연구논문

미국의 사이버안전에 관한 법 제정 동향과 시사점

박 노 형*

차 례

* 고려대학교 법학전문대학원 교수, 법학박사. 본 논문은 2014년 4월 17일 "사이버공간과 국가안보"를 주제로 국가안보전략연구소가 주최한 학술대회에서 발제한 원고를 수정 및 보완하였다.

접수일자 : 2014. 4. 30. / 심사일자 : 2014. 5. 26. / 게재확정일자 : 2014. 5. 30.

Ⅰ. 사이버안전에 관한 법의 문제 일반

해킹 등에 의하여 기업정보는 물론 개인정보가 탈취 또는 침해되고, 군사안보적으로도 중요한 핵시설 등이 Stuxnet 등의 맬웨어에 의하여 그 기능이 마비되는 등 사이버공간의 안전에 대한 우려가 현실이 되고 있다. 이제 사이버범죄, 사이버테러는 물론 사이버전쟁은 일반인에게도 일상에서 쉽게 접할 수 있는 용어가 될 정도이다. 사이버공간의 안전 또는 사이버안전은 현 시점에서 국내는 물론 전 세계의 공통된 심각한 문제임에 틀림없다.

사이버안전은 궁극적으로 법률에 의하여 보장되어야 하는데, 최근에 국내에서도 사이버안전을 위한 법률안이 국회에 제출되었지만, 사이버안전의 책임기관 문제 등에 관한 정치적인 다툼으로 그 내용의 깊은 논의도 이루지 못하고 있다. 이와 관련하여 최근에 미국에서도 사이버안전에 관한 법률이 채택되지 못하고 있지만, 행정부와 의회 사이에서 깊은 논의가 이루어지고 있어서, 국내의 관련 법률의 논의에 중요한 시사점을 줄 수 있다. 본고는 미국의 사이버안전에 관한 입법동향의 분석을 통하여 국내의 관련 법률의 논의에 참고 될 수 있는 시사점을 도출하고자 한다.

1. 기본 개념의 정의

'Cyber' 용어는 다양하게 사용되지만, 사업, 법, 정책 분야에서는 '인터넷과 다른 전자통신으로 창조된 물리적이지 않은 가상세계'(the other than physical, virtual world created by the Internet and other electronic communications)를 가리키는 것으로 이해된다.[1] 'Cyber' 용어에 'Space' 용

1) James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (eds.), *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2,* EastWest Institute and the Information Security Institute of Moscow State University, 2014, p.17. 'Cyber' 용어는 '조종하거나 지배하는데 숙련된'을 의미하는 그리스어 'κυβερνητικός'에서 유래하였다고 한다. *Cybernetics or Control and Communication in the Animal and the Machine* (MIT Press, 1948)을 통하여 'Cyber' 개념이 널리 알려지게 되었는데, 저자인 Norbert Wiener는 'Cybernetics'를 동물세계와 기계적 네트워크의 복잡한 시스템의 통제 맥락에서 사용하였다.

어가 결합한 ‘사이버공간’(cyberspace)은 차원을 가지며, 따라서 넓은 공간을 차지하여야 한다.[2] 사이버공간은 ‘정보가 생성되고, 전송되며, 수신되고, 저장되며, 처리되고, 삭제되는 전자적 매개’(an electronic medium through which information is created, transmitted, received, stored, processed and deleted)라고 정의될 수 있다.[3] 이러한 사이버공간은 육지, 바다, 상공, 우주에 이은 새로운 영역으로 간주되는데, 이들 전통적인 네 가지 영역은 자연적이지만 사이버공간은 인간이 창조하여서 인위적이다. 사이버공간은 육지, 바다, 상공 및 우주의 기존의 구분되는 모든 영역에 스며들어 이들 영역을 아우르는 유일한 영역이다. 또한, 사이버공간은 사이버기반시설에 따라 만들어지기 때문에,[4] 자신을 구성하는 물리적 구성요소 없이 존재할 수 없다.

영어 ‘security’ 용어는 국내에서 문맥에 따라 안전, 안보, 보안 등 다양한 의미의 용어로 이해되고 있다.[5] 보안은 비밀사항의 보호와 같이 다소

2) James B. Godwin III, *ibid*, 2014, p.17.

3) James B. Godwin III, *ibid*, 2014, p.17. 미국 국방부는 사이버공간을 ‘인터넷, 통신네트워크, 컴퓨터시스템 및 내장 처리기와 통제기를 포함한 정보기술기반시설과 상주 데이터의 상호의존적 네트워크로 구성되는 정보환경 내의 세계적 영역’(A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers)이라고 정의한다. United States of America Department of the Army and United States Marine Corps Department of the Navy, “Department of Defense Dictionary of Military and Associated Terms(Joint Publication 1-02)”, 2010.11.8.

4) James B. Godwin III, *ibid*, 2014, p.16. 사이버기반시설(cyber infrastructure)은 ‘사이버공간을 구성하는 사람, 프로세스 및 시스템의 집합’(the aggregation of people, processes and systems that constitute cyberspace)으로 정의된다. James B. Godwin III, *ibid*, 2014, p.18.

5) 흥미롭게도 영어의 ‘security’에 상응하는 러시아어 용어는 보호만을 의미하여 영어의 ‘security’가 포함하는 이러한 보호를 제공하는 수단을 배제한다. James B. Godwin III, *ibid*, 2014, p.33. 예컨대, 미국 대통령의 정책지침인 PPD-21에서 안전(security)은 '침입, 공격, 또는 자연적 또는 인위적 재난의 효과에 대한 물리적 수단 또는 방어사이버조치에 의하여 핵심기반시설에 대한 위험의 감소'(reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters)라고 정의되었다. The White House, “Presidential Policy Directive 21(PPD-21) -- Critical Infrastructure Security and Resilience” (2013.2.12.), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2014.4.30. 검색). 이 같은 용어의 의미 차이로 미국과 러시

기술적이고 전문적인 의미로 이해되고, 안보는 국가의 안전보장의 의미로 이해되며, 안전은 이들을 포함하는 보다 넓은 개념으로 이해될 수 있다. 따라서 'cybersecurity'는 국내에서 '사이버안전' 또는 '사이버안보'로 혼용되고 있는데, 본 논문에서는 사이버공간에 전반적으로 관련되는 점에서 '사이버안전'이라고 부른다. 보다 일반적인 사이버안전이 유지되지 않으면서 보다 민감하면서 특정적인 사이버안보가 유지되지는 않을 것이다.[6] 이러한 사이버안전은 '의도되거나 의도되지 않은 위협에 저항하고 대응하며 회복할 수 있는 능력인 사이버공간의 속성'(a property of cyberspace that is an ability to resist intentional and/or unintentional threats and respond and recover)으로 이해된다.[7]

사이버공간에 관련된 법적 개념 중에서 특히 도발(aggravation)에 관련된 개념, 예컨대 '사이버-위협, 침해, 범죄, 테러, 전쟁' 등에 관하여 국제적인 합의에 따른 통일적인 사용이 필요하다. 특히 사이버공간이 국경개념을 모르는 성격을 가진 점에서 국내법상 의미는 국제법상 의미와 일치해야 한다. 예컨대, '사이버공격'(cyber attack)이 원래는 국제법, 특히 무력

아의 사이버안전에 관한 논의에 혼선이 빚어지기도 한다.

6) 예컨대, 국가안보를 위협하는 사이버공격에 종합적이고 체계적인 대응을 위하여 관계부처 합동의 「국가사이버안보마스터플랜」이 시행되고 있는데, 여기서는 '사이버안보'의 용어가 사용된다. 그러나 「국가사이버안전관리규정」에서는 '보안'의 용어 대신 '안전'의 용어가 사용되는데, 동 규정의 채택 당시 참여정부가 보안의 부정적 어감을 피하고자 '사이버보안' 대신 '사이버안전'의 용어가 사용되었다고 한다. 정필운, "사이버보안이란 개념 사용의 유용성 및 한계", 「연세 의료·과학기술과 법」 제2권 제2호, 연세대학교 법학연구원, 2011, 9쪽; 정완, "한미 사이버보안 법제 동향에 관한 고찰", 「경희법학」 제48권 제3호, 경희대학교 법학연구소, 2013, 216쪽에서 재인용.

7) James B. Godwin III, *supra* note 1, 2014, p.33. 「국가사이버안전관리규정」은 사이버안전을 '사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태'라고 정의한다. 동 규정 제2조 제3호 참조. 한편, 국제전기통신연합(International Telecommunication Union: ITU)은 사이버안전을 '사이버환경과 조직 및 이용자의 자산의 보호에 이용될 수 있는 수단, 정책, 안전 개념, 안전 보호조치, 지침, 위험관리접근, 행동, 훈련, 모범관행, 보장 및 기술의 집합'(the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets)이라고 정의한다. ITU, "Definition of cybersecurity", http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (2014.4.16. 검색).

