://act.jinbo.net/wp/17784/참조.

Ⅱ 미국의 사이버안보 입법동향

1. 미국의 사이버안보관련 정책

미국에서 사이버안보에 대한 관심이 오바마 행정부에 들어서서 갑자기 시작된 것은 아니다. 오바마 행정부에 이르러 보다 적극적으로 관련 정책들이 추진되어 온 것은 사실이지만, 미국은 사이버안보가 국가안보와 직결되어 있음을 인식하여 꾸준히 관련 정책을 추진하여 왔다. 그리고 최근에는 예산 긴축 중에서도 사이버안보에 대해서는 꾸준히 예산을 늘려왔다.

1998년 5월 클린턴 행정부는 '대통령령 63호(Presidential Decision Directive, PDD 63)'[3]를 통해 국가 기반구조보호센터(PCCIP)를 설치하였다. 그리고 1999년에는 국가기반시설보호센터(PCCIP) 및 주요기반시설보증국(CIAO)을 설치 및 운용하였다. 한편, 부시 행정부는 2001년 9.11 테러 이후 사이버안보를 구축하기 위해서 2002년 제정된 「국토안보법(Homeland Security Act of 2002)」을 바탕으로 국토안보부(Department of Homeland Security, DHS)를 신설하였으며[4], 2005년에는 국방부에서 사이버공간에 대한 작전 개념을 정립하였다. 그리고 2008년에는 국가사이버안보센터(National Cyber Security Center)를 국토안보부(DHS) 산하에 설치하여 사이버안보기능을 총괄하게 하였다.

2009년 오바마 행정부가 수립된 이후에도, 사이버안보는 여전히 중요한 정책 이슈였다. 2009년 1월에는 백악관이 사이버안보를 조정하고 통제하도록 하였으며, 5월에는 '사이버공간 정책 리뷰(Cyberspace Policy Review) 보고서'를 발표하여 국가안보차원의 기본 방향을 제시하였다. 뿐만 아니라 국방부, 국토안보부와 '사이버 스톰(Cyber Storm)'이란 명칭으로 사이버보안 훈련도 실시하였다. 2009년 6월에는 사이버사령부(USCYBERCOM)를 창설하

3) 대통령령 63호는 사이버보안이 대통령이 주도하는 중요한 업무의 성격을 띠기 시작했음을 보여주었다.
4) 미국 국토안보부 홈페이지, https://www.dhs.gov/history

고 NSA 국장이 동 사령부의 사령관을 겸임하도록 하였다. 2011년 7월에는 '사이버 공간에서의 국방부 운용전략(Department of Defense Strategy for Operating in Cyberspace)'을 발표하여 사이버공간을 새로운 작전영역으로 천명하고, 동년 8월에는 국가 사이버안보 마스터플랜을 발표하였다.

오바마 행정부는 2013년 2월 '오바마 행정명령(Executive Order 13636)'과 '정책지침(PPD 21)'을 발표해 주요 기반시설의 사이버보안 체계를 정비하기에 이른다. 이러한 배경에는 2기 오바마 행정부의 출범 직후 주요 언론사들과 주요 기반시설이 지속적으로 사이버테러에 노출되면서 주요 기반시설의 보안을 강화하기 위해 제정하려 한 「사이버 정보공유 및 보호법(Cyber Intelligence Sharing and Protection Act)」과 「사이버보호법(Cyber Security Act of 2012)」의 상원 부결이 있다. 2015년 2월, 오바마 대통령은 2015 국가안보전략(the 2015 National Security Strategy)에서 안보 내에 공유된 공간(영공, 영해, 우주, 사이버)의 접근성 보장이란 목표로 사이버보안과 관련된 내용을 제시하고 있다.[5] 그리고 2016년 2월 초에는 '사이버보안관련 국가행동계획(Cybersecurity National Action Plan, CNAP)'을 통해 사이버위협이 미국이 직면한 가장 주요한 도전이라는 점을 다시 강조하면서 2017년 사이버보안예산을 이전 년도에 비해 35% 늘어난 190억 달러를 요구하였다.[6] 동 행동계획은 오바마 대통령 임기 동안의 사이버보안 관련 정책을 집대성하고 국가적 사이버보안 강화를 위한 실천적 행동계획을 발표한 것이라 볼 수 있다.

5) 미국 백악관 홈페이지, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf
6) 미국 백악관 홈페이지, https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

[사이버보안관련 국가행동계획(CNAP)]

계획	주요 내용
국가 사이버보안 증진위원회(Commission on Enhancing National Cybersecurity) 설립	– 민・관・학계 전문가가 참여하는 국가 차원의 사이버보안 증진 대책 마련 – 연방정부, 주정부 및 지방정부, 민간부문 간의 파트너십 강화
IT 현대화 기금(Information Technology Modernization Fund)의 조성	– 기금으로 31억 달러를 조성하고 연방최고정보보안관(Federal Chief Information Security Officer) 제도 신설 및 임명
일반 시민의 온라인 사이버보안 강화	– 국가사이버보안협의체(National Cyber Security Alliance)를 구성 – 구글, 페이스북, Visa 및 여타 금융기관과의 공동대응 체제 구축
관련 예산 증액	– 2017년도 대통령 예산안에 사이버보안 관련 예산을 190억 달러 신청하였음.

출처: The White House

2. 미국의 사이버안보관리체계

미국은 사이버안보와 관련한 행정체계가 잘 정비되어 있고 관련 입법도 매우 활발하다. 전통적인 수사기관으로는 연방수사국(FBI)과 중앙정보국(CIA)이 있으며, 9.11 테러 이후 많이 기구들이 창설되거나 재정비되었다. 9.11 테러 이후 연방수사국(FBI)의 주요 활동목표를 테러공격을 막는데 두도록 기구와 운영방향을 개혁하였다. 그리고 미국의 국토방위가 최우선순위로 여겨지면서 미국내 정보보호 및 대테러업무를 총괄하는 조직으로 국토안보부(DHS)가 창설되었고, 백악관 내 국가안전보장회의(NCS)에 유사한 형태의 국토안보회의(Homeland Security Council)도 설립되었다. 특히 오바마 대통령은 2009년 사이버 안보 관련 보좌관을 신설하였으며, 4성 장군을 사령관으로 하는 사이버 사령부(U.S. Cyber Command, USCYBERCOM)를 2010년에 신설하였다.

(1) 미국 연방수사국(FBI)과 중앙정보국(CIA)

미국 연방수사국(Federal Bureau of Investigation. FBI)은 전통적인 주요 수사기관으로서 사이버테러리즘을 포함한 테러리즘에의 대응을 주요 임무로 인식하고 있다.[7] 연방수사국은 2002년 사이버국(Cyber Division)을 신설하고 미국 내외에서 국내 정보기관 협력조정을 비롯하여 국토안보부 지원, 집행기관과 대응 노력을 주도하고 있다.[8] 이에 대해서는 2003년 대통령 국가 사이버공간 보안 전략(The 2003 National Strategy to Secure Cyberspace)에서도 명시적으로 잘 나타나 있다.[9] 연방수사국과 협력 중인 국내 정보기관으로는 미국정보공동체(U.S. Intelligence Community, USIC), 국가사이버수사공동대응팀(National Cyber Investigative Joint Task Force, NCIJTF) 등이 있다. 2016년 6월에는 대통령 지시명령에 따라, 기존까지 국토안보부가 주무부서로 담당해 오던 연방정부 사이버위협 대응 업무를 연방수사국(FBI)으로 이관하였다. 그리고 중앙정보국(CIA)은 미국의 정책 담당자들에게 국가보안정보를 제공하는 독립기관으로, 대통령과 정책 담당자들이 국가보안에 관한 정책을 결정할 때 도움을 주기 위해 해외 정보를 수집, 평가, 제공하는 것을 주된 임무로 한다. 다만 중앙정보국은 직접 정책을 수립하지 않는다.[10]

(2) 미국 국토안보부 (DHS)

미국 국토안보부(Department of Homeland Security, DHS)는 다음과 같은 사이버안보 대응체계를 갖추고 있다. 즉 사이버사건 발생 시 국토안보부는 피해 기관에 대한 지원, 주요 사회기반시설에 대한 잠재 영향 분석, 법집행

7) FBI 웹사이트, https://www.fbi.gov/investigate/cyber; https://www.fbi.gov/news/stories/new-us-cyber-security-policy-codifies-agency-role
8) FBI 웹사이트 https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view
9) The National Strategy to Secure Cyberspace, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
10) CIA 웹사이트, https://www.cia.gov/about-cia/cia-vision-mission-values

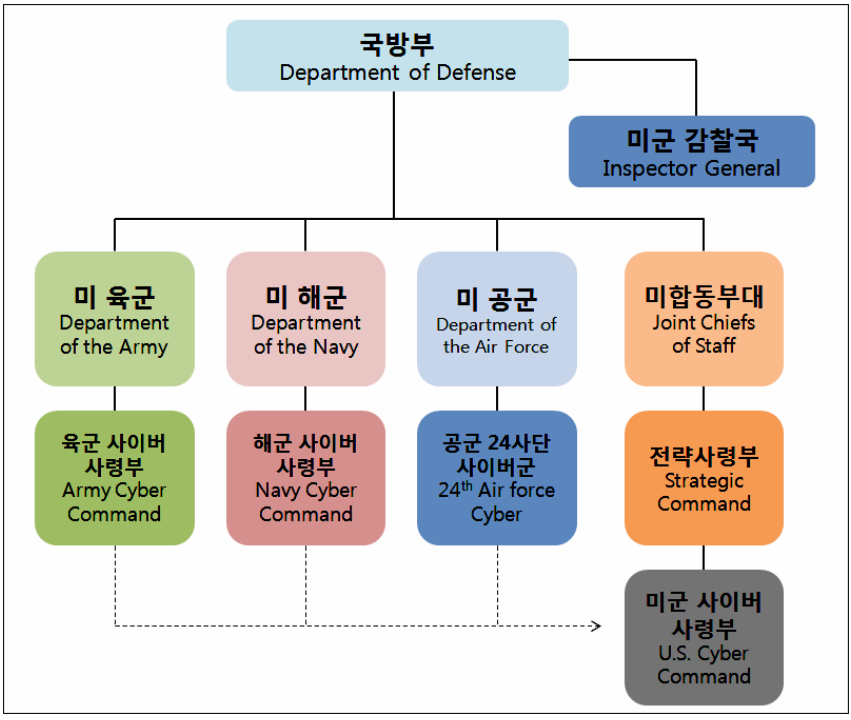
협력기관과 책임자 수사, 중대한 사이버사건에 대한 국가 대응 체제 조정을 담당한다. 또한 국토안보부는 사이버 및 통신 통합의 가교 역할을 하는 국가사이버안보 및 통신 통합센터(National Cybersecurity and Communications Integration Center, NCCIC)를 통해 24시간 실시간 감시, 사건 대응을 담당하고 있다. 뿐만 아니라 NCCIC의 미국 컴퓨터비상태세팀(United States Computer Emergency Readiness Team, US-CERT)에서 국가 네트워크를 대상으로 하는 범죄를 저지하기 위한 최신 네트워크 및 디지털 미디어 분석 전문지식을 갖추고 있다.[11]

(3) 사이버사령부

미 사이버 사령부는 미군전략사령부(U.S. Strategic Command, USSTRATCOM) 산하에 설치되어 미군 전체의 사이버보안 전략, 대응, 기관별 협력 계획을 수립하고 집행하는 기관으로, 육군 사이버 사령부(Army Cyber Command, ARCYBER), 제24 공군(24th USAF), 함대 사이버 사령부(Fleet Cyber Command, FLTCYBERCOM), 해병 사이버 사령부(Marine Forces Cyber Command: MARFORCYBER)로 구성된다. 현재, 사이버 사령부의 사령관은 국가안보국(NSA)의 국장이 겸임하도록 하고 있는데, 최근 펜타곤은 오바마 대통령에게 국가안보국과 사이버사령부를 분리하여 사이버전쟁(cyberwarfare)과 전자스파이(electronic espionage)에 대한 별개의 기관을 만들 것을 권고하였다.[12]

11) 미국 국토안보부 웹사이트, http://www.dhs.gov/cyber-incident-response
12) Pentagon Mulls Splitting Cyber Command, NSA, September 14, 2016. http://www.defensetech.org/2016/09/14/carter-mulls-splitting-cyber-command-national-security-agency/

[미국 사이버사령부 조직 체계]



출처: Department of Defense

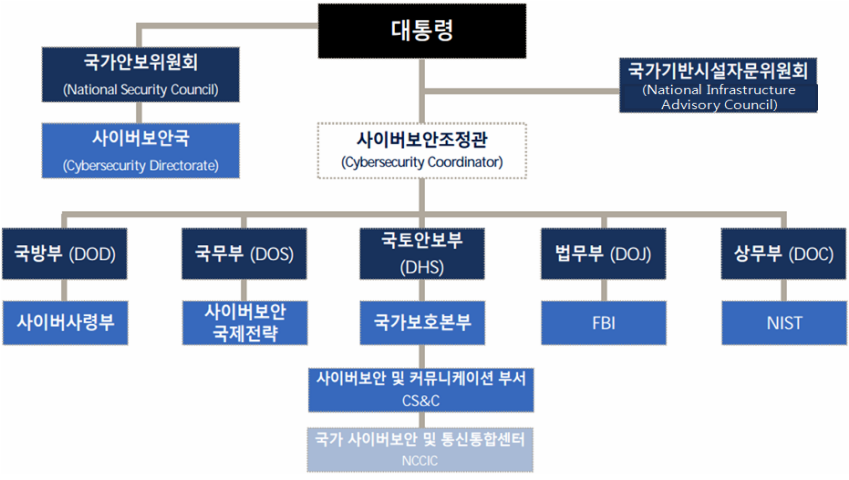
(4) 기타 기구

대통령의 자문기구로서 행정명령 13231호에 근거하여 설립된 국가기반시설자문위원회(National Infrastructure Advisory Council, NIAC)는 적어도 30명 이상의 민간 부분, 학계, 주 및 지방 정부의 고위 간부 기반보호 전문가를 중심으로 구성된다.[13] 국가기반시설자문위원회(NIAC)는 국토안보부 장관을 통해 기반의 보안과 경제의 중요한 분야를 지원하는 물리적 뿐만 아니라 사이버분야에 대한 자문을 대통령에게 제공한다. 대통령의 보좌기

13) 미국 국토안보부 웹사이트, https://www.dhs.gov/national-infrastructure-advisory-council; https://www.dhs.gov/sites/default/files/publications/niac-brochure-03-04-14.pdf

구로서 핵심적 국가안보 및 대외정책을 논의하는 국가안보위원회(National Security Council, NSC)에도 사이버보안국(Cybersecurity Directorate)을 두고, 국내·국제적 사이버보안침해를 국가안보의 핵심 쟁점의 하나로 파악하여 범정부차원에서 문제를 해결할 수 있도록 조직화하고 있다. 한편, 대통령의 소속에 사이버보안조정관을 두고 연방정부의 개별 부서차원에서 행하기 어려운 부처간 권한 배분, 범정부적·통합적 사이버보안정책 마련 및 운영 등의 업무를 담당하게 하고 있다.

[미국 사이버안보관리체계]



출처: The White house

3. 미국의 사이버안보 관련 입법 동향

미국 의회는 사이버안보에 관한 법률을 제정 또는 개정하는 입법조치를 적극적으로 추진하고 있다. 국토안보법(HSA), 연방정보보안관리법(FISMA), 주요기반정보법(CIIA), 사이버보안

강화법(CSEA), 국가사이버안보보호법(NCPA) 등을 근거로 관리예산처(OMB)와 국토안보부(DHS) 등이 정부 전산망과 주요 시설을 보호하고 있다.

(1) 애국법

미국의 애국법(Patriot Act of 2001)은 9·11 테러 이후에 계속되는 테러 위협에 대응하기 위한 수사력 강화와 국가안보 확립이라는 목표 하에 미국을 포함한 세계 각국의 법제도에 큰 영향을 미쳤다. 애국법은 효과적인 테러 예방대책을 마련하고 테러수사의 효율성을 제고하기 위해 법집행기관과 정보기관의 감시·조사 권한을 확대하는 다수의 규정을 두고 있다.[14] 테러범죄와 관련된 연방수사국의 감청권의 확대, 범죄수사를 위한 정보공유권, 유선·대화·전자통신 감청 및 정보공개 제한규정에 대한 광범위한 예외 규정, FBI에 테러범죄와 관련된 첩보·정보 수집 등의 권한부여, 수사기관의 테러관련 범죄수사를 위한 통신기록 추적절차를 용이하게 하고, 테러관련사건 수사를 위한 수색영장 발부권과 영장의 예외규정을 신설, 테러자금의 세탁방지와 테러자금 유입 차단을 위하여 국제적 돈세탁에 대한 추적과 감시 강화, 이민국적법(Immigration and Nationality Act)의 개정을 통한 테러범과 테러혐의자에 대한 강제구금·출정영장·재심리 권한 강화 및 외국학생 감시프로그램을 통하여 그 활동에 대한 정보 수집 강화 등이 그 주요 내용이다.

특히. 동법은 법원의 허가 없이 정부가 의심되는 자에 대해 감시할 수 있다는 점에서 수집되는 정보의 오용 가능성 및 이로 인한 권리 침해가능성 때문에 끊임없이 비판을 받아왔다.[15] 즉, 동법에 따르면, 정황만으로 테러 용의자를 구금하고 기소할 수 있고, 테러의 증거가 없는 경우에도 징역형을 선고할 수 있었을 뿐만 아니라 법원의 영장 없이도 연방수사국(FBI)이 국가안

14) 미국의 애국법 가운데 사이버 테러리즘 행위에 대하여 구체적으로 개발된 요소들을 포함하고 있는 부분이 제8장(Title VIII of the USA Patriot Act of 2001)제814절((USA Patriot Act of 2001, Title VIII, Section 814)인데, 이 규정은 사이버 테러행위의 발생을 억제·예방하고자 고안되었다.

15) EFF Analysis of the Provisions of the USA Patriot Act, Electronic Frontier Found. available at http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.

보레터만 제시하면 통신기록과 거래내역을 볼 수 있게 했고, 대상을 명시하거나 근거를 제시할 필요도 없게 했다. 그럼에도 불구하고 오바마 대통령과 미국 의회는 2015년까지 동법의 시효를 연장했으나, 2013년 에드워드 스노든에 의해 국가안보국(NSA)의 무차별적인 도·감청 사실이 폭로되면서 2015년 6월 1일부터 효력이 정지되었다.

(2) 국토안보법

미국 정부는 9.11테러 직후 사이버테러를 비롯한 모든 테러행위로부터 국가기반을 보호하기 위하여 국토안보법(Homeland Security Act of 2002)을 제정하고, 동법에 근거해 국토안보부(Department of Homeland Security)를 신설하였다. 동법 제2편의 '정보분석 및 기반시설보호(Information Analysis and Infrastructure Protection)'에 관한 규정과 제10편의 '정보보안(Information Security)'에 관한 규정이 사이버테러와 관련된 대표적 규정이라고 할 수 있다. 제2편은 총 4개의 절로 구성되는데, 제1절은 정보분석기반시설보호국에 대해서 규정하고 있고, 제2절은 주요기반시설정보에 대해서 규정하고 있다. 그리고 제3절은 정보보안[16]에 대해서, 제4절은 과학기술실에 관해 규정하고 있다. 제10편은 총 6개의 조문으로 구성되어 있는데, 정보보안(제1001조), 정보기술의 관리(제1002조), 국립표준기술연구소(제1003조), 정보보안과 프라이버시자문위원회(제1004조), 기술적 및 관련규정 개정(제1005조), 해석(제1006조)에 대해 규정하고 있다.

(3) 자유법

2013년 스노든의 폭로 이후, 애국법에 대한 부정적 여론이 확산되자 미국 의회는 애국법 대신 법원의 허가 없이는 시민의 통신기록을 수집·보관할 수

16) 제3절의 내용을 구체적으로 살펴보면 제221조는 정보공유절차에 대해서, 제222조는 프라이버시 책임자에 관해 규정하고 있다. 그리고 제223조는 비연방 사이버보안강화에 관해서 규정하고 있으며, 제224조는 Net guard를 규정하고 있다. 마지막으로 제225조는 2002년 사이버보안강화법을 규정하고 있다.

없도록 하는 미국 자유법(USA Freedom Act)을 발의했다. 동 법안은 난항 끝에 2015년 6월 의회에서 통과하였다.[17] 자유법의 제정으로 애국법의 주요 내용은 복원되었지만, 국가안보국의 대량 전화정보 수집 프로그램은 중지되었으며, 연방법원이 승인하는 경우에만 개별적으로 정보를 열람 및 수집할 수 있게 되었다. 뿐만 아니라 해외정보를 얻거나 수사 목적으로 통신회사 등으로부터 통화기록을 얻기 위해서는 개별사건마다 구체적으로 개인, 장소, 계정, 장치 등을 특정해야 하며 포괄 승인이나 영장은 허용되지 않는다.[18]

(4) 외국정보감시법

외국정보감시법(Foreign Intelligence Surveillance Act, FISA)는 국가안보를 위해 외국요원에 대한 전자적 감청을 규정한 것으로 2008년 다시 개정되어, 정부의 테러방지를 위해 영장 없는 감청에 대한 법원의 심사절차를 완화하였다. 또 영장 없는 긴급감청을 7일간 허용하였고, ISP나 정보통신업체등이 국가안보국에 개인정보 등 필요한 정보를 제공할 경우 면책을 허용하는 규정을 두었다. 또한 미 국민의 해외 통신 및 해외의 미국인에 대한 통신감청을 허용하는 등 국가안전보장국의 정보수집 역량과 범위를 대폭 강화하였다.[19]

(5) 사이버보안법

2015년 12월 18일 오바마 대통령이 법안에 서명함으로써 미국은 민・관 사이버보안 위협정보 공유를 주요 내용으로 하는 사이버보안법(Cybersecurity Act of 2015)[20]을 제정하였다. 사이버보안법은 하원에서 통과된 2개의 법안,

17) 신계균, "자유법 입법과정을 통해서 본 미국 의회의 역할", 의정연구 제21권 제3호, 146쪽.
18) 최창수, "수사・정보기관의 통신이용 정보수집권에 관한 미국의 입법례와 그 함의 - 「2015년 미국 자유법」에 대한 검토를 중심으로", 정보법학 제20권 제1호, 한국정보법학회, 2016, 126-127쪽.
19) 50 U.S. Code Chapter 36, https://www.law.cornell.edu/uscode/text/50/chapter-36
20) http://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf

즉 '사이버 네트워크 보호법(Protecting Cyber Networks Act, PCNA)'과 '국가 사이버보안 보호 증진법(NCPAA: National Cybersecurity Protection Advancement Act)', 그리고 상원에서 통과된 '사이버보안 정보 공유법(CISA: Cybersecurity Information Sharing Act)' 3개의 법안을 합친 것으로 상원의 '사이버보안 정보 공유법'이 근간을 이루며, 지금까지 제정된 연방 사이버관련 법안 중 가장 중요한 법으로 평가되고 있다.[21] 사이버 동법에 대해서 미국 시민단체들과 보안 전문가들은 적절한 프라이버시의 보호 없이 기업이 정부와 사이버 위협 정보를 공유하는 허용할 뿐만 아니라 이러한 정보들을 광범위하게 이용하는 것을 승인한다는 이유로 끊임없이 반대하여 왔다.[22] 그렇지만 많은 산업단체들은 이를 사이버공격으로부터 보호하기 위한 중요한 단계로 높이 평가하였다.[23]

'사이버보안 정보 공유법'의 주요 내용은 다음과 같다. 첫째, 국가기관과 민간기관간의 사이버보안 정보공유체계를 구축하도록 하고 있다. 동법 제103조는 국가정보국장, 국토안보부장관, 국방부장관 및 법무부 장관은 연방기관과 비연방기관간에 정보공유절차를 구축하고 그 가이드라인을 마련하도록 하고 있다. 그리고 민간기관은 제104조에 따라 사이버보안을 목적으로 정보시스템 및 정보를 모니터링하거나 방어조치를 취할 수 있으며, 정보 또한

21) 법안의 구성은 다음과 같다.
Division N - Cybersecurity Act of 2015
Title Ⅰ. Cybersecurity Information Sharing
Title Ⅱ. National Cybersecurity Protection Advancement
Subtitle A - National Cybersecurity and communications integration center
Subtitle B - Federal Cybersecurity Enhancement
Title Ⅲ. Federal Cybersecurity Workforce Assessment
Title Ⅳ. Other Cyber Matters

22) https://static.newamerica.org/attachments/12218-51-civil-society-groups-and-security-experts-tell-congress-they-oppose-cyber-legislation/FINAL_Civil_Society_Security_Expert_Letter%20Opposing_CSA_2015.efca7165edbf4beaa392e5ef66cfff70.pdf

23) A Guide To The Cybersecurity Act Of 2015, http://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015

공유할 수 있다. 또한, 제106조에서 이러한 민간기관의 행위가 소송의 원인(cause of action)이 되지 않도록 규정하고 책임 면제 등의 보호규정을 마련하였다. 다만 연방기관은 사이버보안 목적을 위해서 사이버보안 위협이나 취약점을 확인하는 용도에 한해 공유 받은 정보를 이용할 수 있도록 제한하였다. 둘째, 국토안보부의 '국가사이버보안정보통합센터'(NCCIC: National Cybersecurity and Communications Integration Center)의 기능을 강화하고 연방기관에게 사이버보안을 강화하기 위해 정보시스템 침입 식별 및 제거를 위한 보안 계획을 수립·실행하도록 했다. 뿐만 아니라 연방컴퓨터시스템의 보안 강화, 의료산업분야의 사이버보안 개선 등에 대해서도 규정하였다.

동법은 정보 공유와 관련해서 특정 개인정보를 제거한 후 정보를 공유하도록 하고 있는데, 이와 관련해서 모호한 부분이 많아 미 법무부(the Department of Justice)와 국토안보부(DHS)는 구체적인 가이드라인을 별도로 제시하였다.[24] 동 가이드라인은 핵심 개념인 사이버 위협 지표(Cyber Threat Indicator), 방어 수단(Defensive Measure) 등이 의미하는 바가 무엇인지, 어떠한 경우에 정보가 보호될 수 있는지, 연방정부와 어떠한 방법으로 사이버 위협 지표 및 방어 수단을 공유하는 지 등에 대하여 구체적으로 제시하고 있다.

동 가이드라인에 따르면 CISA가 승인한 연방 기관의 활동은 CISA에 따른 연방 활동의 사생활 및 시민의 자유에 대한 영향을 제한하기 위한 절차를 따라야 한다. 그리고 CISA에 따라 연방 정부에 제공되는 사이버 위협 지표는 연방법의 다른 조항에 따라 연방 정부의 연방 기관 또는 부서, 구성 요소, 임원, 직원 또는 특정 기관만이 공개하고 보존하며 사용할 수 있다. 연방 기

24) The Department of Homeland Security·The Department of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, June 15, 2016. https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20105(a)).pdf

관은 특정 개인의 개인 정보 또는 공유 정보를 공유할 때 해당 연방 기관이 알고 있는 사이버 보안 위협과 직접 관련이 없는 정보가 포함되어 있는지를 검토해야 한다. 이와 관련된 모든 연방 기관 활동에 대한 기본 지침 원칙은 '공정한 정보 실행 원칙(the Fair Information Practice Principles, FIPPs)이다. 동 원칙은 개별 프라이버시에 영향을 주는 시스템, 프로세스 또는 프로그램 평가 및 고려에 사용되는 원칙을 정의하는 데 널리 받아들여지는 체계이다.[25]

Ⅲ 캐나다의 사이버안보 입법동향

1. 캐나다의 사이버안보관련 정책

캐나다는 2001년 9.11 테러 이전에는 대테러법(anti-terrorism laws)을 보유하지 않았다. 그러나 캐나다 정부와 의회는 9.11 테러 이후 테러리즘 관련 법안의 제정에 열정적으로 활동해 온 바, 현재는 테러리즘을 탐지, 저지, 기소하고 처벌하는 엄청난 양의 법을 보유하고 있다. 예를 들면, 2001년 12월 24일에 제정된 테러방지법(The Anti-terrorism Act-Bill C-36), 2004년 5월 6일에 제정된 공공안전법(Public Safety Act-Bill C-42), 2012년 3월 13일에 제정된 테러피해자사법법(Justice for Victims of Terrorism Act-Bill C-10), 2013년 11월 1일에 제정된 핵테러법(Nuclear Terrorism Act-Bill S-9), 2015년 3월부터 시행된 캐나다국민온라인범죄보호법(Protecting Canadians from Online Crime Act-Bill C-13) 등의 법안이 제정되었다.

뿐만 아니라 캐나다 정부는 사이버안보를 중요한 국가안보 정책의 하나로 보고 있다. 왜냐하면, 사이버공간에서의 공격일지라도 그 피해가 현실공간에서 발생할 위험이 크다고 판단하였기 때문이다. 또한 캐나다 정부는 악의적

25) The Department of Homeland SecurityThe Department of Justice, Privacy and Civil Liberties Final Guidelines:Cybersecurity Information Sharing Act of 2015, June 15, 2016, p.4.

인 의도를 지닌 개인, 집단 또는 조직이 실제로 캐나다 영토 안으로 발을 들여놓지 않고도 충분히 캐나다를 공격할 수 있다고 생각하고 있다.[26] 따라서 2010년 캐나다 정부는 '사이버안보전략(Canada's Cyber Security Strategy: For a Stronger and More Prospective Canada)'을 통해 증가하는 사이버위협(Cyberthreats)에 대한 전략적 프로그램을 수립하였다. 이에 따라 2015년 연방 정부는 새로운 법안을 비롯하여, 동 전략을 실행하기 위한 자금 지원을 포함하는 적극적인 계획을 세웠다. 캐나다 정부의 '사이버안보전략'은 법의 지배(rule of law), 프라이버시 등 캐나다의 가치 반영, 사이버 위협에의 대응 노력, 전 정부 차원의 총력 대응 등에 대하여 강조하였으며, 다음의 세 가지 목표를 포함하고 있다.[27]

[캐나다 사이버안보전략 목표]

분야	실현 목표
정부 시스템 보호	• 정부 네트워크 보안 개선을 위한 정보기술 보안 아키텍처 통합 • 정부 네트워크의 복잡한 사고 예방 및 해결 위한 메커니즘 구축 • 정부 사이버 보안기능 강화를 위한 투자
연방정부 외 중요 사이버시스템 보호를 위한 협력	• 외부 파트너와의 협력 • 캐나다 사이버 사고 대응센터(CCIRC)의 능력 향상 • 연구 및 개발 촉진 • 국제사회 참여
캐나다인의 온라인 보안을 위한 지원	• 사이버 공간에서의 보안 지원 • 캐나다 사이버 범죄 유형 초안 작성 • 사이버 공간의 보안 향상을 위한 입법도구 개선

26) 캐나다 안보정보부 홈페이지, https://www.csis.gc.ca/ththrtnvrnmnt/nfrmtn/index-en.php

27) "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," 2010, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf ; 2010년 10월 캐나다의 공공안전부(PSCan) 장관인 Vic Toews와 산업부(IC) 장관인 Christian Paradis는 '캐나다 사이버 안보전략(Canada's Cyber Security Strategy)'을 발표하였으며, 동 전략을 기반으로 캐나다 전역의 정보보호정책을 수행하였다.

사이버보안에 관한 원탁회의는 공공안전부(Public Safety Canada, PSCan)와 법무부(Department of Justice Canada)가 주도하고 있으며, 여기에는 캐나다 안보정보부(CSIS)와 안보과학센터(CSC), 연방경찰(RCMP)이 참여하고 있다. 공공안전부(PSCan)는 산하에 캐나다 안보정보부(CSIS)를 두어 국가안보에 영향을 미치는 사이버위협에 대해 조사 및 분석 등의 업무를 수행하며, 사이버사고대응센터(Canadian Cyber Incident Response Centre: CCIRC)를 설립하여 사이버위협을 실시간 감시하며, 사이버 안보와 관련된 사건에 대한 국가적 대응활동을 조정한다. 뿐만 아니라 국가 중요 인프라 보안 프로그램(National Critical Infrastructure Assurance Program)도 수행한다.[28] 한편, 캐나다 공공안전부는 최근 캐나다의 중요한 사이버 시스템의 보안을 개선하기 위한 수단으로 사이버 보안 협력 프로그램(the Cyber Security Cooperation Program, CSCP)을 시작하였다. 동 프로그램은 캐나다의 사이버 시스템 개선프로젝트를 지원하기 위해 중요한 사이버 시스템의 소유자와 운영자에게 보조금과 기부금을 제공한다.

2. 캐나다의 사이버안보관리체계

캐나다의 보안 및 정보 기관과 관련된 캐나다 정부의 주요 부서는 사이버안보전략에 따라 사이버위협에 적절히 대응하기 위해 유기적으로 연결된다.[29] 그 중에서도 캐나다 공공안전부(Public Safety Canada)는 캐나다의 중요 기반시설을 보호하고 국가의 비상사태 대비에 주도적으로 대처하는 기관이며, 사이버 안보에서 중요한 역할을 하고 있다.[30] 협력 기관에는 캐나다

28) 캐나다는 공공안전부(Public Safety Canada, PSCan)가 캐나다의 정보보호부문 전반을 담당하고 있으며, 산업부(Industry Canada, IC)가 공공안전부의 업무 영역을 지원 및 협력하고 있다.

29) 캐나다 공공안전부 홈페이지, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

30) 캐나다 공공안전부 홈페이지, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-en.aspx

안보정보부(Canadian Security Intelligence Service), 캐나다 연방경찰(Royal Canada Mounted Police), 캐나다 국군센터(Canada Firearms Center) 등이 포함된다. 또한 공공안전부는 미국 국토 안보부가 NIST (National Institute for Standards and Technology)와 공동으로 개발한 NIST 프레임 워크를 지지하며 캐나다에서 NIST 프레임 워크의 적용가능성에 대하여 인정하였다. 뿐만 아니라 공공안전부(PSC)는 산하에 캐나다 사이버 사고대응센터(CCIRC)를 두고 있는데, 동 센터는 사이버위협에 대하여 모니터링하고 사이버 보안사고에 대응한다. 그 중에서도 국가의 중요 기반시설에 대한 보호에 중점을 두고 있다. 그리고 국가 안보를 뒷받침하는 사이버 시스템을 강화하기 위해 민간 및 공공 부문의 협력을 강조하고 있다.

캐나다 안보정보부(CSIS)는 CSIS 법에 따라 캐나다 안보에 위협이 되는 활동을 정부에 보고하고, 캐나다 정부가 사이버 위협에 대하여 전반적인 상황 인식을 하도록 하여, 사이버 스파이 및 기타 사이버 위협으로부터 중요 기반시설을 보호하기 위한 조치를 취하도록 하고 있다. 그리고 국방부와 군대 역시 캐나다 정부에 위협이 되는 정보를 제공할 책임을 지니고 있다. IT 기술 위협에 대한 모니터링 및 보고, 잠재적 군사 대응을 위해 가능한 옵션 분석 제공 등을 통해 정부의 사이버 위협상황 인식에 기여한다.

캐나다 연방경찰은 중요한 정보 기반시설과 연관된 사이버범죄 사건에 대해서 조사할 뿐만 아니라, 국가안보사이버사건에 대해서 주도적으로 조사할 권한이 있다. 또한 사이버범죄의 위협에 대해 국내외 협력기관에 자문을 제공한다. 한편, 캐나다 안보정보 감시위원회(Security Intelligence Review Committee, SIRC)는 안보정보부(CSIS)의 모든 내부 문건과 기록을 확인할 수 있는 권한을 보유하고 있으며, 안보정보부의 행위에 대해서 감시하는 기능을 하고 있다.

[캐나다 사이버안보체계]

출처: 캐나다 공공안전부

3. 캐나다의 사이버안보 관련 입법 동향

(1) 캐나다 2001년 테러방지법(Anti-Terrorism Act, 2001)

캐나다 2001년 테러방지법(ATA, 2001)은 9.11테러 이후 의회에서 채택되었으며, 이에 따라 형법, 증거법, 범죄 및 테러자금방지법 등 여러 법령이 개정되었다. 2001년 테러방지법은 테러방지를 위하여 다음의 네 가지를 핵심 요소로 삼았다. 첫째, 테러 조직이 캐나다에 입국할 수 없도록 하여 캐나다 국민들을 테러 행위로부터 보호한다. 둘째, 테러리스트를 확인, 기소, 유죄 판결 및 처벌 도구를 강화한다. 셋째, 캐나다 국경을 안전하게 유지하고 국제사회와 협력하여 안보에 기여한다. 마지막으로 모든 캐나다 국민의 안전에 대한 의지를 반영하고 캐나다의 가치와 권리 및 헌장에 명시된 권리를 존중하면서 캐나다가 국제 의무를 다할 수 있는 능력을 강화한다. 그리고 2001년 테러방지법은 법안에 통신보안시설부(the Communications Security Establishment, CSE)의 존재를 유지하는 규정을 추가함으로써 국방법(the Nation Defense Act)을 개정하였다. 동법은 공식적으로 통신보안시설부가 다음의 세 가지 활동 영역에 참여

하도록 승인하고 있다. 첫째, 캐나다 정부의 우선순위에 따라 외국 정보를 획득하고 제공하다. 둘째, 캐나다 정부에 중요한 전자 정보 및 기반 시설의 보호를 도울 수 있는 조언, 지침 및 서비스를 제공한다. 셋째, 합법적인 직무 수행에 있어서 연방집행기관 및 보안기관에 기술 및 운영 지원을 한다. 한편, 동법에 따라 캐나다 안보정보부법(CSIS Act)의 '캐나다 안보에 대한 위협(threats to the security of Canada)'에 대한 정의가 변경되었다. 이는 안보정보부법(CSIS Act)에서 정의하고 있는 테러행위의 범위가 의도치 않게 축소되는 것을 피하기 위함이다.[31]

(2) 캐나다 안보정보부법(Canadian Security Intelligence Service Act)

2014년 캐나다 정부는 테러 감시를 강화하기 위해 30년 만에 캐나다 안보정보부법(CSIS Act)의 개정하기로 하였다. 이러한 배경에는 오타와 국회의사당에서 총격 테러로 1명이 숨지고 3명이 부상당한 사건이 있다. 캐나다 정부는 자생적 테러의 위협이 커짐에 따라 정보활동 범위를 해외로 확대하는 등의 권한강화가 필요하다고 판단하였다.[32]

동 개정의 주된 내용은 해외 감청 활동 명문화와 정보원 보호 보장으로 테러혐의자의 해외 통신에 대한 감청 활동을 정보부의 업무활동으로 규정하여 법원의 영장 발부 근거를 명시하고 있다.[33] 동법에 따르면 합리적인 근거에 의해 캐나다 안보에 위협이 되는 것으로 의심되는 활동에 대한 정보를 엄격하게 필요하다고 인정되는 한도 내에서 조사 또는 기타의 방법으로 수집, 분석, 보유해야 하며, 이에 관련하여 캐나다 정부에 보고하고 조언해야 한다. 그리고 이에 대해서는 영토의 제한이 존재하지 않는다.[34]

캐나다의 경우, 이전에는 해외 정보활동을 전담하는 정보기관을 따로 두지

31) Bill C-36, enacted Dec. 24, 2001.
32) 캐나다 법무부 홈페이지, http://laws-lois.justice.gc.ca/eng/acts/C-23/
33) 캐나다 안보정보감시위원회 홈페이지, http://www.sirc-csars.gc.ca/csiscr/amdmod-eng.html
34) Canadian Security Intelligence Service Act, http://laws-lois.justice.gc.ca/eng/acts/C-23/page-2.html#h-7

않고 있으나 최근 들어 해외 파견요원을 운용하고 있다. 스티븐 블레이니 공공안전부 장관은 개정법의 규정이 보다 명확해짐으로써 정보국이 해외 우방과의 정보 교류 협력을 확대할 수 있어 테러 활동으로부터 캐나다를 보호하는 법이 될 것이라고 밝힌 바 있다.[35]

(3) 캐나다 2015년 테러방지법(Anti-Terrorism Act, 2015)

2014년 10월 오타와 테러 이후, 캐나다 정부는 동 테러방지법을 제정하여 시행하고 있다. 동법은 테러를 선동하는 매체, 캐나다에 서버를 둔 테러 선동 웹사이트를 압수·폐쇄할 수 있는 권한을 판사들에게 줬으며, 경찰이 테러행위를 저지르기 이전에 테러용의자들을 구금할 수 있게 했다. 또한 연방정부 부처들과 정부 산하기관들이 국가안보와 관련된 정보를 폭넓게 공유할 수 있게 했고, 테러행위를 저지를 위험이 있는 외국인들의 입국을 좀 더 쉽게 거부할 수 있도록 하였다. 동법의 목적은 캐나다의 안보를 저해하는 활동으로부터 캐나다를 보호하기 위하여 캐나다 정부기관 간의 안보정보 공유를 권장하고 촉진하는데 있다. 그러한 목적을 달성하기 위해 동법은 제1장에서 안보정보공유법(Security of Canada Information Sharing Act, SCISA)을 신설하고 있는데, SCISA는 안보 저해 행위를 9개 유형으로 구체화하고 있으며, 캐나다 연방 정부기관들로 하여금 안보 관련 정보를 안보기관들에게 제공할 수 있게 하고 있다.[36]

동법에 따르면 정보 공유는 다음과 같은 원칙에 따라 진행된다. 첫째, 캐나다와 캐나다 국민을 보호하기 위해 효과적이고 책임있는 정보 공유를 한다. 둘째, 효과적이고 책임있는 정보 공유와 일치하는 공유된 정보에 대한 통보 및 발신자 통제에 대해서 존중한다. 셋째, 캐나다 정부 기관이 정기적으로 정

35) Dylan Robertson, “Government tables bill to give spy agency wider powers, Government tables bill to give spy agency wider powers”, October 27, 2014, available at http://ottawacitizen.com/news/politics/new-spy-agency-powers-to-be-introduced-monday

36) http://news.gc.ca/web/article-en.do?mthd=index&crtr.page=1&nid=988629&_ga=1.105011843.1673647960.1464033807

보를 공유할 때에는 정보 공유 약정을 체결한다. 넷째, 공유된 정보가 어떻게 사용되는지, 그리고 그것이 캐나다의 안보를 약화시키는 활동에 대비하여 보호하는 데 유용한지에 대한 피드백의 제공은 효과적이고 책임있는 정보 공유를 용이하게 한다. 마지막으로 캐나다 안보를 약화시키는 활동에 관해 관할권을 행사하거나 책음을 수행하는 기관 내의 사람들에 한해서 동법에 따라 공개된 정보를 받을 수 있다.[37]

그러나 안보정보의 제공에 대해서는 사생활 보호법(Privacy Act)과 충돌된다는 비판이 있고, 반테러법안이 테러리스트 용의자가 아닌 캐나다의 일반 시민의 개인정보까지 공유할 수 있는 여지를 만들고 있다고 비판이 있다.[38]

Ⅳ 시사점 및 결론

테러리즘에 대한 개념은 시대적 상황·배경에 따라 변화되어 왔다. 오늘날에는 새로운 과학기술의 등장에 따라 테러의 위협이 현실 공간을 넘어서서 사이버공간에까지 미치게 되었다. 현대 사회에서는 대부분의 국가 주요기반시설이 사이버공간에 의존하고 있기 때문에 사이버테러가 발생하면 국가 전체가 혼란에 빠질 가능성이 높다. 게다가 사이버테러의 경우, 테러리스트가 해당 국가에 직접적으로 접근할 필요 없이 원거리에서도 마음대로 공격하는 것이 가능하기 때문에 언제 어디에서 공격을 당할지 예측하기가 힘들다. 이상에서는 미국과 캐나다의 사이버테러관련 정책 및 입법 동향에 대한 검토를 통하여 다음과 같은 시사점을 생각해볼 수 있다.

