미국 사이버 안보전략의 등장과 발전:
역사적 전개와 사이버솔라리움보고서

변진석 | 숙명여자대학교

미국은 1980년대부터 컴퓨터 정보보안정책을 시작한 이후 사이버 위협과 공격의 증가에 따라 사이버보안과 안보정책을 발전시키고 그러한 노력은 최근 사이버솔라리움보고서에서 제시된 사이버 안보전략으로 나타났다. 동 보고서에서 제시된 미국의 사이버 안보전략은 '다층적 사이버 억지' 전략으로서 미국 자신의 사이버 시스템을 정비하여 사이버공격에 대응력을 강화하고, 국제적 연대를 구축하여, 사이버 적대세력이 미국을 공격하지 못하도록 한다는 개념이다. 그러한 미국의 사이버 안보전략에서 나타난 미국 정책의 특징을 간략하게 정리하면 다음과 같다. 첫째, 미국의 사이버 안보전략은 군사안보전략과 달리 정부와 민간부문의 협조에 기반을 둔 전 국가적 차원의 전략을 마련하고 추진하고 있다. 둘째, 과거의 방어적 전략에서 벗어나 공세적 전략, 즉 '선제적 방어'(forward defend)라는, 냉전 시기 군사전략에서 비롯된 개념에 기반을 둔 전략을 추진하고 있다. 셋째, 사이버 안보전략이 대응하고자 하는 사이버 위협, 사이버공격의 특성 때문에 미국은 국제적 규범의 확립, 사이버 위협의 추적과 무력화를 위하여 국제적 협력을 사이버 안보전략의 중요한 내용으로 하고 있다.

주제어: 사이버안보, 선제적 방어, 사이버보안의 안보화, 다층적 사이버억지, 사이버안보 정보공유법, 사이버솔라리움위원회

https://doi.org/10.21051/PS.2022.04.30.1.41

Ⅰ. 서론

미국은 지난 20여 년간 심각한 사이버 위협 및 실제 공격을 받아왔다. 미국 연방정부가 보고한 사이버 사건의 수는 2006년 5,503에서 2015년에는 77,183건으로 열 배 넘게 증가하였다(Johnson, 2021). 미국 내 악성코드 감염사례는 2009년 1240만 건에서 2018년 8억1200만 건으로 증가하였다(Purplesec, 2021). 2020년 미국에서 랜섬웨어 때문에 지불된 금액은 3억5천만 달러에 이르고 이는 전년 대비 3배 이상 증가한 금액이었다. 2009년에서 2019년 사이 발생한 사이버공격을 가장 많이 받은 국가는 미국으로 전체 사이버 공격의 33%가 미국을 상대로 이루어졌다. 두번째 많은 공격을 받은 국가는 독일과 한국으로 같이 4.6%의 사이버공격을 받았다(Robinson, 2020). 특히 지난 1년 동안 '솔라윈즈'(SolarWinds) 해킹사건, 마이크로소프트 익스체인지서버 해킹사건, 콜로니얼송유관(Colonial Pipeline) 해킹사건 등은 러시아와 중국이 실행한 심각한 사이버 사건이었다. 미국은 핵무기 공격보다 사이버공격이 훨씬 더 심각하고 현실적인 안보위협으로서 이에 대하여 국가안보전략으로 대응하고 있다.

미국 정부가 사이버 문제에 초보적이나마 정책적 대응을 시작한 것은 1980년대부터이다. 당시 컴퓨터 사용이 정부와 민간에서 일반화된 이후 미국에서 컴퓨터에 저장된 정보의 침해나 컴퓨터를 이용한 불법적 행위를 금지하기 위한 만들어진 법제는 단순하게 컴퓨터에 저장된 정보를 보호하는 수준이었다. 이후 1990년대 인터넷의 발전으로 그러한 보호의 범위는 더 확대되어 처음으로 사이버보안이라는 용어가 등장하고 연방정부 차원에서 인터넷으로 연결된 국

가 기간시설의 보호를 위한 정책이 등장하였다. 2000년의 911테러를 기점으로 국내적 보안이 국가 안보의 수준으로 격상된 이후 본격적으로 사이버 보안이 사이버 안보로서 국가안보정책의 대상으로 발전하였다. 이에 따라 각 행정부는 백악관이 직접 국가 사이버 안보전략을 발표하고 연방의회에서는 다수의 입법을 통하여 사이버 안보를 위한 정책을 뒷받침하였다. 2020년 3월에 발표된 사이버솔라리움위원회의 보고서(이하 솔라리움보고서, 또는 보고서)는 미국의 사이버 안보를 위한 포괄적이고 근본적인 정책, 전략을 제시하는 것이었다.

본 논문에서는 미국의 사이버 안보전략의 발전과정을 역대 행정부의 정책과 입법부의 법제정을 중심으로 검토하고자 한다. 본 논문은 특히 1980년대부터 현재에 이르는 40여 년의 기간 동안 사이버 안보라는 개념의 등장과 정책, 전략의 발전을, 거시적 관점에서 사이버 안보 정책 내용과 발전 방향을 중심으로 관찰하고자 한다. 본 논문의 요지를 간단하게 말한다면, 미국의 사이버 안보정책은 1980년대 단순한 정보보안의 문제로 출발하여 이후 1990년대 사이버보안이라는 개념으로 발전하였다. 2000년대 초고속 인터넷의 보급에 따른 국가와 사회의 네트워크의 발전과 911테러의 여파로 사이버보안은 궁극적으로 국가안보의 문제로 격상되었다. 이후 사이버 안보의 대상과 접근법, 전략은 꾸준히 확대되고 발전해왔으며 최근에는 사이버솔라리움보고서를 통해서 포괄적이고, 과거 냉전전략에서 영감을 받은, 공세적인 국가 사이버 안보전략을 채택하고 이를 추진하고 있다는 것이다.

미국의 사이버 안보전략의 특징적 내용을 간략하게 정리하면, 첫째, 미국의 사이버 안보전략은 군사안보전략과 달리 정부와 민간부문의 협조에 기반을 둔 전 국가적 차원의 전략을 마련하고 추진하고 있

다. 둘째, 과거의 방어적 전략에서 벗어나 공세적 전략, 즉 '선제적 방어'(forward defend)라는, 냉전 시기 군사전략에서 비롯된 개념에 기반을 둔 공세적 전략을 추진하고 있다. 셋째, 사이버 안보전략이 대응하고자 하는 사이버 위협, 사이버 공격의 특성 때문에 미국은 국제적 규범의 확립, 사이버 위협의 추적과 무력화를 위하여 국제적 협력을 사이버 안보전략의 중요한 내용으로 하고있다.

본 논문의 주제를 논하는 과정에서 한 가지 용어 사용에 대하여 미리 지적하고자 한다. 그것은 보안과 안보, 특히 사이버보안과 사이버 안보라는 용어이다. 이론적으로 보안과 안보는 구분된다. 전통적으로 보안은 주로 특정 보호 대상에 대한 침해를 방지하는 개념인 반면 안보는 국가의 생존에 관련된 외부로부터의 위협에 대한 대응으로 인식되었다. 그러나 본 논문의 주제인 보안의 발전과 궁극적으로 사이버 안보로 격상되는 과정에 대한 논의는 필연적으로 두 용어의 혼용을 초래한다. 그것은 논의 대상의 존재론적 현실이다. 즉 특정 시설을 사이버침해로부터 보호하는 것은 보안이지만 그러한 보호가 실패했을 경우 초래되는 피해가 전 국가적 규모로서 안보를 저해하는 정도일 수 있다는 점, 그리고 그러한 침투가 미국의 안보를 위협하는 전략적 경쟁자로부터 초래될 수 있고 그에 대한 대응 역시 전 국가적 차원의 안보전략의 일환으로 이루어지기 때문이다. 이는 본 논문이 관찰하고자 하는 대상이 초기에 보안에서 시작하지만 본질적으로 같은 내용을 가진 대상이 후에 안보 문제로 격상됨에 따라서 안보 문제로 규정되었기 때문이다. 미국의 금융 시스템, 전력 시스템, 통신 시스템, 선거관리 시스템 등을 해킹으로부터 보호하는 것은 보안이라고 쉽게 인식할 수 있지만 그러한 시스템에 대한 공격이 미국의 안보에 영향을 미칠 수 있는 결과를 가져오기 때문에 사이버 보안과 사이버 안보가 혼용되어 사용되는 것이 얼마간 불가피하다. 저자는 가능

한 한 맥락에 맞게 구분해서 쓰고자 노력하였지만 일부 두 용어가 혼용되는 경우가 있음을 미리 지적해두고자 한다.

