전남대학교 법학연구소 공익인권법센터
인권법평론 제27호 (2021년 8월)
https://doi.org/10.38135/hrlr.2021.27.35

인공지능(AI) 시대에 사이버 안보와 관련된 법제연구

권 수 진*

목차

| 국문초록 |

코로나 19사태 이후 디지털 트랜스포메이션, 5G혁신이 더욱 가속화 되고 있다. 정보통신의 일상화와 사이버공간의 활용·확대는 우리의 실생활에 직접적인 영향을 미치고 있다. 금융, 의료, 교육, 문화 등 모든 사람들의 필수적 일상에서 정보통신의 활용이 당연시되고 있다. 사이버공간은 국민들의 일상생활의 없어서는 안 될 중요한 영역이 되었으며 국가적 활동과 기업의 경제활동에서도 중요한 부분을 차지한다. 사이버 공간의 문제는 비단 어느 특정 집단의 문제가 아니라 모든 국민에게 직결되는 문제이다. 사이버 공간을 일상적으로 사용하고 그 중요성이 높아지면서 이에 비례하여 개인정보침해, 산업기밀유출, 사이버 범죄, 사이버 테러, 사이버 전쟁 등 사이버 공간의 잠재적 위험은 다양해지고 있으며 피해 범위도 점점 커지고 있다. 최근 사이버 공격이 경로의 다양화, 수준의 고도화 및 지능화, 주체의 조직

* 한국데이터산업진흥원 책임 연구원, 법학박사
논문접수일 : 2021. 7. 31, 심사개시일 : 2021. 8. 2., 게재확정일 : 2021. 8. 18.

화가 이루어지면서 사이버 공간은 국가, 기업, 개인들에게 새로운 위험 영역이 되고 있다. 인공지능(AI) 등 새로운 기술들의 등장과 기술 컨버전스로 인해 예측 불가능한 위험발생 가능성이 늘어나고 있다. 스마트시티, 5G 사회로의 급속한 진입은 온-오프라인의 유기적 결합을 통한 일상생활의 사이버 공간화를 촉진시키면서 전사회적인 차원에서 사이버 위험을 확대 재생산하고 있다. 이처럼 증가하는 사이버 위험에 효과적으로 대처하기 위한 사이버 보안의 사회적 중요성 또한 높아지고 있다.

딥러닝의 발전, 빅데이터 기술의 비약적 발전으로 인하여 인공지능의 잠재력은 어느 때 보다 극대화되고 있으며, 전 산업의 미래를 바꾸는 4차산업혁명의 핵심기술로 인식되고 있다. 사이버보안 분야도 예외는 아니다. 매년 인터넷에 연결되는 기기의 수가 기하급수적으로 증가하고 매일 새로운 위협이 100만개 이상 발생하고 있다. 지능형 사이버 공격(advanced persistent treat: APT) 과 같이 나날이 해킹 기법이 고도화되어 감에 따라 보안분야 또한 인공지능의 적용이 필요한 분야 중 하나가 되었다. 사이버공격이 미치는 범위가 사이버공간 뿐만 아니라 물리적인 공간까지 확장되고 있으며 개인뿐만 아니라 사회·경제 더 나아가 국가의 중요 기반시설의 운영에 이르기까지 영향을 끼치고 있다. 인공지능(AI) 기술이 사이버 안보 영역에 미치는 영향과 주요 국가들의 사이버보안 관련 법률 내용과 동향을 살펴보고 한국의 시사점을 살펴보고자 한다.

주제어 : 사이버 안보, 인공지능(AI), 법제정비, 4차산업혁명, 보안, 안전권, 기본권, 개인정보

Ⅰ. 서론

코로나 19사태 이후 디지털 전환이 가속화되고 정보통신의 일상화와 사이버공간의 활용·확대는 우리의 실생활에 직접적인 영향을

미치고 있다. 금융, 의료, 교육, 문화 등 모든 사람들의 필수적 일상에서 정보통신의 활용이 당연시되고 있다. 사이버공간은 국민들의 일상생활의 없어서는 안 될 중요한 영역이 되었으며 국가적 활동과 기업의 경제활동에서도 중요한 부분을 차지한다. 사이버 공간의 문제는 비단 어느 특정 집단의 문제가 아니라 모든 국민에게 직결되는 문제이다. 이처럼 사이버 공간을 일상적으로 사용하고 그 중요성이 높아지면서 이에 비례하여 개인정보침해, 산업기밀유출, 사이버 범죄, 사이버 테러, 사이버 전쟁 등 사이버 공간의 잠재적 위험은 다양해지고 있으며 피해 범위도 점점 커지고 있다. 최근 사이버 공격은 그 경로가 다양해지고 있고 인공지능 기술의 발달로 인하여 사이버 공격의 수준은 고도화 지능화 되고 있다. 또한 사이버 공격을 하는 주체가 과거 개인이 대부분이었다면 현재는 조직화, 국가화 되고 있는 바 사이버 공간은 국가, 기업, 개인들에게 새로운 위험 영역이 되고 있다. 인공지능(AI) 등 새로운 기술들의 등장과 기술 컨버전스로 인해 예측 불가능한 위험발생 가능성이 늘어나고 있다. 스마트시티, 5G 사회로의 급속한 진입은 온-오프라인의 유기적 결합을 통한 일상생활의 사이버 공간화를 촉진시키면서 전사회적인 차원에서 사이버 위험을 확대 재생산하고 있다. 이처럼 증가하는 사이버 위험에 효과적으로 대처하기 위한 사이버 안보의 사회적 중요성 또한 높아지고 있다.

인공지능의 잠재력은 딥러닝, 빅데이터 기술의 비약적 발전으로 인하여 어느때보다 극대화되고 있으며, 전 산업의 미래를 바꾸는 4차산업혁명의 핵심기술로 인식되고 있다. 사이버 안보 분야도 예외는 아니다. 매년 인터넷에 연결되는 기기의 수가 기하급수적으로 증가하고 매일 새로운 위협이 100만개 이상 발생하고 있다. 지능형 사이버 공격(advanced persistent treat: APT)과 같이 나날이 해킹 기

법이 고도화되어 감에 따라 안보분야 또한 인공지능의 적용이 필요한 분야 중 하나가 되었다. 사이버공격이 미치는 범위가 사이버공간 뿐만 아니라 물리적인 공간까지 확장되고 있으며 개인뿐만 아니라 사회·경제 더 나아가 국가의 중요 기반시설의 운영에 이르기까지 영향을 끼치고 있다. 인공지능(AI) 기술이 사이버 안보 영역에 미치는 영향과 주요 국가들의 사이버안보 관련 법률 내용과 동향을 살펴보고 한국의 시사점을 살펴보고자 한다.

Ⅱ. 인공지능(AI)시대의 사이버 안보의 중요성

1. 사이버 안보의 개념

전통적으로 국가안보는 민족국가의 출현과 함께 현실주의자들의 권력정치 개념에 입각하여 국가안보의 위협이 외부로부터 오는 것으로 정의된 개념이었다.[1] 가장 큰 외부의 위협인 적대국가의 군사력으로부터 자국의 이익을 보호하는 것이 국가안보의 문제였다. 기존의 안보개념은 군사적 위협으로부터 국가의 안전을 담보하는데 중점을 두고 있으나 정보통신기술발전에 따른 새로운 위협으로부터 국가의 안전을 보장하지 못한다는 한계가 존재한다. 첨단과학기술사회에서 정보화에 따른 새로운 사이버 위협을 식별하는 새로운 국가안보 개념의 정립이 필요하다. 기존의 영토, 국민과 같은 전통적인 안보개념에서 나아가 새로운 국가안보 개념으로 사이버 공간, 플랫폼 체계의 공정하고 신뢰성 있는 운영을 담보하고 주권자인 국

1) 조명현, "현대 국가안보 개념과 체계적 안보분석틀", 「사회과학연구」 제7권, 충남대학교 사회과학연구소 (1996. 12.), 221면.

민의 의사를 실현하며 그 생명·신체의 안전이 담보될 수 있는 모든 국가적 활동을 포함하는 개념으로 넓게 해석할 필요가 있다. 이러한 국가적 활동은 정부에 의해서 이루어질 수도 있으나 개별 국민들의 활동을 통하여도 이루어질 수 있으며 내외적 위협으로부터 국가의 핵심 기능이 지속적으로 작동되도록 하는 것이 매우 중요하다. 사이버 안보는 정보통신의 발달로 인한 사이버 위협에 대응하기 위하여 기존의 국가안보 대상이 사이버 영역에까지 확장된 개념으로 사이버 공간 속에서의 위협으로부터 국가의 핵심적 가치를 보호하는 것을 의미한다.

2. 사이버 안보와 인공지능(AI)기술

인공지능(AI, Artificial Intelligence)이란 단어는 1955년 존 매카시(John macarthy)가 발표한 '지능이 있는 기계를 만들기 위한 과학과 공학'이라는 논문에 처음 등장했으며 이듬해인 1956년 존 매카시가 개최한 다트머스 학회를 통해 대중에 널리 알려지게 되었다. 1990년대 검색엔진의 등장으로 빅데이터 시대가 개막되고 2000년 중반 컴퓨터 기술의 발달과 함께 딥러닝(Deep learning) 알고리즘 기반의 머신러닝(Machine learning) 기술이 발전하면서 인공지능의 부흥이 시작되었다. 딥러닝의 발전, 빅데이터 기술의 비약적 발전으로 인하여 인공지능의 잠재력이 극대화되고 있으며, 전 산업의 미래를 바꾸는 4차산업 혁명의 핵심기술로 인식되고 있다.