첫째, 테러 공격에 의해서 실제로 큰 피해가 발생하기 전에 미리 예방할 수 있도록 관련 법제를 정비할 필요가 있다. 2001년 9월 11일 알카에다에

37) S.C. 2015, c. 20, s. 2, http://laws-lois.justice.gc.ca/eng/acts/S-6.9/page-1.html#h-4
38) National Post, "'Bill C-51 is a grave threat to our rights in Canada': Groups to launch Charter challenge against law", July 21, 2015.

의해서 자행된 미국 뉴욕 테러는 테러리즘에 대한 대응방식을 완전히 바꾼 계기가 되었다. 테러의 당사국인 미국은 물론이고 세계 여러 나라들이 테러와 사이버테러에 대한 법률을 제정하여 시행하기 시작하였다. 심지어 그전에는 전혀 대테러법률을 보유하고 있지 않았던 캐나다도 테러방지 법률의 제정 및 시행에 동참하였다. 사실, 미국을 제외한 다른 서구 국가들의 경우에 처음부터 테러방지 법률을 적극적으로 제정한 것은 아니다. 대부분의 국가들이 이러한 법률이 인권 침해의 소지가 크다고 제정을 꺼려하였다. 결국, 자국이 테러공격에 노출되고 나서야 뒤늦게 관련 법률의 제정에 힘을 쏟았다. 캐나다의 경우에도 2014년 수도 오타와에 발생했던 테러 이후 더욱 적극적으로 관련 법률들을 정비하였다.

우리나라의 경우, 과거에는 물리적 테러공격을 당한 적이 있지만, 최근 들어서는 사이버 테러공격에 의해 몇 차례 크게 피해를 입었다. 그럼에도 불구하고 아직까지 사이버테러에 적절히 대응하기 위한 법률이 제정되지 않았다. 미국과 캐나다를 비롯한 대부분의 국가에서는 테러가 발생한 이후에 철저하게 관련 법률을 정비하였으나, 우리의 경우에는 아직까지 큰 피해가 발생하기 전 예방의 기회가 남아있다. 따라서 조속히 우리나라의 특수성을 반영함과 동시에 사이버테러에 대하여 총괄적으로 규정한 법률을 제정할 필요가 있다. 한편에서는 기존의 법률로도 사이버테러에 대한 대비를 충분히 할 수 있다고 주장하지만, 모든 부분을 통합하는 법을 만들고, 이를 기준으로 기존의 법제를 정비하는 것이 훨씬 효율적이라고 판단된다. 미국과 캐나다의 법제 동향을 분석한 바에 따르면 새로운 법률을 제정하고 그 법률에 따라서 타법을 개정하거나 폐지하는 방향으로 관련 법제를 정비하였다. 그와 더불어 사이버테러는 새롭게 발전하는 기술을 이용한 테러공격인 만큼 변화에 적극적으로 대처할 수 있도록 기술적 부분에 관한 가이드라인을 마련할 필요가 있다.

둘째, 테러공격에 적절히 대비하고, 공격이 실제로 발생했을 경우에 각 국가기관간 및 민간 부문에 이르기까지 유기적으로 협력할 수 있도록 시스템을 구축할 필요가 있다고 생각된다. 여기에서 가장 중요한 부분은 사이버안보를

관장할 주무기관, 즉 컨트롤 타워를 명확하게 설정하는 것이다. 그와 동시에 컨트롤 타워가 제 역할을 하고 권한을 남용하지 않는지 대하여 감시하는 담당기구도 필요하다. 미국과 캐나다는 사이버보안 전략을 추진, 실행할 전담부처를 지정한 뒤, 세부 추진사항에 대해서는 업무 특성에 따라 해당 관계부처와의 협력을 통해 추진하고 있다. 특히 미국의 경우, 백악관을 사이버안보에 대한 컨트롤 타워로 하고 사이버보안조정관 직위를 신설하여, 국가 최상위 수준에서 사이버안보 전략을 총괄하여 담당하고 있는 것을 살펴볼 수 있었다. 따라서 관련 전략을 추진할 때 필요한 사항을 신속하고 정확하게 판단함과 동시에 책임을 명확하게 할 수 있다는 장점이 있다. 그리고 사이버안보 주무기관을 감시할 전담기구를 마련할 필요가 있다. 캐나다의 경우, 캐나다 안보정보 감시위원회가 안보정보부의 행위에 대해서 철저히 감시하고 있다. 이처럼 모든 행위에 대하여 접근할 권한을 가진 독립된 감시 기구의 설치가 필요하다.

마지막으로 장기적인 관점에서 사이버보안에 대한 전문 인력을 양성하고 주요 기반시설에 연계된 시스템을 잘 정비할 필요가 있다. 우리나라가 생각하고 있는 IT강국의 의미는 주로 인터넷 속도와 보급률을 의미하는 경우가 많다. 그보다는 얼마나 안전한 시스템을 구축하였는지에 더 집중해야 할 것이다. 사이버테러에 잘 대응하기 위하여 정보공유가 유기적으로 이루어지게 되는 경우, 테러에 의해 데이터베이스가 공격당하면 오히려 속수무책으로 당할 수밖에 없다. 따라서 일관성 있게 사이버보안 전문 인력을 양성하고 관리하는 계획을 세워야 한다. 특히 급변하는 기술 트렌드에 맞는 전문 인력을 키워야 한다. 캐나다 경찰은 작년 국제 해커단체에 대응하기 위해서 해킹 부서를 신설하고 40명의 IT전문가를 배치하였다.[39] 우리나라도 이처럼 적극

39) Canada Police Sets Up Hacking Division to Go After Cybercrime and Anonymous, Dec. 3, 2015, http://news.softpedia.com/news/canada-police-sets-up-hacking-division-to-go-after-cybercrime-and-anonymous-497088.shtml

적으로 전문 인력이 배치되어 있는 부서를 신설할 필요가 있다. 해당 기술을 충분히 이해하고 있는 전문가들이 구성원이 되어야 동 부서가 그 맡은 바 역할을 다 해낼 것이라 생각된다.

우리나라의 사이버안보에 대한 법제 정비는 세계 각국에 비해 늦은 감이 있다. 미국을 기준으로 하면 10여년 이상 뒤쳐졌다고 볼 수 있다. 지금이라도 세계적 흐름에 따라 관련 법제의 정비가 필요하다.

유럽연합의 사이버안보 입법동향과 시사점(1)
- 독일을 중심으로 -

성 봉 근*

목 차

Ⅰ 머리말

과학과 기술의 발전으로 인한 경제적 이익과 사이버 산업의 발전 및 사이버안보 등의 이익에 비중을 둘 것인가 아니면 민주주의와 헌법적 가치, 프라이버시 및 정보자기결정권과 각종 기본권의 보호에 비중을 둘 것인가 선택의 귀로에 서 있다. 슈페르트(Schuppert)도 날카롭게 지적하고 있듯이, 이른바 「헌법적 기준」(Verfassungsmaßstab)을 상실하게 된다면 문제는 그리 간단하지 않다.[1)]

* 고려대학교 강사

1) Schuppert, in Aussprache und Schlussworte, Wettbewerb von Rechtsordnungen, in VVDstRL, Band 69, De Gruyter, 2010, S. 114.

그러므로 더욱 비교법적이고 국제적인 연구와 사고가 요청된다. 우리의 입법·사법·행정에 있어서 참고가 될 수 있도록 비교법적인 분석과 소개를 하기로 한다.

물론 독일을 비롯한 유럽에서의 법제나 판례 역시 사이버안보에 대한 정답을 내리고 있다고 하기 보다는 그때그때의 문제를 해결하가는 과정들에 불과한 것임을 유의하여야 한다. 그리고 이러한 비교법적인 접근과 연구는 우리의 법제와 판례에 대한 방향을 설정하는데 있어서 결정적인 오류에서 벗어날 수 있는 안전장치의 역할을 한다.

논의의 범위와 관련하여 사이버안보의 개념에 대하여 논란이 있다. 사이버안보를 협의로 이해하여 사이버테러에 대한 보호로 국한하여 논의하기도 하지만, 사이버안보를 사이버안전과 사이버보안을 포괄하는 개념으로 논의하기도 한다. 그러나 현대에 와서 이 두 가지는 매우 밀접하게 연결되어 있고 엄격하게 분리해서 법제를 파악하는 것은 큰 실익이 없고 부분적인 고찰에 매몰된 나머지 전체를 보지 못하는 오류를 범할 위험이 크다. 따라서 사이버안전을 사이버상의 안전과 사이버상의 보호를 포함하는 광의의 개념과 범위를 가진 것으로 보고 논의하는 입장이 타당하다.[2)]

결국, 사이버안보에 대한 최근의 현실적인 문제를 해결을 함에 있어서 비교법적인 접근 없이는 법적 문제점들을 전체적으로 파악하기가 어렵다. 비교법적 검토는 사이버안보 분야가 요구하는 풍부한 경험들을 간접적이나마 축적하게 할 것이며, 시행착오를 줄일 수 있도록 안내하는 역할을 할 것이다.

이에 법 제도의 연구와 정비에 있어서 체계적이고 실험적인 접근을 해 나가고 있다고 평가받고 있는 유럽연합의 사이버안보 입법 동향에 대하여 독일을 중심으로 하여 법제와 판례를 살펴보고 시사점을 도출해 내고자 한다.

2) 김재광, 진화하는 사이버안보 위협과 법제적 대응방안, in 제4차 산업혁명 물결, ICT 법제 개선방향, 국회 제4차 산업혁명포럼, 2016.7, 47면.

Ⅱ 사이버안보에 대한 새로운 도전

더욱이 기존에 사이버안보에 대하여 정립되었던 시각과 관점들은 새로운 도전을 받고 있다. 기존의 법이론과 법제도들은 또 다시 규범력과 정당성에서 재검증을 요구받고 있는 것이다.

첫째, 사이버와 오프라인이 종래 분리되어 있다가 최근에는 빅데이터와 사물인터넷 기술의 발전으로 인하여 상호 연결되며 접속이 활발해지고 있다. 이에 따라 종래의 사이버상에서만의 안보에 대한 논의는 변화와 수정을 하지 않으면 안 되게 되었다. 사이버안보의 개념과 범위가 처음에는 사이버 상의 정보 자체에 대한 것에만 국한되다가, 사이버 시스템에 대한 것을 포함하는 것을 추가하게 되었으며, 최근에는 빅데이터와 사물인터넷으로 인하여 사이버와 오프라인을 연결하는 것에 대한 것까지 계속해서 수정되고 확장되어가고 있다.

둘째, 기존 법이론의 전제가 되는 법률관계의 변화도 광범위하게 일어나고 있다. 기존의 법이론과 행정이론의 틀은 국가와 국민간의 관계를 전제하여 기본권침해를 방지하고 공익과 사익을 조화롭게 하는 비교적 단순한 유형이었다. 그러나 해커라는 제3의 세력의 등장, 구글이나 페이스북 같은 사이버상에서 막강한 힘을 가진 다국적 기업의 출현, 각종 NGO 단체 등 국경을 초월하는 세력, 국가와 국가 사이의 해킹과 안보다툼 등 수많은 중심축들이 다원적으로 생겨나고 있고 갈등과 조화 관계에 놓이게 된다.

셋째, 사이버안보를 위협하는 공격방법의 진화가 기술적으로 매우 심각할 정도로 광범위하고 빠르게 진행되고 있다.

넷째, 사이버안전을 강화하다보면 프라이버시나 정보자기결정권 등 충돌되는 보호가치들과의 조화가 사이버 안보행위를 적법하게 해 주는 중요한 요건으로 자리를 잡게 된다. 슈펠트(Schuppert)는 최근 독일국법학자 대회에서 테러리스트 등으로 인한 잠식으로 인하여 「법의 지배 체계」(Rule of Law Promotion)는 고사될 우려가 있기 때문에 인권단체들과 안전을 우려하는

사람들, 법체계를 전제로 하는 세계은행 등 이해관계자들의 역할이 매우 중요하다고 한다.[3)]

다섯째, 프라이버시와 기본권 보호수준의 국제기준이 상향되고 있다. 최근 유럽사법재판소는 미국의 완화된 기준을 신뢰할 수 없는 수준의 것으로서 위법하다고 판시하였다. 이에 미국은 기존의 완화된 기준인 『세이프하버』(Safe Harbour)를 포기하고 『프라이버시 쉴드』(Privacy Shield)라는 수준이 상향된 기준을 제시하고 있다. 그러나 우리는 거꾸로 역행하면서 기존의 강화된 기준을 완화하려 하고 있다. 국제사회에서의 기준위반으로 인하여 발생할 잠재적 피해는 국가나 기업에게 막대한 것으로 보이며, 철저한 연구 없는 법개정에 대한 심각한 경각심을 가져야 할 상황이다. 국제사회는 법치주의와 민주주의 발전 수준에 대한 가격과 가치에 대하여 현실적인 제도로 반영하기 시작하였다는 심각한 의미이다.

사이버안보의 끊임없이 변화하는 현실에 대응할 수 있는 힘을 구비하기 위해서 기존의 생각들에 대한 대폭적인 수정이 필요할지 모른다. 사이버안보의 개념과 양상은 휴릭스틱적인 성격이 강하므로 계속해서 변화해 가는 과정을 살피지 않으면 죽은 연구가 되어버리게 된다.

Ⅲ 사이버안보에 대한 독일의 기본법과 일반법

독일은 최근 사이버안보에 대하여 수직적으로는 헌법적 차원인 기본법, 일반법, 그리고 개별법 등의 체계적인 입법구조를 정비해 나가고 있다. 수평적으로는 독일은 최근의 연방헌법재판소 결정에 영향을 받아 「정보 자체에 대한 사이버 안전 입법」과 정보를 전달·보관·처리 등을 하는 「시스템에 대한 사이버 안전 입법」 등으로 나누어 투 트랙으로 상세하게 규정하기 시작하였다.

3) Schuppert, in Aussprache und Schlussworte, Wettbewerb von Rechtsordnungen, in VVDstRL, Band 69, De Gruyter, 2010, S. 114.

1. 독일 기본법

사이버안보를 비롯한 문제들은 그 나라의 특성을 고려하지 않을 수 없고, 전국적인 통일성과 지역적인 자율성 및 독자성을 모두 조화롭게 추구하여야 하는 어려운 과제이다. 우리나라의 법령들을 정비함에 있어서도 이러한 점들을 염두에 두어야 한다.[4)]

『독일연방기본법』은 제1조 제1항에서 인간의 존엄성, 제2조 제1항에서 인격권, 제10조에서 통신의 자유, 제12조에서 직업선택의 자유 등을 규정하고 있을 뿐이었다. 독일 연방은 늦게까지 오프라인 위주의 안전과 행정에 맞추어 입법상태가 머물러 있었다.

특히 독일의 경우 연방이 아니라 지방자치단체들이 제 각각 사이버 사회와 전자정부에 대한 입법과 규율을 주도한 특이한 역사적・사회적 배경을 가지고 있다. 이에 따라 사이버 사회와 전자정부에 대한 체계적이고 효과적인 규율에 실패하였고, 난맥상을 초래하였다.

그동안의 실패를 반성하면서 최근『독일연방기본법』에「전자정부 조항」인 제91조c를 입법하기에 이르렀다. 독일 기본법 제91조c 제4항에서는 연방정부와 지방자치단체들이 제각각 독자적으로 전자정부를 구축하면서 겪었던 실패를 극복하고 지방자치단체의 독자성을 존중하면서도 통일적인 전자정부의 구축을 시도하였다. 이에 연방과 주의 통일적인 하나의 연결망을 수립할 수 있도록 하는 규정을 특별히 추가하고 있다. 이 통일망의 수립과 운영에 관해 상세한 것은 연방 의회의 동의를 얻어 연방 법률에서 정하도록 하여 기본법에서 전자정부의 통합망을 구체화하기 위한 법률유보를 규정하고 있다.[5)]

이에 독일에서 사이버 사회와 전자정부에 대한 헌법적 차원의 규율이 연방과 주 및 지방자치단체들 사이에 가능하도록 변화되었다.[6)] 이것이 독일의 사

4) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 53면.
5) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 53면.

이버안보에 대하여 연방정부가 체계적이고 강력한 입법을 추진할 수 있는 가장 근본적인 배경이다.

언젠가 우리 사회도 점차 「정보화사회」가 고도화되어 가고 있어서 중심을 잡아 줄 헌법 규정이 필요할 수도 있을 전망이다. 충분한 논의가 있을 필요가 있다고 생각되며, 장차 이에 대한 헌법에 개정에 대비할 필요가 있다.[7]

2. 일반법

(1) 『전자정부법』(EGovG, E-Government-Gesetz)[8]

사이버안보를 포함해서 전자정부의 전자행정을 발전시키고 촉진하기 위해서 미국과 우리나라 등에 이어서 『전자정부법』(E-Government-Gesetz - EGovG)이 사이버상의 행정에 대한 일반법으로서 제정되었다. 독일은 이러한 일반법을 두지 못한 채, 오랫동안 체계적이지 못하고 분산된 입법으로 인한 난맥상을 독일 지방자치의 역사와 배경으로 인하여 겪었다. 이러한 반성과 배경을 바탕으로 독일은 슐레스비히-홀슈타인(Schleswig-Holstein)주정부를 시작으로 각주의 전자정부법이 제정되게 되었으며, 『독일연방기본법』에 「전자정부 조항」인 제91조c를 입법하면서 연방 차원에서의 『전자정부법』이 드디어 입법되기에 이르렀다.[9]

특히 동법 제10조에서는 「IT-행정계획 회의(IT-Planungsrats)」를 통해 사이버안보를 포함한 표준화결정의 이행이 가능하도록 입법이 이루어지고 있다. 「IT-행정계획 회의」가 연방과 주들 사이의 공행정의 협력을 위하여 개최되어 특정 주제를 넘어서거나 융합주제와 관련된 IT 운용 및 IT 안보,

6) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 52면.
7) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 48면.
8) http://www.buzer.de/s1.htm?a=10&g=EGovG&dorg=1 최종 방문일 2016.11.27.
9) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 49면.

「IT-행정계획 회의」의 설치, 연방과 주들 사이의 기본법 제91조c의 이행을 위한 계약에 있어서 정보기술의 사용에 대한 협력의 기본원칙 등에 대한 논의를 하게 될 때에 대비한 근거규정을 두었다. 이러한 경우 「연방 IT-위원회」(IT-Rat, der Rat der IT-Beauftragten der Bundesregierung)에서 위의 결정을 연방행정차원에서 실행하도록 되어 있다. 「연방정보기술안보청」(BSI, Bundesamt für Sicherheit in der Informationstechnik)에 대한 법률은 정보기술과 관련하여 준용되어, 동 안보청 역시 사이버안보에 대한 여러 가지 역할을 수행하게 된다.

(2) 독일 『행정절차법』(Verwaltungsverfahrensgesetz)[10]

1) 입법의 의의

행정절차법에서는 사이버상의 행위들을 규율할 필요를 인정하여 제 3a조 전자적 소통(Elektronische Kommunikation)에 대한 것을 추가로 규정하면서, 사이버안보의 '기초'가 되는 규정들을 두기 시작하였다. 행정절차법이라는 일반법의 특성상 구체적인 사이버 안보에 대한 규정을 직접 두기 보다는 기초가 되는 「일반조항」(General Klausel)을 입법하고 있는 것으로 보인다.[11]

2) 입법의 내용

특히 개정된 행정절차법 제3조 a 제1항은 전자문서의 전송은 수신자가 이러한 목적에 대한 접근을 허용하는 경우에만 가능하다고 하여 엄격한 프라이버시와 기본권 보호 기준인 「옵트 인(Opt-in) 원칙」과 「목적구속성의 원칙」에 대한 규정을 두고 있다.

10) https://dejure.org/gesetze/BVwVfG/3a.html 최종 방문일 2016.11.27.

11) Bauer/Heckmann/Ruge/Schallbruch/Schulz, Verwaltungsverfahensgesetz und E-Government (Hrsg.), 2. Aufl. Kommentar, Kommunal- und Schul-Verlag GmbH&Co. KG-Wiesbaden, 2014, S. 101.

3) 입법된 절차규정

가. 사인의 전자적 소통절차

개정된 독일 행정절차법 제3조 a 제2항에서는 종이문서와 전자문서는 특별한 규정이 없는 한 대체될 수 있다고 하여 등가성을 인정하는 규정을 두고 있다.[12] 나아가서 사이버 안보와 관련하여, 전자문서의 등가성을 위해서는 전자서명법에 의해 인정되는 전자서명이 수반되어야 한다고 「보안성」(保安性; Security)에 대한 규정을 입법하고 있다.[13] 전자서명에 의하여 권한 없이 전자문서에 접근하고 훼손하게 될 위험을 방지함으로써 사이버안보의 기초를 형성할 수 있기 때문이다.

이때 가명을 사용하여 사인하는 것은 누구인지를 식별할 수 없게 하는 것이므로 허용되지 않는다.

나. 공공기관의 전자적 소통절차

① 규정의 내용

공공기관의 전자적인 소통에 대하여는 연방 의회의 동의유보 아래 「연방정부가 규정한 보안절차」를 정하여 이에 따르도록 하고 있다. 보안절차의 내용으로는 ① 데이터 전송자의 권한이 전자서명 등으로 인정되어야 하고, ② 정보의 내용이 변경되지 않아야 한다는 데이터에 대한 '무결성'(無缺性; Integrität, Integrity)[14]이 담보되어야 하며, ③ 정보에 접근하는 시스템에 대한 무결성도 인정되어야 한다고 규정하고 있다.[15]

12) 성봉근, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 43면.
13) Skrobotz, Das elektronische Verwaltungsverfahren, Duncker & Humblot, Berlin, Band 14, 2005., S. 66.
14) 성봉근, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 47면.
15) BVerfG, 1BvR 370/07 ; 박희영・홍선기, 독일연방헌법재판소 판례연구 Ⅰ [정보기본권], 한국학술정보(주), 2010, 19면.

② 배경 판례

독일연방헌법재판소가 「인구조사판결」[16]에서 정보자기결정권을 인정하는 기념비적인 판결을 하였던 반면에, 최근에는 「온라인수색판결[17]」을 통하여 이른바 「IT 기본권」을 인정하는 또 다른 기념비적인 판결을 하였다. 동 판결에서 독일 연방헌법재판소는 최근 독일 연방 기본법 제1조 제1항(인간의 존엄성), 제2조 제1항(인격권), 제10조(통신의 자유), 제12조(직업선택의 자유) 등으로부터 국민들에게 정보기술시스템상의 보안이 유지되어야 한다는 「기밀성」(機密性; Vertraulichkeit, Confidentiality)과 정보의 내용이 변경되지 않아야 한다는 「무결성」(無缺性; Integrität, Integrity) 등이 기본권[18]으로서 보장된다고 선언하였다.[19] 인터넷을 이용하는 국민으로서는 익명성 또는 암호화에 대한 권리로 함께 묶여지는 법적 지위를 보장받아야 한다.[20] 이는 정보자기결정권으로는 포섭되지 않기 때문에 이를 기본권으로 인정하는 판결이 필요하였으며, 이른바 『IT 기본권』으로 부른다.[21]

그러면서, 독일 연방헌법재판소는 노르트라인-베스트팔렌 주 『헌법보호법』은 정보기술시스템에의 은밀한 접근을 의미하는 「온라인수색」을 허용하는 규정을 두고 있다는 이유로 위헌결정을 내렸다.[22] 연방헌법재판소는 동 규정은 국민들에게 「기밀성」(機密性; Vertraulichkeit, Confidentiality)과 「무결성」(無缺性; Integrität, Integrity) 등이 기본권으로서 보장된다고 선언하였다. 이른바 『IT 기본권』인 '정보기술시스템의 기밀성과 무결성에 관한 기본권은 인격권에 관한 독일 기본법 제2조 제1항 및 동 조항에 의거한 일반

16) BVerfGE 6, 1 (46)
17) BVerfG, 1BvR 370/07 vom 28.2, 2008
18) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 292면.
19) BVerfGE 120, 274 (315 f.) 서정범・박병욱, 앞의 논문 (주 8), 288면에서 재인용
20) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 292면.
21) 김태오, 사이버 안전의 공법적 기초 -독일의 IT기본권과 사이버안전법을 중심으로, 행정법연구, 제45호, 2016.6, 114면; 박희영・홍선기, 독일연방헌법재판소 판례연구 Ⅰ [정보기본권], 한국학술정보(주), 2010, 19면.
22) BVerfGE 120, 274 (315 f.) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 288면에서 재인용.

적 인격권의 광범위한 내용으로서 인정된다고 보았다. 이 새로운 기본권은 독일 기본법 제10조의 전화통신의 자유와 정보의 자기결정권과 함께 개인의 정보와 관련된 기본권적 지위를 포괄적으로 보장하는 효과를 가지게 된다. 이 새로운 기본권은 기술규범의 성격상 기본권 보장을 위한 다른 제도와의 협력을 통하여 기술적 발전에 따라 형성되어야 한다고 한다.

나아가서 연방헌법재판소는 동 규정이 특히 규범의 명확성의 원칙에 위반된다고 판시하였다. 그리고 연방헌법재판소는 온라인 수색에 관한 법률규정의 합헌성 심사에서 가장 중요한 것은 개인의 사생활의 핵심영역의 보호라고 한다. 따라서 구체적 사정을 고려한 비교형량을 통하여 핵심영역의 보호를 상대화 하는 것은 허용되지 않는다고 하면서, 핵심영역을 침해하는 한도에서 온라인 수색 조치는 위헌이라고 한다.

온라인 수색을 통한 정보의 수집은 필요한 정보가 사생활의 핵심적 영역에서 수집되지 않아야 하는 소극적 요건과 법률의 규정이 있어야 한다는 적극적 요건을 모두 충족하여야 한다. 이에 의하여 온라인 수색의 허용범위는 축소되고 제한된다고 한다.[23]

동 규정은 독일 연방헌법재판소가 최근 「온라인 수색 판결」에서 정보시스템에 대한 무결성과 기밀성 등을 이른바 「IT 기본권」으로 인정하는 판시를 하고 있는 것과 관련성이 있는 것이다. 이에 따라서 독일『IT 행정계획회의』(IT-Planungsrat)는 이러한 내용을 담은『보안절차에 대한 권고규정』을 두기에 이르렀다.

4) 평가

독일『행정절차법』은 이들 IT와 사이버 등에 대한 규정을 추가적으로 규정해 나가게 되면서, 정보화사회 속에서도 행정법의 일반법으로서의 생명력과 실효성을 유지하고 있다고 보여 진다. 우리『행정절차법』도 명목상의 일반법이 아니라 실질적인 규범력을 유지하며 역할을 다하기 위해서는 사이버

23) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 290면.

안보를 비롯한 정보화사회와 전자정부에서 규율이 가능한 일반규정들을 입법하도록 반드시 개정되어야 할 것이다.[24]

(3) 『IT 안보법』(IT-Sicherheitsgesetz)[25]

1) 입법의 의의

2015년부터 사이버안보에 관한 일반법으로서 『IT 안보법』(IT-Sicherheitsgesetz)[26]이 발의된 이후 진통 끝에 발효되게 되었다. 이른바 『IT 안보법』(IT-Sicherheitsgesetz, IT Security Law)이라 부르는 이 법의 정식 명칭은 『정보기술 시스템의 안보를 제고하기 위한 법률』(Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme)이다.

사이버안보라는 공익을 위하면서도 기본권 보호와 조화되기 위하여 적법요건을 규정한 의미 있는 법이다.[27] 특히 이 법은 사이버사회에서 디지털 인프라시스템과 구조를 보호하기 위하여 제정되었다. 앞으로 우리 입법에도 많은 참조를 통하여 입법적 개선에 도움을 줄 것으로 기대된다. 그런 의미에서 『IT 안보법』(IT-Sicherheitsgesetz)을 『사이버 안전법』과 동일하게 보면서 이를 전제로 사이버안전을 논의하는 견해도 나타나고 있다고 이해된다.[28] 다만, 두 명칭 사이에는 어떤 차이가 있을 수 있으며 이에 대한 검토는 아직 열려있다고 생각한다. 따라서 일단, 법의 본래 명칭대로 『IT 안보법』(IT-Sicherheitsgesetz)이라고 용어를 사용하기로 한다.

---

24) 성봉근, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 61면.

25) Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. http://www.loc.gov/law/foreign-news/article/germany-ministry-of-the-interior-publishes-draft-cybersecurity-act/ 최종 방문일 2016. 11. 22.

26) https://dejure.org/BGBl/2015/BGBl._I_S._1324 최종 방문일 2016.11.26.

27) Bundesgesetzblatt(BGBl) Jahrgang 2015 Teil I Nr. 31, ausgegeben am 24.07.2015, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015, Seite 1324.

28) 김태오, 사이버 안전의 공법적 기초 - 독일의 IT기본권과 사이버안전법을 중심으로, 행정법연구, 제45호, 2016.6, 110면.

이 법에 대한『공식적 입법 공고』(Amtliche Gesetzesanmerkung)에 따르면,『IT 안보법』은『유럽공동체 지침』(Richtlinie 98/34/EG des Europäischen Parlaments)을 독일법에 적용하기 위하여 제정된 것이다.[29] 또한『IT 안보법』은 기술적 기준과 규제 분야에서의 정보 규범에 대한 절차와「정보화사회」(Informationsgesellschaft; Information Society)[30]의 규율에 부합하기 위하여 최근 2012년에 개정된『유럽공동체 규정』(Verordnung (EU) Nr. 1025/2012)을 준수하고 따르기 위한 것이다.[31]

2) 입법의 연혁

최근 독일은 새로운『IT 안보법 초안』(Entwurf enines IT-Sicherheitsgesetz, Draft Cybersecurity Act)을 2014.10.에 마련하여『IT 안보법』을 입법하기에 이르렀다.

동법 초안은 독일 정부에 의하여 먼저 법안에 대한 확정절차를 밟은 후 독일 의회의 승인을 밟아 상하 양원을 모두 통과하여 확정되었다.[32] 동법 초안이 만들어지게 된 것은『디지털 아젠다』(the Digital Agenda)의 일환으로서 만들어지게 된 계기도 있다.『디지털 아젠다』는 정보 기술 분야에 있어서 상대적으로 다른 OECD 국가들에 뒤쳐져 있던[33] 독일의 위치를 강화하기 위

29) Bundesgesetzblatt(BGBl) Jahrgang 2015 Teil I Nr. 31, ausgegeben am 24.07.2015, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015, Seite 1324.; ABl. L 204 vom 21.07.1998, S. 37.

30) Hoffmann-Riem, Verwaltungsrecht in der Informationsgesellschaft - Einleitende Problemskizze, in Hoffmann-Riem/Schmidt-Aßmann(Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Nomos Verlagsgesellschaft, Baden-Baden, 1.Auflage, 2000, S.10.

31) Bundesgesetzblatt(BGBl) Jahrgang 2015 Teil I Nr. 31, ausgegeben am 24.07.2015, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015, Seite 1324.; ABl. L 316 vom 14.11.2012, S. 12.

32) Grundgesetz für die Bundesrepublik Deutschland [Basic Law for the Federal Republic of Germany] (May 23, 1949), art. 76(1), BUNDESGESETZBLATT [FEDERAL LAW GAZETTE] I.

33) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문,

해서 독일 정부가 제시한 프로그램이자 행정계획이다.[34]

독일은 증가하는 사이버안보에 대한 위협에 대하여 자각하게 되면서, 동 법안을 결국 2015년 6월에 통과시켰다.[35]

이 법은 「중요기간시설」(Critical Infrastructure)에 대한 사이버안보를 향상시키기 위하여 독일의 여야가 발의하기로 합의를 이루어 발안된 것이다.[36] 게다가 동 법은 독일 연방 정보 기술의 보호 수준을 향상시키기 위한 규정들을 포함하여 입법하였다.

3) 주체에 대한 입법

가. 전문적인 제어기구의 설치・운영 및 권한강화

주체에 있어서 전문적인 제어기구[37]로서 「연방정보기술안보청」(BSI, Bundesamt für Sicherheit in der Informationstechnik, the Federal Office for Information Security or Federal Office of Information Security)을 설치하고, 그 권한을 강화하였다. 그리고 「연방형사경찰청」(BKA, Bundeskriminalamt, the Federal Criminal Police Office)의 책임 범위를 확대하였는데, 특히 국가 전체 구조에 대한 사이버공격이 발생하는 경우에 대비하도록 하였다.[38]

2014, 53면.

34) Deutsche Bundesregierung [Federal Government], Digitale Agenda 2014-2017 [Digital Agenda 2014-2017], Federal Ministry of the Interior website, at 32-33.

35) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.22.

36) Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. 9.http://www.loc.gov/law/foreign-news/article/germany-ministry-of-the-interior-publishes-draft-cybersecurity-act/ 최종 방문일 2016. 11. 22.

37) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 244-245면.

38) Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. http://www.loc.gov/law/foreign-news/article/germany-ministry-of-the-interior-publishes-draft-cybersecurity-act/ 최종 방문일 2016. 11. 22.

「연방정보기술안보청」(BSI)은 「국제 IT 안보 센터」(the international center for IT security)의 기능도 담당하도록 권한과 역할을 확장하였다. 「연방정보기술안보청」(BSI)의 주요 업무 중의 하나는 「중요기간시설」(Critical Infrastructure)에 대한 사이버침해의 위험에 대한 신고를 평가하는 것이다. 사이버침해의 개연성의 정도에 이르는 위험(Gefahr)에 국한하지 않고 사이버침해의 가능성의 정도에 이르는 위험(Risiko)에 대해서까지 평가업무를 포함한다. 이는 사이버침해와 같은 현대형 공격은 위험의 가능성과 위험의 개연성 단계를 명확하게 구분하기도 어렵고, 가능성에서 개연성과 장해(Störung) 등에 이르는 속도가 워낙 빠르고 동시적이라는 특성[39]을 잘 고려한 입법으로 평가된다.

「연방정보국」(BND, The Federal Intelligence Service) 은 악성 서명과 악성 코드들과 연결되어 있는 외국 정보에 접근할 권한이 허용되도록 규정되었다.

나. 행정기관간의 협조와 대화형 행정구조

『IT 안보법』에 대한 입법이유서를 보면, 사이버안보 등을 포함한 입법을 하는 과정에서 독일 연방정부 내의 「행정기관들의 회의」를 반드시 거치도록 되어있다.[40]

「연방헌법보호청」(BfV, the Federal Office for the Protection of the Constitution)은 「연방정보기술안보청」(BSI))이 기간시설에 대한 사이버 공격에 대한 잠재적인 영향 평가를 하는데 협력하고 지원할 수 있다. 「연방형사경찰청」(BKA)이 데이터에 대한 스파이활동과 데이터 가로채기나 조작 등에 대한 수사를 담당하고 책임지고 있는 경우에도, 연방헌법보호청과 연방정

39) 성봉근, 보장국가에서의 위험에 대한 대응 - 전자정부를 통한 보장국가의 관점에서 본 위험-, 법과 정책연구, 제15권 제3호, 2015.9, 1052면.

40) Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. http://www.loc.gov/law/foreign-news/article/germany-ministry-of-the-interior-publishes-draft-cybersecurity-act/ 최종 방문일 2016. 11. 22.

보기술안보청은 사이버공격에 대한 잠재적 영향평가업무를 함께 진행할 수 있다.[41]

이렇듯이 사이버공격이 현재 진행되든 잠재적이든 어느 하나의 기관이 전담을 하는 것이 아니라 「대화형 행정의 구조」 아래 여러 행정기관들이 서로 협조하면서 보다 효과적이고 성과를 올릴 수 있도록 업무를 진행할 수 있다. 행정기관들 사이에 상호 견제와 배타적인 업무처리를 극복하고, 진정한 협력과 대화를 할 수 있어야 하는 패러다임의 전환[42]이 전제되어야 한다.

4) 절차에 대한 입법과 대화형 행정구조

『IT 안보법』에 대한 입법과정에서 「행정기관들의 회의」를 거치도록 되어 있을 뿐만 아니라, 기업체와 사회 구성원 등 「이해관계자들의 참여에 의한 토의」도 필수적으로 거치도록 되어 있다.[43]

『IT 안보법』에 의한 새로운 규율 내용으로서 정보통신업자들로 하여금 고객들에게 '보트넷[44] (botnet) 공격'을 당하거나 '트래픽 데이터'를 수색 목적으로 6개월 이상 저장하도록 조정당하여 잠재적인 프라이버시권(privacy rights) 침해 하에 있는 등의 경우에 고객들의 위험에 대한「통지의무」를 이

41) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.24.

42) 성봉근, 보장국가로 인한 행정법의 구조변화, 지방자치법연구, 제15권 제3호, 2015. 9, 196면 이하.

43) Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. http://www.loc.gov/law/foreign-news/article/germany-ministry-of-the-interior-publishes-draft-cybersecurity-act/ 최종 방문일 2016. 11. 22.

44) 보트넷(botnet)은 인터넷에 연결된 컴퓨터의 숫자를 의미한다. 이들 컴퓨터에 연결된 다른 유사한 기계들은 망으로 연결된 컴퓨터에 위치하는 구성요소들을 이루면서 명령과 통제(C&C, command and control)에 의하여 소통하고 협조하는 행동들을 하게 되거나, 또는 컴퓨터 상호간에 서로 메시지들을 주고 받도록 명령과 통제가 이루어지게 된다. 이러한 방식으로 스팸 매일을 수차례 보내거나 디도스(DDOS, distributed denial-of-service attacks)에 이용된다. 보트넷(botnet)이란 용어는 로봇(robot)과 네트워크(network)를 합성한 용어이다. 보트넷은 부정적이고 악의적인 의도하에 이용되는 경우를 내포하는 용어이다. https://en.wikipedia.org/wiki/Botnet 최종 방문일 2016.11.22.

행하도록 규정되었다.[45]

이렇듯이 사이버안보를 국가 혼자서 책임을 질 수 있다는 사고를 극복하고, 사이버안보와 관련된 모든 이해관계인들 및 관계 행정기관들과 함께 대화하는 구조로[46] 『IT 안보법』이 구성되었다.

5) 내용에 대한 입법

내용상으로는 『IT 안보법』은 첫째, 중요 사업에 대한 「사이버 안보를 위한 최소한의 기준」을 제시하고 있다. 동법은 2000여개가 넘는 중요 서비스 제공자들(service providers)에게 최소한도의 정보 안보기준을 이행하도록 의무를 부과하고 있다.[47] 동법은 기업들뿐만 아니라 연방 행정기관들까지 동법에서 규정한 동 기준을 충족하도록 의무를 부과하였다.[48] 사이버안전에 대한 책임을 국가에게 일방적이고 전부 지우는 것은 정부의 실패를 초래하게 되므로, 국가와 기업이 협력하여 안보책임을 분할하고 분담하는 것이 타당하다.[49]

둘째, 『IT 안보법』은 중요한 「IT 안보 사건에 대한 신고의무」를 규정하고 있다. 『IT 안보법』은 기업과 기관들로 하여금 정보시스템에 대한 사이버 공격이 의심되는 경우에는 반드시 행정청에게 신고할 의무를 부과하고 있는 것이다.

셋째, 『IT 안보법』은 기업과 기관들로 하여금 「연방정보기술안보청」(BSI)의 「인증」(clearance)을 획득하도록 할 의무를 함께 부과하였다.

45) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.22.
46) 성봉근, 보장국가로 인한 행정법의 구조변화, 지방자치법연구, 제15권 제3호, 2015. 9, 197면.
47) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.22.
48) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.22.
49) 성봉근, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 61면.