충돌법(*jus ad bellum*)과 국제인도주의법(*jus in bello*)에서 고유의 의미를 가지고 사용되는 것인데, 이제 신문 등 언론이 일반적으로 사용하고 있어서, 개념의 혼란을 가져오고 있음에 유의하여야 한다. 특히 일상적인 '사이버침해사고'(cyber incident)에 불과한 경우를 '사이버공격'이라고 부름으로써 사이버안전에 대하여 지나치게 민감하거나 아니면 둔감하게 될 우려도 있다.[8)]

2. 사이버안전 관련 법정책의 발전

사이버공간에서의 안전, 즉 사이버안전이 현실적으로 중요하고 민감한 사안으로 인정됨에 따라 OECD와 NATO, EU 및 미국 등 주요 국가와 국제기구가 국가사이버안전전략(national cyber security strategy)을 수립하고, 관련 입법에 박차를 가하고 있다. 예컨대, EU는 아직 완전하게 단일한 국가체제를 갖추지 않고 있음에도 최근 사이버안전을 위하여 EU차원의 입법을 추진하고 있다. 즉, 2013년 2월 유럽위원회와 외교안보정책고위대표(High Representative of the Union for Foreign Affairs and Security Policy)가 제안하고 동년 6월 EU이사회가 추인한 「EU사이버안전전략」(EU Cyber Security Strategy)이 동년 7월 출범하였다.[9)] 동 전략은 EU가 사이버안전에 관하여 채택한 첫 포괄적 정책이다.[10)]

국내에서도 사이버침해로 야기되는 피해가 우리 사회의 전 분야에서 확인됨에 따라 사이버안전에 관한 법제도가 마련되고, 이들 법제도에 대

8) 「국가사이버안전관리규정」은 사이버공격을 '해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위'라고 정의하는데, 이러한 정의는 국제법상 확립되는 정의와 거리가 먼 다소 세속적인 내용이라고 볼 수 있다. 동 규정 제2조 제2호 참조.

9) European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013.2.7.

10) 또한 유럽의회는 2014년 3월 13일 「네트워크/정보안전지침」(Network & Information Security Directive)을 521명 찬성, 22명 반대 및 25명 기권으로 통과시켰다. 동 지침은 중대한 사이버침해사고(cyber incidents)에 대한 EU회원국들의 대응 및 협력을 규정하는데, 2014년 말까지 채택될 것으로 예상된다.

한 연구를 통하여 다양한 문제들이 제기되고 있다. 흥미롭게도 국내 사이버안전에 관한 법제도에서 제기되는 문제는 해당 법규범의 법적 지위와 관련 기관의 권한 행사의 배분에 집중되어 있다.[11] 예컨대, 국내 사이버안전에 관한 대표적인 법규정은 「국가사이버안전관리규정」(대통령훈령 제310호)이다. 동 규정은 '국가사이버안전에 관한 조직체계 및 운영'에 대한 사항을 규정하고 '사이버안전업무를 수행하는 기관간의 협력'을 강화함으로써 '국가안보를 위협하는 사이버공격'으로부터 '국가정보통신망을 보호'함을 목적으로 한다.[12] 동 규정은 대통령훈령의 지위를 가지고 있는 점에서 사이버안전이라는 국가의 핵심적 책무에 적절한지 여부도 문제로 지적될 수 있다. 또한, 사이버안전에 관한 다른 중요한 법률인 「정보통신기반보호법」은 주요정보통신기반시설의 보호를 위한 것인데, 이에 관하여 국가정보원과 안전행정부 사이에서 주요 정보통신기반시설의 총괄관리에 대한 영역배분 및 관련 중앙행정기관의 역할에 대한 정의가 필요하다고 지적된다.[13] 더욱이, 현재의 사이버안전을 직접적으로 다루는 위의 법규정은 물론 기존의 국가안전에 관한 법규정이 사이버라는 특성을 반영하지 못하는 점에서 대폭적인 개편이 필요하다는 주장도 제기된다.[14]

한편, 국내에서 최근 사이버안전에 관한 법률의 채택 등 기본적인 법적 접근 대신 '정책'의 채택이 선호되고 있다.[15] 이러한 사이버안전을 위한 정책은 당시 일련의 심각한 사이버침해를 경험한 후 범정부적으로 마련

11) 국내 사이버안전에 관한 법제도에 관하여 권문택, "국가사이버안전관리 조직의 통합적 체계구축에 관한 연구", 「정보·보안 논문지」제9권 제3호, 한국융합보안학회, 2009; 권창범, "사이버보안 특집: 사이버보안을 위한 국가적 추진체계 검토 및 발전방안",「연세 의료·과학기술과 법」제2권 제2호, 연세대학교 법학연구원, 2011; 정완, 앞의 글; 정준현, "고도정보화사회의 국가사이버안보 법제에 관한 검토", 「단국법학」제37권 제2호, 단국대학교 법학연구소, 2013 등 참조.

12) 동 규정 제1조. 동 규정은 '사이버공격'과 '정보통신망'을 정의하고 있는데, 이들 개념의 국제 및 국내 법체계에서의 타당성에 대한 검토도 필요하다.

13) 윤재석, 2011 경제발전경험모듈화사업: 한국의 정보보호 활동과 시사점, 한국인터넷진흥원, 2012, 54-55쪽 참조.

14) 정준현, 앞의 글.

15) 물론 최근 들어서 국회에 사이버안전 내지 사이버안보를 구체적인 내용으로 하는 가칭 '국가사이버테러방지에 관한 법률안', '국가사이버안전관리에 관한 법률안' 등 법안들이 제출되고 있기는 하다.

된 것이 특징이다. 즉, 2009년 '7.7. DDoS'(분산서비스거부) 공격 이후 「국가사이버위기종합대책」이 마련되었고, 2011년 8월 8일 '3.4. DDoS공격', '농협 전산망 장애사건' 등을 계기로 국가안보를 위협하는 사이버공격에 종합적이고 체계적으로 대응하기 위하여 관계부처 합동으로 마련된 「국가사이버안보마스터플랜」이 발표되었다.[16] 동 마스터플랜에 따라 각종 사이버위협에 총력 대응할 수 있도록 국가사이버안전센터를 중심으로 관계부처 간 협력 공조와 민간전문가 참여가 확대되고, 국가정보원의 컨트롤타워 기능과 부처별 역할이 명확하게 되어 그간 제기되었던 기관 사이의 업무 중복과 혼선 및 사각지대 발생의 문제가 해소될 것으로 기대되었다.[17] 또한, 사이버공간은 영토, 영공, 영해에 이어 국가가 수호해야 할 또 하나의 영역으로서 인정되었다. 그럼에도, 2013년 소위 '3.20. 사이버테러', '6.25. 사이버공격' 등 일련의 사이버위협이 지속됨에 따라 동년 7월 4일 사이버안보의 창조적 기반조성을 위하여 「국가사이버안보종합대책」이 발표되었다.[18] 동 대책은 사이버안보의 강화를 위하여 사이버위협 대응체계 '즉응성 강화', 유관기관 스마트 '협력체계 구축', 사이버공간 보호대책 '견고성 보강' 및 사이버안보 '창조적 기반 조성'의 소위 'PCRC (Prompt, Cooperative, Robust and Creative) 4대 전략'을 내용으로 한다.[19]

---

16) 방송통신위원회, "정부, 「국가 사이버안보 마스터플랜」 수립 - 국가 사이버공간 수호를 위한 범정부 차원의 청사진 마련 -" (2011.8.8.), http://old.kcc.go.kr/user.do;jsessionid=ogBWnpR9bkvnIDIxBUYYn11kOFRL9RmpMwYBKTWPPi8j49DrXwzdKxPIQpLftNGI.hmpwas01_servlet_engine4?mode=view&page=P02020700&dc=K02020700&boardId=1077&cp=1&boardSeq=32030 (2014.4.14. 검색). 그럼에도 동 마스터플랜은 범국가적 차원의 사이버위기관리 종합대책으로는 부족하다고 지적되었다. 이유지, "[취재수첩] 국가 사이버안보 마스터플랜 보완해야", 디지털데일리 (2011.8.10.), http://www.ddaily.co.kr/news/article.html?no=81127 (2014.4.14. 검색). 특히 정부 차원의 대응체계만 규정할 것이 아니라 국가안보를 위협하는 사이버전쟁 등의 상황이 발생했을 때 민간의 역할을 수행할 수 있는 법제도적 근거도 마련되어야 한다고 지적되었다.

17) 국가정보원은 평·위기시 총괄, 방송통신위원회는 방송통신 등 민간, 금융위원회는 금융, 국방부는 국방, 안전행정부는 전자정부대민서비스, 정부전산센터 등 각 부처 및 기관별 소관사항이 분장되었다.

