국제·지역연구 25권 4호 2016 겨울 pp. 61-96

미 오바마 행정부의 사이버안보 정책과 쟁점

신성호 | 서울대학교 국제대학원 교수

미국은 사이버 공간의 가장 큰 기술적 리더이자, 수혜자이며, 또한 각종 사이버 공격의 가장 큰 대상이기도 하다. 미국은 정보의 자유로운 소통과 접근, 개인의 의사표현과 정보 습득 권한 보장, 열린 사이버 공간을 통한 개인과 민간, 국가 이익의 증진 등을 목표로 사이버범죄로부터 이들 가치와 원칙을 지키기 위한 국내정책, 국제협력, 국제규범 창출에 노력하고 있다. 미국 정부가 정의하는 사이버안보 정책은 "사이버 공간과 그 내부의 운영에 대한 보안에 관계된 모든 기준과 정책, 전략을 포괄하며, 지구적 정보통신 인프라의 보안과 안정에 관여된 컴퓨터 네트워크 운영, 정보 보안, 법 집행, 외교, 군사, 첩보 활동 등을 포함하는 모든 범위의 위협축소, 취약성 감소, 억제, 국제 교류, 사고대응, 복원력, 복구 정책과 일체의 활동을 포괄한다." 그러나 미국의 사이버안보 정책은 사이버 공간이 가지는 기술적 특성으로 인해 기존의 여타 안보정책과 다른 많은 도전과 과제를 제시한다. 한편 미국은 사이버 공간과 인터넷 상의 표현의 자유, 개방, 신뢰의 기본원칙에 바탕한 국제규범과 통치제도의 창출을 위해 지역협력과 지구적 차원의 거버넌스 형성에 노력을 경주하고 있다. 그러나 미국의 노력은 이에 대한 다른 이해관계와 접근을 추구하는 중국이나 러시아와의 갈등을 야기하기도 한다. 그럼에도 여전히 사이버안보 관련 정책과 제도, 기술개발, 국제규범 설립 등에서 선도적 역할을 추구하는 미국의 사이버안보 전략은 향후 한국을 비롯한 각국의 사이버안보 전략은 물론 국제 사이버 질서 확립에 많은 시사점을 가질 것이다.

주제어: 오바마 행정부, 사이버안보, 미국, 미중, 글로벌 거버넌스

I. 서론

2013년 미국은 사이버 위협을 테러 위협보다 더 심각한 최고의 국가 안보 위협으로 지명한다. 2016년 초 박빙의 미국 대선이 끝난 후 오바마 대통령은 러시아가 사이버 공작을 통해 자국에 우호적인 특정 후보를 지지한 정황에 대한 미 정보당국의 분석을 제시하며 이에 대한 전면적인 조사를 지시하고, 미국 의회도 초당파적인 별도의 청문회를 열 것을 제안한다. 선거기간 내내 푸틴 대통령에 대한 친밀감을 과시하며 대통령에 당선된 트럼프 후보는 이에 대해 강력 반발하며 자신이 가장 긴밀하게 협의해야 할 중앙정보국을 공개적으로 비난하는 초유의 사태가 발생한다. 바야흐로 사이버 공간의 활동이 초강대국 미국의 안보와 대통령 선거에 실질적인 영향을 미치는 가능성이 제기되고 있다. 지난 반세기 동안 진행된 정보통신 산업의 엄청난 변화와 발전은 정보통신기술이 오늘날 현대사회 일상생활의 거의 모든 부분에 걸쳐 영향을 미치며 통합되는 방향으로 전개되었다. 문제는 정보통신기기들이 기본적으로 상호의존성이 강하고 따라서 어느 한부분의 문제가 여타 수많은 연결된 부분에 영향을 미칠 수 있다는 점이다.

미국 정부는 사이버공간을 “인터넷, 텔레커뮤니케이션 네트워크, 컴퓨터 시스템, 그리고 주요 연관 산업들에 설치되어 있는 프로세서와 통제장치 등을 포함하는 정보통신 인프라의 상호의존적인 네트워크”로 정의한다. 그러나 일반적으로는 “사람들 사이의 정보와 교류가 행해지는 가상의 환경”으로 이해되기도 한다. 정보통신기술 개발과 발전, 그리고 그 사용에 있어서 선도적 역할을 해온 미국은 그 누구보다 사이버공간의 취약성과 이로 인해 야기될 수 있는 위험에 대해 민감하다. 지난 수년간 미국의 전문가들과 정책결정자들은 정보통신체계에 대한 사이버공격의 위험을 그 어느 때보다 심각하게 인식하고 이를 보호할 방법에 대해 고민해 왔다. 많은 전문가들이 사이버공격의 빈도와 심각성이 앞으로 더욱 증가할 것으로 예상한다.