넷째, 『IT 안보법』은 또한 독일에서 '전체적인 사이버안보를 더욱 강화'하기 위한 조치들도 제시하고 있다. 동 법은 공공 원격통신망과 인터넷 서비스에 대한 안보 기준을 상향하도록 요구하고 있다.[50]

6) 적용범위와 실효성 확보수단

독일의 『IT 안보법』은 분야별 적용범위와 관련하여 수송, 건강, 수도, 통신 서비스을 비롯해서 금융과 보험 등에 이르기까지 이른바 「중요기간시설」에 속하는 것으로 규정된 해당 분야에 속한 회사와 행정기관들에게 적용될 것이다. 동법은 이들 분야에 속한 회사들에게 2년 동안의 기한을 설정하여 사이버 안보조치를 취하도록 강제하고 있다.

사이버 안보조치 불이행에 대한 제재로서 10만 유로(약 11만 천 달러)의 벌금이나 이행강제금 등을 내도록 규정하였다.[51]

7) 입법에 대한 평가와 과제

가. 긍정적인 평가와 과제

동 법률 초안에 대하여 대부분의 기업 협회의 대표자들은 만족감을 표시하였다. 그러나 특정 IT 업체들은 소수자들의 적응을 함께 배려한 입법을 요구하였으며, 동 법률을 좀 더 명확하게 입법할 것을 요구하였다.[52]

연방내무부장관인 메지에(Maizière)는 사이버공격에 대비한 『IT 안보법』상에서 계획된 조치들에 대하여 중요한 걸음을 내디딘 것으로 평가하면서, 그 이유는 IT 안보가 공공의 안보를 구성하는 핵심적인 요소이기 때문이라

50) Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. http://www.loc.gov/law/foreign-news/article/germany-ministry-of-the-interior-publishes-draft-cybersecurity-act/ 최종 방문일 2016. 11. 22.

51) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.22.

52) Joachim Jahn & Martin Gropp, Wirtschaft überwiegend zufrieden mit IT-Sicherheitsgesetz [Economy Largely Satisfied with Cybersecurity Act], FRANKFURTER ALLGEMEINE ZEITUNG ONLINE, Aug. 19, 2014.

고 한다. 그러나, 반대론자들은 이와 달리 정부는 기업들에게 안보조치들을 강구할 의무를 요구하기에 앞서서 정부가 먼저 공공기관들의 IT 안보의무를 이행하여야 하는 것이 좋을 것이라고 권유한다.[53]

나. 부정적인 평가와 과제

첫째 민주주의와 법치주의적인 관점에서의 비판이다. 정보 보호에 대한 전문가들은 『IT 안보법』에서 통신서비스 제공자들(telecommunications providers)이 고객들의 인터넷상의 행동들에 대한 정보의 저장을 허용하면서 동시에 시민들의 통신과 소통행위들에 대한 비밀감시를 법적으로 허용하는 것은 문제가 있다고 경고하고 있다.

둘째, 기술적인 관점에서의 비판이 있다. 국제적인 정치그룹인 「해적당」(the Pirates Party)[54]은 지식의 공유와 직접 민주주의, 행정의 투명성, 시민의 참여, 정보 프라이버시와 인터넷 중립성 등을 강조하는데, 이에 속한 독일 킬(Kiel) 의회의원인 브라이어(Breyer)는 기술적 관점에서 보더라도 이러한 조치들은 정당성이 없다고 비판한다. 브라이어(Breyer)에 의하면, 정보통신 제공자들이 고객들의 정보를 가능한 한 최소한도로만 수집할 수 있도록 할 때에야 비로소 법은 IT 안보에 대한 개념에 충실하게 봉사할 수 있다고 한다.[55]

셋째 경제적인 관점에서의 비판이 있다. 『IT 안보법』에 대한 비판론자들은 새로운 IT 안보에 대한 법은 독일 경제를 좀 먹게 하는 반면 이로 인한 이익은 크지 않다고 본다. 독일 하이테크 협회인 「비트코른」(Bitkom)의 최근 연구에 따르면, 안보에 대한 기준을 만들고 수정해 나가기 위해 독일 경제는 매년 10억 유로 내지 12억 3천만 달러의 비용을 지불해야 한다.[56]

53) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.23.
54) https://en.wikipedia.org/wiki/Pirate_Party 최종 방문일 2016.11.23.
55) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일 2016.11.23.
56) https://www.rt.com/news/273058-german-cyber-security-law/ 최종 방문일

다. 중간결론

결국 독일은 최근 사이버안보에 대하여 연방차원에서 『IT 안보법』을 사이버 안보에 대한 가장 전문적인 입법으로 자리매김하게 하고 있다. 이러한 입법적인 개입을 하면서 사이버안보를 강화하는 방향으로 입법하기 시작하였다고 평가할 수 있다. 그러면서도 주체, 절차, 형식, 내용 등의 요건을 엄격히 함으로써 법치주의와 조화될 수 있도록 입법을 진행하고 있다는 점을 주의하여야 한다.

그러나, 독일의 『IT 안보법』 역시 확정된 것이 아니라 사이버 입법의 휴리스틱적 성격[57]을 고려하여 계속 수정되어 나가는 도중의 입법으로서 연구와 개선의 여지가 많이 남아 있다. 좀 더 명확한 입법을 하여야 하며, 정보격차를 겪는 소수 기업들에 대한 경과규정 등의 추가적인 입법이 필요해 보인다.

(3) 『IT망법』 (IT-NetzGesetz)[58]

1) 입법의 의의

『독일연방기본법』에 「전자정부에 대한 조항」인 제91조c를 입법하여 헌법적 차원의 규율이 연방과 주 및 지방자치단체들 사이에 가능하도록 됨에 따라,[59] IT 망들에 대한 체계적인 설치 및 유지와 안보 등을 위하여 이를 구체화하는 입법으로서 『IT망법』(IT-NetzGesetz)이 2009년에 제정되었다. '행정법은 헌법의 구체화법'이라는 고전적인 명제가 사이버 안보와 전자정부의 입법에도 그대로 적용되어 가고 있다.

『IT망법』은 독일 기본법 제91조 c를 구체화하여 연방과 주들 사이의 정보통신기술망을 상호 연결하기 위해 입법되었다.[60] 특히 이를 위하여 제1조

2016.11.23.

57) 성봉근, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 35면.

58) http://www.buzer.de/gesetz/8983/index.htm?dorg=1 최종 방문일 2016.11.26.

59) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 52면.

60) Artikel 4 G. v. 10.08.2009 BGBl. I S. 2702, 2706 (Nr. 53) ; Geltung ab 18.08.

제1항에서는 연방과 주들 사이의 공동업무의 대상 중 하나로서 「협력위원회」(Koordinierungsgremium)를 구성하도록 규정하고 있다. 독일은 연방과 주, 그리고 지방자치단체 등으로 이루어져 있는 체제인데, 이들 사이를 모두 연결하는 정보기술 망을 구축하도록 되었다. 연방과 주들은 『IT망법』에 의하여 상호 협력하고 대화할 의무를 지게 된다. 특히 이들은 연결망의 공통된 기반을 충족할 수 있도록 하여야 한다.

2) 입법의 주체・절차・형식・내용

동 법 제2조에서는 개념정의 규정을 두었다. 제3조에서는 연방과 주 사이의 정보교환이 상호 연결된 망을 통하여 이루어짐을 명문으로 인정하고 있다. 제4조 제1항에서는 연방과 주 사이의 망 연결의 허가결정 요건에 대한 규정을 두고 있다. 제4조 제2항에서는 망 연결 허가결정에 대한 권한을 「협력위원회」에게 부여하고 있다. 제4조 제3항에서는 협력위원회의 구성에 대한 연방과 주들의 의결정족수에 대한 규정을 두어 협력적이고 대화형 행정의 구조를 취하고 있다. 제5조에서는 연방과 주 들 사이에서 권한과 관할의 배분에 대한 규정을 두면서, 신뢰성 있는 문서에 대한 보호를 위한 적절한 조치를 취할 의무를 사이버안보와 관련하여 두고 있다. 제6조 제1항에서는 연방의 연결망 운영에 대한 규정을 두면서 제4조 제1항의 망 연결 요건에 부합하여야 한다고 하고 있다. 제6조 제2항에서는 「협력위원회」가 공통 요건이 되는 규정의 위반 사례에 대한 모니터링 의무를 이행하도록 하면서, 동 연결망의 운영에 대한 주들의 이해관계를 고려하도록 하고 있다. 이는 보장국가를 위한 구체적인 입법 모습 중의 하나이며, 시장과 사회가 제대로 자율적으로 잘 돌아가도록 보장책임을 충실히 이행하기 위한 것이기도 하다.[61]

3) 비용에 대한 입법

동법 제7조 제1항에서는 연결망의 설치와 운영에 대한 비용을 연방에서

2009, §3 gilt ab 01.01.2015; FNA: 206-1 Öffentliche Informationstechnik.

61) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 237면.

담당하도록 규정하고 있다. 독일은 이러한 연결망의 설치와 운영에 대한 것은 일종의 사회기간시설로 바라보면서, 연방과 주 및 지방자치단체가 상호 협력하여야 하는 것과는 별도로 연방에서 담당하여야 할 전국적이고 통일적인 비용부담사항으로 보고 있다. 그러면서도 제7조 제2항에서는 연결망에 대한 이용허가 결정에 따르는 이용비용에 대하여는 연방과 주 및 지방자치단체 및 기타 공법상 법인들이 함께 그때그때마다 담당하도록 규정하고 있다. 제8조에서는 경과규정을 두고 있다.

4) 평가

결국『IT망법』은 독일 기본법 제91조에서 전자정부에 대한 헌법적 규정을 두게 됨에 따라 이를 연방과 주 및 지방자치단체들 사이에서 협력적으로 수행하고, 연방과 주 및 지방자치단체들을 연결하는 망의 설치와 운영 및 이용, 그리고 이에 대한 비용책임의 소재를 구체적으로 입법한 것이다. 독일 내의 국가와 주 및 지방자치단체를 연결하는 「망에 대한 사이버 안보」에 대한 근거규정은 아직『IT망법』내에서 입법되지 못하고 있고, 연방과 주 등 사이의 계약에 맡겨져 있거나 개별법에 의하여 규율되는 것으로 보인다. 연방과 주 및 지방자치단체들을 연결하는 망의 설치와 운영 및 이용, 그리고 이에 대한 비용 등의 문제 못지않게 이들 망에 대한 사이버 안보의 중요성이 인정되므로, 앞으로 보완해 나가야 할 것으로 전망된다.

(4) 연방과 주 사이의 계약(Staatsvertrag)

1) 국가계약의 의의

독일 기본법 제91조c는 제1항에서 연방과 주는 지역을 초월하는 중요한 사안에 대해서는 상호 협조할 수 있으며, 그 방식으로서 협약을 체결하는 방식을 제시하고 있다. 독일 기본법 제91조 c 제2항은 연방과 주는 행정주체 사이의 협약에 의하여 자신들의 정보기술 시스템들 사이의 통신에 필수적인 기준과 안보요건을 정할 수 있도록 규정하고 있다. 그러면서도 연방과 주들 사이의 충돌에 대해서는 협정에서 정하는 다수결에 따라 구체적인 하위 법규

명령들에 의하여 효력을 발생하도록 하되, 연방하원과 관계되는 주 대표의 동의를 반드시 요하도록 입법하고 있다. 이는 복잡한 독일의 연방제도의 특수성과 역사적 배경을 반영하는 것이다. 독일 기본법 제91조 c 제3항에서는 주들은 정보기술적 시스템의 공동 운영 및 이를 위한 시설설치에 대한 협정이 가능하도록 하고 있다.[62]

2) 『IT-국가계약』(IT-Staatsvertrag)

『IT-행정계획 회의(IT-Planungsrats) 설립 계약』 및 『연방과 주들 사이의 정보기술에 대한 규정을 위한 공동작업 계약』 등 역시 독일 기본법 제91조 c를 구체적으로 이행하기 위하여 체결되었다. 이를 『IT-국가계약』(IT-Staatsvertrag)이라고 부른다.[63]

동 계약 제1조는 「IT-행정계획 위원회」의 설립과 과제 및 결정권한의 범위 등에 대하여 규정하고 있다. 특히 동 위원회의 권한 및 과제로서 제1조 제1항에서는 사이버 안보에 대한 IT기술 표준에 대한 결정권한을 규정하면서 나아가 연방과 주들 사이의 정보 기술에 대한 협력, 국가와 주들 상호간의 연결에 대한 결정권한, 정보에 대한 질문 프로젝트에 대한 제어와 소통을 지원하는 업무 등을 구체적으로 규정하고 있다. 동 위원회에게 컨트롤타워 및 제어 기구로서의 역할을 부여하고 있으며, 이는 보장국가와 제어국가에서의 행정조직법상의 특징이 반영되고 있는 것이다.[64]

특히 동 계약 제3조에서는 국가와 주들 사이의 망에 대한 사이버안보의 요건 및 기준들(IT-Sicherheitsstandards)[65]을 규정하고 있다. 동 계약 제3조 제1항에서는 연방과 주들 사이의 정보의 전송이 가능하려면 IT 안보기준

62) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 53면.
63) G. v. 27.05.2010 BGBl. I S. 662, 663 (Nr. 26); http://www.buzer.de/gesetz/9288/index.htm?dorg=1 최종 방문일 2016.11.27.
64) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 244면.
65) http://www.buzer.de/s1.htm?a=3&g=IT-Staatsvertrag&dorg=1 최종 방문일 2016.11.27.

과 정보전송절차와 형식 및 표준 등이 규정되어야 한다고 규정하였다. 그러면서도 동 계약 제3조 제1항 단서에서는 1차적으로는 시장의 자율적인 기준이 우선하고, 2차적이고 보충적으로 동 계약상의 기준이 적용된다고 하고 있다. 이는 국가와 시장과의 관계를 설정한 중요한 입법취지가 담겨 있다. 시장의 자율을 우선적으로 존중하며, 예외적으로 국가가 개입하겠다는 것으로서 최근 독일에서 성공적으로 정착되고 있는 보장국가와 제어국가의 국가관[66]이 명시적으로 입법된 것으로 보인다.

동 계약 제3조 제3항은 이러한 사이버 안보기준 등 표준에 대한 것은 동 위원회에 의하여 선정된 전문적이고 독립적인 기구에 의하여 평가와 심사를 받도록 하고 있다. 사이버 안보기준 등에 대한 심사기구에는 반드시 기업과 과학 등 각종 분야로부터 차출된 전문가들을 포함시키도록 하였다, 이는 사이버 안보기준 등 표준을 마련하는 것의 중요성을 감안하여 또 다른 제어기구를 요구함으로써 공정성과 객관성, 독립성과 전문성을 확보하려는 것으로 보인다.

3) 『무선통신국가계약』(Rundfunkstaatsvertrag)

사이버안보와 관련된 또 다른 국가계약의 예로서 『무선통신국가계약』(Rundfunkstaatsvertrag)을 들 수 있다. 국가와 주들 사이의 공법상 계약으로서 『무선통신국가계약』(Rundfunkstaatsvertrag)이 해킹과 관련된 규범으로도 작용한다. 경찰질서청은 위험방지를 위한 임무를 수행하며, 주의 법률에 규정된 행정관청이 감독권을 가진다. 경찰질서청은 텔레미디어 서비스의 차단과 삭제를 위한 특별법적 근거를 가지고 있지 않으므로, 청소년 보호나 아동 포르노 퇴치를 위한 조치 등만을 할 수 있다. 그러나, 무선통신국가계약 제59조 제3항의 규정에 의하여 감독관청은 법 위반 사실이 있는 경우 서비스 제공자에 대하여 텔레미디어 서비스의 차단과 삭제 등의 조치를 취할 수 있다.[67]

66) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 233면.

Ⅳ 사이버 안보에 대한 독일의 개별법과 관련법

1. 개별법

(1) 독일 연방『전기통신법』(TKG, Telekommunikationsgesetz)[68]

1) 입법의 의의

독일 연방『전기통신법』(Telekommunikationsgesetz)도 사이버 안보에 대한 관련 규정을 제7장 제3절 통신안보와 정보보호 및 공적 안전 파트에서 추가해 나가고 있다. 특히『전기통신법』제111조 제1항은 최근에 카카오톡, 페이스북 등에 대한 수사당국의 정보제공요청거부 사건들과 관련한 규정을 입법하였다. 독일 연방『전기통신법』은 아날로그 방식의 전화에만 적용되는 것이 아니라, 개별법에서 사이버상의 정보제공에 대한 규정이 없는 경우에는 동법 제111조 제1항 제1호에서 「기타 연결정보」(andere Anschlusskennungen)라고 규정하거나, 「고정된 네트워크 주소 또는 추측에 의해 식별 가능한 네트워크 주소」라고 규정하고 있는 것에 비추어 사이버 안보에 대하여도 적용될 수 있도록 입법을 업데이트시키면서 수정해 가고 있는 것으로 해석하여야 할 것이다.

2) 입법의 절차규정

동법 제11조 제1항에 의하면 안보담당관청(Sicherheitsbehörde)으로부터 정보제공요구를 받아 통신서비스를 제공하거나 이와 결합하게 되어 통신상 식별 가능한 정보를 제공하게 되거나 전화번호나 다른 식별정보에 의하여 통신상의 식별정보를 제공하게 될 때에는, 정보제공요구와 관련하여 제112조와 제113조상의 고지절차 등을 준수할 책임을 지도록 규정하고 있다. 고지의 대상이 되는 정보의 내용에는 ① 전화번호 및 기타 연결정보, ② 성명과

67) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 293면.
68) https://dejure.org/gesetze/TKG/111.html 최종 방문일 2016.11.27.

추측에 의해 식별 가능한 주소, ③ 자연인의 생일, ④ 고정된 네트워크 주소 또는 추측에 의해 식별 가능한 네트워크 주소, ⑤ 이동 단말기의 접속과 이동 단말기의 제공을 통하여 이동단말기의 번호의 식별이 가능한 경우, ⑥ 단말기 사용계약의 개시정보 등이 포함된다.

위의 정보들에 대한 제공과 보존 등이 이루어지기에 앞서서 반드시 고지의무 등 동법상의 절차 준수가 이행되어야 한다. 이러한 고지의무 둥 동법상의 절차는 정보 제공과 보존 등이 영업상의 목적이 아닌 다른 목적으로 이루어지는 경우에도 마찬가지로 이행되어야 한다. 이러한 동법상의 절차이행의무는 정보주체 등 고객이 알았다고 하더라도 지켜져야 한다. 또한 동법상의 절차의 이행은 위에서 제시한 항목들의 정보에 열거되지 아니한 경우의 정보에도 적용된다.

3) 입법의 내용규정

독일 연방『전기통신법』은 정보화사회의 발전과 심화에 대비하여 입법을 매우 전문적이고도 상세하게 입법하고 있으며, 결코 추상적이거나 애매모호한 규정들로 일관하지 않는다. 선불카드 전화나 여권, 거주허가증, 상업서류나 관청의 각종 비교 가능한 서류 등에서 추출되는 정보들은 물론이고 클라우드 컴퓨터(Cloud Computing)[69]나 IP 어드레스[70] 등 대해서까지도 이에 대한 적법요건을 준수하지 않으면 안 된다고 구체적으로 사회 현실과 현상을 반영하여 규정하고 있다. 특히 동법 제1조 제6항에서는 정보의 수집과 저장에 대한 보상은 원칙적으로 이루어질 수 없음을 규정하고 있다. 이는 사이버 세계에서 정보에 대한 매매 등의 금전적 거래나 교환이 활발하게 이루어지고 있는 것에 대한 부정적인 태도를 입법적으로 명백하게 하고 있는 것으로 보인다.

69) Arndt・Fetzer・Scherer・Graulich (Hresg.), Telekommunikationsgesetz Kommentar, Erich Schmidt Verlag, 2.Auflage, Berlin, 2015, S.2168.
70) Arndt・Fetzer・Scherer・Graulich (Hresg.), Telekommunikationsgesetz Kommentar, Erich Schmidt Verlag, 2.Auflage, Berlin, 2015, S.2169.

4) 평가

독일『전기통신법』의 이러한 최근의 내용은 프라이버시와 정보자기결정권 및 기타 기본권을 존중하면서도 테러방지 등의 공익과 조화될 수 있도록 적법요건을 절차상으로 마련한 것으로서 타당한 입법이다. 다만, 동법 제111조는 독일 기본법 등에서 직접적으로 근거를 찾기는 곤란하고, 다만 형사소추나 위험방지(Gefahrenabsehr) 등과 관련하여 간접적으로 정보에 대한 감시 등을 헌법적 근거로 찾을 수 있다고 보기도 한다.[71]

정보화사회와 전자정부 등의 키워드들이 대변하듯, 새로운 미지의 분야들에 대한 입법적 규율에 있어서 비교적 후발주자이었던 독일이지만, 라우슈닝(Rauschning)이 법과 제도를 최고의 수출상품으로 자부하는 국가답게[72] 눈부시게 법적 정비에 있어서 발전해 나가는 모습을 보이고 있다.

특히 동법 제1조 제2항에서는 동법상의 의무들은 이메일과 이메일박스 등의 정보에 대하여도 준수되어야 한다고 하여 과학기술과 법의 괴리를 극복하는 입법을 하고 있다.

(2) 독일 연방『텔레미디어법』(TMG, Telemediengesetz)[73]

1) 입법의 의의

사이버안보를 위해 관련되는 법률로서 독일 연방『텔레미디어법』(Telemediengesetz, TMG)이 있다.『텔레미디어법』은 제1조 제1항에서 독일 연방『전기통신법』(Telekommunikationsgesetz)과의 관계를 고려하여 적용범위를 규정하고 있다. 동 법은 모든 전자적 정보와 커뮤니케이션 서비스에 대하여 적용되지만,『전기통신법』이 적용되는 것은 제외하는 것으로 하고 있다. 또한 조세영역에 대하여는 적용을 제외하며, 언론방송법이나 기타 법률

71) Arndt・Fetzer・Scherer・Graulich (Hresg.), Telekommunikationsgesetz Kommentar, Erich Schmidt Verlag, 2.Auflage, Berlin, 2015, S. 2109.
72) Rauschning, in Aussprache und Schlussworte, Wettbewerb von Rechtsordnungen, in VVDstRL, Band 69, De Gruyter, 2010, S.115.
73) https://dejure.org/gesetze/TMG 최종 방문일 2016.11.27.

의 적용을 배제하지 않는다고 하고 있다. 또한『방송에 대한 국가계약』(Rundfunkstaatsvertrag)에서 방송과 텔레미디어를 포함하는 특별요건들이 이 법에 편입되게 되었다.

방송법은 전파를 이용한 프로그램의 제작과 전송을 대상으로 하며, 커뮤니케이션 서비스는 네트워크를 이용하는 것을 대상으로 하는 점에서 차이가 있다. 그런데 동 법은「모든 전자적 정보와 커뮤니케이션 서비스」(alle elektronischen Informations- und Kommunikationsdienste)라고 적용범위를 규정함으로써 방송과 통신네트워크 뿐만 아니라 모든 융합서비스를 포함[74]하여 규율하려고 하는 의도를 가지고 있다고 보여 진다. 또한 동법 제1조 제1항 단서에서는 인적 적용범위도 공영방송을 포함한 모든 서비스제공자들에게 적용되며, 유료방송이든 무료방송이든 불문하고 적용된다고 하고 있다.

정보통신기술의 휴리스틱적 성격에 비추어서 불가피한 입법의 성격을 배려한 것으로 보인다. 그러나, 법률의 적용범위가 지나치게 포괄적으로 규정되어 있어 명확성의 원칙에 위반될 여지가 있어 보인다. 그럼에도 불구하고 동법은 최근 개정을 통하여 제2조 제6호에서「주문형 시청각 텔레미디어」("audiovisuelle Mediendienste auf Abruf" Telemedien)를 추가로 규정하면서 정보화사회의 현실과 변화를 더욱 상세하게 반영하고 있다. 또한 일부 자구를 수정하고『유럽공동체 규정』(Verordnung EU)와『유럽공동체 지침』(Richtlinie EU)을 반영하는 내용으로 수정하였다.[75]

74) http://www.kocca.kr/cop/bbs/view/B0000153/1212490.do;KCSESSIONID=dyyFX7BPTQyGRlpvsLyJ76Jt9ygYxmrxKQZRh2tCdsXgCYmLTZX1!-1867248667!-1690486075?searchCnd=&searchWrd=&cateTp1=&cateTp2=&useAt=&menuNo=&categorys=0&subcate=0&cateCode=&type=&instNo=0&questionTp=&uf_Setting=&recovery=&option1=&option2=&categoryCOM062=&categoryCOM063=&categoryCOM208=&categoryInst=&morePage=&pageIndex=1201 최종방문일 2016.12.2.

75) Bundesgesetzblatt Jahrgang 2010 Teil I Nr. 28, ausgegeben zu Bonn am 4. Juni 2010, Erstes Gesetz zur Änderung des Telemediengesetzes (1.Telemedienänderungsgesetz) Vom 31. Mai 2010, S. 692.

2) 입법의 절차규정

제13조 제1항에서는 서비스제공자들이 이용자들에게 정보의 이용 여부뿐만 아니라, 정보의 종류와 범위 및 목적 등을 함께 알릴 의무를 이행하여야만 정보를 사용 및 저장할 수 있다고 한다. 이러한 정보이용 등에 대한 고지의무는 유럽 내의 다른 나라에서의 정보처리에 대하여도 마찬가지이며, 자동적으로 연속해서 정보가 처리되는 경우에는 첫 단계에서부터 이용자에게 이에 대한 정보가 제공되어야 한다고 규정하고 있다. 제13조 제2항에서는 정보제공에 대한 동의는 전자적인 형태로도 등가하게 인정될 수 있다고 「등가성」에 대한 규정을 두고 있다. 제14조에서는 안보의 대상이 되는 정보의 구성요건에 대하여 상세한 규정을 하고 있다. 제15조에서는 서비스제공자가 이용자의 개인정보를 이용하기 위한 추가요건을 요구하고 있다. 사이버 안보와 관련하여 제15조 a를 최근 개정시 추가하여 불법적인 정보의 식별이 발생하는 경우에 고지의무를 입법하고 있다. 서비스제공자가 저장되거나 사용된 정보에 대한 불법적인 전송이 이루어졌거나, 제3자에게 위법하게 알려지게 되는 등으로 인하여 권리나 정당한 이익을 중대하게 침해할 위험이 있는 경우에는 연방정보보호법에 따라야 할 의무가 있다. 사이버 안보와 관련된 요건을 권리나 정당한 이익이 있는 경우에 한정하면서, 중대하게 침해할 위험이 있는 경우로 한정한 것은 역시 서비스제공자들과 이용자들 및 국가의 이해관계를 이익형량하여 조화점을 입법하려 고민한 것으로 보인다. 그러나 앞으로 정보화사회가 더욱 고도화되어 가고 텔레미디어를 포함한 정보통신 상에서의 개인정보침해나 각종 정당한 이익들의 침해가 지나치게 용이하다는 것이 드러나게 되면, 이 요건은 완화될 수 있을 것으로 보여 지므로 열려진 기준이라고 생각된다.

3) 입법의 내용

가. 텔레미디어 자유의 원칙 등

동법은 제4조에서 텔레미디어에 대하여 사전허가나 신고 등을 일일이 할

의무가 없고 자유롭다고 하여 「텔레미디어의 자유」를 선언하고 있다. 동법 제3조에서는 제1항에서는 유럽공동체 규정 및 지침을 준수하더라도 독일법을 어길 수 없다는 「원산지국가의 원리」(Herkunftslandprinzip)를 규정하고 있다. 그러면서도 동법 제3조 제2항에서 「텔레미디어 서비스 제공의 자유」를 보장하고 있다. 또한 동법 제3조 제3항 제3항 제4호에서는 개인정보보호를 위한 법에 대한 적용을 배제하지 않는다고 한다.

나. 일반적 정보제공의무과 기준

그러면서도 동시에 제5조에서 「일반적 정보제공의무」를 규정하고 있다. 동 규정은 텔레미디어라는 융합산업의 발전과 서로 충돌될 수 있는 사이버안보와 정보자기결정권과 프라이버시 등 다양한 이익을 조화롭게 달성할 수 있는 방안 중의 하나로 서비스제공자 등에게 동법상의 의무를 준수하도록 요구하고 있다. 특히 서비스제공자들에게 개인의 ① 정보에 대한 인식의 용이성, ② 직접 접근의 가능성, ③ 상시적인 처리가능성을 보장하여야 하도록 의무를 지우고 있다는 점에서 매우 구체적인 의무의 기준을 제시하고 있다 할 것이다.

다. 특별 정보제공의무와 기준

동시에 입법의 전문성을 담는 내용으로서 상업적 용도로 커뮤니케이션을 사용하는 경우에는 특별요건을 추가로 요구하는 입법의 형태를 취하고 있다. 이렇듯이 일반요건과 특별요건을 나란히 입법하는 것은 입법방식과 기술적인 면에서도 평가할 만하다고 생각한다.

라. 텔레미디어 이용에 대한 법률관계와 정보보호

독일 연방『텔레미디어법』제4절에서는 정보의 보호에 관하여 제11조부터 제15조 a 규정까지 상세한 입법을 하고 있다. 제11조에서 정보제공자(Anbieter)와 이용자(Nutzer)의 관계를 규정함으로써, 일방적으로 방송하던 시대에서 업로드와 다운로드를 병행하는 시대의 변화를 배경으로 법률관계를 설명하고 있다. 제12조 제1항에서는 「정보보호의 기본원칙」을 선언하고 있다.

제12조에서는 서비스제공자(Diensteanbieter, Service Provider)는 법령에서 명시적으로 텔레미디어에 대한 정보에 대하여 허용하는 규정을 두고 있거나, 이용자가 동의하는 경우에만, 텔레미디어에 관련된 정보를 규정하거나 사용할 수 있다고 하고 있는 것이다. 제12조 제2항에 의하면, 서비스제공자에게 「목적구속성의 원칙」이 적용되며, 예외적으로 텔레미디어에 대한 법령의 명시적인 규정이 있거나, 이용자가 동의하는 경우에만 목적외의 사용이 허용될 수 있다. 제12조 제3항에 의하여 자동적으로 처리되는 정보인지 여부와 상관없이 이러한 원칙들이 적용되게 되었다.

마. 실효성 확보수단

제16조에서는 동법의 실효성을 담보하기 위하여 행정벌로서의 금전부과처분을 할 수 있도록 하고 있다.

바. 보장책임의 입법과 책임성 강조

그런데, 특히 독일 연방『텔레미디어법』에 대한 중요한 입법 내용으로서 주목하여야 할 것은 서비스 제공자들과 국가 등의 책임(Verantwortlichkeit)을 강조하여 제3절에서 제7조부터 제10조까지 규정하고 있다는 것이다.

특히 독일에서는 최근 20년이 넘는 보장국가의 보장책임에 대한 방대하게 축적된 논의를 바탕으로 국가와 기업 등의 책임의 분할과 분담 및 구체적인 책임의 이행방안들에 대한 법제화가 체계적으로 진행되고 있다.[76]

스크로보츠(Skrobotz), 클뢰퍼(Kloepfer), 쇼흐(Schoch) 등도 정보화사회는 '단순한 기술의 발전'(Technisierung)을 의미하는 것이 아니라, 국가와 사회가 경계를 허물고, 책임을 분할하며, 시장과 협조하는 변화를 법적인 배경으로 하고 있다고 한다.[77]

다만, 서비스제공자의 책임에 대하여는 고유한 자신들이 관리하는 정보에

76) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 235면.
77) Skrobotz, Das elektronische Verwaltungsverfahren, Duncker & Humblot, Berlin, Band 14, 2005, S. 94.

대하여는 책임을 인정하지만, 서비스제공자들에게 전송되어오거나 제3자들이 그들에게 저장해 둔 정보들에 대하여는 일일이 감시하고 통제할 책임은 부정하고 있다. 그렇지만 불법적인 정보의 이용에 대하여는 제거하고 차단할 책임이 있다고 하며, 전기통신상의 정보에 대한 비밀은 보장되어야 한다고 하고 있다. 동 법률상의 이 규정은 사이버 안보의 개념과 대상이 점차 확대되어 가는 현실 속에서 기준을 제시하여야 할 입법적 필요에 부응하여 만들어진 것이라고 하겠다.

이와 관련하여 최근 독일 함부르크 지방법원[78]에서 Google 회사는 독일 영역 내에서 유튜브(Youtube)의 서비스제공을 통해서 제3자들에게 원고(독일 음악공연 및 음향기술 저작권협회[79])의 음악작품들이 공개되지 않도록 할 의무가 있으며, 이를 위반하는 경우에는 이행강제금이나 이것이 징수되지 않을 경우 6개월까지의 이행강제를 위한 구금(개별적인 경우에는 최대 25만 유로의 이행강제금이나 전체적으로 최대 2년의 이행강제를 위한 구금)을 받도록 판결하였다.[80]

4) 평가

과거에는 권리와 의무 위주의 구도로 입법되었지만, 특히 독일에서는 보장국가의 보장책임이 강조된 이래 민주주의와 책임을 고려하는 입법적 태도들이 더욱 뚜렷해지고 있다. 시장의 자율을 존중하는 것을 원칙으로 하면서도, 시장이 제대로 작동하지 못할 때는 거리를 좁혀서 국가의 개입을 통해 시장의 기능을 회복할 수 있다는 입법적 사고를 반영하고 있다. 이를 위해 시장과의 거리의 원칙에 따라 「자율규제」(lex mercatoria, Selbstregulierung, Self-Regulation)와 「기존의 고권적 정부규제」(hoheitliche Regulierung; Command-and-Control Regulation) 및 그 중간 형태인 「규제된 자기규제」

78) LG Hamburg, Urteil v. 20.4.2012, Aktenzeichen:310・461/10.
79) Gesellschaft für musikalische Aufführungsund mechanische Vervielfältigungsrechte.; 성봉근, 앞의 논문, 72면에서 재인용.
80) LG Hamburg, Urteil v. 20.4.2012, Aktenzeichen:310・461/10.

(Regulierte Selbstregulierung, hoheitlich regulierte gesellschaftliche Selbstregulierung)를 적절하게 활용하고 있다.[81] 정부의 고권적 규제만으로 사이버 세계를 규율할 수 있다는 사고는 독일을 비롯한 유럽은 물론 영국과 미국에서조차 이미 구태의연한 시대착오적인 것이 되어버리고 있다. 이미 우리나라의 법률들에도 환경법과 정보통신분야의 법령, 소비자보호법령, 증권 등 금융관련법령 등에도 다양하고도 광범위하게 이러한 새로운 규제의 유형들이 산재해 있다.

독일 연방『텔레미디어법』이 명확성의 원칙에 비추어 비판을 받고 있을 정도로 광범위하게 적용대상을 규정하고 있기는 하다. 그러나 동법으로부터 시사 받을 핵심은 앞으로 전개될 사이버 세계에 대한 법적 규율의 방향은 과학과 기술의 발전을 자유롭게 허용하되, 적법요건을 준수하고 책임을 서로 분담하여 지면서 상반되고 상충하는 이익들을 비교형량하여야 한다는 것으로 보인다.

(3) 독일 연방『정보보호법』(BDSG, Bundesdatenschutzgesetz)[82]

1) 입법의 의의

독일 연방『정보보호법』(BDSG, Bundesdatenschutzgesetz)는 개인정보보호를 위하여 입법이 되었다. 이 법의 정식 명칭은『정보보호와 공적 정보에 대한 법률』(Recht des Datenschutzes und der öffentlichen Informationen)이다. 동법 제1조 제1항에서 제정목적은 인격권이 침해될 수 있는 개인정보가 처리되는 과정에서 개인을 보호하기 위한 것이라고 한다.

2) 입법의 내용

가. 개인정보보호의 엄격한 보호

개인정보를 보호하기 위하여 동법 제4조 제1항에서는 개인정보의 국외이전

81) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 257면.
82) https://dejure.org/cgi-bin/suche?Suchenach=bdsg+sicher#Treffer 최종 방문일 2016.11.27.

이나 국가간 이전에 대하여 요건을 엄격하게 규정하고 있다. 동법 제4조 제1항은 특히 정보자기결정권(Informationelle Selbstbestimmungsrechts)을 보장하기 위한 중심이 되는 대표적인 규범으로 평가된다.[83] 개인정보에 대한 침해는 함부로 인정되어서는 안 되며, 입법자가 정보이용에 대한 처분권을 침해하지 않을 수 없는 유일한 수단으로 인정되고, 법령으로 그것이 허용될 때에만 가능하다고 한다.[84] 즉 비례의 원칙과 법률유보의 원칙의 적용아래에서만 개인정보의 침해가 허용된다고 명문으로 규정하고 있는 것이다.

특히 동법 제4조a에서는 개인정보에 대한 조사・사용・처리 등에 대하여 옵트-인(Opt-in) 즉, 사전동의의 원칙을 강조하고 있으며, 사전동의는 진정한 자유로운 자기결정에 근거한 것이어야 하며, 개인정보의 조사・사용・처리 등에 대한 목적이 제시되지 않으면 안 된다.[85] 사전동의의 이러한 요건을 갖추지 못한 경우에는 동법이나 다른 법령에 의한 예외규정이 없는 한, 개인정보에 대한 조사・사용・처리 등은 함부로 인정될 수 없다.[86]

동 요건에 대하여는 제15조, 제16조, 제28조에서 제30조까지 상세한 입법을 하고 있다. 동 조항은 독일 등 유럽의 개인정보보호수준이 미국의 『세이프하버』(Safe Harbour)보다 훨씬 높다는 것을 의미한다.

구체적으로는 공공기관에서의 개인정보조사(Datenerhebung), 개인정보저장・수정・이용((Datenspeicherung, -veränderung und -nutzung), 공공기관에의 개인정보전송(Datenübermittlung an öffentliche Stellen), 사적 기관이나 단체에의 개인정보전송(Datenübermittlung an nicht-öffentliche Stellen), 사적 기관이나 단체 및 공법상 경쟁적 기업 등에의 개인

83) Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2011, S. 415.
84) Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2011, S. 415.
85) Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2011, S. 38.
86) Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2011, S. 415.

정보전송(Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen) 등으로 분류하여 사이버상의 개인정보 보안에 대한 입법을 하고 있다.

나. 「목적구속성의 원칙」

그러면서도 동법 제31조에서는 특별요건으로서 「목적구속성의 원칙」(Besondere Zweckbindung)을 선언하여 함부로 개인정보를 상업적 목적이나 정치적 목적 등으로 전용하여 사용하지 못하도록 엄격하게 규정을 하고 있다. 개인정보는 오로지 개인정보의 통제목적, 정보의 보안목적, 정보처리 시스템의 적절한 운영을 보장하기 위한 목적 등을 위해서만 이들 기관이나 기업들이 사용할 수 있다고 무겁게 규정하고 있다.

이 규정의 배경이 되는 것은 독일의 「인구조사판결」[87]이라고 할 수 있다. 「인구조사판결」은 ① 개인정보의 수집 및 처리에 대하여 법률의 근거가 필요하다고 하였으며, ② 정보자기결정권을 기본권으로 인정하였으며, ③ 기본권을 보호하기 위하여 목적구속성의 원칙을 엄격하게 요구하는 판시를 하였다.

다만, 최근에는 전자정부와 빅데이터 시대에서 이를 완화해서 파악하려는 주장도 제기되고 있다.[88] 독일에서 주의 경찰법들이 정보의 변경과 관련하여 목적변경을 허용하는 규정을 가지고 있기는 하다.[89] 다만, 목적구속성의 원칙의 본래의 취지를 훼손할 정도로 지나치게 완화되거나 희석되어서는 안 될 것이다.

다. 「적절한 정보보호수준」의 요구

특히 동법 제4조 제2항에서는 개인정보의 국외이전에 대하여 보호할 가치가 있는 이익이 있는 경우에는 이전을 제한할 수 있도록 규정하면서, 이전되

87) BVerfGE 6, 1 (46)
88) 계인국, 빅데이터 시대 전자정부에서의 개인정보보호 -개인정보보호 원칙의 변화와 도전-. 안암법학, 제50권, 2016,
89) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 235면

는 나라의 개인정보보호수준이 「적절한 정보보호수준」(angemessenes Datenschutzniveau, adequate level of data protection)이 보장되지 못하는 경우에는 역시 개인정보이전이 제한될 수 있다고 하고 있다. 동 규정을 비롯한 유럽의 높은 개인정보보호기준에 근거하여 유럽연합사법재판소(CJEU)는 「슈렘스판결」(Schrems)[90]에서 미국의 완화된 개인정보보호기준인 『세이프하버』가 「적절한 정보보호수준」을 보장한다고 신뢰할 수 없는 수준의 것으로서 위법하다는 결정을 이끌어내게 되었다.[91]

독일 연방『정보보호법』제4조 제3항은 미국이나 우리나라를 포함하여 유럽연합 이외의 나라들의 개인정보보호수준이 독일 등 유럽연합의 기준까지 미치는지 아니면 그러하지 아니한지를 구별하는 기준을 제시하고 있다. 개인정보호기준이 「적절한 정보보호수준」을 유지하고 있는지 여부는 정보전송과 관련한 모든 제반 사정과 환경을 고려하여 평가된다. 「적절한 정보보호수준」인지는 특히 정보의 종류, 정보의 목적, 예정된 정보처리의 기간, 정보의 원산지국가와 이전대상국가, 이들 나라의 법령과 기준에 대한 규율 및 개인정보를 보호하는 조치 등을 종합하여 평가하도록 되어 있다.

미국마저 이에 위반되어 무역제재의 대상이 되었던 선례에 비추어 우리의 법제는 과연 앞으로 개인정보보호에 대한 입법을 어떻게 수정하여야 하는지 심각하게 고민해 보아야 한다.

3) 평가

독일 연방『정보보호법』은 개인정보보호를 매우 철저하게 국내는 물론이고 국외이전과도 관련하여 철저하게 하는지를 잘 보여주는 수준 높은 입법으로 평가할 수 있다.