18) 같은 날 발표된 「정보보호산업발전 종합대책」에서 최정예 정보보호인력 양성 등의 구체적 계획이 발표되었다.

19) 미래창조과학부, "정부,「국가 사이버안보 종합대책」수립 - 사이버안보 강화를 위한 4대 전략 (PCRC) 마련 -" (2013.7.4.), http://www.msip.go.kr/www/brd/m_211/view.do?seq=406 (2014.4.14. 검색).

행정부의 정책은 필요에 따라 시의적으로 채택될 수 있어서 효과적이라고 볼 수 있지만, 사이버안전의 확보를 위하여 다소 편의적으로 채택될 수 있는 정책 보다는 법률 중심의 법제도가 마련되어야 한다. 사이버안전을 위한 정부는 물론 민간부문의 활동이 헌법의 근간인 법치주의와 민주주의에 기반을 두어야하기 때문이다. 최근 몇 년에 걸쳐 미국에서는 사이버안전을 위한 다양한 입법적 노력이 추구되었는데, 법치주의와 민주주의를 기반으로 추구된 이러한 입법적 노력은 우리의 사이버안전에 관한 법제도의 마련에 큰 시사점을 줄 수 있다.

II. 미국의 사이버안전에 관한 입법 동향

미국은 특히 오바마 정부에서 사이버안전에 관한 입법이 뜨거운 감자로 부각되었다. 이는 사이버범죄 등 사이버침해사고가 현실적인 문제가 되고 있음에 기인한다. 예컨대, 2013년 7월 보도에 따르면, 사이버범죄로 미국에 초래되는 비용이 연간 천억 달러라고 추산되었다.[20] 또한 2006년부터 2012년까지 미국 연방정부에 대한 사이버공격은 782% 증가하였는데, 2012년 한 해에 48,000건의 침해사고가 보고되었다.[21] 테러방지가 미국의 최우선과제이지만, 사이버위협(cyber threat)이 조만간 미국의 최우선과제가 될 것이라고 한다.[22] 2012년 10월 당시 Leon Panetta 국방장관은 국가나 과격단체의 사이버공격은 9/11테러공격 만큼 파괴적일 수 있고, 이러한 파괴적인 사이버테러공격은 미국을 마비시킬 수 있다고 주장하였다.[23]

---

20) Siobhan Gorman, “Annual U.S. Cybercrime Costs Estimated at $100 Billion”, WALL STREET JOURNAL (2013.7.22), http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990 (2014.3.30. 검색).

21) U.S. Government Accountability Office, “Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented (GAO-13-187)”, 2013.2.

22) James R. Clapper(Director of National Intelligence), “Worldwide Threat Assessment of the US Intelligence Community(Statement for the Record, Senate Select Committee on Intelligence)”, 2013.3.12.

23) Jim Garamone, “Panetta Spells out DOD Roles in Cyberdefense”, American Forces Press Service (2012.10.11.), http://www.defense.gov/news/newsarticle.aspx?id=118187 (2014.3.30.

사이버안전에 관한 미국의 입법 노력에 있어서 2011년과 2012년의 2년 동안 제112차 회기에서 전개된 오바마 대통령과 미국 의회 사이의 대결 국면이 주목될 필요가 있다. 이러한 행정부와 의회의 대결 국면에서 사이버안전 관련 입법의 필요성과 그 내용에 관하여 중요한 시사점이 발견될 수 있기 때문이다. 전통적으로 민주당은 프라이버시와 시민적 자유를 옹호하고, 공화당은 국가안전을 옹호하고 있다. 또한 오바마 대통령은 특히 사이버안전을 미국의 최우선 과제로 정하고서 입법과 정책 수립에 많은 노력을 기울였다. 상원은 오바마 대통령과 같이 사이버안전을 위한 종합적인 입법을 추구하지만,[24] 하원은 대체로 개별 문제에 대한 입법을 추진하고 있다.[25]

1. 미국 의회의 입법 노력

사이버안전에 대한 현실적 우려에도 불구하고 미국 의회는 지난 10여 년의 기간 동안 사이버안전에 관한 입법에 있어서 무기력을 보이고 있다. 즉, 2001년 9/11테러 이후 채택된 Federal Information Security Management Act of 2002 이후 사이버안전에 관하여 별다른 법이 채택되지 않고 있기 때문이다.[26] 그럼에도 지난 3년여의 기간에 걸쳐 미국 의회에서 사이버안

검색).

24) 그러나, 미국 상원은 제112차 회기에서 종합적인 Cybersecurity Act of 2012 (S.3414)의 채택에 실패한 후 제113차 회기에서는 보다 세밀한 개별 문제에 대한 입법도 추진하는 것으로 보인다.

25) 예컨대, 미국 하원에서 검토된 개별적 법안의 예는 다음과 같다: Cyber Intelligence Sharing and Protection Act (H.R.624); Federal Information Security Amendments Act of 2013 (H.R.1163); Cybersecurity Enhancement Act of 2013 (H.R.756); Cyber Economic Espionage Accountability Act (H.R.2281); Advancing America's Networking and Information Technology Research and Development Act (H.R.967); Critical Infrastructure Research and Development Advancement Act of 2013 (H.R.2952); National Cybersecurity and Critical Infrastructure Protection Act (H.R.3696); and Homeland Security Boots-on-the-Ground Act (H.R.3107).

26) Eric A. Fischer, "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions(Congressional Research Service Report for Congress)", 2013.6.20, https://www.fas.org/sgp/crs/natsec/R42114.pdf (2014.3.30. 검색). 사이버안전에 관한 연방법은 건강, 금융 및 연방정부의 컴퓨터시스템의 보호에 집중하고 있다. 각각 1996 Health Insurance Portability and Accountability Act(HIPAA), the 1999

전에 관한 입법이 활발하게 시도된 것은 사실이다.[27] 미국 의회는 전기 등 에너지에 대한 스마트그리드나 금융기관 등 핵심기반시설(critical infrastructure)에 대한 사이버침해사고의 현실적 가능성 및 이의 미국 국가안보나 경제에 대한 피해 가능성을 인정하고, 정부와 민간부문의 정보시스템을 보호하도록 사이버안전을 위한 종합적인 입법개혁이 필요함은 인정하고 있다.[28] 그럼에도 미국 의회는 연방정부의 역할, 특히 국토안보부(Department of Homeland Security: DHS)의 책임과 능력, 민간부문의 역할, 정부와 민간부문과의 정보 공유, 핵심기반시설의 보호 기준 및 사이버안전에 필요한 인력 양성 등에 관하여 의견의 일치를 보지 못하였다.[29] 결국 미국 의회는 지난 10여 년 동안 미국의 사이버안전을 위한 다양한 법안을 검토만 하고 이들을 통과시키지는 못하였다.[30] 미국 의회의 사이버

Gramm-Leach-Bliley Act 및 2002 Homeland Security Act에 포함된 Federal Information Security Management Act(FISMA) 참조.

27) 예컨대, 미 하원의 다양한 위원회가 2011년 1월 3일부터 2013년 1월 2일까지의 제112차 회기에서 42건의 사이버안전 관련 청문회를 실시하였고, 2013년 1월 3일부터 2015년 1월 2일까지의 제113차 회기에서는 2014년 2월 현재 적어도 20건의 청문회를 실시하였다. 상원에서는 제112차 회기에서 19번의 청문회가 실시되었지만, 제113차 회기에서 2014년 2월 현재 7건의 청문회가 실시되었다. Mitchell S. Kominsky, “The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress: The Threat and Impact of Cyber Attacks”, Harvard National Security Journal, Harvard Law School, 2014. 참조.

28) Mitchell S. Kominsky, *ibid*, 2014. 이렇게 사이버안전을 위한 종합적인 입법이 필요한 이유 중의 하나는 예컨대, 사이버안전의 침해사고에 관하여 민간부문이 정부에게 관련 정보를 전달하도록 요구되는데, 이러한 전달로 해당 기업은 Electronic Communications Privacy Act 등 관련 미국법상 민사와 형사 책임을 질 수 있기 때문이다. 아래에서 소개되는 미국 대통령의 행정명령이 민간부문과 정부의 정보 공유를 규정하지만, 법적인 한계가 있다고 지적된다. 이러한 문제를 해결하기 위하여 제112차 회기와 제113차 회기의 하원에서 Cybersecurity Intelligence Sharing and Protection Act(CISPA)가 제안되었다.

29) Mitchell S. Kominsky, *ibid*, 2014.