Ⅱ. 사이버보안의 등장과 발전: 보안의 안보화

미국에서는 개인용 컴퓨터가 도입되기 시작했던 1980년대부터 정보보호를 위한 법제가 만들어지기 시작하였다. 1984년 '소기업 컴퓨터보안 및 교육법'(Small Business Computer Security and Education Act), 1986년 '컴퓨터 사기 및 남용방지법'(Computer Fraud and Abuse Act)은 민간 차원의 컴퓨터 관련 정보의 불법적 사용을 방지하기 위한 법이었다(홍순좌, 2019, 53-54). 그러한 법제는 단지 컴퓨터에 저장된 정보를 보호하거나 불법적으로 사용하는 것을 금지하는 전통적 의미로 순수한 보안의 수준에 머무르는 것이었다.

1. 클린턴 행정부의 사이버 보안정책의 등장

컴퓨터가 인터넷으로 연결되기 시작했던 1990년대부터 정보통신 기반시설에 대한 침해의 가능성이 인식되기 시작하였다. 그러한 흐름을 반영하여 1996년에 제정된 '국가 정보기간시설보호법'(National Information Infrastructure Protection Act)은 컴퓨터에 접근하여 보호되는 정보를 탈취하는 것을 범죄로 규정하는 법이었다.[1] 90년대 말 클린턴 행정부는 국가의 주요 기반시설 보호를 위한 정책적 노력을

기울였으며 1998년에 발행된 대통령지시 63호는 국가 주요 기반시설이 사이버 공간의 정보 네트워크에 의존하게 됨에 따라 새로운 위협에 취약성을 가지게 되었다고 지적하면서 이를 위한 범정부적 보호체계를 수립하는 것이었다.[2] 동 지시는 통신, 에너지, 은행과 금융, 수송, 수자원 체계, 그리고 국가 비상대책 등 국가의 주요 기간시설이 과거에는 물리적으로, 개념적으로 서로 별개의 체계였으나 정보기술의 발달과 더 나은 효율성을 위하여 점점 자동화되고 상호 연계되게 되었으며 그러한 상호연계로 인하여 사이버공격을 비롯한 더 많은 취약점을 가지게 되었다고 지적하고 있다.[3]

대통령지시63호는 그러한 상황에서 장래의 적이 국가 주요 기간시설에 대하여 미국 내부에서 사이버공격을 가할 수 있다는 점을 지적함으로써 사이버공격을 안보문제로 볼 수 있는 시각을 제공하였다. 동 지시는 향후 5년 내에 미국의 기간시설을 보호할 수 있는 역량을 마련할 것을 지시하고 있다.[4] 클린턴 대통령의 대통령지시 63호가 미국의 사이버 안보와 관련하여 의미 있는 이유는 사이버 보안을 국가 중요 정책으로 규정하고 향후 미국의 사이버 안보정책, 전략과 관련하여 중요한 정책의 내용과 방향을 미리 제시 하였다는 데 있다.

---

1) National Information Infrastructure Protection Act, P.L. 104-294, Section 201.
2) Presidential Decision Directive/NSC-63.
3) Presidential Decision Directive/NSC-63.
4) Presidential Decision Directive/NSC-63.

2. 부시 행정부의 사이버 보안정책의 안보정책화

미국에서 사이버 보안이 사이버 안보라는 국가 안보문제로 격상되는 본격적인 '안보화'(securitization)과정은 2000년대에 들어서 시작되었다(조화순 외 2017, 109-110). 2000년대는 인터넷을 통한 정보의 전달 속도가 급속도로 증가하는 '초고속 인터넷'이 보편화되는 시기였다. 이는 90년대에 시작되는 미국 사회 내에서 주요 기간시설의 네트워크를 통한 연결이 한층 심화, 확대되는 시기였다. 2000년에 제정된 '정부정보보안개혁법'(Government Information Security Reform Act)은 연방정부 기관에게 정보시스템과 데이터에 대하여 '위협에 기반을 둔 위험평가'를 주기적으로 실시하도록 의무화한 법이다.[5)]

더하여 2001년에 발생한 911테러는 외국의 군사적 공격이 아닌 소수의 비군사적 적대세력의 침투와 활동에 의해서 미국이 전쟁에 버금가는 물리적 타격을 입을 수 있다는 것을 명백히 보여주는 사건이었다. 911테러는 미국의 사회 전반에 걸쳐서 구축되어 있는 '보안시스템'으로 차단되었어야 하는 문제였다는 점에서(Mabee 2007, 390-392) 그리고 그러한 보안의 실패가 국가안보 수준의 피해를 초래했다는 점에서 911테러는 국내적 보안이 안보문제로 격상되는 계기를 제공하였다. 이후 미국 정부가 취하는 국내 보안의 강화조치는 국내 보안의 한 구성부분으로서 사이버보안이 보안의 안보화에 따라 안보문제로 격상되는 과정을 보여준다(Fouad 2019).

당시 부시 대통령은 행정명령 13228을 통해서 국가의 보안을 강화시키는 조치를 취했다. 동 행정명령은 사이버 안보와 관련하여 미국의 통신시설, 정보시스템을 포함하여 미국의 국가 주요 기간시

5) 동 법은 2002년 Federal Information Security Management Act(FISMA)로 대체되었다.

설을 보호할 수 있는 조치를 명령하고 있다.[6] 911테러 직후 미국 의회는 소위 '애국법'(Patriot Act)라고 불리는 테러를 차단하기 위한 법을 제정하였다. 해당 법은 연방정부의 법집행기관, 첩보기관이 테러주의자를 추적, 수사, 차단하기 위한 수색과 감청 등 감시의 권한을 확대하는 법으로써[7] 전통적인 군사력, 군사작전을 통한 국가안보 증진을 도모하기 보다는 국내적 보안을 강화함으로써 미국을 안전하게 하고자 하는 법이었다.

의회는 2001년 '국토안보법'(Homeland Security Act)를 제정했고,[8] 해당 법에 따라서 '국토안보부'(Department of Homeland Security)가 설립되었다. 국토안보부는 전통적으로 군사력을 사용한 국가 안보를 제외하고 다양한 적대세력, 테러주의자들의 비군사적 침투에 대하여 미국의 국내 전반의 안전을 도모하는 부서이다. 이를 위하여 국토안보부는 교통안전청(Transportation Security Administration; TSA), 이민국(Citizenship and Immigration Services; CIS), 관세국경보호청(Customs And Border Protection, CBP), 이민세관단속청(Immigration and Customs Enforcement, ICE)을 산하에 두고 해외에서 미국으로 들어오는 인간과 물건 등 모든 것을 통제, 관리한다.[9] 동시에 미국의 주요 기간시설에 대하여 외부의 침해로부터 안전을 확보하는 역할 역시 국토안보부의 관할

---

6) Executive Order 13228, Section 3(e)

7) 특히 동 법의 Title II Enhanced Surveillance Procedures는 이메일 등 다양한 정보통신수단에 대한 감시, 감청을 허용하는 법적 근거를 제시함으로써 사이버 안보와 연결된다.

8) 동 법의 Title II는 Information Analysis And Infrastructure Protection라는 소제목을 달고 있으며 Information Security라는 하부제목 하에 Cybersecurity 증진 조항을 가지고 있다. Homeland Security Act, P.L. 107-296, Section 211-215, 221-225.

9) Homeland Security Act, P.L. 107-296, Section 401-403, 411-419, 441-446.

사항이다.[10] 국토안보부는 미국의 주요 기간시설을 16개의 범주로 분류하고 이에 대하여 국내외의 침투로 인하여 타격을 받는 것을 방지하는 임무를 맡고 있다.

2003년 국토안보부는 '사이버 안보를 위한 국가전략'(National Strategy to Secure Cyberspace)을 발표하였다. 동 전략보고서는 세 가지 목표로서 미국의 주요 기간시설에 대한 사이버 공격을 방지하고, 사이버 공격에 대한 취약성을 제거하며, 사이버 공격이 발생할 경우 피해를 최소화하고 신속한 복구를 하는 것으로 하였다.[11] 이러한 전략을 후에 나오는 전략과 비교하기 위해서 여기서 한 가지 지적할 점은 동 전략보고서에서 이미 억지라는 용어가 등장했다는 것이다(Harknett & Stever 2011, 456). 당시 그러한 용어가 본격적인 미국의 국가전략으로 채택되지는 않았지만 후에 분석할 사이버솔라리움 보고서에서 제시된 '다층적 사이버 억지'로 연결되는 개념의 시초가 되었다.