독일 연방『정보보호법』으로부터 시사 받을 수 있는 점은 우리 법제가 지

90) EuGH, C-362/14; EuGH, NJW 2015, 3151. 상세한 판례의 내용은 정남철, 독일의 정보보호정책과 입법과제, 2016년도 유럽헌법학회 제4회 학술발표대회 발표문, 2016.11, 46면.

91) http://www.boannews.com/media/view.asp?idx=49489 최종 방문일 2016.11.15.

금의 높은 개인정보보호수준에서 하향기준으로 조정하여 사이버안전과 4차 산업혁명을 함부로 값싸게 달성하려 들어서는 안 된다는 것이다. 미국마저 기준을 수정하는 선례를 보면, 동법 제4조 제2항과 충돌하게 되어 국가적으로는 무역제재와 개인적으로는 기업이 파산할 정도의 과징금을 부과 받을 가능성이 높다. 이제 국제사회는 법과 도덕 등의 가치를 무역상의 활동의 자유와 경제적 이익에 반영하여 신용점수처럼 활용하는 시대가 되어가고 있음을 주의하여야 한다. 경제적인 이익과 법치주의 및 도덕적 책임을 분리해서 평가받을 수 있는 시대가 종언을 고해가고 있다는 냉엄한 법현실의 변화를 너무 늦지 않게 인식할 필요가 있다.

개인정보보호수준을 높게 하면서도 사이버안보와 4차 산업발전을 얼마든지 이룰 수 있다고 생각한다. 다만, 이를 위해서는 국가와 기업들의 기술과 법제에 대한 투자가 필요하지만, 처음부터 제대로 된 입법을 함으로써 그렇지 않은 경우의 국가신인도 하락과 무역제재 및 기업의 파산 등을 방지하는 것이 법정책적으로나 헌법과 법치주의관점에서 더욱 타당하다.

특히 독일 연방『정보보호법』제4조 제3항은 우리가 장차 독일 등 유럽과의 개인정보보호수준에 대한 법적 분쟁이 유럽연합사법재판소 등에서 발생할 때를 대비하여 어떻게 개인정보호호기준을 설정하고 수정해 나갈 것인지에 대한 중요한 판단기준을 제시하여 준다는 점에서 반드시 참고하여야 할 것이다.

(4)『국제적 테러와의 전쟁에 있어서의 정보교환을 개선하기 위한 법률』(Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus)[92]

최근 독일을 비롯한 유럽과 미국 등지에서의 테러참사들이 연달아 일어나자, 사이버상으로 테러에 대한 방비를 효과적으로 하기 위하여『국제적 테러와의 전쟁에 있어서의 정보교환을 개선하기 위한 법률』(Gesetz zum besseren

92) http://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl116s1818.pdf%27%5D__1480600046726 최종 방문일 2016.12.1.

Informationsaustausch bei der Bekämpfung des internationalen Terrorismus)이 2016년 7월에 제정되어 발효되기 시작하였다.[93]

사이버안보의 문제는 국경을 초월하여 발생하는 특성을 가지는데, 이를 고려하여 국제적 협력을 강화하기 위한 입법으로서 의미를 가진다고 평가할 수 있다. 사이버안보에 대한 입법을 할 때 국내적인 규율로만 대응하려해서는 안 된다는 것을 입법에 대한 방향설정과 평가에서 반드시 고려하여야 할 것이다.

(5) 『에너지 산업법』(Energiewirtschaftsgesetz)[94]

사이버공격과 오프라인공격이 결합되는 유형들에 대비하여 독일에서는 에너지발전시설의 네트워킹 안보에 대한 입법이 이루어지고 있다. 『에너지산업법』(Energiewirtschaftsgesetz)이 제정되어 에너지 산업시설의 망을 규율하기 시작하였다. 동 법에서는 국가의 책임만 규정하는 것이 아니라 에너지망을 운영하는 자들에 대한 책임과 과제도 함께 규정하고 있다.

동법 제11조에서는 에너지 공급 업무를 담당하는 자들에게 ① 안전성, ② 신뢰성, ③ 충분한 공급 등이 담보되는 작동・유지 및 최적화의무를 지우고 있다. 또한 이러한 의무는 경제적으로 허용되는 최대한 ① 차별 없이, ② 최적화에 대한 기대와 요구에 부응하면서, ③ 강화되고 확장되는 방향으로 이행할 의무를 진다고 규정한다.

동 규정을 확대해석하여 에너지 산업시설과 망에 대한 사이버공격에 대비할 수도 있다. 그럼에도 불구하고, 독일『에너지산업법』은 제11조 제1항a, b, c 등으로 이에 대비한 특별한 명문규정을 추가로 입법하고 있음을 주목하여야 한다. 안전한 에너지 공급망의 운영이란 정보통신시스템이나 전자정보처리시스템에 대한 위협으로부터 적절한 보호를 포함하는 것이라고 명백하게

93) BundesgesetzblattJahrgang 2016 Teil I Nr. 37, ausgegeben zu Bonnam 29. Juli 2016, S. 1818.
94) https://dejure.org/gesetze/EnWG/11.html 최종 방문일 2016.11.27.

규정을 두고 있다.

그러면서 에너지 산업분야를 규율하는 행정청들은『IT 안보법』에서 규정한「연방정보기술안보청」(BSI)과 함께 이에 대한 행정을 협력하여 수행하도록 하고 있다. 그 일환으로서 안전에 대한 요건들의 목록을 공동으로 설정하여야 하고, 이를 공표하여야 한다. 에너지 산업 분야의 정보통신기술관련 요건 목록에는 안전요건 이행에 대한 적법심사를 위한 규율기준이 포함되어야 한다. 에너지공급 업무에 대한 적합한 보호는 안전요건에 대한 목록이 이행되고, 문서에 의하여 그 이행에 대한 기재가 이루어져야 담보된다.

독일『에너지산업법』은 사이버공격과 안보를 사이버 안에서만 이루어지는 협의의 개념으로 보고 대응하지 아니하고, 현대형 위험의 특징적인 형태인 결합형에 대비하여 확장하여 상세한 입법을 해 나가고 있다는 점에서, 우리 입법의 방향에 큰 참고가 될 것으로 보인다.

(6)『접근차단법』(Zugangserschwerungsgesetz)

사이버안보의 개념을 음란물이나 폭력물의 경우도 포함할 것인가 여부에 대한 논란이 있지만, 최근 이들 음란 및 폭력물과 바이러스 등 악성코드들과 결합하여 사이버 공격이 이루어지고 있으므로 함께 다루는 것이 타당할 것으로 보인다.

독일도 이러한 고민 속에 아동 포르노 사이트의 차단을 허용한 '접근차단법'(Zugangserschwerungsgesetz)을 입법하였다. 그러나. 실질적으로 적용된 적이 없었고, 2011년 법률을 통하여 폐지되었다.

해킹이 가능하도록 한 악성코드 등을 탑재한 인터넷상의 콘텐츠는 콘텐츠를 작성하여 올리는 사람인 콘텐츠 제공자(Content Provider)가 우선적으로 위험제거에 대한 행위책임이 있다. 인터넷접속서비스제공자(Internet Access Service Provider)는 원칙적으로 책임을 부담하지 않지만, 예외적으로 서비스 제공업자가 해킹과 관련된 위법내용을 알 수 있고, 이를 차단하는 것이 기술적으로 가능하다면, 서비스 제공업자도 해킹과 관련된 상태책임

자가 될 수 있다.[95] 행정청이나 사인이 해킹과 관련된 위법한 내용을 지적하였을 때에는 서비스제공업자라도 웹사이트를 자발적으로 차단하는 자율규제를 하여야 한다.[96]

2. 사이버 안보를 위한 인접 분야의 법령

(1) 독일 연방『형법』

독일의 경우는 최근「정보 해킹죄」를 구성요건으로 연방『형법』에서 ①제202조 a의「데이터 감시죄」(Ausspähen von Daten, Spying out data)와 ② 제202조 b의「데이터 가로채기죄」(§ Abfangen von Daten, Interception of data), ③ 제202조 c의「데이터 감시 및 가로채기 예비죄」(§ 202c Vorbereiten des Ausspähens und Abfangens von Daten)[97]를 신설하여[98] 사이버 안보를 해치는 경우에 대비하고 있다.

『형법』제149조에서「컴퓨터 사기죄」(Vorbereitung der Fälschung von Geld und Wertzeichen)를 두어 보이스 피싱 등을 처벌하고[99], 제303조 b에서「컴퓨터 업무방해죄」(Computersabotage, 컴퓨터 작동마비죄)[100]를 입법하여 타인에게 중요한 의미를 가지는 정보처리업무를 방해하는 자에 대한 처벌하는 규정을 두고 있다.

그러나 형사처벌로는 효과가 미미하며, 해외에 서버를 두고 있는 경우 형사처벌이 어렵다는 한계를 여전히 가지고 있다. 따라서 사이버안보에 대한 행정법적 정비를 해 나가는 것이 가장 효과적인 입법 방식이라고 생각한다.

95) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 295면.
96) 서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015, 295면 등.
97) https://dejure.org/gesetze/StGB/202c.html 최종 방문일 2016.11.27.
98) https://dejure.org/gesetze/StGB/202b.html 최종 방문일 2016.11.27.
99) https://dejure.org/gesetze/StGB/149.html 최종 방문일 2016.12.4.
100) https://dejure.org/gesetze/StGB/303b.html 최종 방문일 2016.11.27.

(2) 독일 연방 민법전

마찬가지로 개정된 독일 연방 민법전(BGB) 제126조 a에서도 등가성을 인정받기 위한 요건으로서 전자서명법에 따라 인증된 전자서명과 표의자의 명의가 제공되어야 한다고 요구하고 있다.

사이버안보의 기본적인 전제는 전자서명을 통한 보안성의 확보에 있다는 것을 인식하여 민사거래의 일반법인 민법전에 이를 규정하고 있다. 우리의 경우 기본법인 민법에서 등가성에 대한 규정이 흠결된 채, 개별법에서 등가성에 대한 규정을 두는 경우들이 있어 입법체계상 문제가 있다.[101]

V 유럽연합(EU)의 입법

1. 유럽연합법의 종류

독일을 비롯해서 유럽연합의 국가들은 유럽공동체법과 관계를 맺고 있다.

직접적으로 독일법 등 유럽국내법들의 상위 규범으로 직접 작용하는 것은 『유럽공동체 규정』(EU Verordnung, EU Regulation)이다. 『유럽공동체 규정』은 독일을 비롯한 유럽연합 소속의 국가들에 대하여 일반적인 효력을 가진다. 『유럽공동체 규정』은 회원국들에 대하여 직접적으로 효력이 있으므로, 그 규율내용은 회원국들의 행정청과 법원 및 시민들을 직접적으로 구속한다.[102]

국내법의 규범으로 내용을 전환시켜서 간접적으로 작용하는 것은 『유럽공동체 지침』 (EU Richtlinie, EU Directive)이다. 『유럽공동체 지침』은 기본적으로 유럽연합의 회원국들에게 적용되지만, 회원국들의 국내법의 형식과 방법으로 전환되어 적용되는 것을 목표로 제정되는 규범이다.[103] 보통 지침

101) 성봉근, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6 45면.

102) Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 72 ; Ehlers und Pünder (Hrsg.), Allgemeines Verwatungsrecht, 15. Aufl., Walter de Gruyter GambH, Berlin/Boston, 2016, § 5, Rn 12.

을 몇 년간 시행하다가 그 결과를 지켜보고 시행착오를 수정하면서『유럽공동체 규정』으로 승격되는 경우가 많다.

『유럽공동체 결정』(EU Beschlüß, EU Decision)은 특정인이나 특정 국가에 대하여 발급되며, 이들에게 구속력을 가진다. 104)

『유럽공동체 권고 및 의견』(EU Empfehlungen und Sellungnahmen, EU Recommnedation and Opinion)은 법적인 구속력이 발생하지 않지만, 정치적인 의미를 표할 수 있는 공식적인 선언으로서의 의미를 가진다.105)

『유럽공동체 실행행위』(EU durchführungsrechtsakte, EU Implementing Acts)는『유럽연합업무방식협약』(AEUV, Vertrag über die arbeitsweise der Europäischen Union) 제291조에 의하여 도입된 것으로서 특별한 수권을 받아 구속력 있는 행위를 실행하기 위한 결정에 가까운 성질의 것이다.106)

그밖에도 다양한 형태들이 계속해서 개발되고 있다.107)

2. 독일법과 유럽연합법(EU법)과의 관계 – 유럽연합법의 우위

독일을 비롯한 회원국들과 유럽연합법과의 관계에 있어서는「유럽연합법의 우위」가 적용된다. 따라서 독일을 비롯한 회원국들은 유럽연합법에 위반

103) Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 72 ; Ehlers und Pünder (Hrsg.), Allgemeines Verwatungsrecht, 15. Aufl., Walter de Gruyter GambH, Berlin/Boston, 2016, § 5, Rn 13.

104) 과거에는 EU Entscheidungen으로 불리었다. Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 72; ; Ehlers und Pünder (Hrsg.), Allgemeines Verwatungsrecht, 15. Aufl., Walter de Gruyter GambH, Berlin/Boston, 2016, § 5, Rn 18.

105) Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 72; Ehlers und Pünder (Hrsg.), Allgemeines Verwatungsrecht, 15. Aufl., Walter de Gruyter GambH, Berlin/Boston, 2016, § 5, Rn 24.

106) Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 72.

107) 이에 대하여 상세한 내용은 Ehlers und Pünder (Hrsg.), Allgemeines Verwatungsrecht, 15. Aufl., Walter de Gruyter GambH, Berlin/Boston, 2016, § 5, Rn 25-29.

될 수 없다.

이것의 의미에 대하여 마우러(Maurer)는 「효력의 우위」로 보는 관점에 대하여 반대하면서, 「적용의 우위」(Anwendungsvorrang)로 보고 있다.[108]

3. 유럽연합법 위반의 효과

독일 등 유럽연합의 국내법들이 유럽연합법에 위반되는 경우의 효과에 대하여는 논란이 있다.

효력의 우위로 보게 되면, 유럽연합법에 위반되는 독일 국내법령들은 일반적인 무효가 되지만, 적용의 우위로 보게 되면 충돌되는 경우에 대하여 당해 독일 법령의 적용만 거부가 되고, 다른 사건에서는 그대로 유효하게 된다. 마우러(Maurer)는 적용의 우위로 보게 되므로, 일반적 무효설이 아니라 일시적 적용중지설을 취한다.[109]

4. 유럽연합법상의 사이버상 개인정보 보호 수준

(1) 완전한 보호 수준의 요구

최근 유럽공동체(EC)는 유럽연합(EU)으로 하여금 포괄적이고도 일관되게 개인정보보호권이 '완전하게'(fully)보호되도록 정보보호장치 및 제도를 요구하게 되었다.[110] 우리나라의 법제가 어디로 가야할지 반드시 짚어보아야 할 대목이다. 국제적이고 비교법적인 관점없이 성급하게 개인정보보호수준을 함부로 완화하는 것은 심각한 문제를 초래할 것이다.

108) Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 77.

109) Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011, § 4, Rn 77.

110) EUROPEAN COMMISSION, A comprehensive approach on personal data protection in the European Union, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Brussels, 4.11.2010 COM(2010) 609 final, 4p.

(2) 유럽연합『정보보호 일반규정』(General Data Protection Regulation, Die Allgemeine Daten Schutz Verordnung)[111]

유럽연합『정보보호일반규정』(General Data Protection Regulation, EG-DatenSchutzverordnung)은 정보보호법률의 내용에 대한 것이라기보다 정보보호시스템에 대한 관련성이 더욱 큰 성격의 입법이다. 이는 정보보호를 위한 지속적인 시스템의 구축을 핵심적인 내용으로 한다.[112]

종전의『정보보호규정』(Data Protection Directive 95/46/EC)에 의하면, 구글(Google) 같은 기업이「구글거리지도」(Google Street View)에서 보듯이 개인정보를 침해하는 사업을 하는 경우에 동일한 허가를 수많은「정보보호국」(DPAs, Data Protection Authorities) 으로부터 받아야 하였으며, 이들 행정청 사이에 충돌되는 경우를 조정할 수 있는 시스템이 없었다.[113]

그러나 이번 유럽연합『정보보호 일반규정』은 단순하면서 지속적인 정보보호체계를 구축하였다. 첫 번째는 한 개의「정보보호국」(DPA)에서 이에 대한 규제를 담당하도록 하여 기업이나 각종 기관들은 이른바「원스톱 서비스」((One-stop Service)가 이루어질 수 있게 되었다. 두 번째는 유럽연합내의 복수의「정보보호국」들은 상호 위임에 의하여 권한의 집중이 이루어지게 함으로써 이것이 가능하도록 하고 있다.[114]

또한『정보보호 일반규정』에서는 종전보다 개인정보에 대한 접근권을 강화하면서 개인정보에 대한 조사 등에 대한「고지의무」와「잊힐 권리」(Recht auf Vergessenwerden)' 및 이에 따른「정보삭제권」,「정보이동권」,「단체소송」과「손해배상청구권」 등을 새롭게 추가하여 규정하고 있다.[115]

111) http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm 최종 방문일 2016.12.5.
112) http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm 최종 방문일 2016.12.5.
113) http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm 최종 방문일 2016.12.5.
114) http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm 최종 방문일 2016.12.5.

Ⅵ 결 론

사이버위험이 사이버상의 위험에 그칠 것이라고 보는 것은 이를 '찻잔 속의 위험'으로 착각하는 중대한 결함이 있는 이론적 접근이다. 이제 사물인터넷과 빅데이터 기술의 발전으로 인하여 온라인과 오프라인을 연결하고 상호 접속하게 할 수 있게 되었기 때문이다. 따라서 사이버안보에 대하여도 사이버상의 안보라는 유형과 오프라인과 결합되는 유형을 모두 포함하여 이론적 접근을 하지 않는다면, 변화하는 현실에 대한 규범력을 상실하게 된다. 현대형 위험은 결합형이 특징으로서, 접속의 지속성과 규모의 확대 등으로 인하여 앞으로 발생하게 될 사이버안보에 대한 위험의 구체적인 내용은 미지의 것으로서 더욱 불확실성을 가중시킨다. 종래의 시각에 대한 수정이 필요하다.

따라서 사이버안보를 위해서는 그 자체의 기술력을 제고시키는 과학과 기술에 대한 투자도 당연히 수반되어야 하지만, 헌법과 민주주의 및 적법절차 등에 소요되는 비용을 「죽은 비용」으로 바라보지 말고 반드시 필요한 비용으로 바라보면서 서로 조화될 수 있도록 투자와 제도개선에 노력하는 것이 요청된다.[116]

결국 정보화사회에서 행정이 변화할 수밖에 없다. 그러나 법치주의의 근본을 부정할 수는 없다. 법치주의의 근본을 잘 지키면서 사이버안전과 조화될 수 있도록 하는 방향으로 갈 수 밖에 없다. 따라서 주체, 절차, 형식, 내용상의 적법 요건에 부합하는 법과 판례를 형성해 나가는 것이 앞으로의 중심과제이다.

이러한 기준에 부합하지 못하면, 이제는 국제적으로 혹독한 제재를 받게 되어 있고, 국가신뢰도에도 치명적인 영향을 주게 되어 있다. 따라서 이러한

115) 정남철, 독일의 정보보호정책과 입법과제, 2016년도 유럽헌법학회 제4회 학술발표대회 발표문, 2016.11, 45-46면; 홍선기, 유럽 개인정보보호법상의 과징금에 대한 고찰, 2016년도 유럽헌법학회 제4회 학술발표대회 발표문, 2016.11,, 14면.
116) 성봉근, 행정법에서 '비용'과 '가치' 재검토, 행정법연구, 제43호, 2015.11, 49면.

종합적인 시각으로 대처해 나가면서, 조화로운 이익형량을 하여야 할 것이다.

법치주의와 조화되는 사이버안보를 가능하도록 법과 제도를 정비하는 것이 보장국가의 보장책임[117] 중의 하나임을 강조하고 싶다.

117) 성봉근, 보장국가에서의 위험에 대한 대응 - 전자정부를 통한 보장국가의 관점에서 본 위험-, 법과 정책연구, 제15권 제3호, 2015.9, 1039면

[참고문헌]

<국내문헌>

<단행본>

박희영・홍선기, 독일연방헌법재판소 판례연구 I [정보기본권], 한국학술정보(주), 2010.

서정범・박병욱(역), 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015.

함인선(역), 유럽정보보호법, 전남대학교 출판부, 2014.

홍선기, 유럽인권법원판례연구, 수북이, 2015.

<논문>

계인국, 빅데이터 시대 전자정부에서의 개인정보보호 -개인정보보호 원칙의 변화와 도전-. 안암법학, 제50권, 2016.

길준규, 통합개인정보보호법과 효과적인 개인정보의 보호, 토지공법연구, 제57집, 2012.5.

김남진, 위험의 방지와 리스크의 사전배려, 고시계, 2008. 3.

_____, 公私協力과 행정법상 주요문제, 학술원통신, 제269호, 2015.12.

김동현・강병기, 부동산전자상거래시스템 제도화 방안과 부동산 컨텐츠 보안에 관한 연구, 한국 전자통신학회 학술대회지. 2008.5.

김연태, 환경법에 있어서 사전배려원칙의 실현, 법학논집, 제34권, 1998.

김재광, 진화하는 사이버안보 위협과 법제적 대응방안, in 제4차 산업혁명 물결, ICT 법제 개선방향, 국회 제4차 산업혁명포럼, 2016.7.

김진수・심우민, 지도 데이터의 국외 반출에 대한 주요 쟁점 및 시사점, 이슈와 논점, 제1197호. 2016.8.

김태오, 사이버 안전의 공법적 기초 -독일의 IT기본권과 사이버안전법을 중심으로, 행정법연구, 제45호, 2016.6.

박재윤, 사이버안보의 복합적 특성과 국가사이버안보기본법(안)에 관한 토론문, in 국가사이버안보법제의 제정필요성과 법적 쟁점, 한국행정법학회 등 공동학술대회, 2016.10.

성봉근, 보장국가에서의 위험에 대한 대응 - 전자정부를 통한 보장국가의 관

점에서 본 위험-, 법과 정책연구, 제15권 제3호, 2015.9.
_____, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014.
_____, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6.
_____, 보장국가로 인한 행정법의 구조변화, 지방자치법연구, 제15권 제3호, 2015.9.
_____, 행정법에서 '비용'과 '가치' 재검토, 행정법연구, 제43호, 2015.11.
_____, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6.
손형섭, 개인정보의 보호와 그 이용에 관한 법적 연구, 법학연구, 법학연구 제5집, 2014.6.
오길영, 소위 '옥션판결(대판 2013다43994, 44003)에 대한 비판과 TOM, 공법학회 정보인권연구포럼 발표문, 2016.5.
정남철, 독일의 정보보호정책과 입법과제, 2016년도 유럽헌법학회 제4회 학술발표대회 발표문, 2016.11.
이성엽, 사이버위협과 국가사이버안보법의 제정 필요성, 한국행정법학회·한국사이버안보법정책학회, 개인정보보호법학회 공동학술세미나, 2016.10
최경진, 미래 ICT 환경에 맞는 바람직한 개인정보보호 법과 정책의 개선방향, in 제4차 산업혁명 물결, ICT 법제 개선방향, 국회 제4차 산업혁명포럼, 2016.7.
홍선기, 유럽 개인정보보호법상의 과징금에 대한 고찰, 2016년도 유럽헌법학회 제4회 학술발표대회 발표문, 2016.11.

<독일문헌>

Arndt·Fetzer·Scherer·Graulich (Hresg.), Telekommunikationsgesetz Kommentar, Erich Schmidt Verlag, 2.Auflage, Berlin, 2015.
Bauer/Heckmann/Ruge/Schallbruch/Schulz, Verwaltungsverfahensgesetz und E-Government (Hrsg.), 2. Aufl. Kommentar, Kommunal- und Schul- Verlag GmbH&Co. KG-Wiesbaden, 2014.

Bundesgesetzblatt(BGBl) Jahrgang 2015 Teil I Nr. 31, ausgegeben am 24.07.2015, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07. 2015.

BundesgesetzblattJahrgang 2016 Teil I Nr. 37, ausgegeben zu Bonnam 29. Juli 2016, Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus, Vom 26. Juli 2016.

Bundesgesetzblatt Jahrgang 2010 Teil I Nr. 28, ausgegeben zu Bonn am 4. Juni 2010, Erstes Gesetz zur Änderung des Telemediengesetzes (1.Telemedienänderungsgesetz) Vom 31. Mai 2010.

Drews/Wacke/Vogel/Martens, Gefahrenabwehr -Allgemeines Polizeirecht(Ordnungsrecht) des Bundes und der Länder, Carl Heymanns Verlag, 9. Aufl., 1986.

Ehlers und Pünder (Hrsg.), Allgemeines Verwatungsrecht, 15. Aufl., Walter de Gruyter GambH, Berlin/Boston, 2016.

Hoffmann-Riem, Das Recht des Gewährleistungsstaates, in Schuppert (Hrsg.), Der Gewährleistungsstaat - Einleitbild auf dem Prüfstand, 1.Auflage, Nomos Verlagsgesellschaft, Baden- Baden, 2005.

_____, Verwaltungsrecht in der Informationsgesellschaft - Einleitende Problemskizze, in Hoffmann-Riem/Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Nomos Verlagsgesellschaft, Baden-Baden, 1.Auflage, 2000.

Kloepfer (mitarbeit Walus/Deye/Schärdel), Handbuch des Katastrophenrecht, 1. Auflage, Nomos, 2015.

Kugelmann, Polizei- und Ordnungsrecht, 2. Aufl., Springer-Verlag Berlin Heidelberg, 2012.

Maurer, Allgemeines Verwaltungsrecht, 18. Auflage, Verlag C.H.Beck, 2011.

Rauschning, in Aussprache und Schlussworte, Wettbewerb von Rechtsordnungen, in VVDstRL, Band 69, De Gruyter, 2010.

Schuppert, in Aussprache und Schlussworte, Wettbewerb von Rechtsordnungen, in VVDstRL, Band 69, De Gruyter, 2010.

Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlag-sgesellschaft, Baden-Baden, 2011.

Skrobotz, Das elektronische Verwaltungsverfahren, Duncker & Humblot, Berlin, Band 14, 2005.

Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014. 9.

<프랑스문헌>

Jacques Larrieu Droit de I'nternet, ellipses, 2e édition, 2010.

Waline, Droit administratif, 23e édition, Dalloz, 2010.

<영미문헌>

Alejandre, IT Security Governance Legal Issues, in Human Rights and Ethics -Concepts, Methodologies, Tools, and Applications, IGI Global, 2015.

Kernschnig, Cyberthreats and Internatinal Law, eleven international publishing, 2012.

Neithercutt, Introduction to Tactical Hacking : A Guide for Law Enforcement, Police Technical, 2015.

EUROPEAN COMMISSION, A comprehensive approach on personal data protection in the European Union, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Brussels, 4.11. 2010 COM(2010) 609 final.

Seferovic, under the supervision of Zeldin, Germany: Ministry of the Interior Publishes Draft Cybersecurity Act, Senior Legal Research Analys, 2014.

Spinello, Cyberethics – Morality and Law in Cyberspace, 5th Edition, Jones & Barlett Learning, LLC, an Ascend Learning Company, 2014.

Wade/Maljević (Ed.), A War on Terror? – The European Stance on a New Threat, Changing Laws and Human Rights Implications, Springer, 2010.

유럽연합의 사이버안보 입법동향과 시사점(2)
– 프랑스를 중심으로 –

오 승 규*

목 차

Ⅰ 서 론

프랑스에서의 개인정보보호는 OECD와 EU의 지도방침에 맞추면서도 독자적인 체계 하에 이루어지고 있다. 기본체계는 일반법인 일명 '정보자유법(loi informatique et libertés)'[1]에 의해 설립된 독립적 국가기관인 국가정보자유위원회(Commission nationale de l'informatique et des libertés, 이하 "CNIL")가 운영하는 구도이다. 그리고 중요한 법리는 최고행정법원인 Conseil d'Etat의 판례를 중심으로 형성되면서 사생활 보호의 가치와 자유로운 정보의 유통이라는 현실요청 사이에서 적응해 나가고 있다[2]. 컴퓨터를 이

* 중원대학교 법무법학과 교수

1) 정확한 명칭은 「정보처리, 문서 및 자유에 관한 1978년 1월 6일자 법률(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)」이다.

용한 정보통신의 발달은 인터넷으로 구축된 망을 이용한 하나의 연결고리를 구축하면서 비약적인 정보이용의 증가로 인해 편리성과 위험성을 동시에 가져다주었는데, 이와 관련하여 새로이 등장한 개념 중 하나가 사이버안보의 문제이다.

사이버안보(cybersécurité)는 통신망(réseau)에 직·간접적으로 연결되어 있는 '사람(personnes)'과 국가 또는 조직체의 '물질적·비물질적 정보자산(actifs informatiques matériels et immatériels)'을 보호하는데 사용될 수 있는 안보 관련 법(lois), 정책(politiques), 도구(outils), 조치(dispositifs), 개념(concepts), 구조(mécanismes)와 리스크 관리방식(méthodes de gestion des risques), 운영(actions), 교육(formations), 모범관행(bonnes pratiques)과 기술(technologies) 전체를 가리키는 신조어(néologisme)이다[3]. 사이버안보는 국가의 안보와 관련되는 것으로서 단순한 정보시스템보안(sécurité des systèmes d'information)을 뛰어넘는 경제적(économique), 전략적(stratégique), 정치적(politique)인 문제이면서 또한 통신망으로 연결된 경영정보, 산업정보 기타 관련된 정보의 처리(informatique)에 관한 문제이기도 하다. 정보의 경제적, 사회적, 교육적, 법적, 기술적, 외교적, 군사적 측면을 고려하기 위해서 사이버안보는 전체적으로 이해되어야 한다[4]. 당연히 이 분야에서는 기술적 수월성(excellence technique), 적응성(adaptabilité), 협력(coopération)이 중요하다. 국가적 차원에서 사이버안보가 이뤄지기 위해서는 정책적 일관성(continuité politique)과 장기적 안목(vision à long terme)이 필요하다. 그리고 개별 국가의 정책도 중요하지만 세계가 하나의 정보사회를 이루고 있다는 관점에서 일정한 합의(consensus)를 이루어내고 추진하는 것이 중요하다.

2) 전훈, "프랑스에서의 개인정보 보호 – CNIL의 활동과 판례에 대한 조사분석", 「한국프랑스학논집」 제48집(2004), 467면.
3) ITU, Recommendation X.1205 : Overview of cybersecurity (04/08/2008).
4) Les évolutions de la cybersécurité : contraintes, facteurs, variables. Étude prospective et stratégique de la DGRIS de juin 2015.

Ⅱ 프랑스의 사이버안보정책의 태동

프랑스에서 사이버안보가 국가적 이슈로 자리 잡고 그에 관한 정책이 채택된 것은 2008년 이후이다. 2008년과 2013년 백서(Livre Blanc)에서 사이버안보가 국가적 우선과제(priorité)로 제시되었고 대통령의 승인을 얻었다. 특히 사이버공격(cyberattaque)에 대한 예방(prévention)과 대처(réaction)가 국가안보(sécurité nationale)의 중요과제로 채택되었다.

사이버안보라는 국가적 중요 과제를 추진하기 위하여 2009년에 국가정보보안체제청(Agence nationale de la sécurité des systèmes d'information, ANSSI)이 창설되었다. 이 기구는 총리 소속으로 설치된 유관부처 간 협력조직이다. 2011년에는 행정관청으로 그 기능이 격상되었다. 이러한 일련의 흐름을 타고 2011년 2월에는 「정보시스템의 안전과 방어 국가전략(Stratégie nationale de défense et de sécurité des systèmes d'information)」이 발간되었고 2013년 백서에서는 사이버위협(cybermenace)이라는 개념까지 확립되었다.

국방부(Ministère de la défense)에서는 사이버위기 시에 사이버안보 분야에 관한 조정을 맡는 사이버방어담당총관(Officier général chargé de la cyberdéfense)직을 2011년에 신설하였다. 2013년 12월에 의결된 2014-2019 군사계획법률 제15조는 총리가 통신망의 안정화, 탐지 시스템의 기능, 받을 수 있는 공격에 대한 정보제공, 감독 준수 등에 관해 중요 정보연산자(opérateur d'importance vitale, OIV)에게 부과할 수 있는 의무를 상세히 규정하고 있다. 이 법에서의 의무는 국가안보가 광범위하고 지속적으로 다루어야 할 과업이란 점에 착안한 것이다. 또한 이 법 제22조는 컴퓨터 공격을 탐지할 수 있는 장치를 가동하고 그 운영을 국가정보보안체제청(Agence nationale de la sécurité des systèmes d'information, ANSSI)과 총리에 의해 지정된 여타 국가기관들이 맡을 것을 규정하였다.

경찰을 산하에 두고 있는 내무부(Ministère de l'Intérieur)는 사이버범

죄(cybercriminalité) 대책을 맡고 있다고 할 수 있는데, 2014년에 사이버 위협에 대한 대응을 담당하는 경찰국장직이 신설되었다. 외무부(Ministère des affaires étrangeres)도 사이버안보에 있어서의 프랑스의 국제적 지위의 강화를 위해 노력한다. 2011년 「정보시스템의 안전과 방어 국가전략(Stratégie nationale de défense et de sécurité des systèmes d'information)」의 주요 시책 중 하나가 사이버안보에서의 국제적 협력이었다. 사이버안보정책의 수립과 상호관계설정에서 프랑스가 중요 위치를 차지하기 위해 노력중이고 특히 유엔과 유럽연합에서 활동하는 것이 중요하다.

Ⅲ 프랑스의 사이버안보정책의 발전

2013년 12월 18일자 법률 제2013-1168호에서는 총리가 정보시스템의 안보와 방어에 관한 정책을 수립하고 정부조치들을 조정하도록 규정하고 있다. 앞서 2009년에 설치된 ANSSI는 총리 소속의 국방안보실장(Secrétaire général de la défense et de la sécurité nationale)이 관장한다.

2014년 2월 21일에는 Jean-Marc Ayrault 총리가 "사이버안보는 모든 시민과 모든 프랑스인에 관한 중대한 이익이자 국익의 문제이다. 이것이 바로 정부가 이에 전적으로 관여하는 이유이다."라고 선언[5]하였다. 2015년 7월 6일에는 Axelle Lemaire 디지털 담당 국무장관(Secrétaire d'État au numérique)이 "정부는 곧 사이버안보에 대한 총괄적 국가전략을 제시할 것"이라고 발표하였다. 예정대로 2015년 10월 16일에 Manuel Valls 총리는 유럽차원의 디지털 전략의 자율성을 추구하는 로드맵작성을 제안하고 프랑스가 유엔과 유럽안보협력기구의 사이버안보 다자협상(négociations multilatérales)에 적극 참여할 것을 다짐하면서 이 분야의 교육과 국제협력을 강조하는 「디지털안보를 위한 국가전략(Stratégie nationale pour la

5) Discours du Premier ministre tenu à l'ANSSI.

sécurité du numérique)」을 천명하였다[6]. 이 전략은 전 부처의 공동작업으로 입안되었으며, 여기에는 디지털 분야에서의 혁신과 경제적 발전 그리고 국민의 신뢰를 얻기 위한 인적·기술적 원동력(leviers)을 정의하면서 우리의 중요시설(infrastructures critiques)에 대한 안보와 방어를 강화하고 디지털전환(transition numérique)을 가져오기 위한 달성 목표와 방향을 정하고 있다[7]. 제시한 5개의 목표는 ① 국가주권의 보장, ② 사이버침해행위에 대한 강력한 응징, ③ 대중에의 정보제공, ④ 프랑스 기업을 위해 경쟁의 장점을 살린 디지털보안 구축, ⑤ 국제무대에서의 프랑스의 발언권 강화이다[8]. 이 전략에 따르면 프랑스정부는 2016년 1/4분기에 사이버침해행위(actes de cybermalveillance)의 피해자에 대한 지원[9]에 나서기로 하였다.

사이버안보는 1978년부터 시행중인 대테러시스템 Plan Vigipirate의 12개 분야 중 하나이기도 하다. 위에서 언급한 ANSSI, OIV와 그 수급업체들 및 여타 행정기관들이 직접 관련된다. 지방자치단체와 OIV 외의 정보연산자들은 Plan Vigipirate에 따른 권고를 받는 대상이다. 모두에게 적용되는 공동의 보안조치들의 상시 목표는 당연히 Plan Vigipirate의 성공적인 시행이다[10].

프랑스의 사이버안보대책을 홍보하고 이용자보호의 수준을 높이면서 이용자를 교육하고 제품과 서비스의 품질과 기능을 인증하기 위한 "France Cybersecurity"라벨이 도입되었다[11].

프랑스의 사이버안보에서는 2개의 논점이 있다. 중요 인프라(infrastructures vitales)를 어떻게 보호할 것인가 하는 문제와 공사 분야의 주체들을 어떻게

6) http://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/
7) http://www.gouvernement.fr/egalite-des-droits-la-confiance-socle-de-la-societe-numerique-2402
8) http://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/
9) 예를 들어 디지털 플랫폼(plateforme numérique)을 통해 피해자들의 청원이나 소송을 지원하거나 상황에 맞추어 기술적 지원을 제공하는 일 등.
10) http://www.sgdsn.gouv.fr/site_rubrique98.html.
11) http://www.francecybersecurity.fr/.

협력하게 할 것인가의 문제이다. 그리고 개인정보보호와의 관련성도 문제이다.

Ⅳ 정보통신 기반과 공공정보에 대한 보호

정보통신 기반을 보호하는 법률로는 형법전(Code pénal)이 대표적이고, 세부적으로 전자통신 부문에 대한 규제법률로는 「우편・전자통신법전(Code des postes et des communications électroniques)」가 있고, 암호화 부문의 규제는 「디지털경제에서의 신뢰를 위한 법률(Loi pour la confiance dans l'économie nimérique n° 2004-575)」와 형법전을 통해 이루어진다.

사이버 공격자들은 시민, 기업 및 행정기관에 의해 사용되는 정보통신시스템(systèmemes d'information et de communication, SIC)의 기능과 국가안보에 대한 주요기반시설의 물리적인 완전성을 위태롭게 할 목적을 가지고 행동하고 최근 그 정밀도가 높아지고 있다.

프랑스는 앞서 말한 정보체제보안청 설립에 이어 2011년 2월 정보시스템에 대한 방어 및 안전에 관한 국가전략을 수립하였으며, 2013년 백서는 주요기반시설에 대한 위협을 확인하고 사이버위협에 대한 경계를 강화하였으며, 프랑스 사이버안보전략은 크게 국가주권의 보장, 악의적인 사이버행위에 대한 강력한 대응, 일반대중에 대한 정보전달, 프랑스 기업들의 경쟁이익을 위한 디지털안보, 국제사회에서 프랑스의 목소리 강화를 목표로 하였다. 프랑스의 사이버안보전략은 2013년 유럽위원회(Commission européenne)의 유럽연합사이버안보전략[12] (Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace)의 5대 사항(유럽연합 기구의 유지, 사이버범죄에 대한 대책, 유럽차원의 사이버방위에 대한 문제, 산업적

12) European Commission, JOINT COMMUNICATION TO THE EUROPEAN PALIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Brussels, 7.2.2013.

문제, 사이버공간에서의 유럽연합의 국제정책)을 적극적으로 이행하기 위해 수립한 것으로 보인다.

1. 공공정보에 대한 보호

프랑스 사이버안보 입법동향과 관련하여, 국내안보법전(Code de la sécurité intérieure)을 보충한 「2015년 7월 24일자 정보에 관한 법률(Loi n° 2015-912 du 24 juillet 2015 relative au renseignement)이 중요하다.

안보법전 L.111-1조에서는 "안전은 기본권이며, 개인과 집단의 자유를 수행하기 위한 조건들 중의 하나이다."라고 명시하고 있는데, 이는 안전과 자유의 보호의 관계를 잘 설명해주고 있다고 할 수 있다.

「정보에 관한 법률」 제2조에 의하여 국내안보법전에 추가된 L.811-3조에서는

① 국가의 독립, 영토의 보전 및 국방, ② 국외정책의 주요 이익 및 모든 형태의 외국의 간섭에 대한 예방, ③ 프랑스의 주요 경제적, 산업적, 과학적 이익, ④ 테러리즘 예방 ⑤ 공화정 체제에 대한 훼손, 국가안보를 침해하는 성격의 집단요소 또는 해산된 단체의 재조직 또는 이를 유지하려는 경향의 활동 예방, ⑥ 범죄행위 예방, ⑦ 대량살상무기 확산 예방을 위해서 접속데이터에 대한 행정청의 접근, 전자통신에 의하여 발송된 서신을 차단하거나 열람, 다른 합법적인 방법으로 수집할 수 없는 정보에 대하여 일정한 장소 및 자동차 내부에서 기술적인 장치를 사용하여 청취하거나 전자적 이미지와 데이터에 대하여 캡쳐하는 행위, 국가방위 및 중요한 이익을 증진할 목적으로 국외로 발송하거나 수신되는 통신감시에 대한 정보기술을 특수한 업무에 사용할 수 있도록 규정하고 있다.

프랑스 영토 내에서 위에서 말한 목적을 위하여 정보를 수집하기 위해서는 총리의 사전허가를 받아야 하며 총리는 국가정보기술감독위원회(Commission nationale de contrôle des techniques de renseignement : CNCTR)의 의견을 들은 후 결정하여야 한다. 정보수집기술 실행 허가는 총리 또는 총리가

위임한 사람의 재결서에 의하여 교부되며, 허가 기간은 최장 4개월이고 최초 허가와 동일한 형식과 기간 내에서 갱신할 수 있다. 허가서에는 ① 실행하는 정보기술, ② 추구하는 목적, ③ 유효기간, ④ 관계되는 사람, 장소 또는 자동차가 명시되어야 한다.