30) 사이버안전과 관련한 미국 의회의 입법 노력에서 흥미로운 점은 2013년 이후 특히 최근에 개인정보 침해(data breach)에 집중적으로 대응하려는 노력이다. 2013년 말 미국의 대표적인 대형소매점인 Target에 대한 해킹으로 고객의 개인정보 침해가 발생하여 더욱 촉발되었다. Target은 4억 달러에서 십억 달러의 피해를 볼 것으로 예상하고 있다. Wiggin and Dana, “Cybersecurity Legislation: Is Congress Ready?”, (2014.2.11.), http://www.wiggin.com/14904 (2014.3.30. 검색). 미국 의회는 해킹에 의한 개인정보 침해로 고객인 미국의 수천만 국민의 신분도용(identity theft)으로 야기되는 제2차 피해의 방지에도 주목하고 있다. 이 같은 미국 의회의 개인정보 침해의 대응

법안 처리의 어려움을 해결하기 위하여 최근 John McCain상원의원은 사이버안전을 다루기 위한 특별위원회(Select Committee)의 설치 필요성을 언급하였다.[31]

최근 미국 의회에서 검토된 사이버안전에 관한 법안은 핵심기반시설의 보호와 정부와 민간부문 사이의 정보 공유에 집중하였다. 이는 미국에서 핵심기반시설의 대부분을 정부가 아닌 민간부문이 보유하고 있기 때문이다. 미국에서 이들 핵심기반시설의 85%를 민간부문이 보유하고 있다.[32] 핵심기반시설은 USA Patriotic Act of 2001에 규정된 것과 같은 의미로 이해되는데, '물리적 또는 가상적 시스템과 자산으로서 미국에 핵심적인 것이어서 이들 시스템과 자산의 파괴 또는 불능으로 안보, 국가경제안전, 국가공공보건 또는 안전, 또는 이들의 결합을 약화시키는 영향을 주는 것'(systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters)으로 정의된다.[33] 화학, 상업시설, 통신, 핵심제조시설, 댐, 군수산업시설, 응급서비스, 에너지, 금융, 식품농업, 정부시설, 보건시설, 정보통신, 원자력물질, 운송,

---

입법 추진은 개인정보 침해에 대하여 미국의 46개 주와 D.C. 등에서 시행 중인 서로 일치하지 않는 법을 통일하여 미국 전역에서 일관된 연방차원의 대응요건을 마련하려는 의도를 가진다. 미국 기업들이 주마다 다른 개인정보 침해에 대한 통고 등의 대응요건을 따르는데 큰 불만을 제기하고 피해자인 국민들도 적시에 적확한 피해구제를 받지 못하기 때문이다.

31) Kris Osborn, "Lawmakers Call for New Cyber Security Laws", Dodbuzz (2014.2.27.), http://www.dodbuzz.com/2014/02/27/lawmakers-call-for-new-cyber-security-laws/ (2014.3.30. 검색). 특별위원회는 특정 상설위원회의 권한이 아닌 특별한 기능을 수행하기 위하여 설치되는데, 입법 권한을 가지기도 하지만 대체로 조사 권한을 가진다. Wikipedia, "Select or special committee (United States Congress)", http://en.wikipedia.org/wiki/Select_or_special_committee_(United_States_Congress) (2014.4.14. 검색).

32) StaySafeOnline.org, "Cyber Regulation, Legislation and Policy", http://www.staysafeonline.org/re-cyber/cyber-regulation-legislation-policy/ (2014.3.30. 검색).

33) 42 U.S.C. 5195c(e) 및 Presidential Policy Directive 21(PPD-21) 참조. The White House, "Presidential Policy Directive 21(PPD-21) -- Critical Infrastructure Security and Resilience" (2013.2.12.), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2014.4.30. 검색).

물의 16가지 핵심기반시설이 지정되어 있는데, 이들 핵심기반시설은 국토안보부, 농무부, 재무부, 국방부, 에너지부 등 관련 연방정부부처의 관리를 받는다.[34]

미국 의회가 사이버안전에 관한 법의 필요성을 인정하면서도 관련 법안을 채택하지 못한 주된 이유는 미국 산업계와 시민권단체의 반대 때문이다.[35] 예컨대, 미국상공회의소(U.S. Chamber of Commerce)를 비롯한 산업계는 사이버안전에 관한 법이 미국 기업에게 비용을 부담시키고 불공정한 규제적 부담을 부과한다고 주장한다. 또한 개인정보보호법상 보호되는 정부의 정보를 다루는 기업이 민사 및 형사 책임으로부터 면제되어야 한다고 주장한다. 한편, Electronic Frontier Foundation(EFF), Center for Democracy and Technology(CDT)와 American Civil Liberties Union(ACLU) 등 시민권단체는 특히 정부와 기업 사이의 정보 공유에 반대하는데, 소비자의 프라이버시가 충분하게 보호되지 못한다고 주장한다. 예컨대, 하원에서 지난해에 이어 동일한 내용의 CISPA 2013(Cyber Intelligence Sharing and Protection Act of 2013, H.R.624)이 2013년 2월 13일 다시 제출되자, CDT는 동 법안이 모든 프라이버시법에 대한 전반적인 예외를 규정함으로써 미국 국민의 개인정보가 국가안보국(National Security Agency: NSA)과 군부와 공유되도록 허용될 것이라고 비판하였다.[36]

이 점에서 상원에서 Joseph Lieberman상원의원이 발의한 Cybersecurity

34) Homeland Security, “Critical Infrastructure Sectors”, https://www.dhs.gov/critical-infrastructure-sectors (2014.3.30. 검색).

35) Searchcompliance, “FAQ: What is the current status of U.S. cybersecurity legislation?”, http:// searchcompliance.techtarget.com/guides/FAQ-What-is-the-current-status-of-US-cybersecurity-legislation (2014.3.30. 검색).

36) Center for Democracy and Technology, “Coalition Letter Opposing CISPA After Markup”, (2013.4.15), https://www.cdt.org/letter/coalition-letter-opposing-cispa-after-markup (2014.3.30. 검색). EFF도 같은 이유로 CISPA를 반대하였다. Mark M. Jaycox, “2013 in Review: EFF’s Battle Against Privacy Invasive “Cybersecurity” Bill”, Electronic Frontier Foundation (2013.12.30), https://www.eff.org/deeplinks/2013/12/2013-review-effs-battle-against-privacy-invasive-cybersecurity-bill (2014.4.14. 검색). 2013년 4월 18일 하원에서 채택된 CISPA에 대하여 결국 상원 Select Committee on Intelligence가 아무런 조치를 취하지 않았다. Stephen Joyce, “Congress Won’t Approve Cybersecurity Law Until Attack Compels It to Act, Bayh Says”, Bloomberg BNA (2014.4.7.), http://www.bna.com/congress-wont-approve-n17179889411/ (2014.4.14. 검색).

Act of 2012 (S.2105)의 채택이 부결된 후 2013년 7월 24일 Rockefeller상원의원과 Thune상원의원이 공동 발의하여 공화당과 민주당의 초당적 지지를 받는 Cybersecurity Act of 2013 (S.1353)에 주목할 필요가 있다. 동 법안은 2013년 7월 30일 상원 상무위원회(Committee on Commerce, Science and Transportation)에서 만장일치로 채택되었다.[37] 동 법안은 대체로 오바마 대통령의 행정명령13636의 내용에 따라 사이버안전프레임워크의 개발에 있어 국가표준기술청(National Institute of Standards and Technology: NIST)[38]의 역할을 법제화하려고 하는데, 업계의 지원을 얻은 것으로 보인다. 예컨대, Cybersecurity Act of 2012가 규제 중심의 사이버안전을 추구한다는 이유로 반대하였던 미국상공회의소는 Cybersecurity Act of 2013이 NIST로 하여금 사이버안전프레임워크의 개발에 있어 업계와 공동작업을 하도록 허가하는 등의 이유로 동 법안을 지지하였다.[39] 그러나, 동 법안은 정부와 기업 사이의 정보공유에 관한 조치를 포함하지 않는다. 이는 최근 NSA의 무차별적 감청을 통한 정보수집에 따른 프라이버시의 침해에 대한 우려가 반영된 것으로 보인다.[40]

이외에 2014년 2월 초 현재 하원에서 11건의 사이버안전에 관한 법안이 제출되었는데, 이 중 4개 법안이 통과되어 상원의 관련 위원회에 제출되어 있고, 상원에서 Cybersecurity Act of 2013 (S.1353)을 포함한 10건의

37) 동 법안의 원명은 다음과 같다: “A bill to provide for an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness, and for other purposes” 동 법안의 입법 성공률은 36%라고 한다. GovTrack, "S. 1353: Cybersecurity Act of 2013", https://www.govtrack.us/congress/bills/113/s1353 (2014.4.14. 검색).

38) 1901년 설립된 NIST는 미국 상무부 산하 연방기관으로서, 경제안전을 제고하고 생활의 질을 개선하는 방식으로 계측과학, 표준 및 기술을 발전시킴으로써 미국의 혁신과 산업경쟁력을 촉진하는 임무를 가진다. NIST, “NIST General Information”, (2013), http://www.nist.gov/public_affairs/general_information.cfm (2014.4.14. 검색).