사이버안보 분야도 예외는 아니다. 매년 인터넷에 연결되는 기기의 수가 기하급수적으로 증가하고 매일 새로운 위협이 100만 개 이상 발생하고 있다. 지능형 사이버 공격(Advanced Persistent Treat: APT) 과 같이 나날이 해킹 기법이 고도화되어 감에 따라 안보분야

또한 인공지능의 적용이 필요한 분야 중 하나가 되었다. 인터넷에 연결되는 장치의 수는 매년 폭발적으로 증가하고 있다. 사이버 보안기업 맥아피(MacAfee)의 게리 데이비스는 IEEE ICCE(International Conference on Consumer Electronics)에서 전 세계 인터넷 접속기기 수가 폭발적으로 증가할 것이며 2020년 기준 500만대에 달한다고 발표하였다. 이러한 사물인터넷과 인공지능 기술의 편리함 뒤에는 부작용도 존재한다. 일반적인 해킹사고는 개인정보 유출이나 금전적인 손해를 끼치는 것에 그치지만, 사물 인터넷, 인공지능 환경에서 문제가 생기면 이는 큰 인명사고나 재해로 번질 수 있다. 실제로 스마트 자동차를 해킹할 가능성이 제기된 바 있고, 2015년 유명 해커가 방송에 나와 실제 차량을 대상으로 해킹 시연을 선보이기도 하였다. 최근에는 항공기나 드론, 핵잠수함 같은 군의 첨단 무기시스템에 대한 해킹도 증가하고 있다. 이러한 상황에서 모든 인터넷 기기와 사이버 환경의 보안을 사람의 손으로 일일이 처리하는 것은 불가능에 가깝다. 보안시스템의 자동화 필요성이 대두되며 전세계적으로 인공지능 기술을 활용한 보안시스템 구축을 시도하고 있다. 미국은 10년 이내로 자동 보안 취약점 탐지 및 패치 프로그램을 개발하고 최종적으로 20년 안에 완전 자동화된 인공지능 기반 네트워크 방어 프로그램을 개발할 계획이다. 한국인터넷진흥원은 2019년 주목해야할 7대 사이버공격 전망을 발표하였다.[2] 전세계는 차원이 다른 사이버전을 준비하고 있고, 이러한 사이버안보를 보장하기 위한 인공지능(AI)기술을 활용하고 이를 위한 미래를 대비하여야 한다.[3]

---

2) 유승화, "사이버안보 법제 개선방안 연구", 목포대학교 법학 석사학위논문, 2020, 15-16면.

3. 사이버안보와 헌법상 안전에 대한 국가의 의무

국가는 국민을 자연 재해나 사회적 위험으로부터 지킬 의무가 있으며 이러한 보호 받을 권리인 '안전권'은 '모든 사람의 생명·신체를 보호하는 사회'를 이루기 위한 인권 의 하나이다. 정부는 안전권 확보를 위해 지진 조기경보체계 개선 등 재난 안전관리의 국가 책임체제를 구축하며 국가위기관리센터 역할 강화 등 통합적 재난관리체계 만들어야 한다. 이러한 안전권을 헌법상 기본권으로 인정할 것인지에 관해서는 논란이 있다.[4] 헌법은 안전에 대한 국민의 권리

〈국내 주요 사이버안보 현황에 따른 대응체계〉

기간	사건	주요내용	대응
2004. 6	주요 국가기관 해킹사건	국회, 한국국방연구원, 국방과학연구소, 공군대학, 원자력연구소 등 국가 전산망 마비	-국가사이버안전관리규정 제정 -국가사이버안전센터 창설
2009. 7	7.7 DDos 공격 대란	정부, 금융, 민간 22개 기관 DDos 공격	-국가사이버 위기 종합대책 -국군사이버사령부 신설
2011. 3	3.4 DDos 공격 대란	정부, 금융, 민간 40개 기관 DDos 공격	-국가사이버안보 마스터 플랜
2011. 4	농협 전산망 장애사건	농협전산망 마비	
2013. 3	3.20 사이버테러 방송. 금융망 전산 해킹사건	주요방송사 금융기관 전산마비	-국가사이버안보 종합대책
2014. 12	한국 수력 원자력 문서 유출	문서해킹, 자료공개 협박	-국가사이버안보 강화방안
2016. 12	국방망 해킹사건	국방망을 통한 군사자료 해킹	-국군사이버사령부 신설

3) 정용기, "우리나라의 사이버 안보 위협현황과 대응방안", 원광대학교 경찰학연구소, 경찰학논총 제11권 제4호, 2016, 10면.

4) 우리 헌법은 제10조, 제34조 및 헌법 제35조에서 '국가는 재해를 예방하고 그 위험으로부터 국민을 보호' 하고 '건강하고 쾌적한 환경에서 생활 할 권리'를 규정하고 있다, 이를 이른바 '안전권'이라는 기본권의 근거 조항으로 이해할 수 있는지에 대하여 검토가 필요하다.

와 국가의 의무를 헌법조항에 직·간접적으로 규정하고 있다. 구체적으로 살펴보면 헌법 전문과 인간의 존엄과 가치와 행복추구권, 국가의 기본권 보장의무를 규정한 헌법 제10조, 인간다운 생활을 할 권리에 관한 헌법 제34조, 국가의 재해예방 및 위험으로부터의 보호를 규정한 헌법 제34조 제6항, 보건에 관한 국가의 보호를 규정한 헌법 제36조 제3항, 그리고 열거되지 아니한 기본권을 인정하고 있는 제37조 제1항 등으로부터 안전에 대한 국민의 권리와 국가의 의무를 도출할 수 있다.[5] 첨단과학기술 사회에서 국민의 안전을 보호하기 위한 국가의 역할은 점차 확대되고 있다. 과거에는 개인의 자율적인 판단에 맡기던 영역에까지 국가의 개입이 요구되고 있다.[6] 기존의 국가의 기본권보장의무에 근거하여 국민의 안전을 최대한으로 보장하기는 힘든바, 안전권을 헌법상의 기본권으로 인정하자는 주장이 제기되고 있다. 안전에 대한 헌법적 논의에서는 무엇보다 자유의 완전한 박탈을 대가로 한 절대적 안전은 가능하지 않으므로 국민의 자유와 국가의 안전권 보장 간의 적절한 균형을 유지하여야 한다.[7] 또한 안전권이 각종 국가적 위기와 재해에 국가가 먼저 사전적으로 조치할 의무를 규정한다고 보았을 때 기존의 영토와 물리적 개념만을 국가안보 안전권의 대상으로 보았다면 더 나아가 사이버 공간에서의 안보 위협으로부터 국민의 안전을 보호하고 인권을 보장할 국가적 의무를 인정하여야 할 것이다.[8]

---

5) 백수원, “헌법상 안전에 대한 국가의 의무”, 미국헌법연구 제27권 제3호, 2016, 137면.
6) 백수원, 상게논문, 165면.
7) 백수원, 상게논문, 166-167면.
8) 사이버 안보에 관한 기본권적 문제, 특히 ‘기본권으로서 안전권’ 문제에 관해서는 Sebastian Leuschner, Sicherheit als Grundsatz: Eine grundrechtsdogmatische Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit, Tübingen, 2018.

Ⅲ. 비교법적 검토

1. 부다페스트 조약

국제사이버 범죄와 관련된 조약으로 '부다페스트 조약'(Budapest Treaty)이 있다. 부다페스트 조약은 사이버공간에서의 범죄를 예상하기 위한 목적으로 유럽평의회에 의하여 최초로 국제적 협약을 맺은 조약이다. 부다페스트 조약을 통하여 사이버공간에서의 정보의 오남용을 방지하고, 정보데이터가 가지는 특징인 기밀성(Confidentiality), 무결성(integrity), 가용성(availability)를 침해하는 행위를 방지하도록 하였다.[9] 이 조약을 통하여 사이버공간에서의 범죄에 대한 국가 간의 상호협력과 사이버범죄를 신속하고 효과적으로 처벌하기 위한 국제적 공조를 마련하였다는 점에서 중요성이 인정된다.

2. 미국

오바마(Barack Obama)미국 대통령은 2014년 12월 사이버보안에 관한 5개의 법률을 통과시켰다. 당시의 법률은「연방 정보 보안 현대화법」(Federal Information Security Modernization Act of 2014), 283)과「국가 사이버보안 보호법」(National Cybersecurity Protection Act of 2014), 284)이다. 그리고「사이버보안 강화법」(Cybersecurity Enhancement Act of 2014), 285)과「국토안보부 사이버보안 인력채용 및 유지법」(DHS Cybersecurity Workforce Recruitment and Retention Act), 286) 및「사이버보안 인력평가법」(Cybersecurity Workforce Assessment Act)이다. 287) 이런 사이버보안 관련 입법은 부시 미국

9) 박상철, "기본권 보장 강화를 위한 통신수사 개선방안 연구", 성균관대학교 석사학위논문, 2020, 96-100면.

(George W. Bush) 대통령이 서명한 「전자정부법」(E-Government Act of 2002)이 제정된 뒤 처음이다. 2014년 12월 제정된 법률 중 특히 「연방 정보보안 현대화법」과 「국가 사이버보안 보호법」은 크게 2가지에 초점이 맞추어져 있다.[10]

위 법에서 강조하는 부분은 사이버 안보를 위한 연방정부의 활동 중앙집권화이고, 정부와 민간기관 사이의 정보공유강화에 중점을 두고 있다. 이에 대해 「국토안보부사이버보안 인력채용 및 유지법」과 「사이버보안 인력평가법」은 사이버 안보에 관하여 연방정부의 인력을 강화하는데 주된 목적이 있다. 미국은 사이버 안보에 관하여 통합적인 법을 제정하지 않았으며 우리나라와 같이 개별적인 법률을 제정하여 시행하고 있다. 사이버 안보를 효과적으로 실현하기 위해서 논리 필연적인 통합법제의 제정은 필수적 요건은 아니다.[11] 다만 개별법 형식을 따르는 경우 법제도 자체에 체계적으로 접근하기 어려운 점이 있으므로 법제도의 체계성과 효율성이라는 측면을 생각해 볼 때 통합법 체계의 장점도 고려하여야 한다.

미국은 사이버 안보를 위한 조직 체계에 있어 국토안보부를 중심으로 거버넌스를 구성한다. 이는 「국가 사이버보안 보호법」이 잘 보여주고 있다. 이처럼 국가 사이버보안 문제를 관할하는 중심적인 거버넌스를 설정하므로 사이버보안의 문제, 다시 말해 정보보호 문제가 발생했을 때 통일적이고 신속하게 대응할 수 있도록 하고 있다. 이는 정보보호에 관하여 아직까지 중심적인 거버넌스를 갖추고 있지 못한 우리나라에 시사하는 바가 크다. 우리나라는 현재 정보

10) 양천수, 지유미, "미국사이버보안법의 최근동향: 사이버보안정보공유법을 중심으로 하여", 법제연구 통권 제54호, 한국법제연구원, 2018, 162면.