부시 행정부의 정책은 911을 계기로 국내 보안의 문제가 안보 문제의 수준으로 격상되는 면을 보여주었다. 그에 따라서 주요 기간시설에 대한 사이버 공격에 대응하는 사이버 안보전략 역시 2003년 국토안보부가 작성한 보고서의 제목과 같이 '국가전략'(National Strategy)라는 명칭으로 제시되게 되었다.

---

10) Homeland Security Act, P.L. 107-296, Section 213, 214.

11) The White House. February 2003. The National Strategy To Secure Cyberspace.

3. 오바마 행정부의 정부 민간부문 협조체제 구축과 개인정보보호

오바마 행정부는 출범 3개월 후인 2009년 5월 '사이버공간 정책 리뷰'(Cyberspace Policy Review)를 발표하여 사이버 안보의 중요성을 강조했다. 이러한 점은 오바마 행정부 시기부터 이미 사이버 안보문제가 국가정책에서 최우선 순위를 차지하기 시작했음을 보여주는 것이다. 동 보고서는 디지털시대에 미국의 경제, 공공의 안전, 국가안보 등 미국의 핵심 가치가 사이버 안보에 달려있으며 미국 정부는 과거 여러 정책적 시도를 했지만 충분하지 못했으니 백악관이 리더십을 발휘하여 새로운 정책적 대응을 해야 한다고 하였다.[12] 그리고 그것을 위하여 미국 정부는 국내적으로 민간부문, 그리고 국제적으로 같은 생각을 가진 국가들(like-minded countries)과 협력, 공조체제를 구축해야 한다고 강조하였다. 특히 국제적으로 같은 생각을 가진 국가들과 협조, 공조체제를 구축해야 한다는 점은[13] 이후 미국의 사이버 안보전략에 핵심적인 내용이 되는 것으로서 오바마 행정부의 사이버 안보전략에서부터 본격적으로 강조되기 시작하였다.

오바마 대통령은 국가 주요 기반시설의 보안강화를 위하여 발의되었던 '사이버정보공유 및 보호법'(Cyber Intelligence Sharing and Protection Act)과 '사이버 안보법'(Cyber Security Act)의 입법이 기업의 정부와 사이버 위협 정보의 공유에서 제기된 개인정보보호 문제와 정부와 공유된 정보에 대하여 개인에 정보제공 고지의무 때문에 성사되지 않은(안정민 2018, 265-266) 이후 2013년 행정명

12) The White House. May 2009. Cyberspace Policy Review, pp. 7-9.
13) The White House. May 2009. Cyberspace Policy Review, pp. 20-21.

령 13636호 '주요기간시설의 사이버 안보 증진'(Improving Critical Infrastructure Cybersecurity)과 '대통령정책지시21'(Presidential Policy Directive 21, 이하 PPD21)을 발행하고 이를 기반으로 주요 기반시설의 사이버 안보정책을 추진하였다. 오바마 대통령의 행정명령 13636은 주요 기간시설의 보호체계 구축을 위한 사이버보안 프레임워크의 개발과 보급을 핵심 목적으로 하고 있으며[14] 그 과정에서 사생활과 개인의 자유에 대한 보호를 포함할 것을 강조하였다.[15] 이는 과거 부시 행정부가 911테러의 충격 속에서 테러와의 전쟁을 수행하는 과정에서 테러주의자를 추적하면서 빚었던 많은 사생활 침해의 논란에 대응하여 사이버 안보를 추진하면서도 국민들의 사생활 침해를 최소화하고자 하는 것이었다.[16] PPD21은 주요 기반시설 보호와 관련하여 정부 핵심부서들의 역할과 임무를 명확히 하는 것을 주요 목적으로 하였다. 동 대통령지시는 국가 주요 기간시설에 대한 사이버보안에 있어서 국토안보부의 역할을 더 정교하게 규정하면서 동시에 각 기간시설이 서로 다른 산업영역, 부문에 있어서 전혀 다른 환경에 있음을 지적하면서 각 부문별 기관의 역할과 그 조정을 명령하였다.[17]

2014년 북한의 소니픽쳐스 해킹사건은 백악관이 기업과 정부의 사이버 위협 정보공유에서 발생할 수 있는 개인정보 침해 가능성에 대하여 유연한 태도를 가지게 하는 계기가 되었다. 그러한 환경에서 2015년 '사이버 안보 정보공유법'(Cybersecurity Information Sharing Act)을 핵심으로 하고 '사이버네트워크보호법'(Protecting

14) Executive Order 13636, February 12, 2013, Section, 7.
15) Executive Order 13636, February 12, 2013, Section, 5.
16) Executive Order 13636, February 12, 2013, Section, 1.
17) Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013.

Cyber Networks Act), '국가 사이버 안보증진법'(National Cybersecurity Protection Advancement Act)을 포함하는 '사이버 안보법'(Cybersecurity Act)이[18] 제정되었다. 특히 '사이버 안보 정보공유법'은 미국 사이버 안보정책의 핵심 내용인 정부와 민간의 정보공유에 대한 법적인 기반을 마련한 의미가 있다.[19] 미국의 핵심 기간시설이 대부분 민간이 소유하는 것이기 때문에 사이버 위협과 공격에 대응하는데 있어서 정부와 민간의 정보공유는 필수적인 만큼 동 법을 기반으로 하는 정부와 민간의 정보 공유체제의 마련은 미국의 사이버 안보정책에 있어서 중요한 의미를 지닌다(박상돈. 2017, 51).

그러나 오바마 행정부의 정부와 민간 사이의 협조체제 구축은 민간기업들의 적극적 참여를 유도하지 못함으로써 실질적인 성과를 거두지 못했다(Fidler 2015). 그러나 오바마 행정부가 미국의 사이버 안보정책에 기여한 바는 첫째, 정부와 민간의 정보공유가 핵심적인 내용을 구성한다는 것을 인식하고 이를 위한 구체적인 법적인 근거를 마련했다는 것이다(양천수, 지유미. 2018, 168-184). 둘째, 오바마 행정부는 사이버 안보 보호대상에 미국의 지적재산권을 포함시켰다. 셋째, 미국의 사이버 안보정책, 전략에서 국제적 협력이 필수적이라는 것을 지적했다는 점이다. 이러한 점들은 이후 미국의 사이버 안보정책, 전략의 중요한 내용을 구성한다.

18) Cybersecurity Act of 2015, P. L. No. 114-113. 동법은 2015세출법의 Division N으로 통과되었다.

19) Cybersecurity Information Sharing Act, 15 U.S.C. 12, Section 102, 103, 104.

4. 트럼프 행정부의 공세적 사이버 안보전략

트럼프 행정부도 사이버 안보를 중요한 정책 의제로 간주하였으며 전임자의 정책과 다른 점은 미국 정부가 더 공격적인 대응을 하도록 하고 있다는 것이었다. 트럼프 대통령은 2017년 5월 행정명령 13800을 발행하여 연방정부 차원에서 대응해야 하는 네트워크 사이버보안, 주요 기반시설 보호를 위한 사이버보안 등을 설명하고 정부 각 부서의 임무와 책임을 규정하면서 연방정부의 통합된 정책수행을 강조하였다.[20] 동 행정명령은 사이버 적대자들에 대한 억지 방안을 마련하는 것과 사이버 안보에 국제적 협력의 방안을 마련할 것을 국무부, 국방부, 재무부, 법무부, FBI 등 관련 부서에 지시하였다.[21] 다음 해인 2018년 국토안보부는 '2018 국토안보부 사이버 전략'을 발표하였다.[22] 동 전략은 백악관의 정책을 실행하는 실무적 내용을 가지고 사이버 위협의 식별을 위한 대책, 국가 기간시설 운영자와 동반자관계 수립 및 사이버 위협 정보공유체계 강화, 연방정부 정보체계의 사이버 취약성 제거와 함께 사이버 위협의 제거라는 공세적 조치를 선언하였고 특히 사이버 위협 관리정책 및 활동을 지원하는 국제적 협력을 강조하였다.[23]

같은 해인 2018년 9월 백악관은 '미국의 국가 사이버 전략'을 발표하였다.[24] 동 전략은 4가지 전략적 목표를 제시하였다. 그것은 ▶ 미국 국민, 국토, 미국의 생활방식 보호(Protect the American

20) Executive Order 13800, May 11, 2017, Section 1(a).
21) Executive Order 13800, May 11, 2017, Section 3(a), (b), (c).
22) U.S. Department of Homeland Security Cybersecurity Strategy, May 15, 2018.
23) U.S. Department of Homeland Security Cybersecurity Strategy, May 15, pp. 3-5.
24) The White House, National Cyber Strategy of the United States of America, September 2018.