39) R. Bruce Josten(U.S. Chamber of Commerce), “Letter supporting S. 1353, the “Cybersecurity Act of 2013””, (2013.7.28.), https://www.uschamber.com/letter/letter-supporting-s- 1353-%E2%80%9Ccybersecurity-act-2013%E2%80%9D (2014.4.14. 검색).

40) The Hogan Lovells Privacy Team, “U.S. CYBERSECURITY POLICY DEVELOPMENTS: A YEAR-TO-DATE ROUNDUP”, PrivacyTracker (2013.8.29.), https://www.privacyassociation.org/privacy_tracker/post/u.s._cybersecurity_policy_developments_a_year_to_date_roundup (2014.4.14. 검색).

관련 법안이 제출되어 있는데 아직 표결은 이루어지지 않았다.[41] 예컨대, 2014년 2월 미국 하원 국토안보위원회(Homeland Security Committee)는 만장일치로 Homeland Security Act of 2002를 개정하는 법안(H.R.3696: National Cybersecurity and Critical Infrastructure Protection Act of 2013)을 승인하였다. 동 법안은 국토안보부를 국가안보, 군사 및 정보부문을 제외한 연방정부의 사이버안전에 관한 주된 책임기관으로서 법제화하고, 핵심기반시설의 안전을 위하여 민간부문과 협조할 것을 요구한다. 또한, 동 법안은 정보공유분석센터(information sharing and analysis centers: ISAC)를 설치하여 사이버위협에 관한 정보의 신속하고 효과적인 공유와 분석을 가능하게 한다.[42]

2. 오바마 대통령의 입법 노력

오바마 대통령은 첫 임기를 시작하면서 사이버안전이 자신의 행정부의 최우선 과제라고 선언하였다. 즉, 오바마 대통령은 "사이버위협이 미국이 국가로서 직면한 가장 심각한 경제 및 국가안보의 도전 중의 하나이다" (cyber threat is one of the most serious economic and national security challenges we face as a nation)라고 선언하였다.[43] 이에 2009년 5월 연방정부의 정보통신기반시설의 방위 노력을 점검한 보고서인 *Cyberspace Policy Review*가 발간되었다.[44]

---

41) Mitchell S. Kominsky, *supra* note 27, 2014.

42) 동 법안에서 주목할 부분은 '사이버침해사고'(cyber incident)를 다음과 같이 정의하는 것이다. 즉, 'cyber incident'는 'an incident resulting in, or an attempt to cause an incident that, if successful, would: (1) jeopardize the security, integrity, confidentiality, or availability of an information system or network or any information stored on, processed on, or transiting such a system; (2) violate laws or procedures relating to system security, acceptable use policies, or acts of terrorism against an information system or network; or (3) deny access to or degrade, disrupt, or destruct an information system or network or defeat an operations or technical control of such a system or network'으로 정의된다.

43) The White House, "REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE", (2009.5.29), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (2014.3.30. 검색).

44) 동 보고서는 The White House, "Cyber Security Review Assuring a Trusted and Resilient

(1) 사이버안전 입법 제안

오바마 대통령은 2011년 5월 12일 '사이버안전 입법 제안'(*Cybersecurity Legislative Proposal*)을 발표하였다.[45] 동 제안에서 오바마 대통령은 미국 정부와 핵심기반시설 내의 사이버안전 취약성이 미국의 국가안보, 공공안전 및 경제번영에 대한 위험이 된다고 지적하였다. 오바마 대통령은 사이버위협으로부터 미국을 보호하기 위하여 사이버안전 관련법의 일부 내용이 개선될 필요가 있다고 지적하면서 미국 의회가 고려하여야 할 실용적이고 집중된 입법적 제안을 다음과 같이 제시하였다: 첫째, 미국 국민을 보호하기 위하여 국가적 개인정보 침해의 보고 이행, 컴퓨터 범죄인에 대한 처벌 강화; 둘째, 미국의 핵심기반시설을 보호하기 위하여, 산업계 등에 대한 정부의 자발적 지원, 산업계 등과 자발적 정보 공유, 핵심기반시설의 사이버안전 계획 마련; 셋째, 연방정부의 컴퓨터네트워크를 보호하기 위하여 Federal Information Security Management Act(FISMA)의 개정, 전문가 확충, 연방정부 민간컴퓨터에 대한 침해방지시스템 구축, 데이터센터 설치; 넷째, 개인의 프라이버시와 시민적 자유를 보호하기 위하여 새로운 프레임워크로서 정부의 프라이버시와 시민적 자유 절차에 따른 사이버안전 프로그램의 시행 등.

이러한 입법 제안에 따라 오마바대통령의 행정부와 군부는 상원의 Cybersecurity Act of 2012의 통과를 위하여 전력을 다하였는데, 오바마 대통령 자신은 2012년 7월 19일 *Wall Street Journal*에 동 법안의 통과 필요성을 기고하였다.[46] 동 기고에서 오바마 대통령은 아직 미국의 핵심기반

Information and Communications Infrastructure", 2009.5.29,http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (2014.3.30. 검색) 참조. 동 보고서의 이행을 위하여 Howard Schmidt가 U.S. Cybersecurity Coordinator로 임명되었고, National Security Staff에 설치된 Cybersecurity Office가 Federal Chief Information Officer, Federal Chief Technology Officer 및 National Economic Council과 긴밀히 협조하였다.

45) The White House, "FACT SHEET: Cybersecurity Legislative Proposal", (2011.5.12), http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal (2014.3.30. 검색).

46) Barack Obama, "Taking the Cyberattack Threat Seriously", Wall Street Journal (2012.7.19), http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650 (2014.3.30. 검색).

시설네트워크가 심각하게 훼손되지 않았지만, 외국 정부, 범죄조직 및 개인이 매일 미국의 금융, 에너지 및 공공안전시스템을 시험하고 있다고 밝혔다. 그는 미래의 충돌에서 전장에서의 미국의 군사적 우위를 대항할 수 없는 적대자가 미국 내의 컴퓨터 취약성을 악용할 것이라고 주장하였다. 또한 그는 핵심기반시설 기업들이 잘 대비할 수 있도록 미국 정부가 위협정보를 보다 용이하게 공유할 수 있어야 하고, 이들 기업이 공격받을 때 정보를 정부와 보다 용이하게 공유할 수 있어야 한다고 주장하였다. 또한, 그는 미국 국민의 프라이버시와 시민적 자유가 보호되어야 한다면서 이러한 보호를 결여한 입법안(CISPA 2012)을 거부할 것이라고 선언하였다.[47]

(2) 행정명령13636

미국 상공회의소 등 업계의 반발과 John McCain상원의원 등 공화당의 반대로 상원에서 Cybersecurity Act of 2012가 채택되지 못하자, 2013년 2월 12일 오바마 대통령은 사이버공격으로부터 미국을 보호하기 위한 Executive Order 13636(이하 '행정명령13636'이라 함)을 발표하였다.[48] 행정명령13636은 미국에서 주로 민간부문이 소유하는 핵심기반시설에서 운영되는 컴퓨터네트워크의 안전을 보호하기 위하여 민간부문이 연방정부와 정보를 자발적으로 공유하도록 유인을 제공하고 또한 핵심기반시설의 보호를 위한 프레임워크를 만들고자 한다.[49]

행정명령13636의 주된 내용은 다음과 같다. 첫째, 미국 정부와 민간부

47) 오바마 대통령은 프라이버시 보호의 결여와 정부와 정보를 공유하는 기업에 대한 느슨한 면책 규정 등에 대한 시민권단체 등의 주장을 수용한 것으로 보인다. Mark M. Jaycox, "2013 in Review: EFF's Battle Against Privacy Invasive "Cybersecurity" Bill", Electronic Frontier Foundation (2013.12.30), https://www.eff.org/deeplinks/2013/12/2013-review-effs-battle-against-privacy-invasive-cybersecurity-bill (2014.4.14. 검색).

48) The White House, "Executive Order – Improving Critical Infrastructure Cybersecurity", (2013.2.12.), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (2014.3.30. 검색).

49) 동 행정명령은 민간부문의 자발적 참여를 규정하지만, 기업 등이 정부와 계약할 때 동 행정명령의 내용이 조건으로 작용함으로써 사실상 강제적인 효과를 가질 수 있다고 한다. Mitchell S. Kominsky, *supra* note 27, 2014.