11) 양천수, "제4차 산업혁명과 정보보호 법정책의 방향", 「공법학연구」 제18권 제4호, 한국비교공법학회, 2017, 369-395면; 김득수, 사이버테러 대응을 위한 법제도 구축에 관한 연구, 동아대학교 대학원 박사학위논문, 2020, 116-120면.

보호와 관련하여 공공영역은 정보보호를 국가정보원이 관할하고, 민간영역은 과학기술정보통신부가 관할하고 있다. 또한 개인정보보호는 개인정보보호위원회가 관할한다. 하지만 이렇게 정보보호에 관해 거버넌스를 분리하는 것이 기능적인 측면에서 바람직한지에 대한 검토가 필요하다. 또한 미국은 독자적인 「사이버보안 정보공유법」을 제정하여 시행하고 있다는 점을 주목해야 한다. 지능 정보사회에서 발생되는 정보침해 문제에 효과적으로 대응키 위해서는 무엇보다 정보공유가 필요하다는 점은 다양한 측면에서 확인되고 있다. 특히, 정보침해와 보호에 관련한 정보를 광범위하게 공유해야 하며 정보공유 및 정보보호가 선순환관계를 형성하여야 한다.

정보공유를 적극적으로 활성화하는 법제정비가 필요하며 우리나라도 미국과 같이 현대사회에서 발생하는 정보침해 문제에 대하여 적절한 대응이 가능한 독자적인 정보보호를 위한 정보공유법을 제정하여 시행하여야 한다.

3. 영국

영국은 EU국가들 가운데서도 높은 사이버 안보 기술과 풍부한 전문 인력을 보유한 국가이다. 영국은 2009년부터 일찍 국가차원에서 사이버 안보 전략을 수립하여 체계적으로 추진하였다. 2016년 11월에는 앞으로 5년간 추진할 새로운 사이버 안보 전략(National Cyber Security Strategy 2016-2021)을 발표하였다. 영국은 2016년부터 2021년까지 사이버 안보에 지출했거나 지출예정인 예산은 전체 46억 6,000만 파운드에 이른다.[12] 이러한 사회적 배경에서 2000년

12) 김병운, "초연결산업 사회, 사이버보안 정책", 「과학기술법연구」 제22집 제3호, 한남대학교 과학기술법연구원, 2016, 95면.

대 이후부터 사이버 안보와 관련한 중요 법률을 제정하여 시행해 왔다. 그러나 영국의 사이버 안보 법제의 변천과정, 특히 입법과정에서 구체적으로 어떠한 논의가 있었는지를 깊이 있게 다룬 기존 연구는 찾아보기 어렵다.[13] 영국의 경우에도 사이버안보 전반을 규정하는 일반법은 없으며 사이버 안보와 관련한 행정권한(수사 및 조사 등)에 관련된 법률과 테러 등 안보 위협 관련 법률 등 개별법에서 관련 조항을 규정하고 있다. 사이버 안보와 관련한 핵심법률은 수사기관과 정보기관의 감청 권한 및 통신회사의 통신 데이터 보관 의무 및 이에 대한 수사기관과 정보기관의 접근 권한을 규정한 법으로는 첫째, 수사권규율법(2000, 이하 'RIPA')이다. 둘째, 데이터 보관및 수사권법(2014, 이하 'DRIPA')이다. 셋째, 수사권법, 2016, 이하 'IPA')을 들 수 있다.[14] DRIPA와 IPA의 주요내용은 시민에 대한 공권력의 감시를 규정하고 있다. 특히 IPA는 불특정 다수를 상대로 한 광범위한 통신 데이터를 수집하고 수사할 수 있는 권한과 정보기관과 같은 공권력의 광범위한 정보 접근 권한을 부여하는 것을 규정하고 있다. 사실상 해킹과 같은 '장비 개입권'을 신설하여 많은 논란이 제기되고 있다. 제안 단계에서부터 심사 및 시행에 이르기까지, 그리고 시행된 이후에도 시민단체, 기업 및 언론을 중심으로 반대 여론이 상당하였다. 시민단체, 기업 및 언론에서 제기한 '광

13) 한 예로 미국의 사이버 안보 법제에 관하여는, 양정윤 "미국의 법제도 정비와 사이버안보 강화: 국가사이버안보보호법 등 제·개정된 5개 법률을 중심으로", 「입법과 정책」 제7권 제2호, 국회입법조사처, 2015, 독일의 사이버 안보 법제에 대하여는, 성봉근, "사이버상의 안전과 보호에 관한 독일의 입법동향과 시사점", 「법과정책연구」 제17권 제1호, 한국법정책학회, 2017.

14) 이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구", 「국가정보연구」 제1권 제2호, 한국국가정보학회, 2008, 76-77면; 김상배, "국가 사이버 안보 전략의 국제비교: 한반도 주변4국과 유럽 주요3국의 사례", 「워킹페이퍼」 No.7, 서울대학교 국제문제연구소, 2017, 20면.

범위한 감시 문제', '사생활 침해 문제'가 결국 현실화되어 IPA가 시행 직후 ECJ 및 영국 법원으로부터 잇달아 무효판결을 받았다는 점에서 IPA에 대한 직접적인 도입은 현재 우리나라의 상황에서는 힘들 것으로 보인다.

4. 독일

독일이 사이버 안보에 관한 어떤 정책을 마련하고 추진하는지 크게 4가지를 통해 살펴보고자 한다. 첫째, 독일을 위한 '사이버 보안전략(2016)'이다. 둘째, '디지털 아젠다(2014-2017)'이고, 셋째, '디지털 전략(2025)'이다. 넷째 「네트워크 및 정보보안 지침」의 독일법 전환이다. 먼저 독일을 위한 사이버 보안전략을 살펴보면 정보화 사회가 대두하면서 정보보호에 대한 중요성이 높아졌고 이에 독일 연방정부는 물리적 주요기반시설 외에 사이버공간에 대한 보안정책을 수립하여 시행하였다.[15]

그 첫 단계에 해당하는 정책으로 2011년 2월 독일 연방내무부는 독일을 위한 사이버 보안전략'(Cyber-Sicherheitsstrategie für Deutschland)을 발표했다.[16] 이 보안전략은 미래지향적인 사이버 보안정책에 관한 주요 결정사항을 포함하고 있다. 2016년의 새로운 사이버 보안전략은 아래와 같이 크게 4대 활동범위를 중심으로 구성된다. 첫

15) Hans-Jürgen Lange/Astrid Bötticher(Hrsg.), Cyber-Sicherheit, Springer VS, 2014. 참고.

16) 이는 '독일 연방정보기술보안청'(Bundesamt für Sicherheit in der Informationstechnik)의 전자정부 및 IT에 의한 주요기반시설의 보호업무에 따라 마련된 2005년 '정보기반시설의 보호를 위한 국가계획'(Nationaler Plan zum Schutz der Informationsinfrastrukturen)]을 대체하는 정책이다; Alexander Silhavy, Cyber-Sicherheitsstrategiefür Deutschland: Neue-Bedrohungen? Neue Lösungen?, Norderstedt, 2013.

번째 디지털 환경에서 국민들이 안전하고 독립적으로 행동할 수 있도록 하는 것이다. 이는 사이버 보안의 핵심적인 기초가 된다. 국민들이 정보기술을 사용하면서 자유롭게 이를 활용할 기회를 가져야 하며 위험을 평가하고 이해하며, 자신의 권리가 침해당한 경우 이에 대한 구제를 받을 수 있어야 한다. 이를 위해서 신뢰할 수 있는 기술과 프레임워크(frame work)와 같은 조건이 필요하다. 둘째, 높은 수준의 사이버 보안을 위하여 국가와 경제 간에 신뢰와 긴밀한 협력, 교류를 하여야 한다. 셋째, 국가는 사이버 공간을 포함한 넓은 범위에서 국민들의 자유, 국가 안보, 사회적 정의를 보장해야 한다. 이를 위해서는 연방차원의 지속가능하고 효율적인 국가 사이버 보안 체계를 구축하여야 한다. 넷째, 디지털화 되어 있는 세계에서 이루어지는 다국적 네트워킹을 생각하여 유럽과 국제기구, 타 국가들과의 사이버 보안정책을 제정할 시에 독일이 적극적인 역할을 해야 한다는 것이다. 위 각 전략들의 활동 영역은 개괄적 성질을 지니며 모든 사회 영역에 영향을 미친다.[17]

두 번째 단계에 해당하는 정책으로 '디지털 아젠다'(Digitale Agenda, 2014-2017)가 있다.[18] 이는 ICT 정책을 규정하고 있으며 사이버 보안에 관한 내용 역시 포함되어 있다. 독일 연방정부는 디지털 커뮤니케이션, 전자거래 등 IT 시스템을 기반으로 하는 비즈니스 모델을 성공시키기 위해 IT 보안문제 해결이 필수적이라는 점을 인식했다. 따라서 이를 달성하는데 사이버 보안 규제 강화, 전자상거래 등 비즈니스 섹터 감시강화, 데이터 보호, IT 보안체계확립 등 IT 보안 수위를 높이는 데 주력하였다.

---

17) 양천수·김중길, " 독일의 사이버보안법: 정책·거버넌스·법률", 법제연구 제56호, 2019, 57-58면.