국내안보법전 L.811-3조에 열거된 목적과 관련된 정보를 적법하게 허가된 다른 방법으로 수집할 수 없는 경우① 사적 장소에서의 사적 발언 또는 비밀발언 또는 영상 캡쳐, 고정, 전송 및 저장과 ② 자동시스템을 통하여 경유하는 자동시스템 내의 정보 또는 내용에 대한 정보처리 데이터의 캡쳐, 전송 및 저장을 허용하는 기술장치의 사용을 허가할 수 있다. 이 허가는 최장 2개월의 기간으로 할 수 있고 역시 동일한 내용으로 갱신 가능하다. 허가받은 사항에 대한 실행은 꽁세이데따(Conseil d'État, CE)의 데크레(décret)에서 명시한 권한을 가진 요원(agent)에 의해서만 행해질 수 있다.

정보에 관한 법률이 사이버안보를 포함한 국가안보와 관련된 목적으로 정보를 수집하고 차단하고자 하는 경우에 그 목적과 사용하고자 하는 기술장치, 기한 등을 명시하여 외부의 독립된 기관인 국가정보기술감독위원회(CNCTR)의 의견을 거쳐, 총리의 사전허가를 얻도록 규정하고 있는 점과 불법적인 감시를 받거나 받았다는 것을 확인하고자 하는 모든 사람은 CNCTR에 이의신청을 거쳐 CE에 제소할 수 있다고 규정함으로써 이중통제에 따르도록 하고 있다.

정보에 대한 공공정책은 한편으로는 국가안보전략, 방위, 국가의 중요한 이익의 향상에 기여하여야 하며, 다른 한편으로는 사생활의 존중 특히 서신의 비밀, 주거의 불가침을 보장하여야 한다. 공공기관은 법률에서 규정하고 있는 공익에 대한 필요성이 인정되는 경우에만 법률에서 정한 제한 내에서 비례의 원칙을 준수하면서 이를 침해할 수 있다. 특히 개인정보보호가 중요한 의미를 가진다.

V 프랑스의 개인정보보호제도

1. 개설

정보처리기술의 발달에 따라 1960년대 이후 활발해진 행정 전산화의 추세는 프랑스 특유의 독자적인 행정입법권에 힘입어 정보자동화 체계로의 비약적 변화 및 이에 따른 행정의 효율화가 신속하게 이루어졌다[13]. 반면 이러한 흐름은 역으로 개인정보의 침해 우려를 점점 증폭시키게 되었다. 특히 1970년대 들어 국가의 주요 행정전산망을 통합하려는 움직임이 개인정보보호 논의를 촉발시켰다. 1971년에 국가통계경제연구원(Institut national de la statistique et des études économiques Insee)은 개인별 신원을 마그네틱 처리한 국가 보유 인명카드를 지방행정기관까지 연결하여 집중화하여 연계 검색하는 것을 내용으로 한 '행정문서와 개인별 목록 자동화시스템(Système automatisé pour les Fichiers Administratifs et le Répertoire des Individus : SAFARI) 구축계획, 일명 '사파리 프로젝트(projet SAFARI)'를 추진하면서 개인정보보호제도의 정비 논의가 본격화하였다. 정부는 이 시스템이 구축되면 개인별 사회보장번호와 연금보험번호 및 신원번호를 연결하여 집중 관리하고자 하였다. 즉 각 개인에 대해 일련의 번호를 부여하고 동 번호를 통해 식별하도록 해서 각 행정기관들이 이를 공유하려는 생각이었다[14]. 이 계획에 대해서 1974년 3월 21일자 르몽드(Le Monde)지는 "SAFARI[15]냐 프랑스인을 사냥하는 것이냐"라며 비판하였다. 정부의 입장에서는 개인들의 정보를 통합 관리할 수 있는 효율성을 얻게 된 반면에, 국민들의 입장에서는 사생활의 비밀과 자유가 침해될 가능성이 크다는 우려가 커져서 강력한 비판여론이 조성됨에 따라 Jacques Chirac 총리의 주도로 정보자유위원회

13) 김봉수, "유럽의 개인정보보호법제와 감독체계", 「법과 정책」, 제21집 제3호(2015), 82면.
14) 이에 대한 설명은 전훈, 위의 글, 468면 참조.
15) 아프리카에서 차를 타고 다니며 야생동물을 관광하거나 사냥하는 여행.

(Commission nationale de l'informatique et des libertés)를 구성하여 정책 대안을 논의[16]한 끝에 마침내 1978년 1월 6일자로 '정보처리, 문서 및 자유에 관한 법률'(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. 이하 "정보자유법)이 제정[17]되었다. 그리고 이 법에 따라 공공부문과 민간부문을 통합하여 개인정보처리시스템에 관하여 자문・감독・조사 등의 임무를 수행하는 독립기관인 CNIL이 설치되었다. 이후 개인정보보호의 수준을 강화하고 정보통신기술의 발달에 대응하기 위해 이 법은 개정을 거듭하여왔다. 특히 유럽연합의 규범이 요구하는 수준에 맞추기 위한 개정작업도 있었는데, 특히 1995년의 「EU 개인정보보호지침」의 국내법화를 위한 2004년 8월의 개정으로 법 내용이 대폭 수정되었다[18]. 이 때 개정된 법에서는 개인정보의 개념에 대한 표현을 종전의 기명정보(information nominative)에서 개인적특성정보(donnée à caractère personnel)로 변경하였다. 그 외에도 보건 분야의 연구 목적으로 개인정보를 처리할 경우에 대한 규제를 담은 1994년의 개정, 치료와 예방활동의 평가나 분석을 위한 개인의 건강정보의 처리와 다른 법률 및 행정명령과의 관계 등을 규정한 2002년 3월의 개정을 중요한 예로 들 수 있다.

이 법의 주요원칙을 살펴보면, 먼저 제1조에서는 정보처리(informatique)

16) 위원회는 프랑스 최고행정법원(Conseil d'Etat) 부위원장을 위원장으로 하고 사법관계자, 학계전문가 등 12명의 위원으로 구성하여 관련 행정기관과 기업 및 노동조합 등의 의견을 수렴하는 등 기초조사를 실시한 보고서를 1975년 6월 27일에 대통령에게 제출하였다. 이 보고서는 개인정보 보호를 위한 독립기관을 설치하여 정보시스템의 감독과 공공기관에 의한 시스템 설치에 대한 사전허가제를 실시하고, 정보의 주체인 개인에게는 본인의 정보에 대해 접근할 수 있는 권리를 인정할 것 등을 제안하였다."(이한주, "개인정보보호위원회 제도의 문제점과 개선방안 - 프랑스 CNIL과의 비교를 통하여", 경북대학교 「법학논고」, 제41집(2013), 479면.)

17) 또한 위원회는 이 보고서에서 개인정보보호법의 제정 및 그 적용을 감독할 독립기구의 설립을 주장하였다. 이에 기초한 정부의 법률안이 1976년 8월에 국민의회에 제출되어 1977년 10월에 국민의회를 통과했으며, 1977년 11월에 상원에서 마찬가지로 부분수정 후 통과되었고 1978년 1월에 최종 의결되었다.

18) 김봉수, "유럽의 개인정보보호법제와 감독체계", 「법과 정책」, 제21집 제3호(2015), 83면.

는 개인을 위해 이루어져야 함을 밝히고 있다. 그러면서 정보처리의 발달은 국제협력(coopération internationale)의 차원에서 수행되어야 하고, 신원(identité humaine), 인권(droits de l'homme), 사생활(vie privée), 기본권(libertés individuelles ou publiques)을 침해하지 않아야 함을 규정하고 있다.

제2조에서는 "식별번호(numéro d'identification)나 여러 고유 요소에 의해 식별되거나 식별될 수 있는 자연인(personne physique)에 관한 직간접적인 모든 정보"를 인적특성정보(donnée à caractère personnel) 즉 개인정보의 개념으로 규정하고 있다. 그리고 개인정보의 처리는 "어떤 절차에 의하든 이러한 정보에 관한 모든 작용 또는 작용들의 총체"를 포괄하는 것으로 정의하고 있다. 계속하여 정보처리의 형태로 "수집(collecte), 저장(enregistrement), 조직(organisation), 보존(conservation), 각색(adaptation), 개조(modification), 발췌(extraction), 조회(consultation), 사용(utilisation), 전달에 의한 전파(communication par transmission), 배포(diffusion)나 다른 형태의 처분(mise à disposition), 상호접근(rapprochement) 또는 교차(interconnexion), 잠금(verrouillage), 삭제(effacement)나 파기(destruction)"를 예시하고 있다. 이런 식으로 용어를 축적하는 것은 '처리'라는 낱말에 넓은 의미를 부여하려는 의지를 보여주는 것[19]이라고 볼 수 있다. 판례를 통해서도 이 개념은 확장되고 있다. 비록 파일에 저장은 하지 않더라도 광고를 발송하기 위해 이메일주소를 확인하는 것[20], 전화안내를 목적으로 다른 기업의 가입자들의 개인적 특성이 담긴 자

19) J. Frayssinet, La protection des données personnelles, in A. Lucas, J. Devèze et J. Frayssinet, Droit de l'informatique et de l'internet : PUF, 2001, n° 122.

20) Cass. crim., 14 mars 2006, n° 05-83.423, F - P + F c/ Min. publ. : JurisData n° 2006-032892 ; Bull. crim. 2006, n° 69 ; Rev. Lamy dr. immat. 2006, n° 16, 471, note J. Le Clainche ; Rev. Lamy dr. immat. 2006, n° 17, 498, note P. Belloir ; D. 2006, p. 1066 ; JCP G 2006, IV, n° 1819 ; Comm. com. électr. 2006, comm. 131, A. Lepage.

료를 전달하는 것[21], 보건당국에 전달할 목적으로 구국민건강법전 제11조에 규정된 질병에 관련된 개인들의 정보를 수집하는 행위[22] 역시 여기에 해당한다. 여권발급을 위해 지문을 채취하고 보존하는 것[23]과 외국인등록의 차원에서 외국인의 생체정보를 수집·보존하는 것도 개인정보의 처리의 한 예이다[24]. 또 개인정보파일(fichier de données à caractère personnel)은 "정해진 기준에 따라 접근가능한(accessible) 개인정보들의 구조화되고(structuré) 안정된(stable) 총체"로 정의하고 있다. 동조에서는 이 법의 적용범위에 대해서도 규정하고 있다. 정보처리법은 자동적·수동적으로 이루어지는 정보처리에 적용되고, 공공부문 뿐만 아니라 민간부문에도 적용되며, 정보의 주체는 자연인에 한정되고, 따라서 법인의 정보는 보호대상에서 제외된다(제2조).

다음으로 중요한 원칙적 규정인 제6조에 따르면 정보처리가 적법성을 갖기 위해서는 그 정보가 충실하고 공정·적법하게 수집 및 처리되어야 하고, 정보수집의 목적이 특정됨은 물론 명백성과 정당성을 갖추어야 한다. 그리고 이어서 정보처리를 함에 있어서는 정보주체의 동의(consentement)를 받아

21) CJUE, 5 mai 2011, aff. C-543/09, Deutsche Telekom, point 53 ; Europe 2011, comm. 268, L. Idot.

22) CE, ass., 30 juin 2000, n° 210412, Ligue des droits de l'homme et du citoyen ; JurisData n° 2000-060767 ; AJDA 2000, n° 10, concl. P. Fombeur ; JCP G 2000, IV, n° 46, 2742 ; LPA 13 févr. 2001, n° 31, p. 10, note R. Diane ; Gaz. Pal. 10 mars 2001, n° 69, p. 21, obs. P. Graveleau ; Gaz. Pal. 17 juill. 2001, n° 198, p. 42, note A.-F. Godet.

23) CE, ass., 26 oct. 2011, n° 317827, Assoc. pour la promotion de l'image et a. ; JurisData n° 2011-023099 ; AJDA 2012, p. 35, chron. M. Guyomar et X. Domino. - V. Tchen, La base de données du passeport biométrique ; Dr. adm. 2012, comm. 1. - F. Chaltiel, Le passeport devant le Conseil d'État ; LPA 14 déc. 2011, n° 248, p. 10 ; AJDA 2011, p. 2036, note R. Grand. - CJUE, 17 oct. 2013, aff. C-291/12, Schwarz c/ Stadt Bochum, point 29 ; Europe 2013, comm. 512, obs. F. Gazin.

24) CJCE, 16 déc. 2008, aff. C-524/06, Heinz Huber, point 43 ; Rec. CJCE 2008, I, p. 9705 ; Europe 2009, comm. 53, obs. F. Kauff-Gazin ; JCP A 2009, 2189, obs. M. Gautier.

야 한다는 점을 명시하고 있다(제7조).

정보주체의 권리 역시 중요한 원칙 중 하나이다. 정보주체는 직접 정보처리자에게 접근하여 정보를 취득, 열람 및 복사할 수 있고 제3자에게 정보열람을 요청하고 그 결정으로 정보에 접근하는 것도 가능하다(제39조). 모든 자연인은 자신과 관련된 개인정보가 정보처리의 대상이 되는 것에 대해 정당한 이유로써 반대할 권리를 가진다(제38조). 정보주체가 자신임을 증명하는 모든 자연인은 정보처리자로 하여금 부정한·불완전한·모호한·소멸된 개인정보 또는 그것의 수집·활용·전달 및 보관이 금지된 개인정보가 정정, 보완되고, 명백히 되도록, 그리고 차단 또는 삭제되도록 요청할 수 있으며(제40조), 자신의 정보가 처리의 대상인지 여부에 대한 질문권도 가진다.

정보처리자는 일정한 의무를 부담한다. 법이 정하는 바에 따라 해당 정보처리를 함에 있어서는 CNIL의 허가를 받아야 한다(제25조, 제26조, 제27조). 정보처리가 허가대상이 아닌 경우에는 제36조 2항 상의 '정보처리의 목적이 오로지 고문서의 장기보관인 경우'를 제외하고, 개인정보의 자동처리를 동 위원회에 신고해야 한다(제22조). 정보주체에게 법률이 정하는 소정의 사항을 고지해야 한다(제32조).

2. CNIL의 조직과 기능

(1) CNIL의 의의

1978년 정보자유법에 의해 프랑스의 개인정보보호정책을 담당하기 위해 독립적 기구인 국가정보자유위원회(CNIL)가 설립되었다. 동법 제11조 1항은 본 위원회가 독립행정관청(autorité administrative indépendante)임을 명시하고 있으며, 제21조에 의하면 본 위원회의 권한행사는 어떠한 기관의 지휘(instruction)도 받지 않는다. 즉 CNIL은 입법·사법·행정의 통제에서 상당히 자유롭게 활동한다. CNIL은 개인정보에 관해서 공공 부문과 민간 부문을 구별하지 않고 통합하여 관리하기 때문에 거의 모든 분야의 개인

정보를 포괄하여 관장한다. CNIL의 활동을 통해 정보처리법이 개인정보 보호의 주요 법적 근거로 자리 잡게 되었고, CNIL의 업무범위가 확대되고 전문화되면서 위원회의 활동은 대내외적으로 긍정적인 평가를 받고 있다[25]. 한마디로 CNIL은 권리의 보호와 처리의 통제를 담당하는 개인정보보호의 중추기관[26]이다.

(2) CNIL의 조직

1) CNIL의 구성

CNIL은 전부 18인의 위원으로 구성되는데, ① 국민의회와 상원에서 각각 2인씩 지명되는 4인의 국회의원, ② 경제사회환경위원회(Conseil économique, social et environnemental) 총회에서 선출된 2인의 위원, ③ 최소 프랑스 최고행정법원 판사급에 해당하는 최고행정법원(Conseil d'Etat)의 구성원 또는 구성원이었으면서 전원회의체(general assembly)에서 선출된 2인, ④ 최소 프랑스최고법원판사급에 해당하는 최고법원(cour de Cassation)의 구성원 또는 구성원이었으면서 최고법원의 전원회의체에 의해 선출된 2인, ⑤ 최소 회계법원판사급에 해당하는 회계법원(Cour des Comptes)의 구성원 또는 구성원이었으면서 회계법원의 전원합의체에 의해 선출된 2인, ⑥ 정보기술, 개인의 자유와 관련된 문제들에 대한 학식을 갖춘 인사로 정부의 명령(décret)에 의해 임명되는 3인, ⑦ 정보기술, 개인의 자유와 관련된 문제들에 대한 학식을 갖춘 인사로 국민의회의장과 상원의장으로부터 임명된 2인, ⑧ 행정문서접근위원회(Commission d'accès aux documents administratifs)의 위원장 또는 그 대리인으로 구성된다. 위원회는 위원 중에 1인의 위원장과 2인의 부위원장을 선출하고 부위원장 중의 1인이 대행위원장을 하게 된다. 위원장의 임기는 5년으로 하고, 위원장은 회의에서 가부동수인 경우 결정권을 갖는다(제

25) 이한주, "개인정보보호위원회 제도의 문제점과 개선방안 - 프랑스 CNIL과의 비교를 통하여", 경북대학교 「법학논고」, 제41집(2013), 481면.
26) 전훈, 앞의 글, 468조.

13조 Ⅰ).

위원들의 임기는 5년으로 하고, 1차에 한해 연임할 수 있다. 그러나 다른 직에서 임기가 정해진 위원의 경우 그 임기까지만 재임할 수 있다(제13조 Ⅱ).

그리고 위원회의 업무수행을 위해 사무처를 둔다. 사무처는 사무총장(secrétaire général) 아래에 5개의 국(Direction)[27]으로 이루어져 있다. 2004년 정보처리법의 개정으로 CNIL에 할당된 새로운 의무와 임무의 증가는 구성원들의 증가를 가져왔다[28]. 2016년 11월 현재 총 192명의 직원이 근무하고 있다[29]. 이들 중 48%가 2011년 이후에 임용되었으며, 36%는 법률전문직이다. 여성 비중이 64%로 남성보다 높다. 예산은 1600만 유로이다. 예산은 법무부 예산으로 편성되며 회계검사원(Cour des comptes)에 회계보고서를 제출한다(제12조).

2) CNIL의 성격

CNIL은 재판기관이 아닌 행정기관이고 독자적인 법인격을 갖고 있지는 않다. 비록 법무부 소속으로 설치되어 있긴 하나 어떠한 행정감독도 받지 않으며, 나아가 그 구성원들은 자신들의 임무수행 및 권한행사와 관련하여 어떠한 기관으로부터도 명령을 받지 않는다(제21조 1항). 즉 이 위원회는 독립행정관청(autorité administrative indépendante)이다. 독립행정관청으로 인정되는 기준 또는 특징은 ① 독자적인 행정조치들을 취할 권한을 부여받고 있고, ② 국가에 소속된 공공기관으로 독자적인 법인격을 갖는 것이 아니라 국가조직의 일부에 해당하며, ③ 국가조직에 해당되더라도 누구의 지휘·감독을 받지 아니한다는 것 등이다.

반면 행정각부장관, 공공기관, 공기업과 사기업의 경영진, 여러 단체의 책

27) 지원국(Direction de la conformité), 권리보호제재국(Direction de la protection des droit et des sanctions), 기술혁신관리국(Direction des technologies et de l'innovation), 홍보조사국(Direction de la relation avec les public et la recherche), 관리재무국(Direction administrative et financière)으로 구성된다.
28) 이한주, 앞의 글, 483면.
29) https://www.cnil.fr/fr/le-fonctionnement. 2016년 11월 23일 방문.

임자, 정보처리와 정보축적시스템의 보유자와 이용자들은 위원회나 위원회 구성원들의 활동을 거부할 수 없고 위원회의 업무를 용이하게 하는데 필요한 조치를 취해야 한다. 또한 비밀준수 의무를 이행해야할 경우를 제외하고, 위원회가 수행하는 검사과정에서 정보를 얻는 자는 임무 수행을 위해 위원회가 요청한 정보를 제공해야 할 의무가 있다(제21조 제2항 및 제3항). CNIL은 매년 보고서를 대통령과 의회에 제출한다(제23조).

(3) CNIL의 권한과 기능

1) 결정권

임무를 수행하기 위하여 CNIL은 이 법이 규정한 경우에 권고를 하고, 개별결정(décisions individuelles)이나 규제결정(décisions réglementaires)을 할 수 있다(제11조 제2항). CNIL은 내부규칙을 제정할 수 있다. 또한 법률 제11조 제1항 제3호 (c)에 규정된 적격인증(labellisation)을 이행하기 위한 조건들뿐만 아니라, 특히 심의, 파일조사 및 위원회 제출과 관련된 규칙을 정할 수 있다(제13조 Ⅱ 제4항). 위원 또는 직원이 현장에서 직접 당해 개인정보처리가 법규정을 준수하는지 여부를 조사하고 필요한 정보와 자료의 제출을 요구할 수 있다. 아울러 개인정보처리시스템의 보안과 안전을 위한 지침을 내릴 수 있다. 특히 형사범죄에 관해서는 경고와 함께 관계기관에 고발조치를 취할 수 있다. 이런 모든 활동은 연차보고서에 기재되어 CNIL의 활동과 그 결과를 모든 국민들이 확인할 수 있다.

CNIL은 기명정보와 관련하여 정보주체와 정보처리자에게 그의 권리와 의무를 고지할 임무이자 권한을 갖는다(제11조 제1항 제1호). 고지의 주요 내용은 모든 컴퓨터에 의한 정보처리 기록, 사용목적, 열람권을 행사할 수 있는 장소, 개인정보를 제공받는 제3자 범위 등이 포함되어 있다. CNIL은 개인정보가 처리되는 모든 과정을 통제하는데, 개인정보처리기관은 정보처리와 관련해서 CNIL의 결정을 얻지 못하면 의회의 승인이 없는 한 그 개인정보파일을 사용하지 못한다.

2) 감독권

개인정보의 처리가 정보처리법에서 규정하는 내용에 부합하는지 여부를 감독할 권한을 가진(제11조 1항 2호) CNIL은 개인정보와 관련한 공공부문과 민간부문 모두를 관리·감독한다. 따라서 모든 분야에서의 개인정보를 포괄적으로 관장하게 되고, 다만 국방·안보 분야에서만큼은 동 법의 규정이 부분적으로 적용된다. 감독권의 내용을 자세히 살펴보면, 첫째, 제25조(정치, 철학, 의학, 성생활 정보 등)에서 언급된 정보처리에 대한 권한을 부여하고, 제26조(국가안전과 범죄행위 처리)와 제27조(공적 처리)에서 언급된 정보처리에 대한 의견을 표명할 권한을 갖는다. 둘째, 제24조(단순화된 규정) Section 1.에서 언급한 기준을 제정·공포하고, 필요한 경우 시스템의 안정성을 보장할 규정들을 시행할 권한을 갖는다. 셋째, 개인정보처리를 수행하는 것과 관련된 주장, 청원, 항의 등을 접수하고, 그것들에 대한 답변을 고지할 권한을 갖는다. 넷째, 공권력과 사법부로부터의 요구에 따라 의견을 제시하고, 개인정보를 자동화 처리하려는 개인이나 단체에게 권고하는 권한을 갖는다. 다섯째, 위원회가 알고 있는 형사소송법 제40조에 따라 검사에게 통지하고, 법 제52조에 규정된 조건에 따라 범죄행위에 대해 논평할 수 있는 권한을 갖는다. 여섯째, 특별한 규정으로 구성원들이 법 제44조에서 제공한 조건하에서 모든 처리와 관련된 검사를 하고, 필요한 경우 모든 서류의 복사본이나 그 임무에 유용한 도구(매체)들을 획득할 권한을 갖는다. 일곱째, 제41조(국가안전, 공적 보호 등)와 제42조(범죄와 과세와 관련된 공적 처리)에서 언급된 처리와 관련된 접근요청에 답변할 권한을 갖는다.

3) 정보의 접근권 및 서류제출 요구권

법 제19조 제5항에서 정한 바와 같이 위원회의 승인(habilitation par la Commission)을 얻은 요건을 충족하는 조건으로 CNIL 위원과 직원은 그들의 임무를 수행하기 위해서 오전 6시부터 오후 9시까지 정보에 대한 접근이 가능한데, 전문적인 목적으로 개인정보 처리를 위한 장소, 차폐된 구역, 시

설, 건물의 장비에 대해서도 사적인 목적으로 이용되는 경우를 제외하고는 그들의 임무를 수행하기 위해 접근할 수 있다. 그러나 이 경우 관할 검사장에게 사전에 통지하여야 한다(제44조 Ⅰ). CNIL의 위원과 직원은 임무수행을 위해 필요한 모든 서류를 제출하도록 요청할 수 있고, 즉석에서 또는 소환하여 정보를 수집할 수 있으며 정보프로그램과 정보에 접근할 수 있고, 통제에 유용한 서류를 적절한 처리를 통해 문장으로 옮기도록 요구할 수 있다. 그리고 각각의 기관에서 임명된 전문가들은 위원회 위원장의 요청으로 위원회 업무종사자들을 지원할 수 있다. 그리고 오직 의사만이 의료전문가에 의해 수행된 예방의학, 의학연구, 의료진단, 치료 및 관리 또는 의료서비스 관리를 목적으로 필요한 처리에 포함된 개인의료정보의 의사소통을 위한 정보를 요청할 수 있다(제44조 Ⅲ).

4) 제재권

CNIL은 법률을 위반한 행위에 대해 강력한 제재를 하거나 비록 실정법을 위반한 것은 아니더라도 대상기관의 개인정보 침해 여부에 대해 엄격한 기준으로 조사를 할 수 있다. 이는 ① 위반한 경우뿐만 아니라 위반되지 아니한 경우에 위반의 가능성 판단만으로 해당 기관에 대한 의견청취, 조사 등이 가능하도록 한다는 점에서 CNIL이 강력한 권한을 갖고 있음을 보여준다고 할 수 있고, ② 정보처리법을 근거로 하는 CNIL은 정보의 이용(공개)보다는 보호의 측면을 강조한 것으로 판단할 수 있다는 점에서 시사점이 있다. 이는 앞에서 언급한 바와 같이 정보가 공개될 경우 침해되는 법익이 얻을 수 있는 법익보다 크다고 판단했기 때문으로 이해할 수 있다[30].

CNIL이 직접 부과하는 제재적 처분은 경고(avertissement), 정보처리중지명령(injonction à cesser le traitement), 허가의 철회(retrait de l'autorisation), 특정 정보에 대한 잠금(verrouillage de certaines données),

30) 이한주, "개인정보보호위원회 제도의 문제점과 개선방안 - 프랑스 CNIL과의 비교를 통하여", 경북대학교 「법학논고」, 제41집(2013), 489면.

정보처리를 중지시키기 위해 필요한 조치를 취해줄 것을 총리 또는 법원에 청구하는 등의 비금전적 제재(법 제45조)와 15만 유로(상습적 위반의 경우는 30만 유로) 이하의 과징금(sanction pécuniaire de nature administrative) 같은 금전적 제재(법 제47조)가 있다. CNIL이 부과하는 행정 제재(sanction administrative)는 최고행정법원에만 불복 청구할 수 있다.

3. 프랑스의 개인정보보호와 통제 체계

(1) 정보주체의 권리

1) 통지를 받을 권리(droit d'information)

유럽연합의 1995년의 개인정보처리와 자유로운 유통에 있어서의 개인정보 보호에 관한 지침(Directive) 제12조와 1978년 1월6일 법률에서는 이해당사자의 임의에 따라 중첩적으로 행사할 수 있는 일정한 직간접적인 권리 실행수단의 가능성을 내용으로 하는 개인정보에 관한 통지 및 접근권을 규정하고 있다(제3조). 접근권(droit d'accès)은 통지를 받을 권리에 대한 보충적(complémentaire) 성격이다.

2) 정보처리에 대한 거부권(droit d'opposition)

모든 사람은 정당한 이유를 내세워 자신의 개인정보의 처리를 거부할 수 있다.(제38조). 특히 상업적 목적의 마케팅조사(prospection)에 자신의 정보를 사용하는 것에 대해서 거부할 수 있다. 다만 법률상 의무에 의한 정보처리면서 법률이 정한 절차에 따라 허용된 정보처리는 거부의 대상이 아니다.

3) 정정요구권(droit de rectification)

처리된 대한 개인정보가 잘못 처리되었다고 생각하는 사람은 정보처리의 책임자에게 정보를 정정(rectifier), 보완(compléter), 상황에 맞게 수정(actualiser), 차단(verrouiller)하거나 삭제(effacer)할 것을 요구할 수 있다. 이 요구는 정보를 보유하고 있는 기관에 서면으로 제출되어야 한다(제40조). 이 정정요구에 대한 거부결정은 행정소송의 대상이 되는 결정(décision

faisant grief)이다[31].

(2) 정보처리의 통제

1) 개인정보처리의 신고와 허가

개인정보의 자동화처리를 하기 위해서는 허가를 얻거나 신고해야 한다. 사생활을 침해할 우려가 있는 처리는 CNIL의 허가(autorisation)를 얻어야 한다(법 제25조). 주로 국가에 관한 정보일 경우에는 CNIL에 의견(avis)을 요청한다(법 제26조, 27조).

2) 개인정보수집의 제한

개인정보의 수집은 제한을 두어야 한다. 개인정보의 수집은 적법하고 공정한 절차에 의하며 필요한 경우 정보주체에 알리거나 동의를 받은 후에 이루어져야 한다.

개인정보의 수집은 늦어도 정보의 수집 시 까지는 결정되어야 한다. 정보는 수집 목적의 달성에 모순되지 않고 목적의 변경시마다 정해질 수 있는 것으로 제한된다. 정보의 수집은 그 수집의 목적을 넘어서 과도하게 이루어질 수 없다. 권리와 자유의 보호를 위해서는 데이터와 관련된 사람에게 처리된 정보에 대한 통제권을 허용하는 것만으로는 충분하지 않다. 사전에 정보처리의 책임자에게 예방적 수단으로서 입법자가 제정한 제 원칙들을 준수하고 정보관리에 따르는 위험을 피하도록 해야 한다. 이러한 원칙은 분명하고 안전하며 명시적인 법적 테두리를 가지며, 그 안에서 정보처리와 관련을 가지는 사람들에게 신뢰성과 함께 법을 준수하면서 그 정보처리와 개발을 할 수 있도록 하고 있다. 정보는 충실하고 합법적으로 처리되어야 하며, 경우에 따라서는 관련 인물의 동의를 얻어야 하거나 그에게 통지하거나 CNIL에 신고해야 한다.

31) CE, 30 juillet 1997, Société Consodata.

3) 개인정보의 보유와 이용

수집된 개인정보는 법률에서 달리 규정하는 경우를 제외하고 CNIL이 보유를 허가하지 않는 한 신고(déclaration)나 의견(avis)이 정한 기간을 넘어서 보유하지 못한다(법 제36조). 이는 정보처리의 책임자들에게 부여되는 의무로서 정보처리의 신뢰성과 안전성의 보장은 1978년 법률규정(제29조, 제45조)에서도 선언되어있고, OECD의 1980년 가이드라인(제8조, 제11조), 1981년 유럽위원회의108차 협약(제7조), 1995년의 지침(directive) (제16조, 제17조)에서도 확인되고 있다.

개인정보는 그 이용에 부합되는 것 이어야 하며 이용목적에 필요한 범위 안에서 정확하고 완전하며 최근의 상태를 유지해야 한다. 그리고 개인정보는 분실, 불법적인 접근, 파괴, 사용, 수정, 공개의 위험에 대비한 합리적인 안전보호 장치에 의해 보호되어야 한다.

개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확한 목적 이외의 목적을 위해 공개나 이용 그 외의 사용에 제공되어서는 안 된다. 특히 의료분야 경우의 경우 개인의 건강 상태의 정보의 이용에서 나타나는 의학과 공공보건의 향상의 이익은 이러한 정보의 신뢰성과 민감성을 고려해야 한다. 1985년 이래로 CNIL은 1978년 1월 6일 법률규정과 관련해 공공보건의 관심사항은 환자들의 사생활의 내면의 존중과 조정을 존중하는 방향으로 개정되어야 한다고 요구하고 있다[32]. 의료연구 분야에서 개인정보화처리가 적법한 경우라면 정보는 부과되는 모든 보장조치와 더불어 연구단체가 이를 담당하게 된다. 건강상태의 정보는 그 사람에 대한 가장 깊은 곳에 대해 영향을 끼치며 분명하게 어떤 목적으로도 처리되거나 이용되거나 취급되어져서는 안된다는 것을 환기하는 것이 중요하다.

32) 전훈, 앞의 글, 476면.

V 결 론

우리 삶의 모습을 한꺼번에 바꾸어 놓은 컴퓨터는 불의 발견 이후 인류 최대의 걸작이라고 할 수 있다. 더구나 이를 이용해 전세계를 하나의 망으로 연결한 인터넷으로 대표되는 정보통신망의 발달은 수레의 발견을 능가하는 폭발적인 영향력을 가져다주었다. 그 영향력에는 당연히 명암이 있기 마련이다. 그 암(暗)에 해당하는 것 중의 하나가 사이버범죄로 대표되는 일련의 사이버침해행위라고 할 것이다. 이러한 문제들에 관해 국제사회는 이미 규범정립과 상호협력을 통해 대응해 나가고 있는 중이며 프랑스도 그에 발맞추어 나아가고 있다. 초기에는 사이버범죄대책으로 시작하였으나 지금은 디지털 국가 완성이라는 큰 퍼즐을 맞추기 위한 하나의 중요한 조각으로 인식하고 국가발전의 중요 인프라로 다루고 있다. 특히 프랑스에서는 기업의 경영보안을 가장 우선적인 과제로 인식하고 이를 보호하는 것이 국가경쟁력을 높이는 수단으로 보고 적극적 지원에 나서고 있다.

프랑스도 IT 기반 서비스, SNS, Big Data 등 새로운 문제에 대처하기 위해 끊임없이 노력하고 있다. 디지털 사회에 적합한 법제를 구축하기 위해서 최근에는 '디지털 공화국을 위한 2016년 10월 7일 법률 제2016-1321호(LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique.)'를 제정하였다. 향후 과제는 올해 5월에 제정된 EU 일반정보보호규칙(GDPR)[33]과의 조화를 어떻게 이루어나가느냐 하는 것이다.

결국 사이버안보를 전통적 경찰이나 국방 영역으로 한정하지 않고 국가발전을 위한 총체적 전략 차원에서 다루면서 기업을 지원하고 정보인권을 보장하는 제도를 구축하고 시행하는 것이 바람직한 방향이라 할 것이고 이 점에서 프랑스의 사이버안보정책을 참조할 가치가 있다.

33) 이에 대한 자세한 연구로는 함인선, EU개인정보보호법, 마로니에, 2016 참조.

아시아 국가들의 사이버안보법제 동향과 시사점
– 일본과 중국을 중심으로 –

김 재 광*

목 차

Ⅰ 머리말

공간으로서의 땅, 해양, 하늘에 이어 새로운 공간으로서 등장한 것이 사이버공간이다. 사이버공간은 궁극적으로 국가의 존망을 결정할 전쟁과 경제적 번영의 문제와 직결될 것이기 때문에 이 현상은 단순히 해킹이나 디도스(DDoS)공격과 같은 기술적 문제에 국한돼 방화벽, 백신 프로그램과 같은 기술적 방어나 예방의 문제에 한정시켜 생각하면 큰 실수가 될 것이며, 이는 오늘날 펼쳐지고 있는 문제의 근원과 본질을 제대로 파악하고 있지 못하는 것이다. 사이버 공간은 땅, 바다, 하늘이라는 다른 공간들을 결합시키는 하나의 거대한 공용도로이자 연결통로가 되고 있다. 미래에 사이버공간을 장악한 자는 자신이 원하는 대로 시간과 공간, 그리고 물리력을 통합해 사이버공간

* 선문대학교 경찰행정법학과 교수

을 통해 적을 공격할 수 있을 것이다.[1)]

사이버능력 3대 강국인 미국, 중국, 러시아 간의 갈등이 증폭되며 향후 사이버영역에서의 경쟁이 치열하게 전개·심화될 것으로 전망된다. 미국은 급증하는 사이버위협에 대응하기 위해 예산증액(2015년 49억달러 → 2017년 70억달러) 및 인력충원을 통해서 네트워크방어, 사이버공격 옵션을 위한 인프라 확충 등을 추진하고 있다. 중국은 사이버전력의 확대 및 현대화, 사이버스파이 활동 강화, 사이버 관련 기능·작전 능력의 통합을 꾀하고 있다. 러시아는 사이버능력 강화를 위하여 투자를 늘리고 사이버무기·기술 개발에도 박차를 가하고 있다. 러시아는 능력을 이미 에스토니아, 그루지아에서 과시하였고 2015년 우크라이나전쟁에서는 정부 지원을 받는 핵티비스트(hactivist)를 앞세워 우크라이나정부와 군, NATO를 공격한 바 있다. 그리고 북한은 높은 수준의 인력·조직·기술을 확보하고 있으며, 극비리에 사이버무기 개발 및 공격 능력을 강화하고 있는 것으로 파악되고 있으며 지속적으로 우리를 상대로 사이버공격을 자행하고 있다. 2015년 북한의 공격은 청와대, 국회 해킹 등을 포함해 97건으로 보도되었으나 실제 북한의 정부 및 기간시설 공격은 2014년에만 1,000여건에 육박하는 것으로 판단하고 있다. 지난 10년 간 우리나라의 태풍, 해일, 홍수 등의 자연재난으로 인한 경제적 손실이 1조7000억원인데 비해, 개인정보유출, 사이버범죄, 사이버테러 등 사이버공격으로 인하여 피해를 입은 경제적 손실이3조6000억원에 해당한다.[2)]

미국은 2015년 12월 「사이버안보법(Cybersecurity Act)」을 제정하는 등 사이버안보 관련 법률들을 국가안보적인 차원에서 체계적으로 정비하여 사이버공격에 효율적이고 적극적으로 대응할 수 있는 법제도적 기반을 착실

1) 윤민우, "국운을 좌우할 제4의 전략공간 사이버스페이스" 한국일보 2015년 10월 19일자 칼럼 참조

2) 박춘식, "국가사이버안보전략 시급하다", 디지털타임스 2016년 7월 7일자 시론 참조. 박교수님은 사실 피해를 당한 많은 기관이나 기업 등은 기업 신뢰도 실추 등의 이유로 피해 사실을 숨기려고 한다는 특성을 고려하면, 사이버공격으로 인한 피해는 氷山의 一角에 불과할 것이라고 누구나 쉽게 추정할 수 있을 것이라고 주장한다.

히 구축하고 있으며[3] 일본과 중국 등도 이른바 사이버안보법을 제정하는 등 발빠르게 움직이고 있다.[4]

우리나라의 경우에는 '국가사이버안보 마스터 플랜' 수립을 계기로 사이버안보 강화에 주력하고 있으나 사이버공격 대응체계는 법령의 미비로 인해 민관의 역량을 총동원하지 못하는 중대하고 명백한 법적 한계를 노출하고 있다. 19대 국회에서 사이버안보 관련 법률 제정은 국가안보적 안목이 아닌 당리당략적 접근으로 인하여 구체적인 논의도 되지 못한 채 입법에 실패하고 말았다. 현재 사이버안보 관련 입법시도로는 국회정보위원장인 이철우의원이 발의한 「국가사이버안보에 관한 법률안」[5]과 정부입법인 「국가사이버안

3) 미국과 유럽의 사이버안보 관련법제 정비에 대해서는 김현수, "국가 사이버안보 법정책의 현황과 인식제고방안 - 미국의 사례를 중심으로 -" 「사이버위협의 현황과 법제도방안」 제1회 한국사이버안보법정책학회 월례세미나 발제문, 2013. 3. 20; 이창범, "국내외 사이버안보 관련법제정 동향과 시사점" 「사이버안보법정책논집」 제1호(한국사이버안보법정책학회, 2014. 12), 383쪽 이하; 김성천, "독일의 사이버보안 법제" 「사이버안보법정책논집」 제1호(한국사이버안보법정책학회, 2014. 12), 425쪽 이하; 정태진, "주요 국가별 사이버안보 대응체계 연구" 「국가사이버안전을 위한 법적 과제」(한국사이버안보법정책학회 · 서울대학교 공익산업법센터 2015년 추계 공동학술대회 발표문, 2015. 10. 22 등 참조

4) 정보통신산업진흥원, "초연결 세계에서의 주요국 사이버 보안정책 동향 분석" 「IT R&D 정책동향」(2012-7), 1쪽

5) 법안의 주요 내용은 다음과 같다. ① 사이버안보에 관한 중요한 사항을 심의하기 위하여 대통령 소속하에 국가사이버안보정책조정회의를 둠(안 제4조). ② 국가차원의 종합적이고 체계적인 사이버안보 업무 수행을 위하여 국가정보원장 소속으로 국가사이버안보센터를 둠(안 제6조). ③ 국가정보원장은 사이버안보업무의 효율적이고 체계적인 추진을 위하여 사이버안보 기본계획을 수립하고 이에 따라 시행계획을 작성하여 책임기관의 장에게 배포하여야 함(안 제7조). ④ 책임기관의 장은 사이버공격 정보를 탐지 · 분석하여 즉시 대응할 수 있는 보안관제센터를 구축 · 운영하거나 다른 기관이 구축 · 운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제10조). ⑤ 책임기관의 장은 사이버위협정보를 다른 책임기관의 장 및 국가정보원장에게 제공하여야하며 국가정보원장은 국가차원의 사이버위협정보의 효율적인 공유 및 관리를 위하여 국가사이버위협정보공유센터를 구축 · 운영할 수 있음(안 제11조). ⑥ 책임기관의 장은 사이버공격으로 인한 사고가 발생한 때에는 신속히 사고조사를 실시하고 그 결과를 중앙 행정기관 등의 장 및 국가정보원장에 통보하여야 함(안 제12조). ⑦ 국가정보원장은 사이버공격에 대한 체계적인 대응을 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해 발생을 최소화하거나 피해복구 조치를 취해야 함(안 제14조). ⑧ 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등을 위하여 책임기관 및 지원 기관이 참여하는 사이버위기대책본부를 구성 · 운

보 기본법(안)」[6]이 있다. 일본[7]과 중국에 비해 사이버공격을 가장 많이 받고 있는 우리나라가 사이버안보법 마련이 지지부진한 것은 참으로 아이러니

영할 수 있음(안 제15조). ⑨ 정부는 이 법에서 규정한 업무를 지원할 수 있는 능력이 있다고 인정되는 자를 사이버안보 전문업체로 지정・관리할 수 있음(안 제16조). ⑩ 정부는 사이버안보에 필요한 기술개발・산업육성・인력양성 등 필요한 시책을 추진할 수 있음(안 제19조, 제20조 및 제21조). ⑪ 정부는 사이버공격 기도에 관한 정보를 제공하거나 사이버공격을 가한 자를 신고한 자에 대하여 포상금을 지급할 수 있음 (안 제22조). ⑫ 직무상 비밀을 누설한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처함(안 제23조)

6) 입법예고되었던 법안의 주요내용은 다음과 같다. ① 제1장 총칙 - 목적(안 제1조), 사이버공간, 사이버공격, 국가안보를 위협하는 사이버공격, 사이버위기, 사이버안보 등에 대한 용어 정의(안 제2조), 사이버안보의 기본이념(안 제3조), 다른 법률과의 관계(안 제4조) ② 제2장 국가 사이버안보 수행체계 - 국가사이버안보위원회(안 제5조), 위원회의 기능(안 제6조), 사이버안보 기본계획의 수립 등(안 제7조), 사이버안보 실태의 평가(안 제8조), 책임기관의 책무(안 제9조) ③ 제3장 국가 사이버안보 활동 - 사이버공격의 탐지・대응(안 제10조), 사이버위협정보의 공유(안 제11조), 사이버공격 사고의 신고・조사(안 제12조), 대응훈련(안 제13조), 사이버위기경보의 발령(안 제14조), 사이버위기대책본부의 구성(안 제15조), 사이버안보 전문업체의 지정・관리(안 제16조), 사이버안보 활동의 지원(안 제17조) ④ 제4장 국가 사이버안보 기반조성 - 연구개발(안 제18조), 산업육성(제19조), 인력양성 및 교육홍보(제20조), 국제협력(안 제21조) ⑤ 제5장 보칙 - 비밀 엄수의 의미(안 제22조), 포상 등(제23조) ⑥ 제6장 벌칙 - 벌칙(안 제24조), 과태료(안 제25조), 공무원에 대한 징계(제26조), 국방 분야에 대한 특례(제27조) ⑦ 부칙. 법안은 법제처 심사과정에서 일부 수정되어 2016년 12월 27일 국무회의에서 의결되었다.