문 사이의 사이버위협 정보 공유의 증대; 둘째, 사이버안전 모범관행의 공통프레임워크(common cybersecurity framework) 수립 및 동 프레임워크 채택의 촉진을 위한 자발적 프로그램의 이행; 셋째, 기존 사이버안전 규정의 검토; 넷째, 프라이버시와 시민적 자유의 보호. 동 행정명령에 따라 NIST는 2014년 2월 12일 '사이버안전프레임워크'(Framework for Improving Critical Infrastructure Cybersecurity)를 발표하였다. 동 프레임워크는 정부와 기업이 핵심기반시설에 대한 사이버위험을 감소하기 위하여 자발적으로 사용할 수 있는 모범관행으로 구성되어 있는데, 동 내용은 효과적이라고 입증된 기존의 국제기준 등에 근거하여 마련되었다. 동 프레임워크의 발간 후 2년 내에 '비효과적이고, 충돌하거나, 또는 과도하게 부담이 되는 사이버안전 요건'이 백악관의 행정관리예산국(Office of Management and Budget: OMB)에 보고될 예정이다.

행정명령13636과 별도로 오바마 대통령은 2013년 2월 12일 핵심기반시설의 안전을 위한 정부와 산업의 조정을 개선하기 위하여 대통령정책지침21(Presidential Policy Directive 21(PPD-21) - Crtitical Infrastructure Security and Resilience)에 서명하였다.[50] 동 지침에 따라 미국 행정부는 핵심기반시설에 관련된 정부간 기능적 관계를 확인하도록 요구되고, 정부의 시장기반 혁신을 권장하기 위하여 연구개발이 요구된다.

3. 사이버안전에 관한 법의 관련 쟁점

(1) 프라이버시 보호

사이버공간을 포함한 안전의 문제는 개인의 프라이버시 문제와 함께 고려되어야 한다. 안전을 위한 조치는 자칫 프라이버시를 제한 또는 침해할 가능성이 높기 때문이다. 2001년 9/11테러를 겪은 후 국가안전이 최우선 과제가 되면서 미국 국민들은 국가안전을 위한 프라이버시 제한을 어느 정도 불가피한 것으로 생각하고 있었다. 그럼에도, 미국에서 국민의

50) The White House, "Presidential Policy Directive 21(PPD-21) -- Critical Infrastructure Security and Resilience" (2013.2.12.), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2014.4.30. 검색).

프라이버시 보호는 중요한 법익으로 간주된다. 예컨대, 정부와 민간부문 사이의 정보 공유를 내용으로 하는 하원의 CISPA법안은 개인의 프라이버시 보호에 충실하지 않다는 이유로 프라이버시보호단체는 물론 오바마 행정부의 반대를 받았다. 그럼에도 2013년 4월 하원은 CISPA법안을 통과시켰는데, 2012년과 비교할 때 동 법안을 찬성한 민주당 의원이 42명에서 92명으로 대폭 증가하였다.[51] 결국 상원은 프라이버시 보호의 불충분을 이유로 반대하여 동 법안의 채택은 무산되었다.[52]

2013년 6월 초 Edward Snowden이 NSA에 의한 전세계적인 무차별적 감청행위를 폭로한 뒤 국제사회에서 미국의 감청행위로 야기되는 프라이버시 침해에 대한 비난이 격렬하게 제기되었다.[53] 그동안 미국 행정부는 이러한 감청행위가 해외정보감청법원(Foreign Intelligence Surveillance Court: FISC)의 허가를 받아 해외의 외국인을 대상으로 한 것이라고 주장을 하였다.[54] 이러한 NSA의 감청은 Google, Apple, Microsoft와 Facebook 등 인터넷서비스제공자를 통하여 수행되어서 또 다른 충격을 주었다. Snowden에 의한 미국 정부의 감청행위의 폭로는 미국의 사이버안전에 관한 입법에도 큰 영향을 주었는데, 미국 국민의 프라이버시 침해에 대한 우려가 심각하게 제기되었기 때문이다.[55] 특히 국가지원테러리스트나 외국의 사

51) 전통적으로 프라이버시를 보다 더 옹호하는 민주당이 같은 당인 오바마 행정부의 거부권 행사의 위협에도 불구하고 CISPA법안을 지지한 것은 상당한 논란을 일으켰다. Gregory Ferenstein, “One Year Later, Twice As Many Democrats Vote for Cybersecurity Bill and Defy Obama”, TECH CRUNCH (2013.4.18.), http://techcrunch.com/2013/04/18/one-year-later-twice-as-many-democrats-vote-for-cybersecurity-bill-and-defy-obama/ (2014.3.30. 검색).

52) Jason Koebler, “ACLU: CISPA Is Dead (For Now)”, USNews (2013.4.25), http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now (2014.3.30. 검색).

53) Ewen Macaskill and Gabriel Dance, “NSA Files”, The Guardian (2013.11.1.), http://www.theguardian.com/world/the-nsa-fils (2014.4.14. 검색).

54) 그러나, 오바마 행정부의 외국인을 겨냥한 국가안보국(NSA)의 감청프로그램 일환으로 미국 국민의 통화기록을 영장 없이 조사했다고 James Clapper 국가정보국장(Director of National Intelligence: DNI)이 2014년 3월 28일자 미국 Wyden 상원의원에게 보낸 서한에서 밝혀졌다. Eileen Sullivan, “U.S. government acknowledges it conducted warrantless searches under NSA surveillance operations”, GLOBALNews (2014.4.1), http://globalnews.ca/news/1244540/u-s-government-acknowledges-it-conducted-warrantless-searches-under-nsa-surveillance-operations/ (2014.4.14. 검색).

55) 물론 오바마 대통령의 사이버안전에 관한 정책이나 입법제안에서도 국민의 프라이버

이버침해사고를 방지하고 처리하기 위하여 관련 정보를 정부와 기업 등 민간부문이 공유할 필요가 인정되면서, 이러한 공유 과정에서 개인의 프라이버시 침해가능성에 대한 우려가 제기되었다. 따라서 미국에서의 사이버안전 관련 입법에서 개인의 프라이버시 보호가 더욱 주목받게 될 것이다.

(2) 규제적 또는 비규제적 접근

개인정보보호와 관련하여 미국은 개인정보처리자의 자율규제를 선호하고, EU는 정부와 법에 의한 적극적인 개입을 선호한다. 오바마 대통령이 적극 지지하였던 상원의 Cybersecurity Act of 2012가 채택되지 못한 이유 중에 미국상공회의소를 비롯한 업계의 반발이 있었는데, 사이버안전 관련 법이 미국 기업에게 비용을 부담시키고 불공정한 규제적 부담을 부과한다는 것이다. 또한, 안전을 위한 규제는 혁신을 약화시키고, 소프트웨어제품의 모든 결함에 대하여 제소가 가능하여 '변호사 주도 사회'가 될 것이라고도 한다.[56] 그럼에도, 미국 행정부와 사이버안전 전문가들은 사이버안전에 관한 한 민간부문, 즉 업계의 한계를 지적한다.[57] 따라서 미국의 사이버안전 관련 입법에서 업계에 대한 규제가 강화될 수 있다.

시 보호의 중요성이 언급되는 점에서 사이버안전과 프라이버시의 균형이 추진된 것으로 볼 수 있다. 그럼에도 Snowden의 NSA에 의한 무차별적 감청의 폭로는 사이버안전의 필요성에도 불구하고 프라이버시 보호의 중요성을 더욱 부각시킨 것으로 이해된다.

56) Harris Miller (Information Technology Association of America 회장)의 2005년 2월 RSA Security Conference에서의 발언. Erin Joyce, "More Regulation For The Software Industry?", eSecurityPlanet (2005.2.16.), http://www.esecurityplanet.com/trends/article.php/3483876/More-Regulation-For-The-Software-Industry.htm (2014.4.14. 검색).

57) 전임 백악관 안보보좌관인 Richard Clarke은 "산업은 규제의 위협을 받을 때에만 반응하고, 산업이 동 규제 위협에도 반응하지 않으면 관철해야 한다"고 밝힌 점에서 기업에 대한 규제적 부담의 불가피함을 지적하였다. Carrie Kirby, "Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity", SFGate (2005.2.17), http://www.sfgate.com/business/article/Former-White-House-aide-backs-some-Net-regulation-2729985.php (2014.4.14. 검색). 또한, Clarke는 대형 사고가 발생한 뒤에는 보다 더 강력한 규제가 있게 될 것이라고 경고하였다. Erin Joyce, "More Regulation For The Software Industry?", eSecurityPlanet (2005.2.16.), http://www.esecurityplanet.com/trends/article.php/3483876/More-Regulation-For-The-Software-Industry.htm (2014.4.14. 검색).