18) https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html

또한 독일 연방경제에너지부가 2016년 4월에 발표한 '디지털 전략'(Digitale Strategie 2025)을 들 수 있다. 이는 디지털 아젠다를 보완하기 위해 제시된 것으로 독일 정부는 디지털 아젠다가 중소기업 차원에서는 제대로 실현되지 못하고 있다는 점을 고려하여 이를 보완하기 위해 새롭게 디지털 전략을 신설하였고 내용으로 사이버 보안 강화에 관한 내용이 있다. 이와 더불어 '개인정보 자기통제권'에 관한 내용도 규정하고 있다. 마지막으로 유럽연합 지침인 「네트워크 및 정보보안 지침」이 있다. NIS지침은 사이버 보안과 관련하여 EU(유럽연합) 전체에 적용되는 최초의 법적 규범이다. 이는 관할기관 간 협력, 국가 네트워크 정보보안 체계, 공공행정과 기업의 정보보안 등으로 구성된다. 국가와 민간기업 또한 국가 간의 의무를 규정한다. 독일은 연방정보기술보안청을 통해 독자적인 사이버 보안 거버넌스를 구축하였으며 이에 따라 연방 차원에서 사이버 보안 위험에 대응하고 있다. 또한 사이버 보안과 관련된 타 분야의 문제를 비롯한 국제적으로 대두하는 사이버 안보 관련 문제도 관할하고 있다. 사이버 보안 문제를 총괄적으로 관할하는 전문 거버넌스를 갖추고 있지 않는 우리나라에 독일의 사례는 시사하는 바가 크다. 각 분야별로 존재하는 정보공유 또는 분석센터를 총괄하는 독자적인 거버넌스 구축이 필요하다. 이외에도 연방정보기술보안청이 중심이 되어 정부와 주요기반시설의 사이버 보안을 통합 추진함으로써 사이버 보안과 관련한 각 기관의 기능을 상호 연결하고 이를 효율적으로 통합하여야 한다. 초연결 현대사회에서 사이버 보안 실현을 위해서는 사이버 침해가 발생했을 때 비로소 대응하는 현재적·사후적 조치보다는 사전 예방적 조치가 더 중요하며 독일의 사이버 보안법이 최근 기술적, 관리적 조치 가운데서 특히 기술적 조치에 대한 중요성을 인식하고 있는 점을 살펴볼 필요가 있다. 기술적 조치

는 현대사회에서 새로운 규제수단으로 주목받고 있으며 아키텍처 규제(Architectural regulation)가 그 대표적인 예이다[19]

5. 일본

일본은 2000년부터 국가 차원에서 사이버 안보에 대한 적극적인 대응을 하였다.[20] 일본의 IT기본법 이라 불리는 고도정보통신 네트워크사회형성기본법(이하, IT기본법)이 그 예이다.[21] 동법 22조는 고도정보통신 네트워크의 안전성과 신뢰성을 확보하고, 또한 개인정보의 보호 등 고도정보통신 네트워크를 안심하고 이용하는데 필요한 조치를 요구하고 있다. 일본 정부는 이를 근거로 IT 기반보호를 위한 정책들을 수행했다. 그 중 하나로 2005년 4월 내각관방 소속으로 '정보보안센터'를 설립하였다.[22] 또한 2005년 5월에는 민관에 있어서 통합적인 정보보안 정책을 추진하기 위하여 고도정보통신 네트워크사회 추진전략본부에 "정보보안 정책회의"를 설치하였다. 이는 정부기관과 중요 인프라 사업자의 정보보안 수준을 향상하고 사이버공격에 관한 대처 능력의 강화를 위한 것이다.[23]

---

19) 심우민, "사업장 전자 감시 규제 입법의 성격", 인권법평론 제12호, 전남대학교 법학연구소 공익인권법센터, 2014, 157-183면.

20) 關啓一郎, "サイバーセキュリティ基本法の成立とその影響", 「知的資産創造」(2015. 4), 81頁.

21) 동법은 고도정보통신 네트워크사회의 형성을 기본 목적으로 하고 있는데, 여기서 말하는 '고도정보통신 네트워크 사회'란 인터넷 고도정보통신 네트워크를 통하여 자유롭게 안전하게 다양한 정보 및 지식을 전 세계를 통해 입수하고 공유하고 또한 발송하여 모든 분야에서 창조적이며 활력 있게 발전하는 것이 가능하게 되는 사회를 말한다.(제2조)

22) 내각관방조직령 제12조에 근거한 '정보시큐리티센터의 설립에 관한 규칙'을 통해 성립되었다. NISC는 정보보안정책에 관한 사령탑으로서 기본전략을 입안하고 민관에 있어서 통일적, 횡단적인 정보보안정책의 추진에 관한 기획 및 입안 등을 총괄하는 역할을 담당하였다.

정보보안정책회의와 NISC는 내각관방을 중심으로 하는 범정부적 기구이다. 이들 기구는 사이버 안보 위기상황에서 국가단위의 통일적인 대응이 가능하다는 점이 중요한 의미가 있다. 또한 정보보안정책회의에서는 정보보안에 대한 중장기계획을 수립하여 발표하는데.[24] 이에 따라 범정부차원에서 조직적 대응을 하였다. 일본은 '사이버보안기본법(サイバーセキュリティ基本法)'을 제정하였다. 이를 통하여 사이버보안 관련조직 및 제도의 정비가 이루어졌다.[25] 일본의 기본법 제정을 통해 우리나라가 얻을 수 있는 시사점은 크게 2가지로 정리해볼 수 있다. 첫째, 사이버보안과 관련한 컨트롤 타워를 명확하게 규정하였다는 점이다. 기본법은 내각관방장관을 본부장으로 하는 '사이버보안전략본부'의 설립근거 및 권한을 명확하게 규정하였다. 특히 사이버보안전략본부와 NISC가 각 행정부처에 대해 평상시의 감시권을 가지는 기능적 권한 뿐만 아니라 중대한 사안이 발생할 때 원인규명조사를 할 수 있는 권한을 부여하고 있다는 점에서 특징이 있다. 사이버보안 전략본부가 주체가 되어 각 행정부처뿐만 아니라 독립행정법인과 특수법인 등을 조사하고 사이버테러에 대응할 수 있는 시스템을 갖춘 것이다. 단시간에 광범위하게 발생하는 사이버테러에 적절하게 대응하기 위해 필요한 컨트

23) 고도정보통신네트워크사회추진전략 본부령 제4조의 규정에 근거하여 2005년 5월 30일 고도정보 통신네트워크사회 추진전략본부장 결정으로 '정보시큐리티 정책 회의 설립에 대하여'를 결정함에 따라 성립되었다. 동 정책회의는 전 국가적 관점에서 정보보안 관련 기본전략을 수립하는 역할을 담당하고 있다. 또한 NISC는 정책회의에서 수립된 기본 전략을 수행하는 기관으로서 정보보안정책에 관한 중장기계획 및 연도 계획의 입안, 정부기관 및 중요인프라의 정보 보안 대책 수립, 정보보안정책에 관한 국제제휴의 창구기능을 수행하였다.

24) 곽관훈, "일본의 사이버보안기본법 제정 의의 및 시사점", 「IT와 法연구소」 제18집, 경북대학교 IT와 法연구소, 2019, 122-123면.

25) 곽관훈, "일본의 사이버보안기본법 제정 의의 및 시사점", 경북대학교 법학연구소, 2019, 220면.

롤타워를 명확화하였다는 점에서 의미가 크다. 다만 과도하게 정보보안만을 강조하면, 정보유통이 저해되고 개인의 권리가 침해될 가능성이 있다는 점에 유의할 필요성이 있다. 일본의 사이버보안기본법은 사이버보안과 정보 유통 그리고 개인의 기본권의 보호를 함께 고려하여 시행하는 것을 기본법의 기본이념으로 하고 있다. 이러한 일본의 움직임은 우리에게 많은 시사점을 주고 있다. 향후 일본의 사이버보안기본법의 성과와 문제점에 대해서도 면밀하게 검토할 필요가 있으며, 우리나라 법체계 개선에 중요한 참고자료가 될 것으로 기대된다.

6. 소결

앞서 주요 국가들의 사이버 안보에 관한 내용을 살펴보았는데 이에 대한 결론은 다음과 같다. 미국의 경우를 살펴보면 미국은 사이버보안과 관련하여 통합적인 법을 제정하지 않고 있다. 반드시 통합 법률의 필요성에 당위성이 있는 것은 아니지만 개별법 형식을 취할 경우, 체계적으로 접근하기 어렵다는 점에서 효율성 측면에서는 문제가 있다고 생각한다. 또한 사이버보안에 관해 국토안보부를 중심적인 거버넌스로 설정하고 있다. 이는 정보 침해사고 등이 발생했을 때 신속하면서도 통일적으로 대응할 수 있는 장점이 있다. 독자적인 「사이버보안 정보공유법」도 시행하고 있다. 이는 정보침해와 보호에 대한 정보를 광범위하게 공유해야만 효과적인 정보침해를 방어할 수 있는 여러 가지 방어조치 역시 더욱 수월하게 개발될 수 있다는 장점이 있다. 이런 점에서 독자적으로 정보공유법을 제정하여 시행하는 미국의 입법 경향은 우리나라에 시사하는 바가 크고 우리나라 역시 현대사회에서 심각한 사회적 문제인 정보의 침

해에 대응하기 위한 '정보보호를 위한 정보공유법'을 제정하여야 한다. 영국은 DRIPA와 IPA는 시민에 대한 공권력의 감시를 규정하고 있는 법률이다. 특히 IPA는 불특정 다수인을 대상으로 광범위한 통신 데이터 수집, 수사기관, 정보기관 등 공권력의 광범위한 정보 접근 권한 부여, 사실상 해킹과 같은 '장비 개입권'의 신설과 같이 논란의 소지가 상당한 내용을 규정하고 있다는 점이 특징이다. 독일은 연방정보기술보안청이 사이버 보안 관련 거버넌스를 구축하고 사이버 보안에 관한 모든 문제를 총괄하여 연방차원에서 사이버 보안에 대응하고 있다. 사이버 보안 문제를 전체적으로 관할하는 전문 거버넌스를 아직 구축하지 못하고 있는 우리나라에 좋은 사례가 될 수 있을 것이다.[26] 일본의 경우 2014년 '사이버보안기본법'의 제정을 통해 사이버보안관련조직 및 제도의 정비가 이루어졌다. 기본법의 제정을 통해 사이버보안과 관련한 컨트롤타워를 명확하게 규정하였다는 점과 내각관방장관을 본부장으로 하는 '사이버보안 전략본부'의 설립근거 및 권한을 명확하게 규정하였다는 점에서 우리에게 많은 시사점을 주고 있다. 향후 일본의 사이버보안기본법의 성과와 문제점에 대해서도 면밀하게 검토할 필요가 있으며, 우리나라 법제 개선에 중요한 참고자료가 될 수 있을 것으로 생각된다. 결론적으로 우리나라의 경우, 영국과 같은 급진적 형태의 법안은 국가가 개인사생활 보호 의무를 무시하는 결과를 야기할 우려가 높아 적절하지 않아 보인다. 반면, 일본과 독일의 절충적 형태를 제도화하는 것이 일원화된 법체계를 유지하면서 통일적인 관리 감독체계

26) 현재 우리나라는 공공부문에 대한 사이버 안보와 보안 관련 문제를 국가정보원이 관할한다. 그리고 민간부문은 과학기술정보통신부가 관할한다. 이외에도 행정안전부, 방송통신위원회, 개인정보보호위원회, 금융위원회 등이 각각의 개별 영역에서 근거 법령에 의거 관련 업무를 수행한다.