People, the Homeland, and the American Way of Life); ▶ 미국의 번영 촉진(Promote American Prosperity); ▶ 힘을 통한 평화유지(Preserve Peace through Strength); ▶ 미국의 영향력 확대(Advance American Influence)이다.

이 중에서 과거 행정부의 정책에 비해서 특징적인 점은, 첫째, 과거 미국 정부에서 사이버 안보의 주요 대상이 미국 정부 네트워크와 국가 주요 기간시설의 보호였던데 비해서 트럼프 행정부에서는 이를 확대하여 미국 전체를 보호 대상으로 하였다(김근혜. 2019, 913). 특히 위의 전략목표 중에서 첫 번째 내용 '미국 국민, 국토, 미국의 생활방식 보호'는 기존의 주요 보호 대상인 미국 정부 네트워크와 국가 주요 기간시설에 더하여 미국인, 미국사회 전체, 그리고 미국의 생활방식으로 확대된 것이었다.[25] 이러한 보호 대상의 확대는 2016년 러시아의 미국 대통령선거에 대한 공격적인 개입으로 미국의 사이버 안보가 정보네트워크와 국가 주요 기간시설에 한정되지 않고 미국의 정치제도, 민주주의에 대한 위협까지 포함하는 것으로 확대되었다는 점을 보여주는 것이다.

둘째, 트럼프 행정부는 사이버 위협에 대하여 더 공격적으로 대응한다는 점이다. 위에서 언급한 세 번째 전략적 목표인 힘을 통한 평화의 유지(Preserve Peace through Strength)는 사이버 적대 세력에게 '대가를 치르게 한다'(impose consequences)는 것이다.[26] 동 보고서는 당시 사이버사령부 사령관에게 사이버 적에게 더 자유롭게 공격적으로 대응하도록 재량권을 부여하고 있다(Sanger, New York Times. 2018). 이에 대하여 당시 뉴욕타임스는 트럼프 대통

25) The White House, National Cyber Strategy of the United States of America, September 2018, pp. 6-11.
26) The White House, National Cyber Strategy of the United States of America, September 2018, pp. 20-21.

령이 과거 오바마 대통령의 제약을 떨어버리고 더 자유롭게, 더 자주 적을 공격할 수 있도록 명령을 내렸다고 묘사하고 있다 (Wolff. New York Times, 2018). 트럼프 행정부의 '힘을 통한 평화의 유지'는 부시 대통령의 억지 개념이 발전하여 이후 솔라리움보고서로 이어지는 연결점의 역할을 하였다.

위에서 검토한 4명의 미국 대통령에 의한 정책은 주로 대통령에 의해서, 행정부의 정책으로 추진되었다. 이는 전통적으로 보안과 안보는 대통령의 관할 사항이었기 때문이다. 그러나 사이버보안이 안보로 확대되고, 사이버 안보의 대상이 단순한 정보보호에서 기간시설 보호, 더 나아가 미국의 지적 재산권, 미국의 정치제도와 민주주의를 포함하는 미국 전체의 보호로 확대되는 과정에서 수 많은 정부의 기관, 정책들이 만들어짐으로써 미국 정부의 사이버 안보정책이 일관되고 통합되지 못한 면이 나타났다.

Ⅲ. 사이버솔라리움위원회 보고서

미국 의회는 2019년 국방수권법안에서 통합되고 강력한 사이버 안보전략을 마련할 수 있는 위원회를 만들도록 하였다.[27] 동 위원회는 사이버솔라리움위원회(Cyberspace Solarium Commission)라는 명칭으로 활동하여 2020년 3월 동 위원회 활동을 통해서 사이버 안보전략을 제시하는 보고서를 발표하였다. 2019국방수권법은 "중대한 사이버 공격에 대하여 미국을 방어하는 전략적 접근법에 대한

27) John S. McCain National Defense Authorization Act for Fiscal Year 2019(이하 NDAA2019), P.L. 115-232, Section 1652.

컨센서스(consensus)를 만들어 내는 것"이라고 하였다.[28] 이는 미국의 사이버 안보정책이 정부 내에서 많은, 다양한 부서에 의해서, 다양한 시점에서, 다양한 위협에 대응하여 만들어지고 추진됨에 따라서 각각의 정책, 프로그램들이 서로 다른 인식, 접근법을 가지게 되고 그 결과 중대한 사이버 위협, 공격에 효과적인 대응이 이루어지지 않게 되었던 점을 반영하는 것이었다. 이는 과거 아이젠하워대통령이 1950년대 초 구소련에 대한 냉전을 수행하기 위한 정책, 전략에 있어서 미국 정부 내의 여러 부서들의 입장, 전략들 사이에서 컨센서스를 만들어 내기 위하여 솔라리움보고서를 채택했던 것을 모델로 하여 사이버 안보에 대해서도 미국 정부 내에서 사이버 안보의 중요성을 공유하고 정책, 전략에 대한 정부 내 여러 부서, 기관 사이에 컨센서스를 만들어 내기 위한 것이다.[29]

다만 한 가지 지적할 것은 사이버솔라리움보고서가 제안한 사항 중에서 26개의 사항이 '2021년 국방수권법'(NDAA 2021)에서 입법이 되었고(Hon, Gallagher), 앞으로 더 입법과 행정부의 조치로 나타나겠지만 여전히 보고서는 제안이고, 그러한 제안이 미국 정부의 행동으로 나타나는 것을 확인해야 한다는 점에서 앞서 논의한 의회의 입법이나 행정부가 발표한 전략과는 차이가 있다는 점을 지적하고자 한다.

1. 사이버솔라리움보고서의 전략적 원칙: '억지'(deterrence)

사이버솔라리움보고서가 가장 중요하게 지적하는 점은 미국의

28) NDAA 2019 Section 1652, (a)(1).
29) Cyberspace Solarium Commission Report, p. 20.

적대세력, 그것이 국가이든 범죄집단이든, 아니면 개인이든 그들은 여전히 미국에 사이버공격을 통해서 원하는 것을 얻고자 하며 그 과정에서 자신들의 공격에 대하여 미국이 반격을 할 것이라는 것을 크게 걱정하지 않고 사이버공격을 감행하고 있다는 것이다.[30]

이러한 인식에 기반하여 보고서에서 제시된 전략은 '억지'(deterrence)이다. 보고서는 미국 정부가 사이버 적대세력으로 하여금 그들이 미국에 대하여 사이버공격을 하는 것에 대한 비용과 효과에 대한 계산에서 공격을 하지 않는 것이 본인들에게 이익이 될 수 있도록 해야 한다고 제시하고 있다.[31] 억지가 과거의 정책, 전략과 다른 점은, 과거 미국 정부의 전략이 사이버 위협과 공격의 파악과 제거였으나 이는 해당 위협과 공격이 이루어지고 난 이후에 대응하는 것인 반면 억지는 사이버 위협과 공격을 실행하고자 하는 행위자를 상대로 그러한 위협과 공격을 하지 못하도록 사전에 미리 억누르는 것이다. 전자가 수세적, 방어적이라면, 후자는 방어적이지만 적극적, 공세적 방어이다. 이러한 공세적 방어전략은 앞서 지적한 바와 같이 트럼프 행정부의 사이버 안보전략의 세번째 전략방침(pillar)인 힘을 통한 평화의 보장(Preserve Peace through Strength)에서 시작된 것이지만 그러한 억지가 미국의 사이버 전략의 일부로 제시되었다. 솔라리움보고서에서는 미국의 사이버 전략 전체를 억지라는 틀 내에서 재구성하고자 하는 것이다. 그 내용은 다음과 같다.

사이버전략으로서 억지는 국방부에서는 좀 더 일찍 논의되었나 여전히 제한적 차원에서 논의되었다. 그러나 사이버솔라리움보고서는 억지라는 개념에 기반하여 미국의 사이버 전략을 세우고자 하였

30) Cyberspace Solarium Commission Report, pp. 14-15.
31) Cyberspace Solarium Commission Report, p. 26.

다는 점에서 과거와 차이가 나고, 후에 언급하겠지만 억지라는 전략을 한층 더 공격적으로 운영하고자 하는 점에서 과거의 논의와 차이가 있다.