7) 일본 방위성과 육상 자위대의 통신 네트워크 시스템이 사이버 공격을 받아 민감한 군사정보가 유출됐을 가능성이 제기되고 있다. 2016년 11월 28일 산케이신문과 도쿄신문 등에 따르면 방위성과 자위대의 통신 시스템 '방위정보통신기반(DII)'이 지난 9월 사이버 공격을 받은 사실이 뒤늦게 알려졌다. 이 시스템은 자위대의 주둔지와 기지를 연결하고 방위성 내부에서 정보를 공유하는 데 쓰이는 대용량 통신 네트워크다. 따라서 자위대의 민감한 내부 정보가 유출됐을 가능성도 배제할 수 없는 상황이다. 일본 정부는 2011년 일본의 방위산업을 노린 대규모 사이버 공격이 확인된 이후 사이버 보안 시스템을 강화해왔다. 하지만 이번에 확인된 공격은 보안 시스템으로도 막지 못할 만큼 높은 수준이었다. 특히 흔적이 거의 남지 않아 정확히 어떤 피해가 발생했는지조차 파악하지 못한 상황이다. 이에 따라 국가 차원의 조직적인 공격이 가해졌을 가능성도 거론되고 있다. 지금까지 확인된 것은 방위성 산하 장교 양성 기관인 방위대의 컴퓨터에서 침입 흔적이 발견된 정도다. 이에 따라 침입자가 방위대를 통해 DII에 접속한 뒤 방위성과 육상 자위대를 공격했을 것으로 추정되고 있다. 방위대의 컴퓨터는 외부의 학계나 대학 네트워크와도 연결돼 있어 사이버 공격의 디딤돌 역할을 했을 것으로 추정되고 있다. 방위성은 사이버 공격 사실을 확인한 직후 한때 방위성과 자위대 전체의 인터넷 이용을 일시 금지했다. DII는 인터넷에 접속하는 외부 시스템과 관계자가 내부 정보를 주고받는 내부 시스템으로 나뉘어져 있다. 하지만 한대의 컴퓨터 안에서 두 시스템을 번갈아가며 이용하는 구조이기 때문에 완전히 분리됐다고는 할 수 없다. 세계일보 2016년 11월 29일자 "일 자위대, 사이버 공격에 '뻥'" 기사 참조

한 일이 아닐 수 없다.

향후 사이버공격은 네트워크공격・해킹 등 통상적인 행위보다는 국가 산업기반에 대한 공격이 늘어나고, 국가 전략시설 및 지휘체계 무력화 시도 등 본격적인 위협이 현실화될 것으로 예상된다. 그리고 국제적으로 사이버 군비경쟁이 급증・가속화될 전망이며 이는 전략적 불안정을 심화시키는 요소가 될 가능성이 높다. 「보안뉴스」가 '보안이슈 중 장기적으로 영향이 큰 보안이슈는 무엇이라고 예상하나요?'라는 질문으로 설문조사한 결과, 응답자 2,298명 중에서 가장 많은 700명, 27.69%가 '북한의 사이버공격 및 점점 노골적으로 변해가는 국제 사이버전 양상'이라고 꼽은 것[8]도 이러한 맥락에서 이해될 수 있다. 그런 측면에서「국가사이버안보 기본법」의 제정이 절실하다고 할 수 있다.

이 글은 아시아국가 중 일본과 중국의 사이버안보정책과 법제를 구체적으로 소개함으로써 우리에게 던지는 법적 함의를 생각해 보고자 하는 데 그 목적을 두고 있다.

Ⅱ 일본의 사이버안보 법정책적 동향과 시사점

1. 일본의 사이버안보정책

미국의 사이버정책에 가장 적극적으로 호응하는 나라가 일본이다. 2013년 10월 미-일 안전보장협의회에서 사이버국방분야 협력에 관한 양해각서를 교환했다. 2015년 4월 아베 신조 일본 수상은 미 상하 양원 합동연설을 하고 미-일 방위협력을 위한 지침, 이른바 「가이드라인 2015」를 공동 발표했다.

「가이드라인 2015」는 아태지역 안보에 대한 공동의 목표와 대응방식을

8) 보안뉴스 2016년 4월 20일자 "장기적으로 영향이 가장 큰 보안이슈 '북한 사이버공격'" 기사 참조

담고 있는데, 종전의 가이드라인에 비해 미-일동맹의 연합작전 태세를 한층 강화했다. 특히 상호 협력범위를 아태지역을 넘어 글로벌로 확장했고, 우주 및 사이버공간을 포함시켰다. 이로써 일본 역할이 나토동맹에서의 영국, 프랑스, 독일과 비슷한 수준으로 올라갔다. 그간 미국은 사이버방어를 둘러싼 국제적 규범을 서두르면서 일본의 동참을 호소해 왔고, 해외로부터 해킹 공격에 시달려온 일본도 미국의 협조를 요청하고 있다.

2012년 9월 신카쿠(중국명 다오위다오) 국유화 이후 일본 국회를 비롯한 정부, 금융기관, 무기개발업체에 대한 해킹이 더욱 거세지고 있다. 2015년 5월 최대 규모의 해킹 공격으로 연금기구의 정보시스템에서 125만명의 신상정보가 유출되기도 했다. 이에 일본은 경찰청에서 담당해오던 사이버수사를 대폭 강화함과 동시에 국가 주요시설에 대한 대응을 자위대 수준으로 끌어올렸다.

일본이 사이버테러 대응조직을 만든 건 2000년 1월 16개 정부기관 사이트가 중국 해커들에게 마비된 사건이 계기가 됐다. 이후 사이버방어 조직을 꾸준히 증강시켜오다 2014년 3월 자위대 예하에 사이버공간방위대를 창설했다. 방위대는 100명 규모의 적은 인원으로 발족했지만 예산은 무려 212억엔(약 2,000억원)에 달한다.[9)]

일본정부는 2013년 6월 11일에 종래의 '국민을 지키는 정보시큐리티 전략'을 대신할 새로운 국가전략으로서 '사이버시큐리티 전략'을 결정하였다. 이 전략은 2013년부터 2015년을 대상기간으로 하며 사이버공간의 확대에 따라 리스크도 점차 확대되고 국제화되고 있는 추세에 대응하기 위한전략을 제시하고 있다.[10)] 일본 사이버공간의 환경이 급속하게 변화함에 따라 새로운 전략의 수립이 필요하다고 본 것이다. 사이버공간은 다양한 정보 등이 유

9) 손영동, "[손영동의 사이버세상]<6>사이버맹주에 시동 건 일본", 전자신문 2015년 8월 18일자 칼럼 참조

10) 곽관훈, "최근 일본의 사이버안보 관련법령 현황과 시사점"「사이버 안보위협 대응전략의 법정책적 검토 및 전망」2013년 한국사이버안보법정책학회 월례세미나 발제문, 2013. 12. 17, 11쪽 이하 참조

통되는 가상의 공간으로 급속하게 확대되고 있으며 실생활에도 급속하게 침투하고 있다. 이에 따라 사이버공간과 실공간이 '융합·일체화'가 이루어지고 있으며 글로벌화되고 있는 상황이다. 이에 따라 사이버공간에서 발생하는 리스크도 점차 심각해지고 있으며 그 확산속도도 매우 빠르다. 또한 사이버공간이 점차 글로벌화됨에 따라 리스크도 글로벌화되는 등 문제점도 더욱 심각해지고 있다. 일본정부는 이러한 환경에 적절하게 대응하여 ① 강인한 사이버공간의 구축, ② 활력 있는 사이버공간의 구축, ③ 세계를 솔선하는 사이버공간의 구축을 통해 '사이버시큐리티 입국'의 실현을 목적으로 새로운 정책을 제시하고 있다.

국가는 사이버공간에 관한 국가의 기본적 기능을 강화하는 것이 필요하며 국외로부터의 사이버공격 등에 대응하여 사이버공간의 방위 및 사이버공간의 범죄대책 등을 마련하는 것이 필요하다. 또한 스스로 정보시스템을 운용하는 주체로서 정부기관 및 공공기관의 시큐리티를 강화하기 위한 조치를 취할 필요가 있다.

일본에서 사이버안보 분야의 기본법을 제정하려는 움직임은 「사이버안보기본법」 발의 이전부터 존재하였다. 2003년에 일본변호사협회는 '정보시큐리티기본법' 제정을 요구하는 의견서와 함께 총 7개 장 및 부칙으로 구성된 법안을 발표한 바 있다.[11] 그럼에도 불구하고 일본은 오랫동안 사이버안보 분야의 기본법을 제정하지 않은 채 정보화 분야의 기본법인 「고도정보통신네트워크사회형성기본법」(2000년 11월 제정)에 따라 관련 기구들을 설치하고 정책을 시행하였다.[12] 이 법의 핵심은 정보시큐리티정책회의, 정보시큐리티센터 등을 설치하고 이러한 기구들을 중심으로 관련 정책을 추진한 점이다. 이에 더하여 「부정액서스행위 금지등에 관한 법률」등에 근거하여 부정한

11) 박상돈, "일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점을 중심으로", 「경희법학」 제50권 2호(경희대 법학연구소, 2015), 148쪽
12) 이에 대해서는 김재광·김정임, "일본의 사이버위기 관련 법제의 현황과 전망" 「법학논총」 제33권 제1호(단국대 법학연구소, 2009. 6), 43쪽 참조

행위를 한 자를 처벌하는 등의 형태로 사이버안보 분야에 필요한 조치를 취하여 왔다.[13] 사이버공격이 증가함에 따라 2013년 발표된 '국가안전보장전략'은 사이버안보의 강화를 제시하였고, 동시에 발표된 <방위계획대강>은 각종 사태에 대한 실효성 있는 억지 및 대처 중 하나로서 사이버공간에서의 대응을 제시하였다.

그러나 이와 같은 형태의 사이버안보 대책에 한계가 있다는 인식을 하면서 2020년 개최 예정인 도쿄올림픽과 페럴림픽은 사이버안보 분야의 기본법 제정의 필요성을 환기시키는 직접적인 요인으로 작용한 것으로 분석되고 있다.[14]

그리하여 일본은 2014년 11월 12일 사이버안보를 위한 주체별 책임을 규정한「사이버안보기본법」을 제정했다. 이 법률은 사이버안보 분야의 기본법으로서 사이버안보에 대한 실효성을 강화하였다는 평가를 받고 있다.

2. 일본의 사이버안보 입법동향: 「사이버안보기본법」의 제정

2014년 11월 사이버안보를 위한 주체별 책임을 규정한 「사이버안보기본법」을 제정하여 사이버안보를 강화하고 있다.

(1) 「사이버안보기본법」의 주요내용

「사이버안보기본법」은 사이버시큐리티 관련 시책 추진의 기본 이념과 각 주체별 사이버시큐리티 확보의 책무를 정하고 있다. 또한 정부가 사이버시큐리티전략을 수립하도록 하고, 내각에 사이버시큐리티전략본부를 두면서 내각관방이 그 사무를 처리하도록 하는 추진체계를 정립하였다. 「사이버안보기본법」은 그 밖에도 사이버시큐리티의 강화에 필요한 다양한 조치들을 정하고 있다.

13) 「부정액세스행위 금지등에 관한 법률」에 대한 구체적인 내용에 대해서는 김재광・김정임, 앞의 논문, 47~50쪽 참조
14) 박상돈, 앞의 논문, 149쪽

1) 사이버시큐리티의 의의

'사이버시큐리티'라는 원어를 그대로 사용하고 있는 점이 특징이다. "사이버시큐리티란 전자적 방식, 자기적 방식 및 그 밖의 사람의 지각으로는 인식할 수 없는 방식(이하 "이 조에서 "전자적 방식"이라 한다)으로 기록되거나 발신, 전송 또는 수신되는 정보의 누설, 멸실 또는 훼손 방지 및 그 밖의 정보의 안전관리를 위하여 필요한 조치와 정보시스템 및 정보통신 네트워크의 안전성 및 신뢰성의 확보를 위하여 필요한 조치(정보통신 네트워크 또는 전자적 방식으로 작성된 기록과 관련된 기록매체(이하 "전자적 기록매체"라 한다)를 통한 전자계산기에 대한 부정한 활동에 의한 피해의 방지를 위하여 필요한 조치를 포함한다)가 강구되고 그 상태가 적절하게 유지·관리되는 것을 말한다."고 규정하고 있다.

2) 사이버안보에 관한 기본이념

사이버안보에 관한 기본이념을 여섯 가지 제시하고 있다(제3조). ① 사이버안보 위협에 대해 국가, 지방공공단체, 중요사회기반사업자 등 다양한 주체가 연계하여 적극적으로 대응하여야 한다(제1호). ② 국민 개개인이 사이버안보 관련 인식을 제고하고 자발적으로 대응하도록 하는 동시에, 피해 방지와 신속한 복구를 위한 체제를 구축하는 대책을 적극적으로 추진하여야 한다(제2호). ③ 인터넷 및 그 밖의 고도정보통신네트워크 정비와 정보통신기술 활용에 의한 활력 있는 경제사회 구축 대책을 추진하여야 한다(제3호). ④ 사이버안보 관련 국제질서의 형성과 발전에서 선도적 역할을 담당하며 국제적 협조하에 실시하여야 한다(제4호). ⑤ 「고도정보통신네트워크사회형성기본법」의 기본이념을 배려하여 추진한다(제5호).[15] ⑥ 국민의 권리를 부당

15) 일본은 지난 2001년 1월 「고도정보통신네트워크사회형성기본법」(IT기본법) 제25조에 근거, 내각에 설치된 '고도정보통신네트워크사회추진 전략본부(IT전략본부)'를 중심으로 관계 행정기관간 상호 긴밀한 협조아래 민·관 정보보호 대책을 추진하고 있다. IT전략본부는 IT사회 형성에 관한 중점계획 작성 및 실시와 주요정책의 심의를 담당하고 있으며 정보보안대책추진회의와 정보보안부회로 구성, 수상이 본부장을 맡고 있다. 2005년 4월에는 산하에 있던 내각관방의 정보보안대책추진실을 강화, 내각

하게 침해하지 않아야 한다(제6호).

3) 각 주체별 기본 책무

가. 국가의 책무

국가는 기본이념에 따라 사이버안보에 관한 종합적인 시책을 수립·실시할 책무를 진다(제4조). 그리고 국가는 행정조직의 정비 및 행정 운영의 개선에 노력하여야 한다(제11조).

나. 지방공공단체의 책무

지방공공단체는 기본이념에 따라 국가의 역할을 분담하여 사이버안보에 관한 자주적 시책을 수립·실시할 책무를 진다(제5조).

다. 중요한 사회기반사업자의 책무

중요사회기반사업자는 사이버안보에 대한 관심과 이해를 높이며, 자주적이고 적극적으로 사이버안보 확보에 노력하고, 국가 및 지방공공단체의 시책에 협력한다(제6조).

라. 사이버 관련 사업자의 책무

인터넷 및 그 밖의 고도 정보통신망의 정비, 정보통신기술 활용 또는 사이버안보에 관한 사업을 실시하는 사이버 관련 사업자는 기본이념에 따라 해당 사업에 관하여 자주적이고 적극적으로 사이버안보 확보에 노력하고 국가 및 지방공공단체의 시책에 협력한다(제7조).

관방 국가정보보안센터(NISC)를 설치해 내각관방의 안전보장 및 위기관리 담당 부장관보를 센터장으로 임명하는 등 사이버 보안의 지위를 격상시켰다. 이어 5월에는 본부 산하에 정보보안 정책회의를 설치, 정보보안 정책에 관한 기본전략의 수립과 추진을 강화하는 한편 정보보안 안전기준의 책정과 추진 등을 적극 지원하였다. IT전략본부 산하의 국가정보보안센터(NISC)가 사이버공격정보 수집·위험평가·관련기관에 위기관리대책 수립 지시 등의 업무를 수행하였다. 이 법률은 우리나라의 「정보화촉진기본법」과 비슷한 내용의 정보화 촉진을 위한 개략적인 시책과 정책 등을 천명하고 있는 법률이다.

마. 대학 및 그 밖의 교육기관의 책무

대학 및 그 밖의 교육기관은 기본이념에 따라 자주적이고 적극적으로 사이버안보의 확보에 노력하고 사이버안보 관련 인재 육성과 연구 수행 및 그 성과의 보급에 노력하며 국가 및 지방공공단체의 시책에 협력한다(제8조).

바. 국민의 책무

국민은 기본이념에 따라 사이버안보에 대한 관심과 이해를 높이고 사이버안보의 확보에 필요한 주의를 기울이도록 노력한다(제9조).

사. 정부의 책무

정부는 사이버안보에 관한 시책을 실시하기 위한 법제상, 제정상, 세제상의 조치를 강구하여야 한다(제10조).

4) 사이버안보전략

정부는 사이버안보에 관한 시책의 종합적·효과적 추진을 도모하기 위해 사이버안보에 관한 기본계획으로서 사이버안보전략을 수립하며 사이버안보전략의 실시에 필요한 자금을 예산에 계상하는 등 그 원활한 실시에 필요한 조치를 강구하도록 노력하여야 한다(제12조).

일본은 2015년 9월 사이버안보전략[16]을 수립하고 연차 계획을 착실히 추진하고 있다.

5) 기본적 시책

가. 국가행정기관 등의 사이버안보의 확보

사이버안보 관련 국가의 행정기관 및 독립행정법인의 사이버안보에 대한 통일적인 기준을 수립, 국가 관련 악의적인 활동모니터링 및 분석, 사이버안보

16) 참고로 미국은 2015년 12월 통과된 「사이버안보법」에 근거하여 미국민의 정보를 보호하기 위한 사이버안보행정계획을 수립하고 발표했다. 유럽연합에서도 2013년 유럽위원회가 사이버안보전략을 마련한 바 있으며 2015년 5월 유럽네트워크정보보호청(ENISA)이 사이버안보전략을 마련해 시행하고 있다고 한다. 박춘식, “국가사이버안보전략 시급하다” 시론 참조

연습과 훈련, 국내외 관계기관과 위협에 대응, 국가의 행정기관과 행정법인 등 사이의 사이버안보 정보공유와 필요한 시책을 강구하여야 한다(제13조).

나. 중요한 사회기반사업자 등의 사이버안보전략의 촉진

국가는 중요한 사회기반사업자 등의 사이버안보 관련 기준의 책정, 연습 및 훈련, 정보 공유, 활동 촉진 등 필요한 시책을 강구하여야 한다(제14조).

다. 민간사업자 및 교육연구기관 등의 자발적인 활동의 촉진

국가는 중소기업자 외의 민간사업자 및 대학 또는 교육기관의 사이버안보의 중요성에 대한 관심과 이해, 사이버안보에 필요한 정보의 제공 및 조언에 필요한 시책을 강구하여야 한다(제15조제1항). 국가는 국민이 일상생활에서 전자계산기 또는 인터넷 그 밖의 고동정보통신네트워크의 이용에 있어 사이버안보에 관한 정보의 제공 및 조언에 필요한 시책을 강구하여야 한다(제15조제2항).

라. 다양한 주체의 연계 등

국가는 관계부처 상호간의 연계 강화, 다양한 주체들이 상호 협력하여 사이버안보 시책에 종사할 수 있도록 필요한 시책을 강구하여야 한다(제16조).

마. 범죄의 단속과 피해의 확대 방지 등

국가는 사이버안보 범죄 단속 및 피해 확대 방지에 필요한 시책을 강구하여야 한다(제17조).

바. 안전에 중대한 영향을 미칠 우려가 있는 사건에 대응

국가는 사이버안보사건 중 중대한 영향을 미칠 우려가 있는 것들에 대해 관계기관 체제의 충실 강화, 상호 협력 강화, 역할분담의 명확화를 위해 필요한 시책을 강구하여야 한다(제18조).

사. 산업의 진흥 및 국제 경쟁력 강화

국가는 사이버안보 관련 산업이 고용 기회를 창출할 수 있는 산업이 될 수 있도록 사이버안보 관련 첨단적인 연구개발의 추진, 기술의 고도화, 인재 육

성 및 확보, 경영기반 강화 및 새로운 사업의 개척, 기술의 안전성 및 신뢰성에 관한 규격, 국제표준화 등의 필요한 시책을 강구하여야 한다(제19조).

아. 연구개발의 추진

국가는 사이버안보 연구개발 및 기술 등의 추진 및 성과의 보급을 도모하기 위해 사이버안보 관련 기초연구 및 기반적인 기술연구개발의 추진, 연구자 및 기술자의 육성, 국가시험연구기관, 대학, 민간 등의 연계 강화, 연구개발을 위한 국제협력 등의 필요한 시책을 강구하여야 한다(제20조).

자. 인력 확보 등

국가는 대학, 고등 전문학교, 전수학교, 민간사업자와 연계 협력을 통해 사이버안보에 관한 사무에 종사하는 자의 적절한 처우 확보에 필요한 시책과 인재의 확보, 양성 및 자질 향상을 위해 자격제도의 활용, 젊은 기술자 양성에 필요한 시책을 강구하여야 한다(제21조).

차. 교육 및 학습의 진흥, 보급 개발 등

국가는 국민에 대한 사이버안보 관심과 이해, 교육 및 학습의 진흥, 계몽 및 지식의 보급과 관련된 시책을 추진할 수 있도록 기간의 지정 및 그 밖에 필요한 시책을 강구하여야 한다(제22조).

카. 국제협력의 추진 등

국가는 사이버안보분야에 대해 국제간의 신뢰구축 및 정보공유 추진, 국제기술협력 지원, 범죄의 단속과 관련된 국제협력 추진 등을 위한 필요한 시책을 강구하여야 한다(제23조).

6) 사이버안보전략본부의 설치 및 임무

사이버안보전략본부(본부장: 내각관방장관)의 설치 및 임무는 다음과 같다(제24조~제29조). 사이버안보에 관한 시책을 종합적・효과적으로 추진하기 위해 내각에 사이버안보전략본부를 설치한다. 사이버안보전략본부는 ① 사이버안보전략의 수립 및 실시 ② 국가행정기관 및 독립행정법인의 사이버

안보 관련 대책 기준 작성과 사이버안보 관련 대책 기준에 따른 시책의 평가 등 해당 기준에 근거한 시책 실시 추진 ③ 원인 규명을 위한 조사 등 국가행정기관에서 발생한 사이버안보 관련 중대사건에 대한 시책의 평가 ④ 그 밖의 사이버안보 관련 시책의 중요사항 기획에 관한 조사·심의 ⑤ 관계행정기관의 경비 견적 방침 및 시책 실시에 관한 지침 작성 및 시책 평가 등 시책 실시에 필요한 종합적 조정 등에 관한 사무를 주관한다.

7) 사이버안보전략본부의 협력관계

사이버안보전략본부의 협력관계는 다음과 같다. 관계행정기관의 장은 사이버안보전략본부가 정하는 바에 따라 사이버안보전략본부의 소관 사무에 필요한 관련 자료 및 정보를 사이버안보전략본부에 적시에 제공하여야 한다. 그 밖에 관계행정기관의 장은 사이버안보전략본부의 요청에 따라 필요한 사이버안보 관련 자료 및 정보를 제공하고 설명하는 등 협력하여야 한다(제30조). 지방공공단체를 비롯한 관련자들도 정보 제공 등 협력할 의무가 있다(제31조, 제32조 등).

(2) 「사이버안보기본법」의 시사점

일본의 「사이버안보기본법」은 사이버안보 관련 시책 추진의 기본 이념과 각 주체별 사이버안보 확보의 책무를 정하고 있다. 또한 정부가 사이버안보 전략을 수립하도록 하고, 내각에 사이버안보전략본부를 두면서 내각관방이 그 사무를 처리하도록 하는 추진체계를 정립하였다. 그 밖에도 「사이버안보기본법」은 사이버안보의 강화에 필요한 다양한 조치들을 정하고 있다.

「사이버안보기본법」의 시사점을 살펴보면 다음과 같다. ① 사이버안보 분야의 기본법이 제정되었다는 점 ② 연성규범에 대한 의존도를 감소시키고 법치국가원리를 준수한다는 점 ③ 기본이념에 바탕한 범국가적 사이버안보 추진의 법적 근거를 마련하였다는 점 ④ 사이버안보 총괄기구의 위상을 높이고 이를 법제화하였다는 점 ⑤ 사이버안보 강화 활동의 투명성을 확보하여 일반 국민의 참여 여건을 조성하였다는 점 ⑥ 사이버안보 국제질서 형성에 대한

적극적인 참여를 선언하였다는 점 등에서 큰 의미가 있다.[17)]

[「사이버시큐리티기본법」 구성체계]

제1장	총칙	○ 법의 목적, 정의, 기본이념 등 제시 – 국가, 지방공공단체, 중요사회기반사업자, 교육연구기관 등의 책무 규정(제4조~제11조)
제2장	사이버안보전략 추진	○ 사이버안보 전략 추진을 위한 기본계획 수립 제시 – 종합적인 사이버안보 시책의 수립・공표, 재정범위 내 실시 등(제12조)
제3장	사이버안보 기본시책	○ 사이버안보 기본시책의 주요 규정사항, 수립 방향 등(제13조~제23조)
제4장	사이버안보 전략본부	○ 사이버안보전략본부의 구성 및 운영(제24조~제29조) ○ 관련 자료 및 정보제공 요청권, 협력 요청권 등(제30조~제35조)

Ⅲ 중국의 사이버안보 법정책적 동향과 시사점

1. 중국의 사이버안보정책

중국의 정보화는 1980년 중반부터 발전되었으며 ① 해킹 등 사이버범죄 ② 인터넷을 통한 정치적 선동 ③ 군사적 취약점 공격 등을 사이버위험으로 인식하였다. 경제・사회적 발전에 있어 사이버공간의 중요성을 인식하고 사이버공간을 새로운 안보영역으로 자각하였다. 중국은 '적극적인 방어' 전략을 통해 사이버전쟁과 관련한 지휘, 통제, 통신, 컴퓨터, 정보, 감시, 정찰(C4ISR; command, control, communications, computers, intelligence, surveillance, and reconnaissance)을 설계하고 첨단 무기체계와 전자적 운용체계를 확보하고 있다.

중국은 미국에 버금가는 사이버안보 역량을 갖추기 위해 많은 투자를 하였

17) 구체적인 것은 박상돈, 앞의 논문, 161~165쪽 참조

다. 인민해방군은 1997년 「악성코드 침투가 원자폭탄보다 효율적」이라는 내용의 보고서를 중앙군사위원회에 제출했다. 이후 위원회 직속의 컴퓨터 바이러스 부대, 사이버공격 및 정보교란 모의훈련을 주된 임무로 하는 넷포스(Net Force), 베이징, 광저우, 지난, 난징 등 4대 군구 산하에 전자전 부대를 잇달아 창설했다. 2010년 7월 全軍의 사이버 관련 전략·정보기구를 통할하는 사이버사령부(信息保障基地)가 창설됐다. 특히 자국의 컴퓨터 영재뿐만 아니라 미국에서 유학한 고급 인재를 파격적인 조건으로 채용해 편제에도 없는 사이버특수부대에 배치하고 있다.[18]

서방 선진국들이 중국을 두려워하는 것은 이들 사이버부대만이 아니다. '홍커(紅客. red hacker)'라 불리는 150만 명에 달하는 민간 해커가 있다. 이들은 정부의 통제를 거의 받지 않기 때문에 더욱 공격적이고 무차별적인 해킹을 감행한다. 맹목적이라 싶을 정도의 애국심으로 무장하고 미국, 일본, 한국을 비롯한 전 세계 정부나 기업, 개인까지 타깃이 된다.[19] 중국 공산당은 이 같은 홍커의 행동에 대하여 자국 내 사이트를 공격하지 않는 한 처벌하지 않는 것으로 알려져 있다. 미국은 중국 정부가 프리랜서 해커들을 직·간접적인 국가통제 아래에 두면서 민간 해커들의 애국적 해킹활동을 조장한다고 보고 있다.

중국은 자국 정부와 군 정보시스템에 서방 군사·정보기관이 침투하는 것을 막기 위해 '기린(Kylin)'이라는 운용체계를 개발해 2007년부터 정부기관에 설치했다. 기린이 얼마나 잘 만들어졌는지에 상관없이 중국이 외산 운용체계나 네트워크 장비에 의존하지 않음으로써 외부 침입에 강력한 방어 기반을 갖춘 셈이다. 그러던 중국이 정보기술 부문에서 우리나라를 추월해 미국과 맞대결 국면으로 들어가고 있다. 중국의 바이두·알리바바·텐센트가 미

18) 손영동, "[손영동의 사이버세상]<8>기반기술 국산화 주도하는 중국", 전자신문 2015년 9월 1일자칼럼 참조

19) 이들이 집단 공격 움직임을 드러낸 것은 1998년 8월 일어난 인도네시아 폭동이다. 인도네시아에서 상당한 부(富)를 차지하고 있던 화교들이 공격당하자 홍커들은 인도네시아 정부 사이트를 집단 해킹했다. 2001년 4월 미군 정찰기와 중국 전투기가 추돌하자 양국 해커들은 상대국 정부사이트를 대거 공격했고, 홍커들이 미 백악관 홈페이지를 완전히 마비시킴으로써 그 존재를 알렸다. 손영동, 앞의 칼럼 참조

국의 구글・아마존・페이스북 벤치마킹 수준을 뛰어넘어 양자 간 대칭구도를 형성했고, 화웨이(하드웨어)・샤오미(소프트웨어) 등 자수성가형 성공사례도 잇따르고 있다. 중국 공산당이 오랜 기간 공을 들인 인프라 확충과 국산화 정책이 만들어낸 결실이라 할 수 있다.[20]

[중국의 사이버안보 관련 주요 정책]

순번	정책명	주요내용
1	정보산업발전계획(2013)	○ 2013년 2월, 공업정보화부 국가발전개혁위원회 공포 ○ 중국의 IT산업 발전에 따른 네트워크 정보 안전 보장 능력 제고
2	국무원의 정보화 발전을 적극적으로 추진하고 효과적인 정보보안 수행을 위한 일부 의견(2012)	○ 2012년 6월, 국무원 공포 ○ 주요 분야 정보보안 보장 ○ 네트워크 정보 안전 보장 강화를 위한 역량 구축
3	중화인민공화국 국민경제와 사회발전 제12개5년계획 강령(2011)	○ 2011년 3월, 전국인민대표대회 공포 ○ 정보화 수준 전면 제고 전략제시 ○ 차세대 정보기반시설 구축, 경제사회 정보화 추진, 네트워크와 정보보안 보장 강화 전략 명시
4	2009~2020 행정 정보화 중장기 계획 강령(2009)	○ 2009년 9월, 민정부 발표 ○ 행정 정보화 건설 ○ 행정 정보화를 통한 사회 정보화 추진
5	2006~2020 국가 정보화 발전전략(2006)	○ 2006년 3월, 중국공산당 중앙위원회 사무국, 국무원 사무국 공포 ○ 제15기 5준전회(2000.10.9~2000.10.11.개최)에서 정보화를 국가 전략으로 승격 ○ 정보보안에 있어 장기적이고 유효한 제도 구축 ○ 국가보안보장체계 강화

출처: 양정윤・배선하・김규동, 「중국 사이버 역량 현황 연구」(국가보안기술연구소(NSR)), 2015. 12), 18~19쪽 참조

20) 중국은 미국의 인터넷 기술종속에서 벗어나기 위해 지난 20년간 안간힘을 쏟아 왔다. 그간 중국 정부 인터넷 정책은 외국 하드웨어와 소프트웨어를 국산으로 대체하는 데 초점을 맞추고 있었다. 외산 소프트웨어에의 지나친 의존으로 생기는 위험성은 2008년 마이크로소프트가 윈도 운용체계 무단 사용을 막기 위해 해적 방지 프로그램을 보급하면서 부각됐다. 당시 소프트웨어 80%가 해적판이어서 마이크로소프트의 새 프로그램이 설치되자 컴퓨터 수백만대가 다운되는 큰 혼란이 발생한 적이 있다. 손영동, 앞의 칼럼 참조

2. 중국의 사이버안보 입법 동향

중국은 1994년 2월 18일, 사이버안보에 관한 첫 법제인 「중화인민공화국 컴퓨터 정보시스템안전보호 조례」를 공포한 이래 약 30여개의 법령에서 사이버안보에 관한 사항을 규율하고 있다.

(1) 사이버안보 관련 법률

순번	법률명	주요내용
1	사이버안전법 (2015) ※ 2017.6.1.시행	○ 사이버안전 보장, 사이버공간의 주권과 국가안전 유지 ○ 국가인터넷정보판공실[21]이 사이버안전 업무 총괄
2	국가안전법(2015)	○ 사이버안전에 관한 세부적인 내용 규율 ○ 사이버안전 전략 및 계획, 네트워크 운영, 정보 안전, 주요 정보기초시설 운영 안전, 관리감독 및 긴급처치 등
3	온라인정보보호 강화에 관한 결정(2012)	○ 인터넷상 개인 프라이버시 보호 ○ 개인정보 수집 원칙 및 수집된 정보의 비밀 보장을 통해 온라인 정보의 안전을 유지하여 공공이익 보호
4	치안관리처벌법 (2006)	○ 컴퓨터 정보시스템에 대한 피해 방지 ○ 국가규정을 위반한 컴퓨터 정보시스템에 대한 침입, 삭제, 수정, 교란, 프로그램의 삭제 및 수정, 고의적 컴퓨터 바이러슺[p작, 전파 등 처벌
5	전자서명법 (2004)	○ 국무원 정보산업주무부가 전자인증서비스의 구체적 관리 방안을 제정 ○ 전자인증서비스제공자에 대한 관리・감독 실시
6	인터넷 안전보호에 관한 결정(2000) ※ 2009년 개정	○ 국가사무 컴퓨터 시스템에 침입하거나, 컴퓨터 바이러스 제작 등을 통한 컴퓨터 통신 네트워크 침해 방지 ○ 인터넷을 이용한 요언 날조, 정권 전복, 국가분열 선동, 통일 파괴 등에 대한 처벌사항 규정

21) 2014년 설립된 '중앙인터넷안전정보화영도소조'는 '국가정보화영도소조'와 '국가인터넷・정보안전협조소조'를 통합한 조직으로, 사이버안보와 인터넷 여론을 단속하는 정책을 총괄하는 기구이다. 정보화 및 인터넷안전에 대한 최고 정책을 결정하고 사무국 역할을 하는 곳은 '중앙인터넷안전정보화영도소조 판공실'에서 수행한다.

순번	법률명	주요내용
7	국가비밀보호법 (1989)	○ 국가비밀을 지키고 국가안전과 이익보호를 위하여 제정 ○ 국가비밀을 저장하거나 처리하는 컴퓨터 정보시스템은 비밀 관련 정도에 따라 등급을 나누어 보호
8	형법 (1980)	○ 제285조에서 컴퓨터 정보시스템 불법침입죄, 제286조에서 컴퓨터 정보시스템 피괴죄 규정 ○ 국가보안 침해죄, 공공보안 침해죄, 사회주의 시장경제질서 피괴죄, 공민권리 침해죄, 재산침해죄, 사회질서 교란죄, 컴퓨터정보시스템 불법 침입죄, 컴퓨터정보시스템 파괴죄 규정

출처: 양정윤・배선하・김규동, 앞의 보고서, 3~4쪽 참조

(2) 사이버안보 관련 행정법규

순번	행정법규명	주요내용
1	인터넷정보내용관리책임에 관한 통지(2014)	○ 인터넷 발전을 통한 개인・법인・조직의 권익보장 ○ 국무원의 국가인터넷부서에 국가 전체 인터넷 정보관리 및 법집행에 관한 감독 권한 부여
2	국제네트워크 컴퓨터정보안전보호 관리방법(2014)	○ 개인의 허락 없이 인터넷 정보를 변형하여 대중에 공개하는 것에 대해 금지 ○ 정보주체의 요구가 있을시 인터넷 정보 삭제
3	인터세정보확산보호조례(2013)	○ 정보주체의 동의 없이 인터넷상 개인정보 유포 금지 ○ 정보주체의 요구가 있을 시 정보제공자는 개인의 권리를 침해하는 정보를 인터넷상 삭제할 것
4	컴퓨터소프트웨어보호조례(2013)	○ 소프트웨어 저작권에 대하여 국무원 저작권관리행정부서에 등록 후 사용 가능 ○ 개인・법인・기타 기관이 외국인에 소프트웨어 저작권을 양도할 시 「중화인민공화국 기술수출입관리조례」의 규정을 따라야 함을 명시
5	인터넷서비스사업장관리조례(2011)	○ 인터넷서비스제공사업장은 ‘인터넷문화경영허가증’을 소지하여야 함 ○ 인터넷서비스제공장은 ‘인터넷문화경영허가증’을 임의로 수정・대여・양도할 수 없음

순번	행정법규명	주요내용
6	외국인투자무선통신사업관리규정(2008)	○ 외국인 무선통신 투자 사업자는 '외국인투자기업허가증'을 소지하여야 함 ○ 국무원 공업정보화 주관 부서의 '전신업무경영허가증'을 취득하여야 함
7	인터넷정보서비스관리방법(2000)	○ 인터넷 정보서비스 활동 규범화 및 발전 촉진을 위하여 제정
8	전신조례(2000)	○ 전신 네트워크를 이용한 국가안전 손상, 국가비밀 누설, 정권 전복, 국가통일을 피괴하는 정보 제작, 복제, 반포 혹은 전파하는 행위를 불법으로 규정
9	컴퓨터정보망의 국제네트워크워킹관리잠정규정(1996) ※ 1997년 개정	○ 컴퓨터 정보망의 국제 네트워킹에 대한 관리 강화 ○ 국제 네트워킹에 대한 관리를 국무원에 위임
10	컴퓨터정보시스템 안전보호조례(1994) ※ 2011년 개정	○ 컴퓨터 정보시스템의 안전 보호 ○ 공안부에 컴퓨터 정보시스템 보호에 대한 권한 위임 ○ 2011년「국무원의 일부 행정법류 폐지와 개정에 관한 결정」에 의해 개정

출처: 양정윤・배선하・김규동, 앞의 보고서, 5~6쪽 참조

(3) 사이버안보 관련 부문규정

순번	규정명	주요내용
1	중국 내 외국금융기관의 정보관리규정(2014)	○ 사이버안전 보장, 사이버공간의 주권과 국가안전 유지 ○ 국가인터넷판공실이 사이버안전 업무 총괄
2	인터넷통신사업 개인정보보호 규정(2012)	○ 사이버안전에 관한 세부적인 내용 규율 ○ 사이버안전 전략・계획, 네트워크 운영・정보 안전, 주요 정보기초시설 운영 안전, 관리감독 및 긴급처치 등
3	인터넷정보서비스 시장질서규범에 관한 규정(2011)	○ 인터넷상 개인 프라이버시 보호 ○ 개인정보 수집원칙 및 수집된 정보의 비밀 보장 ○ 온라인 정보의 안전을 통한 공공이익 보호

순번	규정명	주요내용
4	인터넷 문화관리 잠정규정(2011)	○ 통신망 안전관리 강화 ○ 공업정보화부가 통신망 안정을 관리하고각 성・자치구・직할시의 통신관리국이 행정구역 내 통신 네트워크 안전보호업무를 지도・조율
5	인터넷 방송신청서비스 관리규정(2007)	○ 공안부가 정보안전등급 보호업무 총괄 ○ 정보시스템에 대한 안전보호등급(총 5등급) 중 국가안전에 손해 여부 및 그 엄중성에 따라 제3등급부터 제5등급으로 분류
6	인터넷신문 정보시비스 관리규정(2005)	○ 인터넷 정보서비스 활동 규범화 및 발전 촉진
7	인터넷 등 무선망을 통한 방송시청관리방법(2004)	○ 정보산업국이 수행하는 전자인증서비스 관련 사항 규정

출처: 양정윤・배선하・김규동, 앞의 보고서, 6~7쪽 참조

(4) 「중화인민공화국 네트워크 안전법」의 제정

2015년 7월 중국 전국인민대표회의(전인대)는 사이버상에서의 공격과 범죄, 유해정보 확산 위협으로부터 사이버주권과 국가안보를 수호하기 위한 중화인민공화국 네트워크 안전법(일명 사이버안전법) 초안을 마련했다. 이 법의 입법취지는 “네트워크 안전을 보장하고 네트워크 공간의 주권과 국가 보안, 사회의 공공 이익을 수호하고 공민, 법인 그리고 그 밖의 조직의 합법적인 권익을 보호하며 경제 사회 정보화의 건전한 발전을 촉진하기 위하여 본 법안을 제정한다”는 것이다. 그리고 이 법은 “중국인민공화국 국내에서 네트워크를 건설, 운영, 유지와 사용, 그리고 네트워크 보안을 감독 관리하는데 적용한다”(제2조)고 규정하고 있다.