를 유지할 수 있는 장점이 있을 것으로 생각된다. 즉 사이버 안보관련 기본 법률을 제정하여 법률의 일원화를 기하고, 이에 근거하여 각 영역별로 존재하는 정보공유와 분석센터를 총괄하는 독자적인 거버넌스를 구축하는 것이 바람직하다.

Ⅳ. 사이버 안보 법제정비 방안

1. 사이버안보의 입법부제

국내 사이버 안보 관련 법안이 처음 등장한 것은 2006년 12월 공성진 의원 대표발의에 의한 '사이버 위기 예방 및 대응에 관한 법률안'이었다. 그러나 임기만료로 심사되지도 못한 채 폐기 되었다. 이후 18대 국회에서 다시금 공성진 의원 대표 발의로 '국가사이버위기관리법안'이 발의되어 정보위원회에서 2009년 4월에 상정되었으나, 법안심사소위원회에 이르지 못하고 임기만료로 폐기되었다. 19대 국회에서는 사이버안보와 관련하여 2013년 3월 하태경 의원 대표발의로 '국가 사이버안전 관리에 관한 법률안'을 발의하였고, 2013년 4월에 서상기 의원 대표발의로 '국가사이버테러 방지에관한 법률안', 2015년 5월 이철우 의원 대표발의로 '사이버위협정보 공유에 관한 법률안', 2015년 6월 이노근 의원 대표발의로 '사이버테러 방지 및 대응에 관한 법률안'이 발의되었다. 20대 국회에는 이철우 의원 등 122인이 공동발의한 '국가 사이버 안보에 관한 법률안'이 2016년 6월 13일 소관위인 정보위원회에 회부되고 2017년 2월 27일 상정만 되었을 뿐 처리는 불투명한 상황이다. 이처럼 지속적으로 법안이 발의 되는 데는 사이버 안보에 관한 공통적인 관심과 우려

가 있기 때문으로 보인다.[27)]

27) 김득수, "사이버테러 대응을 위한 법제도 구축에 관한 연구", 동아대학교 대학원 박사학위논문, 2020, 170면.

법안	제안이유
사이버위기 예방 및 대응에 관한 법률안(공성진 의원 대표발의, 2006. 12. 28.)	정부와 민간부분을 포함한 국가차원에서 사이버공격을 사전 탐지하고 정보를 공유할 수 있는 체계를 구축함으로써 사이버위기 발생을 예방하고 사이버 위기가 발생하였을 경우에는 효율적으로 대처할 수 있는 체계의 구축 및 대응활동 등을 명확히 규정함으로써 사이버위기로 인한 피해확산을 방지하고 이를 조기에 극복하고자 함
국가 사이버위기관리법안(공성진 의원 대표발의, 2008. 10. 28.)	정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함
국가 사이버안전 관리에 관한 법률안(하태경 의원 대표발의, 2013. 3. 26.)	국가차원에서 사이버안전에 관한 기본계획을 수립·시행하도록 하고, 국무총리 소속으로 국가 사이버안전 전략회의를 두어 국가 사이버안전에 관한 중요하상을 심의하도록 하며, 사이버위기 대응 훈련·사이버위기경보 발령·사이버공격으로 인한 사고의 통보 및 조사 등에 관한 법적 근거를 담은 법률을 제정함으로써 사이버안전을 확보하며 국가의 안전보장과 국민의 이익에 이바지하고자 함
국가 사이버테러 방지에 관한 법률안(서상기 의원 대표발의, 2013. 4. 9.)	정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하고, 이를 통하여 사이버테러를 사전에 탐지하여 사이버위기 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함
사이버위협정보 공유에 관한 법률안(이철우 의원 등 22인, 2015. 5. 19.)	사이버위협을 신속히 차단하여 피해를 최소화하는 등 효과적으로 대처할 수 있도록 공공·민간이 함께 사이버위협정보를 공유·분석하는 등 협력을 활성화하여 사이버위협을 조기 탐지·전파할 수 있는 체계를 구축하고자 함
사이버테러 방지 및 대응에 관한 법률안(이노근 의원 대표발의, 2015. 6. 24.)	사이버테러를 사전에 탐지하여 사이버위기 가능성을 조기에 차단하며, 위기 방생 시 국가의 역량을 결집하여 신속히 대응하기 위한 범국가적인 차원의 사이버테러 방지 및 대응 체계를 구축하고자 함
국가 사이버안보에 관한 법률안(이철우 의원 등 122인, 2016. 5. 30.)	정부와 민간이 함께 협력하여 국가차원의 체계적이고 일원화된 대응 체계를 구축하고, 이를 통해 사이버공격을 사전에 탐지하여 사이버위기 발생가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응 할 수 있도록 함
국가 사이버안보법안(정부발의, 2017. 1. 3.)	공공 및 민간 영역의 구분 없이 광범위하게 발생하는 사이버공격으로 인하여 막대한 경제적 피해와 사회 혼란이 유발되고 있는바, 국가안보를 위협하는 사이버공격을 신속히 차단하고 피해를 최소화하기 위하여 국가사이버 안보를 위한 조직 및 운영에 관한 사항을 체계적으로 정립하려는 것

2. 사이버보안 법제정비의 방향과 내용

가. 현행 사이버안보 추진체계

정부는 2013년에 발생한 '3·20 사이버테러 방송·금융전산망 해킹 사건' 이후 '국가 사이버안보 종합대책'을 발표하였다. 그간 사이버 공격이 발생하였을 때 국가 차원에서 총괄하는 컨트롤 타워를 강화하기 위해 청와대 국가안보실을 컨트롤타워로 하며, 국가정보원을 사이버 공격의 실무총괄과 국가, 공공부문을 담당하게 하고 있다. 민간영역에서는 과학기술정보통신부, 국방영역에서는 국방부가 담당하는 수행체제이다. 이는 사이버 공격에 대응하는 컨트롤타워를 일원화하여 사이버 위기상황에 대한 보고체계와 대응활동을 총괄함으로써 유관기관과의 협력을 좀 더 체계적으로 추진하기 위함이다.[28] 사이버 공격과 같은 국가 위기상황이 발생할 경우 해당기관은 국가안보실과 국정원에 동시에 통보를 하며 국정원은 피해내역과 대응상황을 국가안보실에 통보하여 대통령에게 보고하여야 한다.[29]

나. 사이버안보 관련 주요법령

우리나라의 사이버안보 법체계는 공공부문과 민간부문, 공공과 민간을 불문하고 주요기반시설에 대한 규정 크게 3가지로 나뉜다. 공공부문은 대통령훈령인 「국가사이버안전관리규정」, 민간부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 주요기반시설인 「정보통신기반보호법」으로 나뉜다.[30]

---

28) 권혁천 "북한의 사이버 공격양상 비교연구", 건국대학교 박사학위논문, 2020, 20면.
29) 권혁천 "북한의 사이버 공격양상 비교연구", 건국대학교 박사학위논문, 2020, 10-15면.
30) 김득수, 전게논문, 171-175면; 유승화, "사이버안보 법제 개선방안 연구", 목포대학교 일반대학원 석사학위논문, 2020, 10면.

1) 공통부문「정보통신기반 보호법」

「정보통신기반보호법」은 2000년 제정되었으며, 첨단과학기술사회에서 정보화로 인해 주요기반기설의 정보통신시스템에 대한 의존도가 심화되면서 해킹, APT공격 등에 의한 사이버 공격이 국가안보를 위협하는 새로운 요소로 대두됨에 따라 주요정보통신기반시설을 보호하기 위해 정부에 의해 제안되어 발의된 법률이다. 사이버 위협에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.「정보통신기반보호법」은 총칙규정과 주요정보통신기반시설의 보호체계, 주요정보통신기반시설의 지정 및 취약점 분석, 침해사고에 대한 대응, 기술지원 및 민간협력, 벌칙규정으로 구성된다.[31]

2) 공공부문「국가사이버안전관리규정」

「국가사이버안전관리규정」은 2004년 발생한 '주요 국가기관 해킹 사건' 이후 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 효율적으로 보호하고 사이버안전에 관한 조직 및 운영에 대한 사항을 체계적으로 정립하는 것을 목적으로 하는 대통령 훈령이다.[32]「국가사이버안전관리규정」의 주요 내용으로는 국가사이버안보에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의의 설치와 효율적인 운영을 위한 국가사이버안전대책회의 설치, 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위한 국가정보원장 소속하에 사이버안전센터 설

31) 김득수, 전게논문, 175-178면.
32) 유승화, "사이버안보 법제 개선방안 연구", 목포대학교 일반대학원 석사학위논문, 2020, 25-27면.

치, 또한, 사이버 공격에 대한 사전예방조치로 사이버안전대책의 수립·시행, 사이버위기 대응훈련, 사이버공격과 관련한 정보 외에도 사후적으로 대응하기 위한 보안관제센터의 설치 및 운영과 경보발령, 통보 및 사고조사 및 처리 등에 관한 사항을 정하고 있다.[33]

3) 민간부문「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

「전산망보급확장과이용촉진에관한법률」의 첫 제정당시 전산망의 개발보급과 이용 등을 촉진하여 정보화사회의 기반을 조성함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다. 현재 정보통신망의 이용촉진 등에 관한 사항 외에 정보통신서비스이용자의 개인정보의 보호제도에 관한 사항이 대폭 규정됨에 따라「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 변경하였다.[34]

다. 현행법상 문제점

1) 관련기본법의 부재와 관계법령의 체계화 필요성

우리나라 국회는 국가 사이버테러방지법의 제정을 두고 찬반논란이 있었다. 논의의 쟁점은 국가사이버테러 방지법에서 규정하는 국가정보원의 '정보수집'이다. 2016년 3월 19대 국회 마지막 회기에서 입법이 배제된 이유도 사이버테러방지법 제8조에서 규정한 "책임기관의 장은 사이버테러 정보를 탐지·분석하여 즉시 대응조치를 할 수 있는 기구(이하 보안관제센터)를 구축·운영'하거나 동법 제2조 제5호, 제6호 의 보안 관제 전문 업체에 업무를 위탁하는 부분이

33) 유승화, "사이버안보 법제 개선방안 연구", 목포대학교 일반대학원 석사학위논문, 2020, 30-35면.
34) 김득수, 전게논문, 171-175면.