그렇다면 21세기의 정보통신기술의 가장 큰 선구자이자, 수혜자이며, 동시

에 가장 큰 공격이 대상이 되고 있는 미국의 사이버 안보 정책과 전략은 무엇인가? 또한 국경을 초월하여 연결되는 정보통신기술의 속성상 미국의 사이버 안보 전략은 필연적으로 국제적 차원의 대응과 새로운 규범 및 통제 체제 수립을 위한 노력으로 연결될 수밖에 없다. 이러한 미국의 국제적 노력은 중국을 위시한 다른 강대국들의 사이버 안보에 대한 이해관계와 맞물려 어떻게 조화 혹은 충돌 될 것인가? 미국의 사이버 안보 전략을 살펴보는 것은 이 분야의 중요성과 영향이 날로 점증하는 한국을 비롯한 여타 정보통신 선진국들에게도 중요한 정책적 함의를 가질 것이다. 최근에 발표된 기존의 연구들은 사이버 안보의 일반 개념이나 국제정치적 쟁점을 소개하거나(장노순·한인택, 2013; 민병원, 2015), 미국과 상대국의 정책을 비교(장노순, 2013; 배병환·송은지, 2014), 미국 사이버 안보 정책의 전략적 측면이나 기간산업의 보안 등(김형우·이광호, 2015; 장노순·김소정, 2016) 제한된 분야에 초점을 맞추어 미국 정부의 사이버 안보 정책과 전략에 관한 포괄적 연구는 아직 수행되지 않았다. 본 논문은 지금 미국이 당면한 사이버안보 위협이 무엇이고, 특히 오바마 행정부를 중심으로 진행된 미국 내의 사이버안보 정책의 전개와 전략, 그리고 국제적 협력 노력을 양자와 다자적 협력의 틀에서 개관, 분석코자 한다. 그리고 그것이 장차 사이버 안보전략 수립에서 가지는 문제와 정책적 함의를 알아볼 것이다.

II. 국내 정책과 제도

1. 사이버안보 위협과 정의

2008년 중동의 한 미군기지 주차장에 버려진 이동식 USB 드라이브가 이를 무심코 사용한 부대 내 한 개인 컴퓨터를 통해 국방부의 중동사령부에 접속하여 악성 코드를 심고 군 전체의 기밀 정보 유출 및 보안 시스템이 교란된 사고가 발생한다. 이를 발견한 미군 당국은 14개월에 걸쳐 Buckhot

Yankee로 명명된 대규모 작전을 통해 agent.btz라는 바이러스를 제거한다. 미군 역사상 최악의 사이버 공격 피해로 기록된 이 사건이후 미국 정부는 국방부 산하에 사이버사령부를 설치하고 21세기의 새로운 전장으로 떠오른 사이버 공간에서의 위협과 공격에 대비한다(Knowlton, 2010). 사이버공격은 국가 간 정보 수집이나 무기체계에 대한 교란 시도만을 의미하지 않는다. 각종 보도에 따르면 오늘날 개인이나 단체가 영리를 목적으로 민간 산업의 정보나 개인 정보를 훔쳐 이를 범죄에 사용하는 경우가 매일 수천, 수만 건씩 일어나는 것으로 알려졌다. 2008년 미국의 산업계에 의하면 해킹에 의해 도난당한 데이터로 인한 지적재산권의 손실액이 1조 달러에 육박한다고 보고되었다(McAfee, 2009). 2013년의 경우 미국 정부에 의하면 최소 3000개의 미국 기업이 해킹을 당함과 동시에, 4천만 명의 개인 정보가 도난당한 것으로 보도 되었다. 2014년 한 해 동안 사이버 범죄가 전 세계 경제에 미친 손해는 4천억 불에 달하며 앞으로 더욱 증가할 것으로 분석된다(CSIS, 2014). 한편 2014년 10월 김정은 정권을 비꼰 영화를 제작한 소니 영화사에 대한 해킹이 발생하여 내부의 기밀문서가 유출되고 일부 컴퓨터 시스템이 파괴되는 사건이 발생한다. 당시 오바마 대통령이 직접 나서서 이것이 북한 정부기관에 의한 공작이었음을 밝히고 강력한 경고와 함께 북한 기업에 대한 제재 및 북한 컴퓨터에 대한 보복 공격을 취하였다(Peterson, 2014). 2015년에는 중국 정부기관으로 보이는 조직에 의해 미국 정부 인사관리청의 컴퓨터가 해킹을 당하여 2천1백만 명이 넘는 정부업무 관련 인사들의 정보가 유출된 사건에 발생하였다. 그 규모와 내용에서 미국 정부사상 최악의 정보유출 사례로 알려진 이 사건 이후 인사관리청의 책임자가 사임하고 미국정부는 이후 수개월에 걸쳐 인사관리 파일과 시스템을 보완하는 작업을 벌이는 한편 중국 정부에 대한 대응방안과 수위를 놓고 심각한 딜레마에 봉착한 것으로 알려졌다(Davis, 2015).