2. 사이버솔라리움보고서의 전략: 다층적 사이버억지

솔라리움 보고서에서는 동 보고서의 사이버 안보전략을 '다층적 사이버 억지'로 호칭하고 있다. 이는 사이버 적대세력의 공격을 억지하기 위하여 3가지 차원, 즉 다층적 차원에서 적대세력을 유도, 압박, 처벌한다는 의미이다. 그리고 이를 실행하기 위하여 다음과 같은 3가지 영역에서의 조치를 제시하고 있다.

1) 사이버 행위자의 행위 교정

첫째는 사이버 공간에서 불법행위에 대하여 국제적 규범을 확립하고, 법을 집행할 수 있는 수단을 강화함으로써 사이버 공격을 하고자 하는 행위자의 행위를 제약하는 것이다. 미국은 이를 위해서 비군사적 수단, 즉 법집행 활동, 제재, 외교, 정보공유를 통해서 위협을 가하고자 하는 행위자가 규범에 순응하도록 설득하고, 규범을 위반할 경우 처벌이 따른다는 것을 인식하게 하는 것이다. 동 보고서는 이를 이행하기 위하여 다음을 제안하였다.

- ▶ 의회는 입법을 통하여 국무부 내에 차관보급으로 '사이버 안보와 신기술국'(Cyberspace Security and Emerging Technologies)을 신설하도록 한다. 동 부서는 사이버공간에서 국제규범을 발전, 강화하는 미국 정부의 정책을 주도한다.
- ▶ 행정부는 국제정보통신 기술표준을 설정하는 국제적 논의에 적극

적으로 참여하고, 특히 '국립기술표준연구소'(National Institute of Standard and Technology)는 그러한 국제 논의에 정부, 학계, 전문가단체, 업계가 적극적으로 참여하도록 노력한다.

▶ 의회는 사이버공간에서 법집행활동을 위한 국제적 장치를 개선하기 위한 노력을 기울여야 한다. 예컨대, 사법공조조약(Mutual Legal Assistance Treaty), 사법공조과정을 개선하고 연방수사국(FBI)의 해외 파견 사이버법률관의 숫자를 늘리는 것도 포함된다.[32]

2) 사이버 공격자의 혜택 거부

억지를 위한 두 번째 차원의 대응은 사이버 공격자가 설사 공격을 실행해도 그러한 공격으로부터 이득을 얻을 수 없게 함으로써 사이버공격을 단념하도록 한다는 것이다. 이러한 차원의 대응은 주로 미국의 내부적 네트워크가 사이버공격을 받지 않도록 취약점을 최소화하고 설사 사이버공격을 받더라도 그러한 공격에 견디고, 피해를 짧은 시간 내에 복구할 수 있는 역량을 갖추는 것이다. 이를 위하여 보고서는 국가적 '내구 회복력'(resilience)을 강화하고, 사이버 생태계의 기본적인 보안 수준을 격상시켜서 사이버 공격자의 활동을 제한하는 것, 그리고 민간부문과의 협조체제가 원활하게 운영될 수 있도록 위협에 대한 정보의 제공, 상황에 대한 인식을 제고할 수 있도록 소통을 증진하는 것을 다음과 같이 제안하고 있다.

▶ 미국 사이버시스템의 내구, 회복력을 증강시킨다. 이는 사이버보안 및 인프라보안국(Cybersecurity and Infrastructure Security Agency, CISA), 그리고 개별 분야기관들이 분야별 위협을 파악, 평가, 관리하는 활동을 강화하고 사이버 사건에 대응할 수 있도록

32) Cyberspace Solarium Commission Report, p. 3, pp. 46-53.

'사이버 대응 및 복구기금', 선거지원위원회에 대한 지원을 강화하는 것이다. 이는 미국 사이버시스템의 사이버 위협, 공격에 예비, 대응 능력을 강화하는 것이다.

▶ 사이버 생태계를 강화한다. 이는 '사이버안전 인증 및 표시국'(National Cybersecurity Certification and Labeling Authority)을 설립하여 사이버안전 인증 및 표시프로그램 시행, 클라우드 보안 인증제도의 개발, 제조, 판매업자가 안전한 제품, 소프트웨어 판매하도록 하는 제도를 강화하는 것이다. 이는 주로 정보통신, 네트워크 산업의 영역에서 사이버 위협의 취약점을 제거하고 강력한 산업체계를 구축하기 위한 것이다.

▶ 사이버 공격자가 사이버 공격으로 얻을 수 있는 혜택을 제거한다. 이를 위하여 의회가 국가 기간시설의 개념을 법적으로 규정하고, 그에 대한 정부의 지원, 의무 등을 규정한다. 정부와 민간부문이 위협정보, 분석과 여타 관련자료를 공유하기 위한 협조체제를 강화한다.[33]

3) 사이버공격에 대한 대가의 부과

다층적 사이버 억지의 세 번째 차원은 미국에 대한 적대적 사이버 공격에 대하여 군사적 수단을 포함한 모든 종류의 힘을 사용하여 대가를 치르게 하는 것이다. 보고서는 언제든지 군사력을 사용할 수 있는 선택지의 하나로 유지하기 위하여 준비해야 한다고 제안하고 있다.[34]

▶ 사이버군의 구조평가, 핵무기 관리시스템의 사이버 취약성 평가,

33) Cyberspace Solarium Commission Report, pp. 4-6, pp. 31-45, pp. 54-109.

34) Cyberspace Solarium Commission Report, p. 6.

여타 무기체계의 사이버 취약성 평가한다.

▶ 방위산업계가 사이버 위협 정보공유 프로그램에 참여하도록 하고 방위산업 네트워크에서 위협을 추적할 수 있도록 요구한다.

특히 다층적 사이버 억지를 위한 세 번째 차원의 조치로서 사이버공격에 대한 대가의 부과에서 보고서는 2018년 국방부의 사이버 전략에서 제시되었던 '선제적 방어'(defend forward)라는 개념을 제시하고 있다. 보고서는 미국은 사이버공격이 발생한 이후에 대응하는 것이 아니고 선제적으로 위협을 관찰, 추적, 대응해야 하며, 선제적 방어는 사이버공격이 진행되는 중에 저지, 파괴하고 장래 사이버공격을 억지하며 우호적인 국제 행위규범을 강화하는 것을 목적으로 한다고 하고 있다.[35] '선제적 방어'는 과거 냉전시기 구소련의 팽창정책에 대응하는 미국의 전략인 '전진방어'(forward defense)와 유사한 개념이다.[36] 냉전 시기 전진방어는 구소련이 팽창하는 원점에 가장 가까운 지점에서 방어함으로써 미국과 동맹국의 영토를 가능한 한 완전하게 지킨다는 개념이다. 이를 위하여 유럽과 동아시아에 미군을 주둔시키는 전략으로 나타났다. 사이버 안보의 경우, 냉전 시기와 달리 물리적 공간이 큰 의미가 없고 시간이 중요한 변수이다. 사이버 안보의 선제적 방어는 사이버 적대세력의 활동이 시작되기 전, 활동이 시작되는 순간, 그리고 최소한 활동이 진행되는 것과 동시에 그러한 활동을 선제적으로 관찰, 추적, 대응한다는 개념이다.[37]

그러나 선제적 방어 개념은 2018년 국방부 사이버 전략에서 제시되었을 때 상대국의 사이버공간에 침투하여 공격작전을 할 수도 있다는 우려도 제기될 정도로 공격적인 개념이었다(신소현 2020,

35) Cyberspace Solarium Commission Report, p. 24.
36) Cyberspace Solarium Commission Report, p. 33.
37) Cyberspace Solarium Commission Report, p. 33.

68-70). 보고서는 선제적 방어는 용인되는 일상적인 첩보 행위와 전략적인 사이버공격의 사이, 중간 정도의 악의적 행위에 대응하기 위한 것이라고 설명하였다.[38]

Ⅳ. 미국의 사이버 안보전략의 접근법: 지속과 발전

지난 1980년대부터 현재까지 미국 정부의 사이버 안보 전략의 특징적 내용은 다음과 같다.