국민이 기본권을 과도하게 제한할 수 있다는 점이다. 국가사이버테러 방지법안은 국정원을 사이버테러대응의 컨트롤타워로 정하여 '민간영역' 다수의 사업자들까지 규율대상으로 하고 있다. 이는 사이버테러 가 발생하였을 경우 대응 업무를 빠르고 효과적으로 하기 위한 것이다. 다만 '민간영역'에서의 감시와 규제는 자칫 정보기관의'민간사찰'로 이어질 수 있으므로 비판이 존재한다. 또한 현행 정보통신법의 개정 및 영역 확대 정도로는 민간사찰에 대한 명확한 기준을 정하기 어려운 것도 사실이다. 사이버테러 방지법에 대해 토론하는 자리에서 반대의견은 "현재도 '국가사이버안전규정'이 있고, 주요정보통신기반보호법이 있는 만큼 이미 시행령, 시행계획 등 여러 부분을 통해 사이버 위협을 막기 위한 근거를 마련할 필요가 있고 실제로 그렇게 집행되고 있다고 주장한다. 오히려 기존의 법률을 조정하는 것이 더 중요하고 사이버테러방지법의 제정보다는 현행 법제의 수정가 검토가 필요한 시점이라고 하였다. 국가사이버테러 방지법의 국회 입법을 둘러싸고 이처럼 각종 찬반 논란이 끊이지 않는 것은 결국 현행 국내 법체계 및 안보, 이념 등의 이론들과 상당한 인과관계가 있다. 국가사이버테러 등 사이버범죄에 대응할 수 있는 '정보통신산업진흥법'이나 '통신비밀보호법' 등은 개인의 통신비밀'의 자유에 관한 보장을 가장 최우선 가치로 규정한다. 이는 그 법익을 자유주의 민주국가의 개인적 인권과 사생활 보호에 초점을 맞추고 있으므로 사실상 사이버테러 범죄예방이나 처벌 등에는 다소 미약한 부분이 많다. 따라서 국회의 '국가 사이버테러 방지법' 제정은 국가차원에서 사이버 안전, 국가안보라는 포괄적 '안보개념'을 수립하는데 중요한 지침이 될 수 있다. 현재 개별법으로 분산되어 있는 사이버 안보에 관련된 기능을 일원화하여 통합하는 경우, 현재 개별법에 중복적으로 기재된 것과 같이 비효율성이 발

생하는 문제도 제거할 수 있다.

2) 사이버테러 대응 업무의 전문성과 체계성 부족

첨단과학기술사회에 진입하면서 개인정보 유출, 사이버범죄, 사이버테러 등 사이버공격으로 인한 피해 규모는 매우 크다. 특히 우리나라는 분단국가의 특수한 상황으로 북한 사이버공격이 계속 이어지면서 각종 기밀정보유출이나, 업무마비 등 크고 작은 피해들이 줄을 이었다. 따라서 북한의 이 같은 사이버테러가 만일 원자력발전 등 전력공급 시설이나 이동통신망, 금융망 등의 파괴 및 마비 사태로 연계될 경우 대한민국의 안보는 물론 국가기간의 모든 정보라인은 순식간에 무너지게 되고, 이렇게 되면 국가존립까지도 위태로운 상황에 직면한다.[35] 따라서 이처럼 날로 발전을 거듭하고 있는 사이버테러 위협에 효율적으로 대응하기 위해서는 사이버테러 범죄에 대비한 법체계의 정립이 중요하다. 구체적으로 컨트롤타워 기관을 구성하고 사이버테러 전문기술인력을 확보하여야 한다. 주요국의 경우를 예로 들어보면 미국은 사이버테러의 대응책으로 2014년 12월 4일 미국 법무부 산하에 사이버범죄조사 및 예방 활동을 강화하기 위한 사이버보안 유닛을 신설 공표했다.[36] 일본도 2014년 11월 제정해 2016년 1월 9일부터 시행한 사이버보안기본법에 근거해 사이버보안 전략을 관장하는 전략본부를 중심으로 구체적인 실무를 담당하는 사이버보안센터(NISC)를 만들고, 본격적인 사이버보안 정책을 시행중에 있다.[37] 영국에서는 국가 전반에 걸쳐 14개의

35) 김득수, 사이버테러 대응을 위한 법제도 구축에 관한 연구, 동아대학교 대학원 박사학위논문, 2020, 170면.

36) 미국 법무부(DoJ),사이버범죄 소탕 및 보안강화를 위한 조사팀 신설 인용 (https://blog.naver.com/theboan/220246190214, 2021.07.25.검색)

37) 김득수, 사이버테러 대응을 위한 법제도 구축에 관한 연구, 동아대학교 대학원

사이버보안 전문 클러스터를 보유할 정도로 사이버보안 분야에 많은 노력을 기울이고 있다. 세계 주요국들의 이런 움직임들을 볼 때 결국 선진국은 이미 10여 년 전부터 사이버 위협과 공격의 심각성을 인식하고 상설 사이버보안 조직 등을 도입하고 있는 것을 볼 수 있다. 특히 미국은 2009년 대통령 직속으로 국가사이버보안정책을 총괄 지휘하는 '사이버보안조정관'을 임명하고, 전담조직도 국가안전회의 소속으로 끌어올려 조직 활동의 중요성을 더욱 부각시키고 있다. 그러나 우리나라는 아직도 국가위기관리센터에 범정부 사이버위기 대책본부를 비상설조직으로 두고 있는 수준이며, 그 조직도 국가정보원(공공·국가기관)과 방통위(민간), 국방부로 역할이 나누어져 있어 사이버테러에 대한 대응능력이 떨어질 수 있다. 또한 매년 3만 건이 넘는 사이버공격을 국정원과 경찰·인터넷진흥원의 인력으로 감당하는 것은 한계가 있다. 그러므로 국가안보를 대비한 전문 사이버테러 대응 인력의 체계적인 육성과 대규모의 전문인력 확보는 무엇보다 시급하다.[38] 사이버테러는 더욱 고도화 될 것이며 우리나라도 사이버 범죄들로부터의 피해를 사전에 방지하기 위해서는 국가차원의 사이버테러 대응체계를 확고하게 구축하여 21세

박사학위논문, 2020, 171-175면.

38) 일례로 초대형 인터넷 쇼핑몰인 '인터파크'가 2016년 5월 초 전문해커들에 의해 해킹을 당해 전체 회원 2,000여만 명의 절반이 넘는 1,030만 명 회원의 이름, 생년월일 등 개인정보가 유출되는 사건이 발생했다. 사건 발생 후 경찰청 사이버안전국과 정부 합동조사팀이 수사를 한 결과 북한 정찰총국 소속 전문해커들의 소행으로 밝혀졌다. 이 사건의 경우 비록 국가를 상대로 한 테러는 아니었지만, 사건의 규모나 방법 등에서는 충분히 국가기관을 파괴할 수 있을 정도의 상당한 위험을 안고 있었다. 당시 경찰청 사이버안전국의 조사를 보면, 이 정보 유출 사건은 해외에 서버를 둔 APT(Advanced Persistent Threat) 해킹 조직의 소행으로 파악됐다. APT 해킹은 이메일이나 웹문서를 통해 악성코드를 설치해 놓고 오랜 기간 잠복했다가 D-DAY가 오면 일제히 공격을 하는 방식이다. 이 사건의 경우도 해커가 인터파크 직원들의 이메일에 미리 악성코드를 심어 놓은 후 일정 기일을 잡아 실행에 옮기는 수법을 쓴 것이다.

기의 새로운 사이버범죄에 적극적으로 대비하여야 한다.

3) 사이버안보와 개인정보 보호의 충돌 문제

최근 사이버 안보에 대한 위협에 강력하게 대응하기 위한 조치가 개인정보보호와의 갈등 양상을 보이면서 사이버 안보와 개인의 정보와 관련한 인권의 중요성도 가조되고 있다. 국가 안보와 개인정보 보호는 상호 갈등관계로만 보기는 힘들며 오히려 개인정보 보호를 위한 조치는 정보보안 수준의 향상에도 긍정적인 영향을 미치는 협력적 관계로 보아야 한다. 정보의 보안과 개인정보의 보호간의 관계가 상호 선순환의 관계가 될 수 있도록 정책의 방향을 제시하여야 한다. 현행 「개인정보보호법」은 제58조(적용의 일부 제외) 제1항 제2호에서 “국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보”에 대해서는 개인정보보호법 제3장부터 제7장까지를 적용하지 아니함을 규정하여 사이버 안보와 관련한 예외적 조치에 관한 근거를 마련하고 있다. 그러나 정보 수집에 있어 비식별화 조치에 관한 사항 등 세부적인 절차에 관하여는 따로 논의되지 못하고 있다. 또한 정부 입법안에서는 개인정보보호법 제58조의 취지를 충분히 반영하지 못한 지나치게 광범위한 예외 가능성이 있다는 비판이 존재한다. 사이버 안보와 사이버위협정보의 개념 및 범위, 정보 공유 기타 제공 목적, 정보 제공범위 등을 명확하게 규정할 필요가 있다. 현행 「국가사이버안전관리규정」에서 사이버공격을 탐지하고 대응 체계로 보안관제센터를 구축하며 운영하는 것은 국민들의 개인정보에 대한 합법적인 범위를 넘어선 수집과 이용에 대한 직접적 근거 될 수 없다.[39] 그러므로 보안관제센터가

39) 권종필, 「국가 사이버안보 기본법」 제정안에 대한 개인정보 침해요인 평가 결과, 개인정보보호위원회 결정(의안번호 제2016-20-44호),2016, 1-5면.