(3) 국토안보부의 역할

미국 국토안보부의 사이버안전에서의 역할이 논란의 대상이 된다. 국방과 정보 부문을 제외한 정부와 민간부문의 안전의 책임을 맡고 있는 국토안보부는 사이버안전에 관하여도 미국 정부의 책임을 맡는다. 국토안보부는 국가사이버안전·통신통합센터(National Cybersecurity and Communications Integration Center) 등의 하부기관이나 관련 프로그램을 보유하고 있기 때문에 사이버안전의 적임 기관이라고 평가되지만, 미국 대통령도 사이버안전에 대한 의미 있는 역할을 하여야 한다는 주장도 제기된다.[58] 오바마 대통령의 행정명령13636의 시행을 통하여 국토안보부의 민간부문의 사이버안전에 대한 상당한 개입 내지 영향이 예상된다.[59] 미국 의회에서 채택되는 사이버안전에 관한 법이 국토안보부의 역할을 명확하게 규정할 수 있을 것이다.

III. 한국의 사이버안전에 관한 입법에 대한 시사점

미국에서의 사이버안전에 관한 입법 동향의 시사점은 다음과 같이 간략하게 정리될 수 있다. 첫째, 미국에서 사이버공간의 안전이 국가안보와 경제발전의 최우선적 과제라는 인식 아래 대통령과 의회가 사이버안전에 관한 입법 경쟁을 하였다. 특히 오바마 대통령은 사이버안전에 관련된 국내외 정책의 전략을 수립하고 이를 바탕으로 종합적인 사이버안전 관련 입법의 필요성과 그 내용을 제시함으로써 적극적인 활동을 하고 있다. 북한은 물론 중국과 러시아 등 지정학적 안보의 취약성을 가지고 있는 한국에서 국회는 물론 대통령도 보다 적극적으로 사이버안전에 관한 국가차원의 방향을 제시하고 필요한 입법조치를 마련하여야 한다. 둘째, 오바마 대통령과 의회는 사이버안전의 중요성은 공유하면서, 아래와 같은 개

58) Mitchell S. Kominsky, *supra* note 27, 2014.

59) Jason Miller, “DHS revs up its part of the cyber executive order”, FEDERAL NEWS RADIO (2014.1.31.), http://www.federalnewsradio.com/473/3553526/DHS-revs-up-its-part-of-the-cyber-executive-order (2014.4.14. 검색).

별적인 주요 쟁점에 있어서 그 접근방법에서 차이를 보였다. 정치권에서 '반대를 위한 반대'가 아니라, 국민의 안전과 국가의 안보를 위한 보다 나은 방법의 모색에서 치열한 다툼이 필요하다. 셋째, 사이버안전이 컴퓨터 네트워크를 중심으로 하는 점에서 미국에서 동 네트워크가 운용되는 핵심기반시설의 보호가 사이버안전 관련 입법의 중심에 있다. 미국에서 현재 16개 부문의 핵심기반시설이 관련 정부부처의 통제를 받고 있다. 사이버안전을 위한 보호 대상이 되는 핵심기반시설의 범위와 그 보호 방법에 대한 지속적인 검토가 필요하다. 넷째, 미국에서 핵심기반시설의 대부분은 민간부문의 소유이다. 핵심기반시설의 보호를 위하여 정부와 민간부문 사이의 사이버위협정보 등의 정보 공유가 필요한 점에서 정부와 민간부문 사이의 관련 정보 공유가 사이버안전 관련 입법의 중심에 있다. 사이버공간은 국가적 경계를 모르지만 동시에 민간부문, 정부 및 군사부문의 경계도 모르는 점에서, 사이버안전을 위한 관련 주체들 사이의 정보 공유 등 긴밀한 협력이 필요하다. 다섯째, 사이버안전을 위한 정부와 민간부문의 정보 공유는 국민의 개인정보보호 및 프라이버시의 침해 가능성을 높이는 점에서 미국에서 프라이버시와 시민적 자유의 보호가 사이버안전 관련 입법의 중심에 있다. 안전을 위한 법제도의 마련은 국민의 프라이버시와 개인정보보호 등의 기본권 보호와 균형을 이루어야 한다. 여섯째, 미국에서 핵심기반시설의 대부분을 보유한 민간부문의 사이버안전을 위한 자발적인 행동의 유인이 사이버안전 관련 입법의 중심에 있다. 즉, 사이버안전을 위한 민간부문의 자율규제와 정부규제의 적절한 균형점이 쟁점이 된다. 업계와 국민의 이익을 고려하여 공정한 균형이 이루어지도록 규제 수준이 정해져야 할 것이다. 소위 '착한 규제'도 필요하기 때문이다. 일곱째, 미국에서 군부와 정보 부문을 제외한 정부와 민간부문의 사이버안전에 관한 책임이 국토안보부에 주어져 있는데, 국토안보부의 책임과 능력의 적절성 여부가 사이버안전 관련 입법의 중심에 있다. 북한과 대치하고 있는 한국의 안보실정에 맞는 사이버안전의 책임있는 정부 운용이 필요하다. 특정 기관의 과거의 잘못에 대한 고정된 관념에서 탈피하여 국내외의 사이버안전 동향을 직시하여 국가와 국민을 안전하게 보호

할 수 있는 체제가 구축되어야 한다. 결론적으로, 정부와 정치권은 물론 업계 및 전문가들의 적극적인 논의를 거쳐 한국의 사이버안전에 관한 법제도의 형식은 물론 내용이 발전되어야 한다. 특히 법학계의 사이버안전에 대한 보다 큰 관심이 요구된다.

참 고 문 헌

1. 국내 문헌

〔저 서〕

윤재석, 2011 경제발전경험모듈화사업: 한국의 정보보호 활동과 시사점, 한국인터넷진흥원, 2012.

〔논 문〕

정완, “한미 사이버보안 법제 동향에 관한 고찰”, 「경희법학」제48권 제3호, 경희대학교 법학연구소, 2013.
정준현, “고도정보화사회의 국가사이버안보 법제에 관한 검토”, 「단국법학」제37권 제2호, 단국대학교 법학연구소, 2013.
권창범, “사이버보안 특집: 사이버보안을 위한 국가적 추진체계 검토 및 발전방안”, 「연세 의료·과학기술과 법」제2권 제2호, 연세대학교 법학연구원, 2011.
정필운, “사이버보안이란 개념 사용의 유용성 및 한계”, 「연세 의료·과학기술과 법」제2권 제2호, 연세대학교 법학연구원, 2011.
권문택, “국가사이버안전관리 조직의 통합적 체계구축에 관한 연구”, 「정보·보안 논문지」제9권 제3호, 한국융합보안학회, 2009.

〔인터넷 기사 및 자료〕

이유지, “[취재수첩] 국가 사이버안보 마스터플랜 보완해야”, 디지털데일리 (2011.8.10.), http://www.ddaily.co.kr/news/article.html?no=81127 (2014.4.14. 검색).
미래창조과학부, “정부,「국가 사이버안보 종합대책」수립 - 사이버안보 강화를 위한 4대 전략 (PCRC) 마련 -”, (2013.7.4.), http://www.msip.go.kr/www/brd/m_211/view.do?seq=406 (2014.4.14. 검색).
방송통신위원회, “정부, 「국가 사이버안보 마스터플랜」 수립 - 국가 사이버공간 수호를 위한 범정부 차원의 청사진 마련 -” (2011.8.8.), http://old.kcc.go.kr/user.do;jsessionid=ogBWnpR9bkvnIDIxBUYYn11kO

FRL9RmpMwYBKTWPPi8j49DrXwzdKxPIQpLftNGI.hmpwas01_servlet_engine4?mode=view&page=P02020700&dc=K02020700&boardId=1077&cp=1&boardSeq=32030 (2014.4.14. 검색).

2. 외국 문헌

〔저 서〕

James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (eds.), *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2,* EastWest Institute and the Information Security Institute of Moscow State University, 2014.

〔논 문〕

Mitchell S. Kominsky, “The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress: The Threat and Impact of Cyber Attacks”, *Harvard National Security Journal*, Harvard Law School, 2014.

〔인터넷 기사 및 자료〕

Siobhan Gorman, “Annual U.S. Cybercrime Costs Estimated at $100 Billion”, WALL STREET JOURNAL (2013.7.22), http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990 (2014.3.30. 검색).

Jim Garamone, “Panetta Spells out DOD Roles in Cyberdefense”, American Forces Press Service (2012.10.11.), http://www.defense.gov/news/newsarticle.aspx?id=118187 (2014.3.30. 검색).

Kris Osborn, “Lawmakers Call for New Cyber Security Laws”, Dodbuzz (2014.2.27.), http://www.dodbuzz.com/2014/02/27/lawmakers-call-for-new-cyber-security-laws/ (2014.3.30. 검색).

Mark M. Jaycox, “2013 in Review: EFF’s Battle Against Privacy Invasive “Cybersecurity” Bill”, Electronic Frontier Foundation (2013.12.30), https://www.eff.org/deeplinks/2013/12/2013-review-effs-battle-

against-privacy-invasive-cybersecurity-bill (2014.4.14. 검색).