이 법은 제1장 총칙, 제2장 네트워크 보안 지원과 촉진, 제3장 네트워크 운영 안전(제1절 일반 규정, 제2절 중요 정보 인프라의 운행 안전), 제4장 네트워크 정보 보안, 제5장 모니터링 경보와 비상 대응, 제6장 법률적 책임, 제7장 부칙 등으로 구성되어 있다.[22] 결과적으로 ‘사이버 만리장성’을 구축

한 셈이다.

사이버안전법은 크게 ① 네트워크 안전 ② 개인정보보호 ③ 불법정보 규제 등으로 구성되어 있다. 법의 주요내용을 살펴보면 다음과 같다.

1) 용어의 정의

'네트워크'란 컴퓨터 또는 그 밖의 정보 단말기 및 관련 설비로 구성된 일정한 규칙과 프로그램에 따라 정보에 대한 수집, 저장, 전송, 교환, 처리하는 시스템을 말한다(부칙 제76조제1호). '네트워크 안전'이란 필요한 조치를 통해 네트워크의 공격, 침입, 교란, 파괴와 불법 사용 및 불의의 사고를 방지하고 네트워크가 안정적인 운행 상태를 유지하게 하는 네트워크 데이터의 완전성, 기밀성, 가용성의 능력을 말한다(제2호).

'네트워크 운영자'란 네트워크의 소유자, 관리자와 네트워크 서비스 제공자를 말한다(제3호). '네트워크 데이터'란 네트워크를 통해 수집, 저장, 전송, 처리, 생성한 각종 전자 데이터를 말한다.

'개인정보'란 전자 또는 그 밖의 방식으로 기록한 단독적으로 또는 그 밖의 정보와 결합하여 식별하는 해당자의 개인 신분의 각종 정보를 말한다. 해당자의 성명, 출생일, 신분증 번호, 개인의 생물적 식별 정보, 주소, 전화 번호 등이 포함되지만 이에 국한되지는 않는다.

2) 국가 및 네트워크 운영자의 의무

가. 국가의 의무

먼저 국가의 임무에 관한 사항으로는 ① 완전한 사이버 보안 보장 체계 구축 및 네트워크 안전의 보호 능력의 향상 ② 네트워크 보안 전략의 제정 및 개선 ③ 네트워크 공간의 안전과 질서의 보호 ④ 사회주의 핵심 가치관의 전파 추진 ⑤ 평화롭고 안전하며 개방적이면서도 협력하는 사이버 공간의 구축

22) 법안에 관한 규체적인 내용에 대해서는 보안뉴스 2015년 7월 27일자 "[中 '사이버 보안법' 뭘 담았나 ①] 네트워크·인터넷 보안 총망라" 기사 참조

추진 ⑥ 네트워크를 이용한 국가의 안전 및 사회주의 제도를 뒤엎으려는 책동 금지 ⑦ 미성년자에게 안전하고 건강한 네트워크 환경 제공 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 완전한 사이버 보안 보장 체계 구축 및 네트워크 안전의 보호 능력의 향상

국가는 네트워크 보안과 정보화 발전을 동시에 중요시하고, 적극적인 이용, 과학적 발전, 법적 관리, 보안 확보의 방침에 따라 네트워크 인프라 건설과 연결과 교환을 추진하고, 네트워크 기술의 혁신과 응용을 장려하며, 네트워크 보안 인재의 양성을 지원하고, 완전한 사이버 보안 보장 체계를 구축하며, 네트워크 안전의 보호 능력을 향상시킨다(제3조).

② 네트워크 보안 전략의 제정 및 개선

국가는 네트워크 보안 전략을 제정하고 또 끊임없이 개선하고, 사이버 보안의 기본 요구와 주요 목표를 명확히 하며, 중요 분야의 사이버 보안 정책, 업무 임무와 조치를 제기한다(제4조).

③ 네트워크 공간의 안전과 질서의 보호

국가는 조치를 취하여 중화인민공화국 국내·외에서 오는 사이버 보안 위험과 위협을 모니터링하고 방어하며 처리하고, 중요 정보 인프라를 공격, 침입, 교란과 파괴로부터 보호하며, 법에 따라 네트워크 위법 범죄 행위를 처벌하고, 네트워크 공간의 안전과 질서를 보호한다(제5조).

④ 사회주의 핵심 가치관의 전파 추진

국가는 성실하고 건강한 사이버 행위를 선도하고, 사회주의 핵심 가치관의 전파를 추진하며, 전 사회의 네트워크 보안 의식과 수준을 높이기 위한 조치를 취하고, 전 사회가 사이버 보안을 공동으로 촉진할 수 있는 양호한 환경을 형성한다(제6조).

⑤ 평화롭고 안전하며 개방적이면서도 협력하는 사이버 공간의 구축 추진

국가는 사이버 공간의 관리, 네트워크 기술의 연구 개발과 기준 제정, 사이버 상의 불법 범죄를 단속하는 등에서 국제교류와 협력을 적극적으로 펼치고, 평화롭고 안전하며 개방적이면서도 협력하는 사이버 공간의 구축을 추진하며, 다각적이고 민주적이며 투명한 네트워크 관리 체계를 건설한다(제7조).

⑥ 네트워크를 이용한 국가의 안전 및 사회주의 제도를 뒤엎으려는 책동 금지

국가는 공민, 법인과 그 밖의 조직의 법에 따라 네트워크를 사용하는 권리를 보호하고, 네트워크 접속의 보급을 촉진시키며, 네트워크 서비스 수준을 향상시켜 사회에 안전하고 편리한 사이버 서비스를 제공하고, 네트워크 정보가 법에 따라 질서 있고 자유롭게 흐르는 것을 보장한다. 어떤 개인이나 조직에서 네트워크를 사용할 경우, 헌법 법률을 준수하여야 하고 공공 질서를 지키며 사회의 공공 도덕을 존중하고 네트워크 보안을 해쳐서는 안되며, 네트워크를 이용하여 국가의 안전, 명예와 이익을 해치거나 국가 정권의 전복을 선동하고 사회주의 제도를 뒤엎으며, 국가 분열을 선동하고 국가의 통일을 파괴하며, 테러리즘과 극단주의, 민족 증오, 민족 차별을 선양하며, 폭력, 음란 정보를 전파하고 허위 정보를 날조하고 전파하여 경제 질서와 사회질서를 교란시키고, 타인의 명예, 개인 정보, 지식 재산권과 기타 합법적 권익을 침범하는 등 활동에 가담해서는 안 된다(제12조).

⑦ 미성년자에게 안전하고 건강한 네트워크 환경 제공

국가는 미성년자의 건강한 성장에 도움이 되는 네트워크 제품과 서비스를 연구 개발할 수 있도록 지원하고, 법에 따라 네트워크를 이용하여 미성년자의 심신 건강을 해칠 수 있는 활동을 엄벌하며, 미성년자에게 안전하고 건강한 네트워크 환경을 제공한다(제13조).

나. 국가의 네트워크 정보 부서의 임무

국가의 네트워크 정보 부서의 임무는 네트워크 보완 업무와 관련 감독 관리 업무의 총괄·조절이다. 즉, 국가의 네트워크 정보 부서에서 네트워크 보

완 업무와 관련 감독 관리 업무를 총괄하여 조절하는 것을 책임진다. 국무원 산하의 정보 통신 주관 부서, 공안 부서와 기타 관련 기관에서 본 법과 관련 법률, 행정 법규의 규정에 의거하여 각자의 직책 범위 내에서 사이버 보안 보호와 감독 관리 업무를 책임진다. 현급(県級)이상의 지방 인민 정부 관련 부서의 네트워크 보안 보호와 감독 관리 책임은 국가의 관련 규정에 의해 확정된다(제8조).

다. 네트워크 운영자의 의무

네트워크 운영자의 의무에 관한 사항으로는 ① 네트워크 보안 보호 의무를 이행 ② 네트워크의 안전하고 안정적인 운영 보장 ③ 네트워크 보안 보호 지도의 강화 ④ 어떤 개인이나 조직에서 네트워크 보안을 해치는 행위에 대해 정보 보안, 통신 보안, 공안 등 부서에 신고 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 네트워크 보안 보호 의무를 이행

네트워크 운영자는 경영과 서비스 활동을 진행함에 있어 반드시 법률, 행정 법규를 준수하고, 사회의 공공 도덕을 존중하며, 성실히 상업도덕과 신용을 지키며, 네트워크 보안 보호 의무를 이행하고, 정부와 사회의 감독을 받으며 사회의 책임을 부담한다(제9조).

② 네트워크의 안전하고 안정적인 운영 보장

네트워크를 건설하고 운영하거나 네트워크를 통해 서비스를 제공하는데 있어 법률, 행정 법규의 규정과 국가 기준의 강제적 요구에 따라 기술 조치와 그 밖의 필요한 조치를 취하여 네트워크의 안전하고 안정적인 운영을 보장하고, 네트워크 보안 사고에 효과적으로 대응하며, 사이버 불법 범죄 활동을 방지하고, 네트워크 데이터의 완전성, 기밀성, 가용성을 보호하여야 한다(제10조).

③ 네트워크 보안 보호 지도의 강화

사이버 관련 업종은 규정에 따라 업종의 자체 단속을 강화하고 네트워크

안정 행위 규범을 제정하며, 회원에게 네트워크 보안 보호 지도를 강화하고, 네트워크 보안 보호 수준을 향상시켜 업종의 건강한 발전을 촉진시킨다(제11조).

④ 어떤 개인이나 조직에서 네트워크 보안을 해치는 행위에 대해 정보 보안, 통신 보안, 공안 등 부서에 신고

어떤 개인이나 조직에서 네트워크 보안을 해치는 행위에 대해 정보 보안, 통신 보안, 공안 등 부서에 신고할 권리가 있다. 신고를 받은 부서에서는 즉각 법에 따라 처리를 하고; 본 부서의 직책에 속하지 않은 사안에 대해서는 즉시 처리할 수 있는 권리가 있는 부서로 이전시켜야 한다. 관련 부서에서는 신고자의 관련 정보에 대해 기밀을 유지하고 신고인의 합법적 권익을 보호한다(제14조).

3) 네트워크 보안 지원과 촉진

가. 사이버보안 표준 체계 등의 수립

국가는 사이버보안 표준 체계를 수립하고 완전하게 한다. 국무원 산하 표준화 행정 주관 부서와 국무원의 그 밖의 관련 부서는 각자의 직책에 따라 네트워크 보안 관리 및 네트워크 제품, 서비스와 운영 보안과 관련되는 국가 기준과 업계 기준을 제정하고 또 적시에 수정하여야 한다. 국가는 기업, 연구기관, 대학, 네트워크 관련 업계에서 네트워크 보안 국가 기준과 업계 기준의 제정에 참여하는 것을 지원한다(제15조).

나. 중요 사이버 보안 기술 산업과 프로젝트 사업 등의 지원

국무원과 성, 자치구, 직할시 인민정부는 전면적으로 기획하고 투입을 늘여 중요 사이버 보안 기술 산업과 프로젝트 사업을 지원하고, 네트워크 보안 기술의 연구 개발과 응용을 지원하며, 안전하고 신뢰할 수 있는 네트워크 제품과 서비스를 확대하고, 사이버 기술의 지식 재산권을 보호하며 기업, 연구기관과 대학 등이 국가 네트워크 보안 기술의 혁신 프로젝트에 참여하는 것을 지원한다(제16조).

다. 공공 데이터 자원의 개방 촉진

국가는 네트워크 데이터 보안 보호를 개발하는 것을 장려하고 기술을 이용하여 공공 데이터 자원의 개방을 촉진하며 기술의 혁신과 경제 사회의 발전을 추진한다. 국가는 혁신 네트워크 보안 관리 방식을 지원하고 네트워크 신기술을 활용하여 사이버 보안 보호 수준을 높인다(제18조).

라. 사이버 보안 관련 교육과 훈련 지원 및 사이버 보안 인재 양성

국가는 기업, 대학, 직업학교 등 교육 기관에서 사이버 보안 관련 교육과 훈련을 실시하는 것을 지원하고, 여러 가지 방식을 통해 사이버 보안 인재를 양성하고 사이버 보안 인재의 교류를 촉진시킨다(제20조).

4) 네트워크 운영 보안

가. 일반 규정

일반규정에 관한 사항으로는 ① 네트워크 보안 등급 보호제도의 실행 ② 네트워크 제품, 서비스는 관련 국가 기준의 필수 요구 부합 ③ 네트워크 중요 설비와 네트워크 보안 전용 제품의 판매 및 제공시 보안 인증 또는 보안 테스트 부합성 ④ 네트워크 운영자의 사용자에 대한 서비스 규제 ⑤ 네트워크 운영자의 사이버 보안 사건의 비상 대책 마련 ⑥ 타인의 네트워크에 불법 침입하거나 타인 네트워크의 정상적 기능 방해 금지 ⑦ 네트워크 운영자의 국가 안보와 범죄수사 활동에 대한 기술 지원과 협조 제공의무 ⑧ 네트워크 운영자의 보안 보장 능력의 향상 ⑨ 네트워크 보안 보호 직책을 이행시 획득한 정보의 용도외 사용 금지 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 네트워크 보안 등급 보호제도의 실행

국가는 네트워크 보안 등급 보호제도를 실행한다. 네트워크 운영자는 네트워크 보안 등급 보호제도의 요구에 따라 아래(1. 내부 보안 관리 제도와 조작 규정을 제정하고 네트워크 안전 책임자를 확정하여 사이버 보안 보호 책임을 실행한다. 2. 컴퓨터 바이러스와 네트워크 공격, 네트워크 침입 등 네트워크 보안을 해치는 행위로부터 보호하는 기술 조치를 취한다. 3. 네트워크 운행

상태와 네트워크 보안 사건을 기록하고 모니터링 할 수 있는 기술 조치를 취하고, 규정에 따라 관련 네트워크 일지를 6개월 이상 보관한다. 4. 데이터 분류와 중요 데이터 백업 및 암호화 등 조치를 취한다. 5. 법률과 행정 규정에서 규정한 그 밖의 의무)와 같은 보안 보호 의무를 이행하여 네트워크 간섭, 파괴 또는 권한이 부여되지 않은 접속을 허용하지 않는 것을 보장하고, 네트워크 데이터 유출 또는 절취, 변조를 방지해야 한다(제21조).

② 네트워크 제품, 서비스는 관련 국가 기준의 필수 요구 부합

네트워크 제품, 서비스는 관련 국가 기준의 필수 요구에 부합하여야 한다. 네트워크 제품, 서비스의 제공자는 악성 프로그램을 설치해서는 안 되고; 해당 네트워크 제품, 서비스에 안전 결함, 취약점 등 위험이 있다는 것을 발견하였을 경우 즉시 보완 조치를 취한 후 규정에 따라 즉시 사용자에게 고지하고 또 관련 주관 부서에 보고해야 한다. 네트워크 제품, 서비스 제공자는 네트워크 제품 서비스에 대해 지속적으로 보안 유지 보호를 제공하고; 규정되었거나 당자사가 약정한 기간 내에 보안 유지 제공을 중지해서는 안 된다. 사용자의 정보를 수집하는 기능을 가지고 있는 네트워크 제품, 서비스는 반드시 사용자에게 명시하고 또 동의를 얻어야 한다; 사용자 개인 정보에 관련되는 경우에는 본 법과 관련 법률, 행정 법규에서 개인 정보 보호에 관한 규정을 지켜야 한다(제22조).

③ 네트워크 중요 설비와 네트워크 보안 전용 제품의 판매 및 제공시 보안 인증 또는 보안 테스트 부합성

네트워크 중요 설비와 네트워크 보안 전용 제품인 경우, 관련 국가 기준의 필수 요구에 따라 자격을 갖춘 기관에서 보안 인증 혹은 보안 테스트 요구에 부합한 후에야 판매 혹은 제공이 가능하다. 국가 인터넷 통신 부서는 국무원의 관련 부서와 함께 네트워크 중요 설비와 네트워크 보안 전용 제품 목록을 제정하고 발표하며 보안 인증 및 보안 검사의 결과를 서로 인정하여 중복 인증과 테스트를 피한다(제23조).

④ 네트워크 운영자의 사용자에 대한 서비스 규제

네트워크 운영자는 사용자를 위해 네트워크 접속, 도메인 등록 서비스, 유선전화, 무선 전화 등 접속 절차를 처리하고 또는 사용자에게 정보의 발표, 실시간 통신 등 서비스를 제공한다. 사용자와의 계약 체결 혹은 서비스 제공을 확인할 경우에는 사용자에 실제 신분 정보를 제공할 것을 요구한다. 사용자가 신분 정보를 제공하지 않을 경우 네트워크 운영자는 해당 사용자에게 관련 서비스를 제공해서는 안된다. 국가는 네트워크 신뢰 가능한 신분 전략을 실시하여 안전하고 편리한 전자 신분 인증 기술의 연구 개발을 지원하고 각 전자 신문 인증 사이의 상호 인증을 추진한다(제24조).

⑤ 네트워크 운영자의 사이버 보안 사건의 비상 대책 마련

네트워크 운영자는 사이버 보안 사건의 비상 대책을 마련하여 시스템 약점, 컴퓨터 바이러스, 네트워크 공격, 네트워크 침입 등 안전 위험을 즉시 처리한다; 네트워크 안전 사건이 발생할 경우 비상 대책을 즉시 가동하고 그에 해당하는 보완 조치를 취하여야 하며 규정에 따라 관련 주관 부서에 보고를 한다(제25조). 네트워크 보안 인증, 테스트, 위험 평가 등 활동을 진행하고 시스템 약점, 컴퓨터 바이러스, 네트워크 공격, 네트워크 침입 등 네트워크 보안 정보를 사회에 발표할 경우 국가의 관련 규정을 지켜야 한다(제26조).

⑥ 타인의 네트워크에 불법 침입하거나 타인 네트워크의 정상적 기능 방해 금지

어떤 개인이나 조직에서도 타인의 네트워크에 불법 침입하거나 타인 네트워크의 정상적 기능을 방해하고, 또 네트워크 데이터를 훔치는 등 네트워크 보안을 위협하는 프로그램, 도구를 제공해서는 안 된다. 타인이 네트워크 보안에 해를 끼치는 활동을 하고 있는 것을 알면서도 그에게 기술지원, 광고 확대, 지급 결제 도움을 제공해서는 안 된다(제27조).

⑦ 네트워크 운영자의 국가안보와 범죄수사 활동에 대한 기술 지원과 협조 제공의무

네트워크 운영자는 공안 기관, 국가 안전 기관을 위해 법에 의거하여 국가 안보와 범죄수사 활동에 기술 지원과 협조를 제공해야 한다(제28조).

⑧ 네트워크 운영자의 보안 보장 능력의 향상

국가는 네트워크 운영자 사이의 네트워크 보안 정보의 수집, 분석, 통보와 응급 처치 등 협력하는 것을 지원하여 네트워크 운영자의 보안 보장 능력을 향상시킨다. 관련 분야 조직은 해당 분야의 네트워크 보안, 보호 규범과 협력 체제를 갖추고 네트워크 보안 위험에 대한 분석 평가를 강화하며, 정기적으로 회원들에게 위험 경고를 진행하고, 회원들이 네트워크 보안 위험에 대한 대응을 지원한다(제29조).

⑨ 네트워크 보안 보호 직책을 이행시 획득한 정보의 용도외 사용 금지

인터넷 통신 부서와 관련 부서에서 네트워크 보안 보호 직책을 이행하면서 획득한 정보는 네트워크 보안의 필요에 의한 경우에 사용되어야 하며, 그 밖의 용도로 사용되어서는 안 된다(제30조).

나. 중요 정보 인프라의 운영 보안

중요 정보 인프라의 운영 보안에 관한 사항으로는 ① 중요 정보 인프라에 대한 네트워크 보안 등급 보호 제도와 중점적인 보호의 실행 ② 중요 정보 인프라의 운영 보안 보호 업무를 지도 및 감독 ③ 중요 정보 인프라의 구축의 업무 안정성 및 지속적 운영성능 구비 ④ 중요 정보 인프라의 운영자의 보안 보호 의무 이행 ⑤ 중국 국내에서 운영하면서 수집하고 생성된 개인 정보와 중요 데이터의 중국 국내 저장 의무 ⑥ 중요 정보 인프라의 운영자의 네트워크의 보안성에 대한 검사와 평가 의무 ⑦ 국가 인터넷 부서의 중요 정보 인프라의 보안 보호 조치 의무 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 중요 정보 인프라에 대한 네트워크 보안 등급 보호 제도와 중점적인 보호의 실행

국가는 공공 통신과 정보 서비스, 에너지, 교통, 수력, 금융, 공공 서비스,

전자 민원 등 중요한 업계와 분야가 파괴되었거나 기능을 상실하였거나 혹은 데이터가 유출이 되어 국가 안보, 국민 생계, 공공 이익에 심각한 해를 끼치게 될 수 있는 중요 정보 인프라에 대해 네트워크 보안 등급 보호 제도를 바탕으로 중점적인 보호를 실행한다. 중요 정보 인프라의 구체적인 범위와 안보 보호 방법은 국무원에서 제정한다. 국가는 중요 정보 인프라 외의 네트워크 운영자가 자발적으로 중요 정보 인프라 보호 체계에 참여하는 것을 장려한다(제31조).

② 중요 정보 인프라의 운영 보안 보호 업무를 지도 및 감독

국무원에서 규정한 직책 분담에 따라 중요 정보 인프라 보안 보호 업무를 책임지는 부서에서는 해당 업계, 해당 분야의 중요 정보 인프라 보안 기획을 편성하고 또 실시하며 중요 정보 인프라의 운영 보안 보호 업무를 지도하고 감독한다(제32조).

③ 중요 정보 인프라의 구축의 업무 안정성 및 지속적 운영성능 구비

중요 정보 인프라의 구축은 업무를 안정적이고 지속적으로 운영하게 하는 성능을 구비하여야 하고 보안 기술 조치의 동시 기획, 동시 구축 및 동시 사용을 보장하여야 한다(제33조).

④ 중요 정보 인프라의 운영자의 보안 보호 의무 이행

본 법안의 제21조 규정 외에 중요 정보 인프라의 운영자는 다음(1. 전문적인 보안 관리 기관과 보안 관리 책임자를 지정하고 책임자와 중요 직위에 있는 관계자에 대해 보안 배경을 심사한다. 2. 정기적으로 해당 인력에 대해 네트워크 보안 교육과 기술 훈련 및 기능 심사를 진행한다. 3. 중요 시스템과 데이터 베이스에 대해 재난 대비 백업을 진행한다. 4. 네트워크 보안 사건의 비상 대책을 정하고 정기적으로 조직적인 훈련을 실시한다. 5. 법률, 행정 법규에서 규정한 기타 의무를 지킨다.)과 같은 보안 보호 의무를 이행하여야 한다(제34조). 중요 정보 인프라 운영자는 네트워크 제품과 서비스를 구매할 때 국가 안보에 영향을 미칠 수 있는 경우에는 국가 인터넷 통신 부서와 국무

원 관련 부서에서 조직한 국가 보안 심사를 거쳐야 한다(제35조). 중요 정보 인프라 운영자는 네트워크 제품과 서비스를 구매할 때 반드시 규정에 따라 제공자와 보안 유지 계약을 체결하여 기밀 유지 의무와 책임을 명확하게 한다(제36조).

⑤ 중국 국내에서 운영하면서 수집하고 생성된 개인 정보와 중요 데이터의 중국 국내 저장 의무

중요 정보 인프라의 운영자는 중화인민공화국 국내에서 운영하면서 수집하고 생성된 개인 정보와 중요 데이터는 국내에 저장하여야 한다. 업무 수요에 의해 외국에 제공하여야 할 경우, 국가 인터넷 통신 부서와 국무원 관련 부서에서 제정한 방법에 따라 보안 평가를 진행하여야 하고; 법률, 행정 법규에서 별도의 규정이 있을 경우는 해당 규정에 따른다(제37조).

⑥ 중요 정보 인프라의 운영자의 네트워크의 보안성에 대한 검사와 평가 의무

중요 정보 인프라의 운영자는 반드시 자체적으로 혹은 네트워크 보안 서비스 기관에 의뢰하여 네트워크의 보안성 및 존재할 수 있는 위험에 대해 해마다 최소 1회씩 검사와 평가를 진행하고 검사 결과와 개선 조치를 중요 정보 인프라 보안 보호 업무의 관련 부서에 제출한다(제38조).

⑦ 국가 인터넷 부서의 중요 정보 인프라의 보안 보호 조치 의무

국가 인터넷 부서에서는 관련 부서의 협조를 총괄하여 중요 정보 인프라의 보안 보호에 대해 아래(1. 중요 정보 인프라의 보안 위험에 대해 표본 검사를 진행하고 개선 조치를 제출하여 필요시 네트워크 보안 서비스 기관에 의뢰하여 네트워크에 존재하는 보안 위험에 대한 검사 평가를 진행한다. 2. 중요 정보 인프라 운영자는 정기적으로 네트워크 보안 비상 훈련을 조직하여 네트워크 안전 사건에 대응하는 수준과 협동 능력을 기른다. 3. 관련 부서, 중요 정보 인프라의 운영자 및 관련 연구기관, 네트워크 보안 서비스 기관 등 사이의 네트워크 안전 정보의 공유를 촉진한다. 4. 네트워크 보안 사건의 비상

대책 및 네트워크 기능의 복구 등에 대해 기술지원과 협조를 제공한다)와 같은 조치를 취한다(제39조).

5) 네트워크 정보보안

가. 네트워크 운영자의 개인정보보호 의무

네트워크 운영자의 개인정보보호 의무에 관한 사항으로는 ① 수집한 사용자 정보에 대한 보안 유지와 완전한 사용자 정보 보호 제도의 수립 의무 ② 수집 및 사용하는 개인 정보의 합법적이고 정당하며 필요한 원칙에의 부합 의무 ③ 수집한 개인정보의 무단 유출 등 금지 및 피수집자의 동의 없이 제3자에 대한 제공 금지 ④ 정보주체의 정정요구에 따른 해당 정보의 삭제 및 정정 의무 ⑤ 개인 정보의 불법획득 금지 및 해당 정보의 불법 판매와 제3자 제공 금지 의무 ⑥ 직책 이행에서 알게 된 개인 정보등 기밀 유지 의무 ⑦ 자신이 사용하는 네트워크의 행위에 대한 책임 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 수집한 사용자 정보에 대한 보안 유지와 완전한 사용자 정보 보호 제도의 수립 의무

네트워크 운영자는 수집한 사용자 정보에 대해 철저히 보안을 유지하고 완전한 사용자 정보 보호 제도를 수립한다(제40조).

② 수집 및 사용하는 개인 정보의 합법적이고 정당하며 필요한 원칙에의 부합 의무

네트워크 운영자가 수집하고 사용하는 개인 정보는 합법적이고 정당하며 필요한 원칙에 부합하여야 한다. 이 정보는 공개적으로 수집하고 규칙적으로 사용하며, 정보를 수집, 사용하는 목적, 방식 그리고 범위를 명시하고 피 수집자의 동의를 얻어야 한다. 네트워크 운영자는 제공하는 서비스와 무관한 개인정보를 수집해서는 안 되고 법률, 행정 법규의 규정과 양자의 약정을 위반하여 개인정보를 수집하고 사용해서는 안 되며, 법률, 행정 법규의 규정 또는 사용자와의 약정에 의거하여 보존하고 있는 개인 정보를 취급한다(제41조).

③ 수집한 개인정보의 무단 유출 등 금지 및 피수집자의 동의 없이 제3자에 대한 제공 금지

네트워크 운영자는 수집한 개인정보를 함부로 유출, 훼손, 수정해서는 안 되며 피수집자의 동의 없이 제3자에게 개인 정보를 제공해서는 안 된다. 하지만 특정 개인 식별이 어렵고 또 복원 불가능한 경우는 제외된다. 네트워크 운영자는 반드시 기술 조치와 그 밖의 필요한 조치를 취하여 수집한 개인 정보의 보안을 확보해야 하고 정보의 유출, 훼손, 분실을 방지한다. 개인 정보의 유출, 훼손, 분실 상황이 발생하였거나 발생할 가능성이 있을 경우에는 반드시 즉시 보완 조치를 취해야 하고 규정에 따라 사용자에게 알리고 관련 부서에 보고한다(제42조).

④ 정보주체의 정정요구에 따른 해당 정보의 삭제 및 정정 의무

개인이 네트워크 운영자가 법률, 행정 법규의 규정 또는 양측의 약정을 위반하여 자신의 개인 정보를 수집하고 사용하였을 경우, 네트워크 운영자에게 정정 요구를 할 권리가 있으며 네트워크 운영자는 조치를 취하여 해당 정보를 삭제하거나 정정하여야 한다(제43조).

⑤ 개인 정보의 불법획득 금지 및 해당 정보의 불법 판매와 제3자 제공 금지 의무

어떤 개인이든 조직에서 절취 혹은 기타 불법적인 방식으로 개인 정보를 획득할 수 없고 해당 정보를 불법 판매하거나 제3자에게 제공해서는 안된다(제44조).

⑥ 직책 이행에서 알게 된 개인 정보등 기밀 유지 의무

법에 따라 네트워크 안전 감독 관리 직책을 담당하고 있는 부서 및 실무자는 반드시 직책 이행에서 알게 된 개인 정보, 프라이버시와 상업 비밀에 대해 기밀 유지를 해야 하고 관련 정보를 유출, 판매 혹은 불법적으로 타인에게 제공해서는 안 된다(제45조).

⑦ 자신이 사용하는 네트워크의 행위에 대한 책임

어떤 개인이나 조직에서든 자신이 사용하는 네트워크의 행위에 대해 책임을 지고 사기 행각이나 범죄 방법 전수, 금지 물품, 관리 물품 등을 제작하고 판매하는 범죄 사이트, 통신 그룹을 설립해서는 안 된다. 또 네트워크를 이용하여 사기, 금지 물품과 관리물품의 제작, 판매 및 기타 불법 범죄 활동의 정보를 퍼뜨려서는 안 된다(제46조).

나. 네트워크 운영자의 네트워크 정보보안 의무

네트워크 운영자의 네트워크 정보보안 의무에 관한 사항으로는 ① 사용자가 발표한 정보에 대한 관리 강화 ② 모든 개인과 조직에서 발송한 전자 정보, 제공한 응용 소프트웨어에의 악성 프로그램 설치 금지 ③ 네트워크 정보보안 클레임, 신고 제도 수립 의무 ④ 법령에서 발표 또는 전송을 금지한 정보를 발견할 경우 네트워크 운영자에 대한 전송 중지 요구 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 사용자가 발표한 정보에 대한 관리 강화

네트워크 운영자는 사용자가 발표한 정보에 대한 관리를 강화하고 법률, 행정 법규에서 금지한 정보를 발표하거나 전송하는 경우를 발견할 경우 즉시 해당 정보의 전송을 정지하고 제거 등의 처치를 취하여 정보의 확산을 방지하고, 관련 기록을 보존하여 주관부서에 보고를 올린다(제47조).

② 모든 개인과 조직에서 발송한 전자 정보, 제공한 응용 소프트웨어에의 악성 프로그램 설치 금지

모든 개인과 조직에서 발송한 전자 정보, 제공한 응용 소프트웨어에는 악성 프로그램을 설치해서는 안 되고 법률, 행정 법규에서 발표 혹은 전송 금지한 정보를 포함하여서는 안 된다. 전자 정보 발송 서비스 제공자와 소프트웨어 다운로드 서비스 제공자는 반드시 보안 관리 의무를 이행하되, 사용자가 위 조항에서 규정한 행위가 있는 인지할 경우 즉시 서비스 제공을 정지하고 제거하는 등의 조치를 취한다. 또 관련 기록을 보존하여 주관 부서에 보고한

다(제48조).

③ 네트워크 정보 보안 클레임, 신고 제도 수립 의무

네트워크 운영자는 반드시 네트워크 정보 보안 클레임, 신고 제도를 수립하고 클레임, 신고방식 등 정보를 공개하며 네트워크 정보 보안에 관한 신고 사항들을 즉시 처리한다. 네트워크 운영자는 인터넷 통신 부서와 관련 부서의 감독과 검사 실시에 협조해야 한다(제49조).

④ 법령에서 발표 또는 전송을 금지한 정보를 발견할 경우 네트워크 운영자에 대한 전송 중지 요구

국가 인터넷 통신 부서와 관련 부서는 법에 따라 네트워크 보안 감독관리 직책을 이행하되, 법률, 행정 법규에서 발표 또는 전송을 금지한 정보를 발견할 경우 네트워크 운영자에게 전송 중지 요구를 해야 하고 또 제거 등의 조치를 취하면서 관련 기록은 보존하여야 한다. 또 국외에서 온 상기 정보들에 대해서는 관련 기관에 통보하여 기술적 조치와 그 밖의 필요한 조치를 취하여 전파를 막는다(제50조).

6) 모니터링 경보와 비상조치

모니터링 경보와 비상조치에 관한 사항으로는 ① 국가: 네트워크 보안 모니터링 경로와 정보 통보 제도의 수립 ② 국가 인터넷 통신 부서: 관련 부서의 통합과 네트워크 보안 정보의 수집, 분석과 통보 업무 강화 ③ 중요 정보 인프라 보안 보호 업무를 담당하는 부서: 네트워크 보안 모니터링 경보 제도의 보고 ④ 국가 인터넷 통신 부서: 완전한 네트워크 보안 위험 평가와 비상 업무 체제의 수립 ⑤ 성급 이상의 인민정부의 관련 부서: 네트워크 보안 위험에 대한 모니터링 강화 등 조치 ⑥ 네트워크 보안 사건으로 인해 돌발 사건 혹은 생산 안전 사고가 발생 한 경우의 조치 ⑦ 중대한 돌발 안전 사건의 처리가 필요할 경우 네트워크 통신에 제한 조치 등 임시 조치 등을 들 수 있다. 차례대로 살펴보면 다음과 같다.

① 국가: 네트워크 보안 모니터링 경로와 정보 통보 제도의 수립

국가는 네트워크 보안 모니터링 경로와 정보 통보 제도를 수립한다(제51조).

② 국가 인터넷 통신 부서: 관련 부서의 통합과 네트워크 보안 정보의 수집, 분석과 통보 업무 강화

국가는 네트워크 보안 모니터링 경로와 정보 통보 제도를 수립한다. 국가 인터넷 통신 부서는 관련 부서를 통합하여 네트워크 보안 정보의 수집, 분석과 통보 업무를 강화하고 규정에 따라 네트워크 보안 모니터링 경보 정보를 일괄적으로 발표한다(제51조).

③ 중요 정보 인프라 보안 보호 업무를 담당하는 부서: 네트워크 보안 모니터링 경보 제도의 보고

중요 정보 인프라 보안 보호 업무를 담당하는 부서에서는 해당 분야, 해당 업계의 네트워크 보안 모니터링 경보와 정보 통보 제도를 수립하고 규정에 따라 네트워크 보안 모니터링 경보 제도를 보고한다(제52조).

④ 국가 인터넷 통신 부서: 완전한 네트워크 보안 위험 평가와 비상 업무 체제의 수립

국가 인터넷 통신 부서는 관련 부서와 협조하여 완전한 네트워크 보안 위험 평가와 비상 업무 체제를 수립하고 네트워크 보안 사건 비상 대비안을 제정하여 정기적으로 훈련을 진행한다. 중요 정보 인프라 보안 보호 업무를 담당하는 부서는 해당 업계, 해당 분야의 네트워크 보안 사건 비상 대비안을 제정하여 정기적으로 훈련을 진행한다. 네트워크 보안 사건 비상 대비안은 사건 발생 후의 위험 수준, 영향 범위 등 요소에 따라 네트워크 안전 사건에 대해 등급을 나누고 또 그에 상응한 비상 조치를 규정한다(제53조).

⑤ 성급 이상의 인민정부의 관련 부서: 네트워크 보안 위험에 대한 모니터링 강화 등 조치

네트워크 보안 사건의 발생 위험이 커질 때 성급(省级) 이상의 인민정부의

관련 부서는 규정된 권한과 절차, 그리고 네트워크 안전 위험의 특징과 초래할 수 있는 피해에 따라 아래(1. 관련 부서, 기관과 인원은 즉시 관련 정보를 수집, 보고하여 네트워크 보안 위험에 대한 모니터링을 강화한다. 2. 관련 부서, 기관, 그리고 전문 인력을 조직하여 네트워크 보안 사건 정보에 대한 분석과 평가를 진행하고 사건 발생의 가능성, 영향 범위와 피해 수준을 예측한다. 3. 사회에 네트워크 보안 위험 경보를 발표하고 피해를 피하거나 줄이는 조치를 발표한다.)와 같은 조치를 취한다(제54조). 네트워크 보안 사건이 발생하는 즉시 네트워크 안전 사건 비상 대응안을 가동하고 네트워크 보안 사건에 대해 조사와 평가를 진행하며, 네트워크 운영자가 기술조치와 기타 필요한 조치를 취할 것을 요구하여 안전 위험을 제거하고 피해의 확대를 방지하며 즉시 대중들에게 대중들과 관련이 있는 경보 정보를 공시한다(제55조). 성급 이상 인민정부의 관련 부서는 네트워크 보안 감독 관리 업무를 수행할 때 네트워크에 비교적 큰 보안 위험이 존재하거나 보안 사건이 발생한 것을 발견할 경우, 규정된 권한과 절차에 따라 해당 네트워크 운영자의 법적 대리인 혹은 주요 책임자와의 상담을 진행할 수 있다. 네트워크 운영자는 요구에 따라 조치를 취하고 개편을 진행하여 위험을 제거하여야 한다(제56조).

⑥ 네트워크 보안 사건으로 인해 돌발 사건 혹은 생산 안전 사고가 발생한 경우의 조치

네트워크 보안 사건으로 인해 돌발 사건 혹은 생산 안전 사고가 발생 한 경우, <중화인민공화국 돌발사건 대응법>, <중화인민공화국 안전 생산법> 등 관련 법률, 행정 법규의 규정에 따라 조치할 수 있다(제57조).

⑦ 중대한 돌발 안전 사건의 처리가 필요할 경우 네트워크 통신에 제한 조치 등 임시 조치

국가 안보와 사회 공공 질서를 유지하기 위하여 중대한 돌발 안전 사건의 처리가 필요할 경우, 국무원의 결정 혹은 인가를 거쳐 특정 구역에서 네트워크 통신에 제한 조치 등 임시 조치를 취할 수 있다(제58조).

7) 그 밖의 사항

국가 기밀과 관련된 정보를 저장하고 처리하는 네트워크의 운행 보안 보호는 본 법안을 준수하는 것 외에 반드시 비밀유지 관련 법률과 행정 법규의 규정도 함께 지켜야 한다(제77조).

군사 네트워크의 보안 보호는 중앙 군사 위원회에서 별도로 규정한다(제78조).

8) 소결

위에서 살펴 본 사이버안전법의 법적 함의를 정리하면 첫째, 중요정보인프라에 대한 보안심사와 안전평가, 둘째, 온라인 실명제 도입, 셋째, 인터넷 검열 및 정부당국 개입 명문화, 넷째, 네트워크 운영자의 불법정보 차단 및 전달 금지 의무화, 다섯째, 네트워크(인터넷) 관련 제품 또는 서비스에 대한 규제 등이라 할 수 있다.[23]

가. 중요정보인프라에 대한 보안심사와 안전평가

① 사이버안전법은 통신・방송, 에너지, 교통, 금융, 의료 등의 네트워크 안전과 관련되는 정보인프라시설을 '중요정보인프라(關鍵信息基礎施設)'로 정의하고 각종 보안심사와 안전평가를 받아야 한다고 규정하고 있다(제35~제38조).

② 공공통신 및 정보서비스, 에너지, 교통, 수리시설, 금융, 공공서비스, 전자정부 등 중요한 분야와 기능파괴 또는 데이터 유출 시 국가안전과 공공이익에 영향을 미치는 정보통신 시설을 '중요정보인프라시설'로 규정하고 있다(제31조).

③ 중요정보인프라 보안방법은 최고행정부처인 국무원에서 정하고(제31조), 이들 시설들은 안전보호 의무 이행, 네트워크 제품 및 서비스 구매 시 보안 심사, 매년 안전 평가 및 보고 등의 규제를 받아야 한다(제38조).