접근기록자료를 수집·이용할 수 있다는 근거를 별도로 규정하여야 한다. 무엇보다 사이버보안 위협정보의 원활한 공유를 하여야 한다. 민간이 정보를 수집하고 활용함은 물론 수집된 정보를 공공에 제공하는 과정에서 개인정보보호를 위한 법적 의무를 충실하게 이행하여야 하며, 이에 대한 구체화된 기준을 정립하여야 한다.

4) 국제사회와의 공조체제의 미흡

인터넷의 세계는 물리적 한계가 존재하지 않는다. 국경과 영토를 초월하는 사이버범죄는 매년 증가하고 있으므로 이에 대한 국제적 공조는 필수가 되었다. 사이버 범죄의 증거는 신속한 확보가 관건이며, 휘발성이 강하므로 증거를 빠르게 확보하지 못하는 경우 범인을 검거해도 처벌하기가 쉽지 않다. 따라서 신속한 수사체계를 위하여 기존의 형사사법공조시스템이나 인터폴 등을 통한 수사로는 한계가 존재한다. 현재 우리나라는 국제공조가 가장 활발하게 이루어지고 있는 사이버범죄협약(일명 부다페스트협약)에는 국내문제로 가입을 유보하고 있다. 그 결과 국제적인 공조수사가 원활하지 못하여 사이버 범죄에 대한 수사의 어려움이 많다. 사이버범죄는 날로 진화되고 체계화 분업화되고 있다. 사이버공간을 통한 도박이나 음란물유포, 또는 마약거래 뿐 아니라 국가 안보를 위협하는 사이버 공격을 대응하기 위한 국제공조가 절실하다.

라. 법제정비 방안

1) 사이버테러기본법의 제정 및 대응체제의 일원화 구축

우리나라의 사이버보안과 관련된 현행 조직체계는 법률이 아닌 대통령 훈령(행정규칙)에 근거한다. 국가사이버전략회의, 국가사이버안전대책회의 및 국가사이버안전센터 등의 사안별 임시적 성격

을 갖고 있는 조직에서 관련 업무를 관장하고 있다. 뿐만 아니라 각종 법령상 근거에 기반을 두어 국가정보원, 미래 창조과학부 등이 실질적인 대응 업무를 공동으로 수행하고 있다. 결국 법률상 업무의 중첩과 불명확성이 국가 안보차원의 사이버테러 사안에 대한 원칙적 대응하기 힘든 구조이다.[40] 비교법적 검토에서 살펴보았듯이 일본의 경우와 같이 우리나라도 통합 '사이버테러(안보)관련기본법'을 제정해서 대응체계를 일원화가 필요하다. 그리고 최소한 기존 국가사이버전략회의와 국가사이버안전대책회의 및 국가사이버안전센터의 운영에 대한 법률적 근거와 지침을 마련해야 한다. 또한 보다 구체적으로 이들의 권한까지도 규정해서 사이버보안 분야의 컨트롤타워와 실무책임자의 지위를 실질적으로 부여해야 할 것이다. 뿐만 아니라 정부기관과 민간부문을 전체 포함한 관련 기관간의 경보체계 및 정보공유 관련된 법제도의 정비가 필요하다. 예를 들자면 사이버테러 대응 기구 간에 정보공유를 위한 법적 근거를 확보해야 한다. 그리고 해당정보에 관한 오·남용을 방어하기 위한 제도적 장치가 필요하다. 또한 사이버테러 위협에 대응하기 위해 국가차원에서 경보체계의 도입시행에 관한 사항이 규정되어야 한다. 또한 국가의 인프라를 담당하는 주요정보통신기반시설을 포함한 국민의 생활과도 바로 연결되는 사이버 인프라의 기술과 운영의 표준화를 위한 지침을 명확히 할 필요가 있다. 현재는 정부기관, 국방, 민간에 대하여 별도로 관리되고 있다. 하지만 일원화된 신속한 대응과 활동수준의 평가와 효과적인 정책이 제대로 이루어지기 힘들어 보이며, 현행 법제의 문제점을 살피고 이에 관한 개선을 하여야 한다.

---

40) 미래창조과학부, "사이버세상의 새로운 규범체계 정립방안 연구", 미래창조과학부 연구자료, 2014, 112면.

2) 사이버테러 대응을 위한 전문가 양성

장기적으로 사이버테러에 대비한 전문인력을 양성을 하여야 한다. 우수한 전문인력을 확보하는 것은 미래의 국가 안보를 위해서도 매우 중요하다. 점차 진화되고 있는 사이버테러 공격에 대응하기 위해서 사이버무기를 개발하거나 운영할 뿐 아니라 또한 이를 통제하고 방어하는 전문적인 사이버 안보 인력을 양성하여야 한다. 사이버안보와 관련한 전문인력 양성은 가장 필수적인 정책이다. 구체적으로 초등학교 방과 후 특기수업을 통해 인재를 양성하고, 중·고등학교에서의 인재를 발굴하며 대학, 대학원에서 전문적인 수업과 실습을 통한 전문인력이 양성되어야 한다. 국방 사이버전쟁의 기획과 계획수립, 사이버전쟁의 시행 및 사이버 전쟁을 수행할 전문 인력의 육성과 기술을 개발하여야 한다.

3) 사이버안보와 개인정보 보호 간의 균형과 조화

사이버 안보와 국민의 개인정보 보호가 양립 불가능한 관계인지에 대한 검토를 하여야 한다, 먼저 국민의 개인정보 보호와 관련하여 헌법은 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다(제10조). 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다(제17조). 모든 국민은 통신의 비밀을 침해받지 아니한다(제18조). 언론·출판에 대한 허가나 검열과 집회·결사에 대한 허가는 인정되지 아니한다(제20조 제2항).”고 규정하고 있어 개인의 정보보호 역시 당연히 보호되어야 하는 헌법적 권리로 규정하고 있다. 즉 개인정보 자기결정권은 자기 자신에 관한 정보가 언제 누구에게 어느 정도의 범위까지 알려지고 또한 이용되도록 할 것인지를 정보 주체인 자신이 스스로 결정할

수 있는 권리이다. 개인정보 자기결정권의 보호대상은 개인의 신체와 신념 또는 사회적 지위 및 신분 등과 같이 개인의 인격주체성을 특징짓는 사항이다. 다시 말해 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있다. 이는 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다.[41] 개인정보는 포괄적으로 보호된다고 할 수 있다. 반면, 국가 안보, 사이버 안보와 관련하여 헌법 제37조 제2항은 "국민의 모든 자유와 권리는 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다."라고 규정하여 개인 권리라 하더라도 필요한 경우 제한이 가능하도록 규정되어 있다. 이는 국가 안보라는 측면에서 개인정보보호 부분에 관한 어느 정도 제약을 가할 수 있는 근거에 해당한다. 국가 안보와 개인정보 보호는 상호 충돌하는 모습을 보이지만 이들은 상호 조화를 이루어야만 국가와 개인 모두 사이버 위협으로부터 안전을 보장받을 수 있다. 다만 방법론적 측면에서 이를 어떻게 구현할 것인가는 중요한 문제이다. 현행 형사소송법과 통신비밀보호법 등 관련 법률에서는 일반적 절차적인 면을 규율하지만, 사이버 공간에서의 개인정보의 종류와 접근 방법 등이 다양함에 따라 사이버 공간에서의 개인정보와 관련된 일반적 규정을 제정하는 것도 고려해 볼 필요가 있을 것으로 생각된다.

4) 국제사회와의 공조체제 강화

해외 국가들과의 국가 사이버안보 공조대응을 위해서는 사이버 공격, 취약점, 전문가, 기술, 수사와 처벌에 대한 국제적 관계를 정립하고 공조체계를 수립하여야 한다. 사이버범죄와 사이버 공격,

41) 대법원 2014. 7. 24. 선고 2012다49933 판결.

더 나아가 사이버 전쟁에 대비하기 위하여 국제적 공조관계는 필수적이다. 사이버테러 정보보호와 사이버테러 수사공조를 위한 상호협조와 보안기술의 공동개발을 해야 한다. 또한 사이버테러 위협에 공동 대응하기 위한 합동 전력 개발을 해야 한다. 마지막으로 IT 산업이 취약한 국가에 인터넷을 비롯한 네트워크 인프라 지원을 통해 적극적인 국제 협력체계를 강화해야 한다. 셋째, 유엔 아시아 태평양 정보통신교육원(UN APCICT)426)과 국제경제 협력기구(OECD), 국제 인터넷 주소관리기구(ICANN), 국제전기통신연합(ITU), 인터넷 소사이어티(ISOC), 사이버스페이스 총회(Conference on Cyberspace)를 비롯한 국제 다자기구 및 다국적과 적극적으로 협력해야한다. 이를 통해 사이버공간에서의 사이버범죄, 경제, 사회적 혜택, 사이버 보안, 국제공조, 국제안보 사이버경고와 통합체계구축, 예방체계 등 사이버테러 안전을 위한 적극적인 협력체계를 강화해야한다. 넷째, UN (United National), UN 정부전문가그룹 (UN Group Governmental Experts), UN의 국제통신연합 및 인터폴(Interpol) 등 국제기구와 글로벌 조직을 통하여 사이버테러 정보공유 및 중요한 국가 기반시설을 보호해야 한다. 또한 사이버테러 범죄에 대하여 국내법과 국제법사이의 정책적 조화 및 조정을 통하여 국제 사이버테러 안전을 보장받기 위한 대응체계를 마련하여야 한다.[42)]

V. 결론

첨단과학기술사회에서 발전된 기술들로 우리는 수없이 많은 부

42) 미래창조과학부, "사이버세상의 새로운 규범체계 정립방안 연구", 미래창조과학부 연구자료, 2014, 112면.