Stephen Joyce, “Congress Won’t Approve Cybersecurity Law Until Attack Compels It to Act, Bayh Says”, Bloomberg BNA (2014.4.7.), http://www.bna.com/congress-wont-approve-n17179889411/ (2014.4.14. 검색).

The Hogan Lovells Privacy Team, “U.S. CYBERSECURITY POLICY DEVELOPMENTS: A YEAR-TO-DATE ROUNDUP”, PrivacyTracker (2013.8.29.), https://www.privacyassociation.org/privacy_tracker/post/u.s._cybersecurity_policy_developments_a_year_to_date_roundup (2014.4.14. 검색).

Barack Obama, “Taking the Cyberattack Threat Seriously”, Wall Street Journal (2012.7.19), http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650 (2014.3.30. 검색).

Gregory Ferenstein, “One Year Later, Twice As Many Democrats Vote for Cybersecurity Bill and Defy Obama”, TECH CRUNCH (2013.4.18.), http://techcrunch.com/2013/04/18/one-year-later-twice-as-many-democrats-vote-for-cybersecurity-bill-and-defy-obama/ (2014.3.30. 검색).

Jason Koebler, “ACLU: CISPA Is Dead (For Now)”, USNews (2013.4.25), http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now (2014.3.30. 검색).

Ewen Macaskill and Gabriel Dance, “NSA Files”, The Guardian (2013.11.1.), http://www.theguardian.com/world/the-nsa-fils (2014.4.14. 검색).

Eileen Sullivan, “U.S. government acknowledges it conducted warrantless searches under NSA surveillance operations”, GLOBALNews (2014.4.1), http://globalnews.ca/news/1244540/u-s-government-acknowledges-it-conducted- warrantless-searches-under-nsa-surveillance-operations/ (2014.4.14. 검색).

Erin Joyce, “More Regulation For The Software Industry?”, eSecurityPlanet (2005.2.16.), http://www.esecurityplanet.com/trends/article.php/ 3483876 /More-Regulation-For-The-Software-Industry.htm (2014.4.14. 검색).

Carrie Kirby, “Former White House aide backs some Net regulation / Clarke says government, industry deserve ‘F’ in cybersecurity”, SFGate (2005.2.17), http://www.sfgate.com/business/article/Former-White- Hous

e-aide-backs-some-Net-regulation-2729985.php (2014.4.14. 검색).

Jason Miller, “DHS revs up its part of the cyber executive order”, FEDERAL NEWS RADIO (2014.1.31.), http://www.federalnewsradio.com/473/3553526/DHS-revs-up-its-part-of-the- cyber-executive-order (2014.4.14. 검색).

The White House, “Presidential Policy Directive 21(PPD-21) -- Critical Infrastructure Security and Resilience” (2013.2.12.), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (2014.4.30. 검색).

The White House, “REMARKS BY THE PRESIDENT ON SECURING OUR NATION’S CYBER INFRASTRUCTURE”, (2009.5.29), http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (2014.3.30. 검색).

The White House, “FACT SHEET: Cybersecurity Legislative Proposal”, (2011.5.12), http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal (2014.3.30. 검색).

The White House, “Executive Order – Improving Critical Infrastructure Cybersecurity”, (2013.2.12.), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (2014.3.30. 검색).

ITU, “Definition of cybersecurity”, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (2014.4.16. 검색).

Wiggin and Dana, “Cybersecurity Legislation: Is Congress Ready?”, (2014.2.11.), http://www.wiggin.com/14904 (2014.3.30. 검색).

Wikipedia, “Select or special committee (United States Congress)”, http://en.wikipedia.org/wiki/Select_or_special_committee_(United_States_Congress) (2014.4.14. 검색).

StaySafeOnline.org, “Cyber Regulation, Legislation and Policy”, http://www.staysafeonline.org/re-cyber/cyber-regulation-legislation-policy/ (2014.3.30. 검색).

Homeland Security, “Critical Infrastructure Sectors”, https://www.dhs.gov/critical-infrastructure-sectors (2014.3.30. 검색).

Searchcompliance, “FAQ: What is the current status of U.S. cybersecurity

legislation?", http:// searchcompliance.techtarget.com/guides/FAQ-What-is-the-current-status-of-US-cybersecurity-legislation (2014.3.30. 검색).
Center for Democracy and Technology, "Coalition Letter Opposing CISPA After Markup", (2013.4.15), https://www.cdt.org/letter/coalition-letter-opposing-cispa-after-markup (2014.3.30. 검색).
GovTrack, "S. 1353: Cybersecurity Act of 2013", https://www.govtrack.us/congress/bills/113/s1353 (2014.4.14. 검색).
NIST, "NIST General Information", (2013), http://www.nist.gov/public_affairs/general_information.cfm (2014.4.14. 검색).

〔기타 문서〕

United States of America Department of the Army and United States Marine Corps Department of the Navy, "Department of Defense Dictionary of Military and Associated Terms(Joint Publication 1-02)", 2010.11.8.
European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013.2.7.
U.S. Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented (GAO-13-187)", 2013.2.
James R. Clapper(Director of National Intelligence), "Worldwide Threat Assessment of the US Intelligence Community(Statement for the Record, Senate Select Committee on Intelligence)", 2013.3.12.
Eric A. Fischer, "Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions(Congressional Research Service Report for Congress)", 2013.6.20.
The White House, "Cyber Security Review Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009.5.29.

<국문초록>

오바마 대통령의 취임 이후 특히 최근 몇 년 동안 미국에서는 사이버안전에 관한 법의 제정을 위한 노력이 지속되었다. 대통령과 의회가 사이버안전이 미국의 국익에 중요하다는 점에 대하여 의견을 같이 함에도 사이버안전을 위한 구체적인 접근 방법이나 그 내용에 있어서는 의견을 달리하였다. 그 결과 2001년 9/11테러 이후 10년이 지나도록 사이버안전에 관한 의미 있는 법이 채택되지 못하고 있다. 대신에 오바마 대통령은 자신의 권한에 따른 행정명령을 통하여 사이버안전에 관한 법의 공백을 채우고 있다. 미국에서 사이버안전에 관한 입법이 성공하지 못하고 있지만, 입법의 노력 과정에서 많은 쟁점이 도출되었는데, 이들의 논의는 우리에게 큰 교훈이 될 수 있다. 사이버안전은 우리에게도 현실적으로 중요한 사안이다. 미국과 달리 우리는 북한과 대치하고 있는 사정이어서 사이버안전은 더욱 민감한 사안이다. 최근에 국회에서 사이버안전에 관한 법안이 제출되었지만, 충분한 논의가 이루어지지 않고 있고, 아직 채택되지 않고 있다. 본 논문은 미국에서의 사이버안전에 관한 입법 노력을 의회와 대통령의 활동을 통하여 점검하고, 미국에서의 논의가 우리에게 줄 수 있는 입법적 시사점을 도출하였다. 사이버안전에 관한 법이 채택된다면, 적어도 정부와 민간부문의 정보 공유 등의 협력이 강조되고, 국민의 프라이버시가 침해되지 않도록 하여야 하며, 민간부문의 자율규제와의 균형이 필요하고, 관련 국가기관 사이의 역할에 따른 책임이 주어지는 내용이 되어야 할 것이다. 사이버안전에 관한 법학계의 보다 큰 관심이 필요하다.

주제어 : 사이버안전, 법, 미국, 대통령, 의회

Legislative efforts on cybersecurity in the U.S. and their implications for Korea

Park, No-Hyoung*

Since Mr. Obama became the President of the U.S., and in particular for the past few years, there have been considerable efforts to legislate laws on cybersecurity in the U.S. Although they have the same idea on the necessity of cybersecurity, Mr. Obama and the Congress have been different in approaching the issue over how to and what to legislate for cybersecurity. As a result there have been no meaningful and significant law adopted in the Congress since the so-called 9/11 terror. Nevertheless, Mr. Obama was able to make up a legislative gap by taking an executive order under his authority. Although the U.S. is regarded to have failed in cybersecurity legislations, the discussion over the issue should be a good lesson to the Republic of Korea (Korea). As a matter of fact, cybersecurity is also important and more serious to Korea which has been threatened by North Korea. In this regard there have been several drafts of law for cybersecurity proposed in the National Assembly, but there have not been serious and meaningful discussion over them with no success. This paper examines the legislative efforts for cybersecurity by checking the activities of Mr. Obama and the Congress in the U.S., and tries to find any implications and lessons for Korea. Any law on cybersecurity, to be adopted in Korea, should emphasize the cooperation, including in sharing the information concerned, between the governments and the private sector, protect the privacy of the people while cybersecurity is provided, keep the self-regulation in the private sector respected, and make the governments responsible for cybersecurity under their own jurisdictions. Legal scholarship should work hard in the matter of cybersecurity.

Key Words : cybersecurity, legislation, the U.S., the President, the Congress

* Professor, Korea University Law School