23) 정진우, "中 사이버보안법 시행 예정, 인터넷 단속 강화된다"「KOTRA해외시장뉴스」 2016년 11월 28일자 기사 참조

④ 중요정보인프라시설 네트워크 운영자는 보안제품의 작동 방식을 중국 정부에 공개해야 하고, 데이터를 중국 현지 서버에 저장하여야 한다(제37조).

나. 온라인 실명제 도입

① 인터넷 서비스를 제공하는 네트워크 운영자는 통신망 가입 수속이나 정보 공개 서비스의 제공을 위해 이용자의 실제 신분정보를 제공하여야 한다.

② 제공받은 개인정보 보호제도를 마련하고 개인정보를 수집하고 이용할 때는 합법적이어야 하며 목적, 방식, 범위 등을 명시하며 사용자 동의를 받도록 규정하고 있다(제41조).

③ 특히 중요정보인프라와 관련되는 개인정보를 저장할 경우 반드시 중국 현지 서버에 저장해야 한다(제37조).

다. 인터넷 검열 및 정부당국 개입 명문화

① 「사이버안전법」은 당국에 국외에서 들어오는 인터넷 정보를 네트워크 운영자 등을 통해 규제하거나 삭제할 수 있는 권한을 부여하고 있다(제50조).

② 네트워크 운영자 등이 당국에 기술 제공과 수사에 협력하는 것을 의무화하고(제28조), 돌발 사태가 발생시 특정지역의 통신을 제한한다는 규정도 포함하고 있다(제58조).

③ 또한 '국가정권과 사회주의제도 전복, 국가분열 선동, 국가통일 파괴, 테러와 극단적 민족주의 선양, 음란물과 허위정보 전파 등 행위를 금지한다'고 명시하고 있다(제12조).

라. 네트워크 운영자의 불법정보 차단 및 전달 금지 의무화

① 네트워크 운영자는 불법정보를 발견하면, 전송 중단, 제거, 확산 방지, 기록 보관 등의 조치를 수행하고 유관기관에 보고하여야 한다(제47조).

② 전자정보와 소프트웨어 제공자의 상품에 악의적인 프로그램을 포함하거나 불법정보를 발표와 전달을 금지하였다(제48조).

③ 나아가 네트워크 운영자의 수사기관 협조를 의무화하고(제28조), 주관부처는 국가 안전, 사회질서 유지 등을 위하여 네트워크 운영자에게 그 사용을 제한하는 임시조치를 내릴 수 있도록 하였다(제58조).

마. 네트워크(인터넷) 관련 제품 또는 서비스에 대한 규제

① 네트워크(인터넷) 관련 제품과 서비스는 중국 국가표준의 강제규정에 부합하여야 하며, 악성 프로그램 설치를 금지하였다(제22조).

② 제품 및 서비스가 사용자의 정보를 수집하는 기능이 있을 경우, 이에 대한 지속적인 보안 유지와 약정 기간내 보안 유지를 지속하여야 한다.

③ 네트워크(인터넷) 관련 제품과 서비스의 핵심설비 및 전문제품은 국가표준의 강제성 기준에 부합해야 하며, (이 표준에 통과된 이후) 판매(혹은 제공) 가능하다.

(5) 국가안전법의 제정

중국이 지난 7월 1일 새로운 「국가안전법」 제정을 계기로 온라인과 정보보안 능력을 키울 것이라는 관측이 나오고 있다. 새 「국가안전법」은 2014년 중국 정부가 창설한 중앙국가안전위원회의 활동 근거가 되는 것으로 2017년 6일부터 시행에 들어갔다. 새로운 「국가안전법」은 지난 1993년 제정된 기존 「국가안전법」의 대체입법이다.

모두 7장으로 이뤄진 새 「국가안전법」은 정치 안전, 국토 안전, 군사 안전, 문화 안전, 과학기술 안전 등 11개 영역에서 국가 안전을 수호하는 것에 관한 임무와 책임을 규정했다. 또 국가안전 제도, 국가안전 보장, 국민과 조직의 의무와 권리 등을 명시하고 있다. 이 법은 국가는 국가안전의 수호를 위해 자주 창신 능력 건설을 강화해야 하며, 자주적으로 통제 가능한 전략적 첨단 신기술, 중요한 영역의 핵심기술의 발전을 가속화해야 한다고 요구했다. 새 「국가안전법」은 또 지식재산권의 운용·보호 및 과학기술 비밀보호 능력 건설을 강화하고, 중대한 기술과 공정의 안전을 보장해야 한다고 강조했다. 제정이유로는 현대 국가의 안보는 엄중한 위협과 도전에 직면하고 있

고, 특히 테러와 사이버 해킹 등 예측 불가능한 영역에서 (안보)위협이 더욱 커지고 있다는 것을 들 수 있다. 새 「국가안전법」이 '사이버 안전' 강화에 중점을 뒀다는 것이 일반적인 평가이다. 실제로 새 「국가안전법」은 국가가 네트워크와 정보 안전을 보장하는 체계를 구축하고, 네트워크와 정보안전 보호 능력을 향상시키며, 네트워크와 정보기술의 혁신 연구·개발 응용을 강화해야 한다고 명시했다. 새 법은 또 네트워크와 정보 핵심기술, 핵심 기초시설과 중요 영역 정보시스템 및 데이터의 안전에 대한 통제 가능성을 실현해야 한다고 강조했다.

하지만 중국 일각에서는 새 「국가안전법」이 국가안보 적용 범위를 크게 넓힌 까닭에 개인의 자유 억압, 이념 통제 등 사회에 전방위적인 통제를 가할 것이란 우려도 나오고 있다. 지난 1993년에 제정된 「국가안전법」은 안보 위협의 범위와 법 적용 범위를 국가 전복과 분열 선동, 매국 행위, 국가기밀 누설 등으로 규정했다. 그러나 새 「국가안전법」은 이 범위를 경제, 금융, 문화, 인터넷, 식량, 에너지, 종교, 우주, 심해, 극지방 등으로까지 넓혔다.[24]

2. 시사점

중국은 네트워크와 인터넷을 포함한 뉴미미어 전반에 대해 엄격한 규제를 가하고 있다. 1996년 「국제 컴퓨터 네트워크 관리에 관한 잠정규정(1997년 개정)」을 시작으로 다양한 인터넷 관련 규제제도를 정비해 왔다.[25] 2000년 「전국인민대표회의 상무위원회 인터넷 보안에 관한 결정」에서는 인터넷상의 유언비어 유포나, 유해정보 게시, 체제에 위협되는 정보의 통제를 규정하였으며, 「인터넷 정보서비스 관리방법」에서는 인터넷 정보서비스 진입 및 허가 조건을 명시하였다. 또한 2005년에는 「인터넷 뉴스 정보서비스 관리규정」을

24) 보안뉴스 2015년 7월 6일자 "'中 새 '국가안전법' 제정…"정보보안 능력 키울 것"" 기사 참조

25) 중국의 사이버공간 규제에 대해서는 김유향, "중국 「네트워크안전법(안)」의 주요 내용과 함의"「이슈와 논점」(제1033호)(국회입법조사처, 2015. 11. 9) 참조

통해 뉴스웹 사이트 규제를 강화하였다.[26] 더불어 2010년 「국가비밀보호법」 개정을 통해 인터넷 및 통신회사가 검열에 참여하도록 강조하였다.

이후 중국정부는 규제의 범위를 새롭게 성장하던 온라인 서비스로까지 확장하였다. 2011년 중동과 아프리카의 민주화 시위 과정에서 '시마 웨이보'(Sina Weibo)를 비롯한 SNS에 대한 규제를 단행한 바 있다. 이후 2014년 8월 7일에는 모바일 메신저 이용에 있어 실명 가입을 강화하고 정치 뉴스를 제한하는 것을 주 내용으로 하는 「인스턴트 메신저 및 대중정보서비스 발전 관리에 관한 점정규정」을 발표했다.

2014년 이후에는 네트워크 보안을 국가안보 차원에서 격상하는 법률이 연이어 정비되었다. 같은 해 발표된 「반테러리즘법(초안)」은 중국정부의 반테러 조사를 돕기 위해 통신 및 인터넷 관련 회사는 소프트웨어에 백도어를 설치하고, 암호키를 제공하도록 하는 규정이 포함되어 있으며, 2015년 7월에 발표된 「국가안전법」은 국가안보의 적용 범위를 인터넷에까지 확장하고 있다. 그리고 2017년 6월 1일부터 시행되는 「사이버안전법」은 이러한 중국의 사이버공간 규제체제를 보다 광범위하면서 체계적으로 정비, 강화하는 계기가 될 것으로 예상된다.[27]

「사이버안전법」은 네트워크 전반을 망라한 규제법으로서 네트워크에 대한 통제를 강화하는 한편, 사이버공격을 방어하고, 중국의 이용자에 관한 정보를 보호하는 정부의 역량 강화를 목표로 하고 있다. 시사점으로는 다음 네 가지를 들 수 있다.

첫째, 대외적으로는 사이버안보에 대한 중국정부의 높은 관심을 보여주고 있다(사이버주권 수호).

둘째, 대내적으로는 중국의 네트워크 보안체계를 종합적으로 정비하려는 전략적 목적을 가지고 있다.

26) 김유향, "중국의 인스턴트 메신저 규제정책과 함의" 「이슈와 논점」(제917호)(국회입법조사처, 2014. 10. 16) 참조
27) 김유향, "중국 「네트워크안전법(안)」의 주요 내용과 함의" 참조

셋째, 현재 국제적으로 쟁점이 되고 있는 국가간 정보 이전 및 저장과 관련하여, 자국민 개인정보를 처리하는 기업은 수집한 데이터를 중국영토 내에 보관해야 하며, 비즈니스 목적으로 해외에 저장한 데이터는 중국정부의 승인이 필요하도록 함으로써 자국데이터에 대한 통제의도를 명확히 밝히고 있다.[28]

넷째, 총괄기구를 정점으로 하는 사이버안보 추진체계를 구축하였다. 「사이버안전법」은 국가인터넷부를 정점으로 하고 국무원의 유관부처와 각 지방인민정부가 소관 사무를 처리하는 사이버안보 추진체계를 구축하도록 하였다. 국가인터넷부의 모체로 추정되는 현행 국가인터넷정보판공실은 국무원 산하기구인 동시에 시진핑 주석을 조장으로 하는 중국공산당의 관련 소조 사무를 담당하며, 이는 당의 권위가 큰 사회주의 국가의 특성을 고려하면 총괄기구로서의 위상을 지니게 될 것이다.[29]

Ⅳ 결 론

지금까지 일본과 중국의 사이버안보 법정책에 대해 살펴보았다. 사이버안보를 국가안보의 중요사항으로 국가적 노력을 경주하고 있음을 확인할 수 있었다.

먼저 일본은 2014년 11월 12일 「사이버안보기본법」을 제정했는데, 이 법률은 사이버안보 분야의 기본법으로서 사이버안보에 대한 실효성을 강화하였다는 평가를 받고 있다. 사이버안보 관련 시책 추진의 기본 이념과 각 주체별 사이버안보 확보의 책무를 정하고 있으며 정부가 사이버안보전략을 수립하도록 하고, 내각에 사이버안보전략본부를 두면서 내각관방이 그 사무를 처

28) 중국의 사이버공간 규제에 대해서는 김유향, "중국 「네트워크안전법(안)」의 주요 내용과 함의" 참조
29) 박상돈・김규동・양정윤, 「2015년도 사이버안보 법제도 연구」(NSR, 2015. 12), 79~80쪽 참조

리하도록 하는 추진체계를 정립하였다. 그 밖에도 「사이버안보기본법」은 사이버안보의 강화에 필요한 다양한 조치들을 정하고 있다.

다음으로 중국은 2015년 7월 중국은 사이버상에서의 공격과 범죄, 유해정보 확산 위협으로부터 사이버주권과 국가안보를 수호하기 위한 「중화인민공화국 네트워크 안전법」(사이버안전법)을 제정하였는데, 입법취지는 네트워크 전반을 망라한 규제법으로서 네트워크에 대한 통제를 강화하는 한편, 사이버공격을 방어하고, 중국의 이용자에 관한 정보를 보호하는 정부의 역량을 강화한다는 것이다. 이 법은 네트워크 보안 지원과 촉진, 네트워크 운영안전(제1절 일반 규정, 제2절 중요 정보 인프라의 운행 안전), 네트워크 정보보안, 모니터링 경보와 비상 대응 등으로 구성되어 있는바, 결과적으로 '사이버 만리장성'을 구축하였다는 평가를 받고 있다. 2017년 6월 1일부터 시행되는 「사이버안전법」은 중국의 사이버공간 규제체제를 보다 광범위하면서 체계적으로 정비, 강화하는 계기가 될 것으로 예상된다.

사이버안보는 정보사회에서 등장한 새로운 국가안보 문제이며 이 역시 민간영역에 대한 제한이 수반될 개연성이 높은 분야이다. 따라서 사이버안보에 관한 규율에 있어서도 연성규범[30]의 남용은 법치국가원리에 위배될 수 있기 때문에 국회의 입법을 통하여 제정된 법률로서 규율하는 것이 더욱 바람직하다.

우리나라의 현행 사이버안보 관련법률은 부문별로 적용범위와 추진체계(대응체계)가 분산되어 있으며 체계완결성이 부족하다. 특히 공공부문의 경우 대통령훈령의 형태로 2005년에 「국가사이버안전관리규정」을 제정하여 규율하는 것이 현재까지 이어져 오고 있는 것은 중대한 문제점이 아닐 수 없

30) 연성규범(soft law)에 대하여는 명확한 정의가 정립되어 있지 않지만, 일반적으로 '직접적으로 법적 강제력을 갖지 않으나 간접적으로 사회구성원의 행위에 실질적인 영향력을 미치기 위하여 만들어진 행위규범의 일종'이라고 볼 수 있다. 즉, 국가에 의하여 규율이 강제되는 경성규범(hard law)에 해당하지 않는 법규범을 총칭하는 것으로 이해할 수 있다. 최난설헌, "연성규범(Soft Law)의 기능과 법적 효력" 「법학연구」 제16집 제2호(인하대학교 법학연구소, 2013) 국문초록 참조

다. 공공부문의 사이버안보에 관한 실질적인 최고규범이 법률이 아닌 대통령 훈령이라는 것은 해당 규범의 효력범위 등에서 태생적 한계를 내포하며 궁극적으로는 법치행정의 원칙[31]에도 부합하지 않는다.[32] 따라서 법률 제정을 통해 궁극적으로 해결할 필요가 있다. 정부입법으로 추진하고 있는 「국가사이버안보 기본법」의 조속한 제정을 기대한다.

31) 법치행정의 원칙에 대해서는 박균성, 「행정법강의」(제13판)(박영사, 2016), 12쪽 이하 참조

32) 박상돈, "정부3.0 성공을 위한 사이버보안의 역할" 「정부3.0시대의 사이버안보」(한국사이버안보법정책학회 2015년 상반기 정기 학술대회 발표문(발표자: 이창범박사)에 대한 토론문, 30쪽 참조

[참고문헌]

강달천, “최근 사이버테러의 현황과 법적 의의 -”「사이버테러와 법정책적 대응」2013년 한국사이버안보법정책학회 정기학술세미나 발제문, 2013. 5. 3

강달천, “사이버 침해사고 현황과 법적 의의”「사이버안보법정책논집」 제1호, 한국사이버안보법정책학회, 2014. 12

곽관훈, “최근 일본의 사이버안보 관련법령 현황과 시사점”「사이버 안보위협 대응전략의 법정책적 검토 및 전망」2013년 한국사이버안보법정책학회 월례세미나 발제문, 2013. 12. 17

권현준, “IOT환경과 사이버안보의 법정책적 문제”「초연결사회와 사이버안보」 2014년 한국사이버안보법정책학회 추계학술대회 발제문, 2014. 11. 28

김성천, “최근 독일의 사이버안보 관련법령 동향과 시사점”「외국의 사이버안보 관련법제 동향 및 법정책적 과제」 2014년 한국사이버안보법정책학회 춘계학술대회 발제문, 2014. 5. 29

김성천, “독일의 사이버보안 법제”「사이버안보법정책논집」 제1호, 한국사이버안보법정책학회, 2014. 12

김성천, “사이버보안 법제에 관한 연구”, 중앙법학 제13집 제3호, 2011. 9

김유향, “중국「네트워크안전법(안)」의 주요 내용과 함의”「이슈와 논점」(제1033호), 국회입법조사처, 2015. 11. 9

김유향, “중국의 인스턴트 메신저 규제정책과 함의”「이슈와 논점」(제917호), 국회입법조사처, 2014. 10. 16

김인중, “사이버안보 추진체계의 이슈와 과제”「사이버안보법정책논집」 제1호, 한국사이버안보법정책학회, 2014. 12

김일환, “독일 기본법상 대테러관련기관과 법제도들에 관한 고찰”「성균관법학」 제15권 제1호(2003)

김재광,「국가 정보보호 추진체계 관련법제 분석」, 한국정보화진흥원, 2009. 12

김재광, “사이버안보의 사회적 인식 제고를 위한 법정책적 개선방안”「사이

버안보법정책논집」 제1호, 한국사이버안보법정책학회, 2014. 12
김재광, “사이버안보 입법환경 변화에 따른 입법전략” 「국가사이버안전을 위한 법적 과제」 2015년 한국사이버안보법정책학회/서울대 공익산업법센터 공동학술세미나 발제문, 2015. 10
김재광, “진화하는 사이버안보 위협과 법제적 대응방안”, 인터넷법제도포럼 발표문, 2016. 7
김재광・김정임, “일본의 사이버위기 관련 법제의 현황과 전망” 「법학논총」 제33권 제1호(2009. 6, 단국대 법학연구소)
김정임, “인도의 IT법제(사이버안보)의 분석과 시사점” 「외국의 사이버안보 관련법제 동향 및 법정책적 과제」2014년 한국사이버안보법정책학회 춘계학술대회 발제문, 2015. 5. 29
김태오, “주요 국가별 사이버안보 대응체계 연구” 「국가사이버안전을 위한 법적 과제」, 한국사이버안보법정책학회・서울대학교 공익산업법센터 2015년 추계 공동학술대회 발제에 대한 토론문, 2015. 10. 22
김현수, 「주요정보기반보호(CIIP) 동향 -미국과 EU를 중심으로-」, 한국법제연구원, 2012. 10
김현수, “국가 사이버안보 법정책의 현황과 인식제고방안 - 미국의 사례를 중심으로 -” 「사이버위협의 현황과 법제도방안」 제1회 한국사이버안보법정책학회 월례세미나 발제문, 2013. 3. 20
박균성, 「행정법강의」(제13판), 박영사, 2016
박상돈・박현동・홍순좌, “미국 사이버보안 입법의 신경향 연구”, 정보보안논문지 제11권 제4호, 2011. 9
박상돈, “정부3.0 성공을 위한 사이버보안의 역할” 「정부3.0시대의 사이버안보」(한국사이버안보법정책학회 2015년 상반기 정기 학술대회 발표문(발표자: 이창범박사)에 대한 토론문, 2015. 6. 25
박상돈, “일본 사이버시큐리티기본법에 대한 고찰: 한국의 사이버안보 법제도 정비에 대한 시사점을 중심으로” 「경희법학」 50권 2호, 경희대 법학연구소, 2015
박상돈・김규동・양정윤, 「2015년도 사이버안보 법제도 연구」, 국가보안기술연구소, 2015, 12

박춘식, “국가사이버안보전략 시급하다”, 디지털타임스 2016년 7월 7일자 시론

손영동, “[손영동의 사이버세상]<6>사이버맹주에 시동 건 일본”, 전자신문 2015년 8월 18일자 칼럼

손영동, “[손영동의 사이버세상]<8>기반기술 국산화 주도하는 중국”, 전자신문 2015년 9월 1일자칼럼

양근원, “사이버테러 대응과 현행 절차법 검토”, 「인터넷법연구」 제3권 제1호, 2004

양정윤・배선하・김규동, 「중국 사이버 역량 현황 연구」(국가보안기술연구소(NSR)), 2015. 12

오승진, “국제법상 사이버공격의 적용가능성”, 한국사이버안보법정책학회 2016 춘계 학술세미나, 2016. 6. 29

윤민우, “국운을 좌우할 제4의 전략공간 사이버스페이스” 한국일보 2015년 10월 19일자 칼럼

이정현, “국가 사이버안보(cyber security) 추진체계의 이슈와 과제” 「사이버안보법정책논집」 제1호, 한국사이버안보법정책학회, 2014. 12

이창범, “국내외 사이버안보관련 법제정 동향과 시사점” 「사이버테러와 법정책적 대응」 2013년 한국사이버안보법정책학회 정기학술세미나 발제문, 2013. 5. 3

정보통신산업진흥원, “초연결 세계에서의 주요국 사이버 보안정책 동향 분석” 「IT R&D 정책동향」, 2012-7

정준현, “국가 사이버안보를 위한 법제 현황과 개선방향” 「디지털 시대와 국가 정보 발전」, 2012

정태진, “주요 국가별 사이버안보 대응체계 연구” 「국가사이버안전을 위한 법적 과제」(한국사이버안보법정책학회・서울대학교 공익산업법센터 2015년 추계 공동학술대회 발표문, 2015. 10. 22

지성우, “독일의 사이버위기 관련 법제의 현황과 전망” 「사이버위기관련 법제의 현황과 전망」, 단국대 법학연구소, 2009. 5. 29

최경진, “정부 조직 개편에 따른 사이버안보법체계 개선방안” 「사이버위협의 현황과 법제도방안」 제1회 한국사이버안보법정책학회 월례세미

나 발제문, 2013. 3. 20
최난설헌, “연성규범(Soft Law)의 기능과 법적 효력” 「법학연구」 제16집 제2호, 인하대학교 법학연구소, 2013
한국인터넷진흥원, 「사이버보안법제 선진화 방안 연구」(방송통신정책연구 11-진흥-라-02), 2011. 12
현대호, “미국의 사이버위기 관련 법제의 현황과 전망” 「법학논총」 제33권 제1호, 단국대 법학연구소, 2009. 6

한국사이버안보법정책학회 정관

제1장 총 칙

제1조 (명칭) 이 학회는 사단법인 한국사이버안보법정책학회(이하 “학회”라 한다)라 칭하고, 영문 명칭은 “Korean Cyber Security Law & Policy Association”(약칭: KCSA)라 한다.

제2조 (목적) 학회는 회원들의 사이버안보법학 및 정책 관련 학문의 연구·발표 응용 활동을 지원함으로써 사이버안보 법학과 정책의 발전과 법치주의의 진작에 기여함을 목적으로 한다.

제3조 (사무소의 소재지) 학회의 사무소는 서울특별시에 둔다.

제4조 (사업) 학회는 그 목적을 달성하기 위하여 다음의 사업을 한다.

1. 사이버안보법 및 정책에 관련된 학술의 연구
2. 연구발표회 및 강연회의 개최
3. 회지 및 그 밖의 간행물의 발행
4. 학회와 목적을 같이 하는 내외 여러 단체와의 제휴
5. 사이버안보법과 정책과 관련한 쟁점에 관한 의견 표명
6. 그 밖의 학회의 목적을 달성함에 필요한 사업

제2장 회 원

제5조 (회원) ① 학회의 회원은 정회원, 준회원, 단체회원, 특별회원으로 한다.

② 정회원은 학회의 목적에 찬동하는 다음의 자로서 정회원 2인 이상의 추천에 의하여 상임이사회의 승인을 얻은 자가 된다.

1. 대학(고등교육법 제2조 각호의 학교 및 동법 제30조의 대학원대학을 포함한다)의 전임강사 이상의 직에 재직하고 있거나 재직하였던 자
2. 사이버안보 법학 및 정책과 관련한 학문을 전공한 박사학위 소지자

3. 국회의원, 판사, 검사, 변호사의 직에 재직하고 있거나 재직하였던 자
4. 사이버안보 관련분야에 5년 이상 재직하고 있거나 재직하였던 자

③ 준회원은 학회의 목적에 찬동하는 다음의 자로서 정회원 2인 이상의 추천에 의하여 상임이사회의 승인을 얻은 자가 된다.

1. 대학원 또는 이에 준하는 연구기관에서 사이버안보법학 및 이에 관련된 분야의 연구에 종사하는 자
2. 사법연수원생과 법학전문대학원생

④ 제3항의 준회원이 제2항 각호의 1에 해당하게 된 때에는 정회원이 된다.

⑤ 단체회원은 국내외의 단체 또는 연구기관으로서 상임이사회의 승인을 얻어 된다.

⑥ 특별회원의 자격은 이 학회의 발전에 크게 기여하거나 기여할 수 있는 국내외의 개인 또는 단체로 한다.

제6조 (권리와 의무) ① 회원은 학회의 제반 사업에 참가할 수 있으며, 이사회가 정하는 바에 따라 입회비 회비를 납부하여야 한다.

② 제8조 제2호에 따른 회장 및 감사 선임을 위한 총회 개최 전까지 학회의 회비를 납부하지 아니한 자는 회원의 권한을 행사할 수 없다.

제7조 (퇴회 및 자격정지) ① 학회의 명예를 훼손하였거나 정관 구 밖에 학회의 규칙을 위반하였을 때에는 이사회의 의결을 거쳐 퇴회시킬 수 있다.

② 회원이 정당한 사유 없이 3년 이상 회비를 납부하지 아니한 때에는 상임이사회의 의결을 거쳐 회원으로서의 자격을 정지시킬 수 있다.

제3장 임 원

제8조 (임원) 학회에 다음의 임원을 둔다.

1. 회장: 1인
2. 법정이사(민법 그 밖의 법령에 의하여 두어야 하는 이사로서, 이사장 1인을 포함한다): 5인
3. 부회장: 5인 내외

4. 상임이사: 30인 내외
5. 이사: 50인 내외
6. 감사: 2인
7. 연구위원: 50 내외
8. 고문: 약간인

제9조 (임원의 선임) ① 회장은 총회에서 부회장 중에서 선임한다.

② 감사는 정회원 중에서 총회가 선임한다.

③ 법정이사는 회장, 부회장, 이사 중에서 회장이 지정하는 자가 되며, 회장인 법정이사는 회장의 직에서 퇴임한 후에도 법정이사의 직을 보유한다.

④ 상임이사 및 이사는 정회원 중에서 총회가 선임한다.

⑤ 부회장은 회장의 제청으로 상임이사회가 선임한다.

⑥ 연구위원은 정회원 중에서 회장이 위촉한다.

⑦ 고문은 역대회장 또는 부회장을 역임한 자 및 사이버안보법정책과 학회발전에 현저한 공로가 있는 자 중에서 총회의 의결을 거쳐 회장이 추대한다.

⑧ 회장은 상임이사 중에서 총무이사, 연구이사, 출판이사, 국제이사, 기획이사, 섭외이사, 재무이사 및 홍보이사 각 약간명을 위촉한다.

제10조 (임원의 임기) ① 회장, 부회장의 임기는 1년으로 하되, 연임할 수 있다.

② 법정이사의 임기는 4년으로 하되, 연임할 수 있다.

③ 상임이사의 임기는 2년으로 하되, 연임할 수 있다.

④ 총무이사, 연구이사, 출판이사, 국제이사, 기획이사, 섭외이사, 재무이사 및 홍보이사의 보직임기는 1년으로 하되 연임할 수 있다.

⑤ 이사의 임기는 3년으로 하되 연임할 수 있다.

⑥ 감사의 임기는 2년으로 하되 연임할 수 있다.

제11조 (임원의 직무) ① 회장은 학회를 대표하고 회무를 통할하며, 법정이사회의 이사장이 된다.

② 부회장은 회장을 보좌하며, 회장이 사고로 인하여 직무를 수행할 수 없을 때에는 부회장 중에서 연장자의 순서로 그 직무를 대행한다. 부회장은 총무

이사 등의 집행이사를 겸직할 수 있다.

③ 총무이사는 학회의 서무를, 연구이사는 학회의 학술연구에 관한 사무를, 출판이사는 학회의 출판사무를, 국제이사는 국제교류에 관한 사무를, 기획이사는 학회의 제반 활동에 관한 기획사무를, 섭외이사는 학회의 섭외활동에 관한 사무를, 재무이사는 학회의 수입·지출 등 제반 회계에 관한 사무를, 홍보이사는 학회의 홍보에 관한 사무를 각각 관장한다.

④ 감사는 다음 각호의 직무를 행하며, 이에 필요한 자료의 제출 또는 의견을 관계임원에 대하여 요구하거나 법정이사회·이사회 또는 상임이사회에서 발언할 수 있다.

1. 학회의 업무와 재산상황을 감사하는 일
2. 제1호의 감사 결과 불법 또는 부당한 점이 있음을 발견한 때 이를 법정이사회·이사회 또는 상임이사회에 보고하는 일
3. 제2호의 보고를 하기 위하여 필요한 때에는 법정이사회·이사회 또는 상임이 사회의 소집을 요구하는 일
4. 감사의 결과를 총회에 보고하는 일

⑤ 연구위원은 회장의 지시를 받아 연구이사 및 출판이사를 보좌하며, 전문분야의 조사·연구에 종사한다.

제12조 (간사) ① 학회에 간사 약간인을 두며, 회장이 이를 임면한다.

② 간사는 회장의 지휘를 받아 학회의 사무를 처리한다.

제13조 (직원) ① 학회에 직원 약간인을 둘 수 있으며, 회장이 이를 임면한다.

② 직원은 회장의 지휘를 받아 서무에 종사한다.

제4장 회 의

제14조 (회의) 학회의 회의는 정기총회·임시총회·법정이사회·이사회 및 상임이사회로 한다.

제15조 (총회의 구성) ① 총회는 정회원과 준회원으로써 구성한다.

② 총회의 의장은 회장이 된다.

제16조 (총회의 권한) 총회는 다음의 사항을 의결한다.

1. 정관의 개정
2. 예산 및 결산의 승인
3. 법정이사회・이사회 및 상임이사회가 부의하는 사항
4. 회원 5인 이상이 제의하는 사항
5. 이 정관에 의하여 총회의 권한으로 되어 있는 사항
6. 그 밖에 필요한 사항

제17조 (총회의 소집) ① 정기총회는 매년 1회 개최하고, 임시총회는 회장이 필요하다고 인정하거나 법정이사회의 의결 또는 정회원 100인 이상의 서면 요구가 있을 때 회장이 이를 소집한다.

② 총회의 소집은 회의 7일전까지 회의의 목적과 일시・장소를 명시하여 공고함으로 써 한다.

제18조 (총회의 의결방법) ① 총회의 의결은 정회원 3분의 1이상의 출석과 출석한 정회원 과반수의 찬성으로써 하며, 가부동수일 때에는 의장이 결정권을 가진다.

② 부득이한 이유로 회의에 불참하는 회원은 서면으로 의결권을 의장 또는 출석하는 다른 회원에게 위임할 수 있으며, 이 경우에는 출석한 것으로 본다.

제19조 (법정이사회・이사회 및 상임이사회의 구성) ① 법정이사회는 법정이사로 구성하고, 회장이 이사장으로서 그 의장이 된다.

② 이사회는 회장・부회장・상임이사・이사로 구성하고, 회장이 그 의장이 된다.

③ 상임이사회는 회장・부회장・상임이사로 구성하고, 회장이 그 의장이 된다.

④ 명예회장 및 고문은 법정이사회・이사회 및 상임이사회에 출석하여 발언할 수 있다.

제20조 (법정이사회・이사회 및 상임이사회의 권한) 법정이사회는 다음의 사항을 심의・결정한다. 다만, 법정이사회는 그 권한을 이사회에 위임할 수 있고, 회장이 필요하다고 인정할 경우에는 이사회의 업무를 상임이사회로 하여금 대행케 할 수 있다.

1. 학회의 목적을 달성하기 위한 각종 사업의 계획과 각종 위원의 선임

2. 학회의 예산·결산 및 재산의 취득·관리·처분에 관한 사항
3. 정관 그 밖의 회칙의 개정안
4. 법령 및 이 정관에 의하여 법정이사회의 권한으로 되어 있는 사항
5. 그 밖에 중요하다고 인정하는 사항

제21조 (법정이사회·이사회 및 상임이사회의 소집) ① 법정이사회는 회장이 필요하다고 인정할 때나 감사 또는 법정이사 3분의 1이상의 요구가 있을 때 회장이 소집한다. 회장은 회의 7일전까지 회의의 목적과 일시·장소를 명시하여 각 법정이사에게 통지하여야 한다.

② 이사회 및 상임이사회는 회장이 소집하되, 회의 3일전까지 회의의 목적과 일시· 장소를 명시하여 함으로써 한다.

제22조 (법정이사회·이사회 및 상임이사회의 의결방법) ① 법정이사회는 법정이사의 과반수의 출석과 출석한 법정이사 과반수의 찬성으로써 의결하며, 가부동수인 때에는 의장이 결정권을 가진다.

② 법정이사회의 의사는 서면결의에 의할 수 없다.

③ 이사회는 이사 과반수의 출석과 출석한 이사 과반수의 찬성으로써 의결하며, 가부동수인 때에는 의장이 결정권을 가진다.

④ 상임이사회는 상임이사 과반수의 출석과 출석한 상임이사 과반수의 찬성으로써 의결하며, 가부동수인 때에는 의장이 결정권을 가진다.

⑤ 회장·법정이사·상임이사·이사가 학회와 이해관계가 상반하는 때에는 당해 사항에 관한 의결에 참여하지 못한다.

제5장 자산, 재정 및 회계

제23조 (재산) ① 학회의 재산은 다음과 같다.

1. 출연금품
2. 회원이 납부한 입회비 및 회비
3. 기금
4. 국가 기타 공공단체의 보조금

5. 기부금 및 찬조금
6. 사업에 따른 수입금
7. 재산으로부터 발생한 과실
8. 그 밖의 수입

② 제1항 제1호와 제3호부터 제5호까지에 해당하는 금품의 접수에 관하여는 상임이사회가 결정한다.

③ 제1항 제2호에 정한 입회비 및 회비의 액수는 상임이사회가 결정한다.

제24조 (재산의 구성) ① 학회의 재산은 이를 기본재산과 보통재산으로 구분한다.

② 다음 각호의 1에 해당하는 학회의 재산은 이를 기본재산으로 하며, 별지 목록의 기재와 같다.

1. 학회의 설립시 기본재산으로 출연한 재산
2. 기부에 의하거나 기타 무상으로 취득한 재산. 다만, 기부목적에 비추어 기부재산으로 하기 곤란하여 주무관청의 승인을
ⓐ 11얻은 것은 예외로 한다.
3. 보통재산 중 총회에서 기본재산으로 편입할 것을 의결한 재산
4. 세계잉여금 중 적립금

③ 보통재산은 기본재산의 원본 이외의 모든 재산으로 한다.

제25조 (재산의 관리) ① 학회 재산의 보존 그 밖의 관리는 회장이 이를 관장한다.

② 회장이 다음 각호의 1에 해당하는 행위를 함에는 법정이사회와 총회의 의결을 거쳐 법령이 정하는 바에 따라 주무관청의 허가를 얻어야 한다.

1. 기본재산의 처분, 임대, 담보제공, 또는 용도변경
2. 제4조 제1호부터 제3호까지 이외의 사업과 관련하여 학회가 의무를 부담하는 행위 또는 학회의 권리를 포기하는 행위(예산으로 총회의 승인을 받은 경우는 제외한다)
3. 기채 또는 금전차입(상임이사회가 정하는 금액의 범위 내에서 당해 회계연도의 수입으로 상환하는 일시차입의 경우는 제외한다)

제26조 (회계원칙) ① 학회의 회계는 모든 회계거래를 발생의 사실에 의하여 기업회계의 원칙에 따라 처리한다.

② 학회의 회계는 관계법령이 정하는 바에 따라 학회의 목적사업경영에 따른 회계와 수익사업경영에 따른 회계로 구분한다.

③ 학회의 회계연도는 정부의 회계연도에 의한다.

제27조 (재산의 평가) 학회의 모든 재산은 취득당시의 시가에 의한다. 다만, 재평가를 실시한 재산은 재평가액으로 한다.

제6장 위원회

제29조 (학회지 편집위원회) ① 학회에 학회지 편집·간행을 위하여 학회지 편집위원회(이하 "위원회"라 한다)를 둔다.

② 위원회는 회장이 위촉하는 위원 10인 이내로 구성하며, 학회지에 게재하고자 하는 논문 심사 및 편집과 간행에 관한 전반적인 사업을 관장한다.

③ 위원회의 구성과 사업에 관한 자세한 사항은 따로 규정으로 정한다.

제30조 (연구윤리위원회) ① 학회에 회원의 연구윤리의 확립과 연구 부정행위 방지 및 검증을 위한 연구윤리위원회(이하 "윤리위원회"라고 한다)를 둔다.

② 윤리위원회는 위원장 1인과 회장이 지명하는 부회장 2명을 포함하여 총무이사, 출판이사, 연구이사, 재무이사, 감사로 구성하며, 학회의 연구윤리 확립과 연구 부정행위 발생 시 공정하고 체계적인 진실성 검증을 위한 활동을 한다.

③ 윤리위원회의 구성과 직무에 관한 자세한 사항은 따로 규정으로 정한다.

제7장 보 칙

제31조 (공고방법) 이 정관에 의한 공고는 일간지 또는 학회의 인터넷 홈페이지에 게시함으로써 한다.

제32조 (해산에 따른 잔여재산의 귀속) 민법 제77조에 따라 학회가 해산한 때에는 학회의 잔여재산은 대한민국에 귀속된다.

제33조 (정관개정) 이 정관은 총회에 출석한 정회원 3분의 2 이상의 찬성으로

개정할 수 있다.

부 칙

제1조 (시행일) 이 정관은 2012년 월 일부터 효력을 발생한다.

제2조 (설립당초의 임원 및 임기) 학회의 설립당초의 임원 및 임기는 다음과 같다.

직책	성명	소속 및 직위	임기	비고
고문	김기표	(현)경기대학교 대학원 교수	2년	
회장	정준현	(현)단국대학교 법과대학 교수	2년	
이사	김민호	(현)성균관대학교 법학전문대학원 교수	2년	
이사	김재광	(현)선문대학교 법학과 교수	2년	
이사	김일환	(현)성균관대학교 법학전문대학원 교수	2년	
이사	지성우	(현)성균관대학교 법학전문대학원 교수	2년	
감사	김현수	(현)한국법제연구원 연구위원	2년	

한국사이버안보법정책학회 임원 명단

[고 문] 김기표(전 한국법제연구원 원장, 부산대)

[회 장] 정준현(단국대)

[부회장] 김민호(성균관대), 김일환(성균관대), 김재광(선문대)
배대헌(경북대), 이규정(한국정보화진흥원), 이창범(김&장)

[감 사] 박영철(용인송담대), 박영우(KISA)

[집행이사]

총무이사 : 김재광(선문대), 전학선(한국외대)
연구이사 : 지성우(성균관대), 이호용(한양대)
출판이사 : 김명식(조선대), 방동희(경성대), 임현(고려대)
국제이사 : 신영수(경북대), 장철준(단국대), 함태성(강원대),
김현경(한국과학기술대)
섭외이사 : 정필운(교원대), 김성호 변호사, 이성엽(서강대),
배지혜(선문대)
기획이사 : 김인중(NSR), 김현수(한남대), 이민영(가톨릭대),
이정현(KISA), 최경진(가천대)
재무이사 : 곽관훈(선문대), 김성배(국민대)
홍보이사 : 권헌영(고려대), 문병효(강원대)

[상임이사]

강달천(KISA), 계인국 박사 (사법정책연구원), 곽관훈(선문대),
곽대훈(충남대), 권헌영(고려대), 김명식(조선대), 김상태(순천향대),
김성기(선문대), 김성배(국민대), 김성천(중앙대), 김성호 변호사,
김소정(NSR), 김원중(청주대), 김인중(NSR), 김정임(국회),
김현경(한국과학기술대), 김현수(한남대), 나채준(한국법제연구원),
민만기(성균관대), 박상돈(NSR), 박완규(숭실대), 방동희(부산대),
배지혜(선문대), 성봉근(고려대), 성중탁(경북대), 손승우(단국대),
신영수(경북대), 심미나(성결대), 안성경(국회), 오승규(중원대), 오일석(국회),
윤석진(강남대), 이경렬(성균관대), 이민영(가톨릭대), 이상직 변호사(법무법인
태평양), 이성엽(서강대), 이정현(KISA), 이종구(김&장), 이호용(한양대),
임종선(우석대), 임준태(동국대), 임현(고려대), 장민선(한국법제연구원),
장철준(단국대), 전태석(KISA), 전학선(한국외대), 정대원(NSR),
정태진(사이버폴리싱 연구센터), 정필운(교원대), 조인혜(미래기술연구센터),
주덕규(KISIA), 지성우(성균관대), 최경진(가천대), 최호진(단국대),
함태성(강원대), 황창근(홍익대), 홍강훈(단국대), 홍선기(동국대)

[이 사]

김희정(성균관대), 나강(국민대), 노성민(지방공기업평가원),
양정윤(NSR), 이근혁(정보통신진흥협회), 이지연(경희대 법학연구소),
이헌수(NSR), 이헌진(KISA), 윤기중(경희대 법학연구소),
조정은(건국대), 정관선(헌법재판연구원), 최종권(서울대 법학연구소)

[간 사]

총무간사 : 강주영(단국대 대학원 석사과정)
간　　사 : 권오민(단국대 대학원 박사과정), 김선남(단국대 대학원 박사과정),
김경민(선문대 대학원 석사과정)

사이버안보법정책논집 제2호

2016년 12월 26일 인쇄
2016년 12월 30일 발행

발행처 (사)한국사이버안보법정책학회
경기도 용인시 수지구 죽전로
단국대학교 법대 534호

발행인 정 준 현

편집인 김 재 광

제작처 한국컴퓨터인쇄
Tel (02) 2267-8956

사이버안보법정책논집

KOREAN JOUNAL OF CYBER SECURITY LAW

사단법인 한국사이버안보법정책학회