분에서 혜택과 편리함을 누리고 있다. 인류의 기술은 최근 100년 동안 진화의 속도보다 훨씬 빠른 속도로 문명의 발전을 만들어내었고 미래의 10년은 더욱 빠르게 우리의 삶을 변화시킬 것이다. 사이버 안보도 인공지능(AI)기술과 같은 과학기술의 발전으로 인하여 위협을 받기도 하고 더욱 발전하기도 한다. 4차 산업혁명으로 초연결사회가 형성되면서 이를 위협하는 새로운 유형의 사이버테러는 더욱 진화되고 있는 시점에서 산발적으로 규정 되어있는 기존의 개별 법령으로는 효율적으로 대응하기에는 어려움이 많다. 따라서 이를 총괄할 수 있는 사이버테러 관련 기본법 제정을 하여야 한다. 현재 우리나라의 사이버 안보 관련 법체계는 2005년 대통령 훈령(제141호)으로 제정된 국가사이버안전관리규정을 비롯하여 정보통신망법, 정보통신기반보호법, 전자정부법 등을 들 수 있다. 특히, 명목상으로 국가사이버 안보를 주도하고 있는 국가사이버안전관리 규정은 법률의 형식이 아닌 대통령훈령으로서 공공분야만 규율하고 민간분야는 규율하지 못한다는 한계를 지니고 있다.[43] 또한 사이버테러 관련 내용을 직간접으로 규율하고 있는 주요 법률로는 "「정보통신망이용 촉진 및 정보보호등에 관한 법률」, 「정보통신기반보호법」, 「국가정보화기본법」, 「전자정부법」, 「개인정보보호법」, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 등이 있다. 그러나 이러한 법률들은 국가안보 문제를 심도있게 규정하고 있지는 않으며 정보통신 산업의 진흥과 이를 악이용 하려는 행위자들의 처벌에 대하여 주안점을 두고 있거나, 각 분야의 시스템을 안정적으로 유지하기 위한 수단으로 활용되는 실정이다. 결과적으로 개별 법령들만

43) 김일환, "초연결사회에서 개인정보보호법제 정비방안에 관한 연구", 성균관법학 제29권 제3호, 2017, 70-73면; 김일환 외 4명, "통합적 사이버 위기관리 체계의 필요성에 관한 연구", 한국융합보안학회 제9권 제1호, 2009, 30-37면.

으로는 명확한 의미에서 사이버 공격으로부터 국가안보를 보장하는데 부족한 것으로 보인다. 이와 관련하여 사이버 테러에 대한 컨트롤 타워가 부재하다는 평가와 함께 체계적인 협력이 어렵다는 지적과 비판도 있다. 그러므로 사이버테러를 통할할 수 있는 기본법안의 제정이 필요하다. 북한은 지난날 사이버테러 공격으로 우리의 국가기능을 일시에 무너뜨렸다. 지금도 평양의 사이버 해커들은 그 능력을 나날이 높여가고 있다. 이들은 사회 인프라가 우리나라에 비해 턱없이 부족하면서도 사이버 테러 능력을 강화하는 이유는 사이버 공간의 특징을 충분히 활용한다면 전략적으로 우위를 선점할 수 있기 때문이다. 과거 북한은 정부기관, 금융기관, 언론사를 막론하고 무차별적인 사이버테러를 감행했고, 지금도 공격태세를 강화하고 있다. 그러나 이를 방어하는 우리는 그 속도를 따라가지 못할 뿐 아니라 해외 주요 선진 국가가 갖추고 있는 대응체계에 비하여 취약한 점을 가지고 있다. 분단국가라는 특수한 상황에서 북한의 공격을 방어하기 위하여 사이버공격이 일어났을 때 피해를 최소화하고 즉각적인 대처가 가능하도록 하는 실질적인 컨트롤 타워를 구축하는 등 법제정비가 필요하다. 국가 안보와 개인정보 보호는 상호 충돌하는 모습을 보이지만 이들이 상호 조화가 이루어질 때 사이버 테러로부터 안전한 국가가 보장된다. 다만, 그 방법론적 측면에서 어떻게 접근할 것인지에 대한 검토가 필요하다. 현행 형사소송법과 통신비밀보호법 등 관련 법률에서는 일반적 절차적인 면을 규율하고 있으나, 사이버 공간에서의 개인정보의 종류와 접근 방법 등이 다양함에 따라 사이버 공간에서의 개인정보와 관련된 일반적 규정을 제정하는 것도 고려해 볼 필요가 있다. 또한 국경을 초월하고 있는 사이버테러에 대응하기 위해서는 국제사회와의 공조가 필수적이다. 따라서 사이버테러의 역량을 강화하고 대응속도를 높이

기 위해서는 국제공조가 가장 활발하게 행해지고 있는 사이버범죄 협약에 가입하여야 하며 해외 주요 국가들과 조속히 협력체계를 구축하여 국제협력 네트워크를 형성해야 한다.[44] 사이버 공간의 문제는 어느 특정 집단만의 문제가 아니라 모든 국민에게 직결되는 문제로 중요성이 인식된다. 이러한 현실에서 사이버테러, 위협, 더 나아가 사이버 전쟁으로부터 사이버보안체계를 구축하는 것이 어느 때보다 중요하다. 특히 북한으로부터의 전쟁 위협과 미국 등 선진국들이 사이버안보 위협에 대처하기 위해 정보역량 확충에 매진하고 있는 만큼, 우리나라도 국가정보기관도 보다 더 유기적이고 효율적인 정보협력 체제를 구축하고, 구체적이고 체계적인 법체계를 구축하여야 한다.

44) 김득수, 사이버테러 대응을 위한 법제도 구축에 관한 연구, 동아대학교 대학원 박사학위논문, 2020, 150-155면.

참 고 문 헌

1. 단행본

미래창조과학부, “사이버세상의 새로운 규범체계 정립방안 연구”, 미래창조과학부, 2014.

2. 국내논문

곽관훈, “일본의 사이버보안기본법 제정 의의 및 시사점”, 경북대학교 법학연구소, 2019.

권혁천, “북한의 사이버 공격양상 비교연구”, 건국대학교 박사학위논문, 2020.

김득수, 사이버테러 대응을 위한 법제도 구축에 관한 연구, 동아대학교 대학원 박사학위논문, 2020.

김상배, “국가 사이버 안보 전략의 국제비교: 한반도 주변4국과 유럽 주요3국의 사례”,「워킹페이퍼」No.7, 서울대학교 국제문제연구소, 2017.

김병운, “초연결산업 사회, 사이버보안 정책”,「과학기술법연구」제22집 제3호, 한남대학교 과학기술법연구원, 2016.

박상철, “기본권 보장 강화를 위한 통신수사 개선방안 연구”, 성균관대학교 석사학위논문, 2020.

백수원, “헌법상 안전에 대한 국가의 의무”, 미국헌법연구 제27권 제3호, 2016.

성봉근, “사이버상의 안전과 보호에 관한 독일의 입법동향과 시사점”,「법과정책연구」제17권 제1호, 한국법정책학회, 2017.

심우민, “사업장 전자 감시 규제 입법의 성격”, 인권법평론 제12호, 전남대학교 법학연구소 공익인권법센터, 2014.

양정윤, “미국의 법제도 정비와 사이버안보 강화: 국가사이버안보보호법 등 제·개정된 5개 법률을 중심으로”,「입법과 정책」제7권 제2호, 국회입법조사처, 2015.

양천수·지유미, “미국사이버보안법의 최근동향: 사이버보안정보공유법을

중심으로 하여", 법제연구 통권 제54호, 한국법제연구원, 2018.
양천수, "제4차 산업혁명과 정보보호 법정책의 방향",「공법학연구」제18권 제4호, 한국비교공법학회, 2017.
유승화, "사이버안보 법제 개선방안 연구", 목포대학교 법학 석사학위논문, 2020.
이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구",「국가정보연구」제1권 제2호, 한국국가정보학회, 2008.
정용기, "우리나라의 사이버 안보 위협현황과 대응방안", 원광대학교 경찰학연구소, 경찰학논총 제11권 제4호, 2016.
조명현, "현대 국가안보 개념과 체계적 안보분석틀",「사회과학연구」제7권, 충남대학교 사회과학연구소, 1996.

3. 해외논문

Alexander Silhavy, Cyber-Sicherheitsstrategiefür Deutschland: Neue-Bedrohungen? Neue Lösungen?, Norderstedt, 2013.
Hans-Jürgen Lange/Astrid Bötticher(Hrsg.), Cyber-Sicherheit, Springer VS, 2014.
Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit, Tübingen, 2018.
Sebastian Leuschner, Sicherheit als Grundsatz: Eine grundrechtsdogmatische.
關啓一郎, "サイバーセキュリティ基本法の成立とその影響",「知的資産創造」, 2015.

<Abstract>

A Study on cyber security in the age of artificial intelligence (AI)

Kwon Su Jin*

Digital transformation and 5G innovation are accelerating even more after the COVID-19 crisis. The daily use of information and communication and the use and expansion of cyberspace have a direct impact on our real life. The use of information and communication technology is taken for granted in the essential daily life of all people, such as finance, medical care, education, and culture. As dependence on cyberspace increases and its importance increases, the potential risks of cyberspace, such as personal information infringement, industrial secret leakage, cybercrime, cyber terrorism, and cyber warfare, are diversifying and the extent of damage is increasing in proportion. Cyberspace is becoming a new risk area for countries, companies, and individuals as cyberattacks have recently diversified their routes, advanced levels and intelligence, and organized subjects. With the advent of new technologies such as artificial intelligence (AI) and technological convergence, the possibility of unpredictable risks is increasing. The rapid entry into the smart city and 5G society promotes the cyber-spatialization of daily life through the organic combination of on-offline and expands and reproduces cyber risks at the whole social level. The social importance of cyber security to effectively deal with such increasing cyber risks is also increasing. Due to the development of deep learning and the rapid development of big data technology, the potential of artificial intelligence is being maximized more than ever, and it is

* Senior Researcher, Korea Data Industry Promotion Agency, Ph.D.

recognized as a core technology of the 4th industrial revolution that will change the future of all industries. The field of cybersecurity is no exception. Every year, the number of devices connecting to the Internet grows exponentially, with more than one million new threats emerging every day. As hacking techniques are advanced day by day, such as advanced persistent treat (APT), the security field has also become one of the fields requiring the application of artificial intelligence. The scope of cyberattacks is expanding not only in cyberspace but also in physical space, affecting not only individuals, but also society and economy, as well as the operation of important national infrastructure. The impact of artificial intelligence (AI) technology on the cybersecurity field and We will examine the contents and trends of cybersecurity-related laws and examine implications for Korea.

Key Words : Cybersecurity, Artificial Intelligence (AI), Legislative Reorganization, 4th Industrial Revolution, Security, Safety right, basic right, personal information