1. 방어대상의 확대와 전 국가적 사이버 안보전략

1980년대 미국의 사이버공간에서 보호 대상은 단지 컴퓨터에 저장된 정보의 보호에 그쳤다. 1990년대에 들어서서 인터넷 사용의 급증으로 사이버공간이 창출되고, 클린턴 대통령의 대통령지시63호는 이러한 사이버공간에서 국가 주요 기간시설로 사이버 안보정책의 방어 대상을 확대하였다. 2000년 들어서서 초고속통신망이 확대되어 사이버공간이 급격하게 확대되고 911테러를 통해서 보안이 안보의 수준으로 격상됨에 따라서 부시 대통령 시기 사이버 안보의 대상은 1990년대 국가 기간시설에 더하여 다중이용시설 등이 사이버 안보의 보호 대상으로 포함되었다.

오바마 행정부에서는 국가 기간시설 뿐만 아니라 미국의 산업과

38) Cyberspace Solarium Commission Report, p. 110.

지적재산권을 사이버 침투를 통하여 탈취하는 것도 중요한 보호 대상으로 포함되었다. 2016년 러시아의 미국 대통령선거에 대한 공격적인 개입은 이후 연방, 주, 지방정부 차원의 선거제도를 사이버 안보의 대상으로 포함시키는 결과를 초래하였다. 2018년 백악관의 '국가사이버전략'은 보호 대상을 '미국 국민, 국토, 미국의 생활방식 보호'라고 하면서 사실상 미국의 국민, 사회를 포함한 모든 것을 보호하는 것으로 제시하였다.[39]

이후 4차 산업혁명이 초래할 초연결성, 즉 사물인터넷, 클라우드, 인공지능, 자율주행차 등은 한 사회의 연결성을 극단적으로 확대시킬 것이다. 이러한 변화를 반영하여 사이버솔라리움보고서는 '전 국가적 접근법'(a whole-of-nation)을 만들어야 한다고 하면서 그러한 접근법을 표현한 그림에서 가장 기초로서 '국민'(citizen)을 정부, 민간부문과 함께 포함시켰다.[40] 미국의 사이버 안보정책의 보호 대상은 처음에는 컴퓨터에 저장된 정보에서 시작하여, 국가 주요 기간시설과 다중이용 시설, 지적재산권을 포함하게 되고 나아가 미국의 정치제도, 미국인들의 생활방식까지 확대되어왔다.

2. 미국 정부의 공세적 방어전략

미국 정부가 지난 40여 년 동안 사이버 안보정책을 추진하는 과정에서 나타난 특징은 그 정책적 접근법이 점차 공세적으로 변화하고 있다는 것이다. 처음 사이버보안이 정책적 문제가 되었을 때 미국 정부의 정책은 순수한 방어, 즉 침해가 발생하면 책임자를 찾고

39) The White House, National Cyber Strategy of the United States of America, September 2018, p. 6, p. 9.
40) Cyberspace Solarium Commission Report, p. 23.

피해를 복구하는 것이었다. 그러한 수동적인 순수 방어정책은 이후 점차 적극적인 대응의 방향으로 변화하였다. 특히 트럼프 행정부의 사이버 전략에서부터 '힘을 통한 평화'라는 개념으로 실제 사이버공격에 대하여 처벌하는 것을 강조하기 시작하였다. 그러나 사이버 공격자를 처벌하는 것은 여전히 사이버 적대자가 미국의 네트워크에 침투하여 미국에 피해를 입히고 난 이후에 처벌하는 것으로서 미국 사회의 안전을 보장하는데 한계가 있는 것이다.

사이버솔라리움보고서는 미국의 사이버 안보 전략 자체를 억지라는 개념적 틀에 맞추어서 다시 만들고자 하였다. 보고서의 억지전략은 미국의 국내 네트워크, 사이버공간을 사이버 위협, 공격을 당하지 않도록 취약점을 제거하고, 공격을 당할 경우에도 공격에 대하여 미국의 사이버 시스템이 강한 내구성, 회복력을 가지도록 함으로써 공격자의 공격 의도가 실현되지 않도록 한 후에 공격을 실행한 사이버 적대세력에 대가를 치르게 한다는 것이다. 이를 위하여 사이버 적대세력의 공격을 선제적으로 차단, 저지시키고, 필요할 경우에 군사력을 동원하여 보복할 수 있도록 한다는 것이다.[41] 보고서는 이것을 선제적 방어라는 개념으로 제시하고 있다. 이러한 점은 사이버 공격에 방어적으로 대응했던 과거의 정책, 전략에 비해서 미국의 사이버 전략이 대단히 공세적으로 나아가는 방향을 보여주는 것이다.

3. 정부와 민간의 협조체제 구축

미국의 사이버 안보정책, 전략의 가장 중요한 내용, 가장 특징적인 면은 그것이 안보정책이지만 정부가 전적으로 담당하는 전통적

41) Cyberspace Solarium Commission Report, pp. 23-25.

인 군사안보와 달리 정부 혼자서 성공적으로 달성할 수 없고 민간부문과 함께 해야 한다는 것이다. 그것은 앞서도 언급했지만 미국의 사이버 안보의 가장 중요한 보호 대상인 국가 주요 기간시설이 거의 대부분, 약 85% 정도를 민간이 소유, 운영하고 있기 때문이다. 사이버 안보는 지켜야 할 대상도 미국 사회 전역에 산재해 있고 이를 지키기 위하여 취해야 하는 조치, 활동 역시 정부가 관할하는 영역보다 훨씬 크고 광범위하기 때문에 전통적 군사안보와 전혀 다른 접근법과 정부조직이 필요한 것이다.

이를 위한 미국 정부의 접근법은 정부와 민간의 협조체제구축이다. 그리고 협조체제 구축의 핵심은 두 부문 사이에 위협정보와 대응조치의 공유이다. 그것은 미국의 시스템 하에서 민간이 소유하고 있는 기간시설에 대하여 정부의 개입이 여타 다른 국가, 사회에 비해서 더 제한적이기 때문이다. 결국 정부가 관할권을 가지지 못하는 대상을 보호해야 하는 미국의 딜레마에서 도출되는 접근법이 정부와 민간부문 사이 '사이버 위협 정보와 대응조치의 공유'이다. 그러한 정보공유체제는 2015년 '사이버안보정보공유법'으로 마련되었다. 그리고 트럼프 행정부는 2018년 국토안보부에 '사이버보안 및 인프라안보국'(Cybersecurity & Infrastructure Security Agency, CISA)을 설립하여 미국 정부가 주요 기간시설을 사이버공격으로부터 보호하기 위한 임무를 담당하도록 하였다. 동 부서는 부시 행정부가 2007년 국토안보부에 설립한 '국가보호프로그램국'(National Protection and Programs Directorate, NPPD)을 확대 개편한 것이다.

그러나 사이버솔라리움보고서는 정부 민간협조체제의 핵심은 사이버 위협정보의 공유이며, 그러한 정보공유를 통해서 공동의 상황인식을 제고할 수 있고, 이를 기반으로 공동 대응, 협동작전이 가능하다고 하면서 정부가 민간단체들과 협력할 수 있는 구조와 절차를

만들어야 한다고 지적하고 있다.[42] 미국의 딜레마는 정보의 공유가 개인 사생활의 침해 가능성, 또는 반대 방향에서 기업활동 자유의 침해 가능성이 있다는 점이다. 이는 정부와 민간의 협조체제의 구축에 한계가 있다는 것을 보여준다. 그러나 2014년 소니픽쳐스에 대한 해킹이 그러했던 것처럼 향후 미국이 직면할 사이버공격이 미국 사회에 어떠한 충격을 주는지에 따라 돌파구가 생길 수도 있다.

4. 미국의 사이버 안보정책과 개인정보보호

지난 40여년 간 미국의 사이버 안보정책의 가장 큰 딜레마는 사이버 안보와 개인정보보호 사이의 충돌이었다. 이는 사이버 위협, 침투, 공격을 추적하고 대응하기 위해서 네트워크 상에서 이루어지는 다양한 활동에 대한 정보가 필요하기 때문이며 그러한 정보는 특정 서버와 계정의 사용, 데이터 송수신 등과 관련된 개인정보를 포함하는 것이기 때문이다.

사이버 안보를 위하여 개인정보의 침해, 또는 보호의 문제가 제기된 것은 부시 행정부에서 테러와의 전쟁을 수행하면서 유, 무선상, 사이버 상에서 개인정보를 침해한데서 시작되었다(Risen, James & Lichtblau, Eric. 2005). 반면 오바마 행정부 시기 공화당의 지지를 받던 '사이버 정보공유 및 보호법(Cyber Intelligence Sharing and Protection Act, CISPA)은 민주당의 반대로 입법이 되지 않았다. 반대로 민주당이 상원에서 발의한 2012년 '사이버 안보법'(Cyber Security Act, CSA)은 공화당 상원의원들이 기업의 자유를 침해한다며 반대하여 법안은 상원도 통과하지 못하였다. 이러한

42) Cyberspace Solarium Commission Report, p. 101.

견해 대립 상태에서 2014년에 발생한 북한의 소니사 해킹사건으로 프라이버시와 개인정보보호에 엄격했던 백악관의 태도가 바뀌면서 2015년에는 '사이버보안정보공유법'(Cybersecurity Information Sharing Act, 이하 CISA)이 제정되어 민간과 정부가 사이버 위협에 관한 정보를 공유할 수 있는 법적인 근거가 마련되었다.[43]

CISA가 정부가 민간으로부터 사이버 위협 관련 정보를 받을 수 있는 법적인 근거를 마련해주었으나 민간기업이 정부에 자신의 네트워크 상에서 발견된 사이버 위협 정보를 제공하기 위해서는 그러한 정보제공에 따르는 법적인 책임을 면제해주는 법적인 근거, 즉 면책조항이 필요했다. CISA는 동 법을 이행하기 위한 행동에 대해서는 제소를 할 수 없도록 함으로써 민간기업이 사이버 위협과 관련한 정보를 정부와 공유하는데 대한 법적인 부담을 제거하였다.[44] 더하여 CISA는 민간기업들이 사이버 위협과 관련하여 서로 소통하는 것에 대하여 독점금지법의 적용을 면제해주었다.[45] 이러한 법적인 장치에도 불구하고 사이버 위협에 관한 정부와 민간의 정보공유는 여전히 어려운 점이 있다. CISA가 제정된 이후 2018년 현재까지 정부와 정보제공 프로그램에 참여한 민간기업은 6개에 불과할 정도로 저조하다(Marks, Joseph, 2018).

사이버솔라리움보고서는 그러한 문제를 정부와 민간의 자발적 정보공유 프로그램으로 해결하고자 하였다. 더 나아가 보고서는 사이버 위협에 대응하고 네트워크 상의 취약점을 찾기 위해서 일부 행정부서에 행정적 문서제출명령을 발부하는 권한을 부여하는 것을 고려하도록 제안하고 있다.[46] 이는 민간기업, 단체, 개인에게 사이

43) Cybersecurity Information Sharing Act, Section 104(c)(1)
44) Cybersecurity Information Sharing Act, Section 106(b)(1)
45) Cybersecurity Information Sharing Act, Sections 104(e)(1), (2), 108(e)

버 위협에 대응하기 위하여 정보를 제공하도록 강제할 수 있는 권한을 의미한다. 현재 행정부서가 문서제출명령을 할 수 있는 경우는 연방부서의 감사부서(Offices of Inspector General), 마약단속국(Drug Enforcement Administration), 1996년 의회가 연방수사국(FBI)에 건강보험 사기 수사를 위하여 일시적으로 부여한 적이 있고, 재무부의 '해외자산통제국'(Office of Foreign Asset Control)이 제재 위반을 조사하기 위하여 빈번하게 사용하고 있다. 그러나 사이버 위협에 대응하기 위하여 문서제출명령권을 행정부서가 행사하는 것은 위의 사례와 달리 광범위한 영역에 적용되고 기업의 책임, 개인의 사생활이 관련되기 때문에 논란이 발생할 가능성이 높다.

5. 사이버 안보전략에 대한 민주당과 공화당의 입장 차이

앞서 미국의 사이버 안보전략에 대하여 논의하면서 부분적으로 지적된 사항이지만 미국의 주요 두 정당, 민주당과 공화당은 입장 차이를 보여주고 있다. 첫째, 공화당 대통령이었던 부시와 트럼프는 공세적인 전략을 선호하였다. 부시 대통령과 트럼프 대통령 모두 사이버 적대세력에 대해서 미국의 힘을 사용하는 억지라는 개념에 기반을 두고 접근하는 모습을 보였다. 2003년 사이버 안보를 위한 국가전략에서도 적대세력을 억지하는 접근법을 제시하였고, 트럼프 대통령 역시 미국의 국가 사이버전략에서 힘을 통한 평화를 제시하면서 억지라는 개념을 기반으로 하였다. 반면 오바마 대통령은 상대적으로 억지라는 개념 보다는 국제적 협력의 중요성을 강조하였다.

46) Cyberspace Solarium Commission Report, p. 100.

둘째, 민주당의 경우 사이버 안보전략, 특히 정부와 민간의 협조체제, 정보공유를 실행하는 과정에서 개인정보의 침해가능성에 우려를 가지고 있었던 반면 공화당에서는 마찬가지 정보공유를 실행하는 과정에서 기업의 보고의무가 기업활동의 자유를 침해할 수 있는 가능성에 우려를 가지고 있었다. 셋째, 부시, 트럼프 대통령은 사이버 안보전략을 추진하는데 있어서 국토안보부가 주된 역할을 하도록 한 반면, 클린턴, 오바마 대통령은 백악관이 주도적 역할을 하는 모습을 보였다. 사이버솔라리움보고서는 그러한 정당 사이의 차이를 극복하는 국가전략을 제시하고자 하는 시도였다. 그리고 과거에 사이버 위협, 공격이 증가하는 경향, 그리고 초연결사회의 전개 속도에 비추어 볼 때 사이버문제가 더 심각하게 제시되면 이러한 정당 사이의 차이가 중요하지 않게 될 가능성도 있다.

6. 사이버 안보를 위한 국제적 연대의 구축

미국의 사이버 안보 정책, 전략에 있어서 정부와 민간부문의 협조체제 구축만큼이나 핵심적이고 중요한 것이 국제적 연대의 구축이다. 국제적 연대의 구축은 오바마 행정부에서 미국의 사이버 안보 정책의 일환으로 제시되었지만 만족할 만한 성과를 거두지는 못했다.

사이버 안보를 위한 국제적 연대의 구축은 두 가지 의미를 가진다. 첫째, 잠재적 사이버 적대세력을 억지하기 위해서 미국 정부는 국제규범을 강화하는 것을 자신의 중요한 정책목표로 하고 있다. 사이버솔라리움보고서 역시 다층적 사이버 억지에서 국제규범의 강화에 미국 정부가 적극적으로 나서도록 주문하고 있다. 보고서는 사이

버공간을 위한 국제적 규범의 수립, 강화는 미국 혼자서 하기는 어려운 일이고 국제적 동맹과 파트너와의 네트워크를 강화함으로써 이룩하도록 제안하고 있다.[47] 보고서는 이를 위하여 국무부에 차관보급을 수장으로 하는 '사이버 안보 및 첨단기술국'(the Bureau of Cyberspace Security and Emerging Technologies, CSET)를 신설하도록 하였고,[48] 해당 부서는 실제로 2021년 1월 신설되었다.

둘째, 국제적 협력의 틀을 확대하는 것은 한편으로 사이버 적대세력에 대항하여 싸울 수 있는 우군을 강화하는 면이 있을 뿐만 아니라 적대세력이 활동할 수 있는 공간을 축소시키는 효과를 가질 수 있다. 미국 정부는 미국의 동맹국, 파트너와 협력관계를 통하여 사이버 적대세력이 동맹국이나 파트너의 사이버공간을 사용하여 사이버공격이나 불법행위를 하지 못하도록 할 경우 그만큼 사이버 적대세력의 활동공간을 제한하는 효과를 가질 것으로 보고 있다. 사이버솔라리움보고서는 동맹, 파트너와 협력관계를 강화함으로써 동맹국의 네트워크에 접근하여 사이버 적대세력의 공격의 책임의 증거를 찾고, 이를 차단할 수 있는 작전을 수행할 수 있다고 제안하고 있다. 보고서는 국방부, 국무부 등 관련부서가 동맹국들과 협력을 통해서 '선제적 방어'전략을 수행하도록 해야 한다고 제안하였다. 특히 미국의 사이버군이 동맹국과 파트너국들의 네트워크에서 '위협사냥'(threat hunting), '적대자 추적'(pursue adversaries)등 '선제적 사냥'(hunt forward) 활동을 할 수 있도록 해야 한다고 하였다.[49]

47) Cyberspace Solarium Commission Report, p. 46.
48) Cyberspace Solarium Commission Report, p. 47.
49) Cyberspace Solarium Commission Report, p. 116.

Ⅴ. 결론

본 논문에서는 지난 50여년에 이르는 기간 동안 미국의 사이버 안보정책과 전략이 발전해오는 과정을 관찰하고 그 내용을 거시적 관점에서 조망함으로써 정책의 등장과 발전과정, 정책의 내용을 중심으로 이해하고자 하였다. 과거 미국의 사이버 안보전략의 발전과정은 사실 미국 정부가 주도적으로 자신의 구상에 의해서 이룩하기보다는 미국에 집중적으로 가해지는 사이버공격에 대응하는 과정에서 이루어졌다. 미국 정부는 그러한 대응적(reactive) 정책이 결국 만족할 만한 사이버 안보를 가져오지 못했다는 인식하에 좀더 적극적, 선제적으로 사이버 안보정책을 마련하고자 사이버솔라리움보고서를 마련하게 되었다.

앞서 지적했듯이 솔라리움보고서에는 행정적 문서제출권, 위협사냥 등 현실을 앞서가는 부분이 있다. 그러나 그 역시 과거 미국의 사이버 안보 정책과 전략이 발전하는 과정을 돌이켜보면 멀지 않은 장래에 현실이 될 수도 있다. 그 이유는 미국에 가해지는 사이버 위협과 공격이 항상 미국 정부의 준비상태를 넘어서는 것이었기 때문에 조만간 미국인들이 놀라는 사이버공격이 가해지고 그러한 공격이 초래하는 미국 사회에 대한 충격이, 보고서에서 제시된, 현재의 상태로 볼 때 약간 앞서가는 내용들이 현실로 이루어지는 것을 허용할 수도 있기 때문이다. 2014년 소니픽쳐스에 대한 해킹이 백악관의 정부와 민간의 정보공유에 대하여 더 허용적인 태도를 가지도록 했던 것이 유사한 사례이다.

마지막으로 이러한 미국의 사이버 안보를 위한 정책과 전략을 관찰한 결과 그러한 미국의 정책이 한국에 가지는 의미는 다음과

같다. 사이버 안보의 분야에서 미국은 다른 분야에서 보다 더 다른 국가들에 앞서 있다. 그것은 전 세계의 모든 잠재적, 현실적 사이버 위협, 공격이 압도적으로 미국에 집중되어 있고 미국은 수십 년 동안 그러한 위협과 공격에 대응해왔기 때문이다. 그러한 경험을 통하여 미국은 미국의 안보를 위하여 사이버 위협과 공격을 선제적으로 방어해야 한다는 판단에 이르게 되었고, 그것을 위하여 사이버 억지, 선제적 방어라는 전략적 개념들을 만들게 되었다. 이러한 점은 한국이 미국의 사이버정책, 전략을 관찰하고 참조해야 한다는 것을 의미한다.

더하여, 사이버 안보를 위한 미국의 전략은 이제 미국의 동맹국과 파트너국가들과 함께 연합하여 사이버 위협, 공격에 대응하겠다는 방향으로 나가고 있다. 이는 미국이 동맹국인 한국에게 높은 수준의 사이버 안보협력을 제안할 가능성이 있다고 판단할 수 있는 근거가 된다. 한국 정부는 미국의 높은 수준의 사이버 안보협력에 대하여 어떻게 대응할지 미리 생각해두는 것이 필요하다고 본다.

투고일: 2022년 03월 10일
심사일: 2022년 03월 11일
게재확정일: 2022년 04월 18일

참고문헌

국문논문

김근혜. 2019. “트럼프 행정부의 주요기반시설 사이버보안 정책분석에 관한 연구.”『정보보호학회논문지』29권 4호, 907-918.

박상돈. 2017. “미국 사이버 안보 정보공유법(CISA)의 규범적 의의.”『융합보안논문지』17권 1호, 45-52.

신소현. 2020. “사이버억지와 미국의 선제적 방어전략의 국제법적 검토.”『경희법학』, 55권 2호, 55-84.

안정민. 2018. “미국 사이버 안보 정보공유법(Cybersecurity Information Sharing Act)에 대한 소고.”『법학연구』28권 4호, 259-282.

양천수·지유미. 2018. “미국 사이버보안법의 최근동향: 사이버보안 정보공유법을 중심으로 하여.”『법제연구』54호, 155-192.

조화순·권웅. 2017. “한국과 미국의 사이버 안보 거버넌스: 사이버 위협의 안보화 관점에서의 비교.”『정보사회와 미디어』18집 2호, 97-120.

홍순좌. 2019. “미국의 사이버보안 역량 강화를 위한 연방법률 발전 현황 분석.”『정보보호학회지』29권 3호, 51-65.

영문자료

Cybersecurity Act of 2015, P.L. No. 114-113.

Cybersecurity Information Sharing Act, 15 U.S.C. 12

Cyberspace Solarium Commission Report, March 2020.

Executive Order 13228

Executive Order 13636

Executive Order 13800

Fidler, David P. 2015. Sidetracked Obama’s Cybersecurity Legacy, *World Politics Review*,

https://www.worldpoliticsreview.com/articles/17468/sidetracked-obama-s-cybersecurity-legacy (검색일: 2021.12.28)

Fouad, Noran Shafik. 2019. The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016), The 18th European Conference on Cyber Warfare and Security (ECCWS 2019). https://www.researchgate.net/publication/334291099_The_Peculiarities_of_Securitising_Cyberspace_A_Multi-Actor_Analysis_of_the_Construction_of_Cyber_Threats_in_the_US_2003-2016, (검색일: 2021.12.28)

Harknett, Richard J. & Stever, James A. 2011. The New Policy World of Cybersecurity, *American Society for Public Administration*, 71. No. 3.

Homeland Security Act, P.L. 107-296

John S. McCain National Defense Authorization Act for Fiscal Year 2019, P.L. 115-232

Johnson, Joseph. Annual number of cyber incidents according to U.S. federal agencies 2006-2018, Statistam Jun 11, 2021. https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/ (검색일: 2021.12.28)

Mabee, Bryan. 2007. Re-imagining the Borders of US Security after 9/11: Securitization, Risk and the Creation of the Department of Homeland Security, *Globalizations.* 4. No. 3.

Marks, Joseph. The government's big idea to bolster the nation's collective cyber defense isn't attracting private-sector participants, https://www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/ (검색일: 2021.12.28)

National Information Infrastructure Protection Act, P.L. 104-294

Mike Gallagher(Congressman) website,

https://gallagher.house.gov/media/press-releases/solarium-co-chairs-welcome-26-recommendations-2021-national-defense, (검색일: 2021.12.26)
Presidential Decision Directive/NSC-63
Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, February 12, 2013
Purplesec, 2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends, https://purplesec.us/resources/cyber-security-statistics/ (검색일: 2021.12.28)
Risen, James & Lichtblau, Eric. 2005. Bush Lets U.S. Spy on Callers Without Courts, The New York Times, (Dec. 16).
Robinson, Joe. 2020. Cyberwarfare statistics: A decade of geopolitical attacks, Privacy Affairs https://www.privacyaffairs.com/geopolitical-attacks/ (검색일: 2021.12.28)
Sanger, David E. 2018. Trump Loosens Secretive Restraints on Ordering Cyberattacks. The New York Times (September 20).
The White House, The National Strategy To Secure Cyberspace, February 2003.
The White House, Cyberspace Policy Review, May 2009.
The White House, National Cyber Strategy of the United States of America, September 2018.
Wolff, Josephine. 2018. Trump's Reckless Cybersecurity Strategy, The New York Times (October 2).
U.S. Department of Homeland Security Cybersecurity Strategy, May 15, 2018.

The Development of the US Cybersecurity Strategy: Historical Overview and Cyberspace Solarium Commission Report

Jinsuk Byun (Sookmyung Women's University)

The US has pursued cybersecurity policy and strategies responding to cyber threats and attacks since its computer information security policy in the 1980s. The US efforts brought 'Cyberspace Solarium Commission Report' in March 2020. The Commission proposed 'layered cyber deterrence' as the US cybersecurity strategy. The strategy proposes to strengthens US domestic network for resilience to cyber threats and attacks and to impose costs on potential cyber adversaries along with international allies and partners so that they give up illegal activities. The features of the US cybersecurity strategy are: first, unlike its military security strategy, the US cybersecurity strategy is based on the cooperation with private sector; second, the US pursues 'forward defend' strategy unlike its defensive prior cybersecurity strategy; third, the US pursues to build international network of cybersecurity with which it can disrupt and neutralize cyber adversary.

Keywords: Cybersecurity, forward defend, securitization of cybersecurity, layered cyber deterrence, Cybersecurity Information Sharing Act, Cyberspace Solarium Commission