사이버안보 위협은 2016년 미국 대선에서도 뜨거운 문제로 부상하였다. 미국과 러시아가 러시아의 크리미아 및 우크라이나 침공, 시리아 내전을 놓고 신냉전에 준하는 갈등을 겪고 있는 상황에서 대선 경합중인 민주당 지도부 인사의 민감한 이메일이 해킹되어 노출된 사건이 발생한 것이다. 민주당

경선이 한창이던 6월에 경선을 관리하는 민주당전국위원회와 민주당 지도부, 힐러리 대선 캠프 측 인사 100여 명의 이메일이 러시아 정부와 연관된 것으로 추정되는 해커집단에 의해 유출되어 공개되었다. 이 과정에서 공정해야 할 민주당 지도부가 힐러리 측에 유리한 경선 구도를 만들기 위해 노력하였다는 점을 암시하는 메일의 내용이 알려지면서 선거가 혼선에 빠지게 되었다. 특히 러시아 대통령 푸틴에 대해 평소 친근감을 표시한 공화당 트럼프 후보가 공개적으로 러시아 당국에 힐러리 후보의 비리 정보를 캐낼 것을 주문하면서 러시아가 자신들에게 우호적인 후보를 돕기 위해 각종 사이버공작을 펼치고 있다는 강한 의구심이 제기되었다(Lichtblau and Schmitt, 2016). 실제로 미국 정보기관은 러시아의 이러한 공작 가능성에 대한 사전 정보를 입수하여 심각한 우려를 이미 하고 있었으며(Perez, 2016), 사건 이후 러시아에 대해 어떠한 공식적인 대응을 할지에 대해 많은 고민을 하고 있는 것으로 보도 되었다(Harris and Youssef, 2016). 일부에서는 러시아 정부가 대통령 선거 투표과정에 개입하여 선거결과를 조작할 가능성까지 제기되었다. 투표 방식이 각 주마다 다른 상황에서 일부 경합주의 경우 종이 용지를 사용하지 않고 컴퓨터 화면 터치 방식만을 사용하는 상황에서 해커가 이를 조작할 경우 실제 어떤 투표가 이루어 졌는지 확인할 방법이 없다는 것이다. 사이버 안보 위협이 미국 대통령 선거 결과를 좌우하는 초유의 상황이 거론된 것이다. 실제 이후 치러진 초박빙의 대선 투표에서 트럼프 후보가 예상을 깨고 근소한 차로 위스콘신, 펜실바이나 등 주요 경합지역의 승리를 토대로 대통령에 당선되자, 힐러리 후보의 대선패배의 주요 요인 중 하나로 러시아의 사이버 공작이 제기되기도 하였다.

그렇다면 미국이 보는 사이버 안보의 정의는 무엇이며, 어떻게 접근되고 있는가? 미국이 이를 어떻게 정의하고 규정하는 지를 알아보는 것은 사이버 안보 전략의 주요한 단초를 제공한다. 일반적으로 사이버 안보란 다양한 “사이버 공격으로부터 정보통신기술(ICT: information communication technology) 체계와 그 콘텐츠를 보호하는 것”을 의미한다. 이 경우 사이버 공격이란 “절취, 교란, 손상, 혹은 다른 불법적 의도에 의해 정보통신기술 체계에 인가되지 않은 개인이 접속을 하려는 의도적 행위”로 정의된다. 그러나 여전히 사

이버 안보의 개념은 모호하고 정확한 정의가 어렵다. 그러나 일반적으로 사이버 안보는 다음의 세 가지 중 하나를 의미한다. 첫째, 컴퓨터와 그 네트워크, 혹은 연관된 하드웨어와 장치 소프트웨어 및 그 장치들이 보유하거나 교신하는 소프트웨어, 데이터와 기타 사이버 공간의 요소들에 대한 공격, 교란, 혹은 여타 위협으로부터 보호하려는 일종의 행위와 기타 수단; 둘째, 앞서 언급된 위협으로부터 보호되고 있는 상황이나 그 수준; 셋째, 보호 활동이나 그 수준을 실행하고 개선하기 위한 광의의 노력으로 정의된다(Fischer, 2016: 1-2). 한편 사이버 안보는 종종 정보보안이나 개인의 사생활 보호 등과 혼용되기도 하지만 엄밀하게는 다른 개념이다.

한편, 미국이 규정하는 사이버안보 위협은 크게 다섯 부류로 나뉜다. 첫째, 절취나 갈취와 같은 범죄를 통해 돈을 벌려는 범법자들, 둘째, 정부나 민간단체의 기밀정보나 정보자산을 훔치는 스파이들, 셋째, 특정국가의 전략적 목적을 지원하기 위해 사이버 공격능력을 배양하고 감행하는 국가소속의 전투원들, 넷째, 비금전적인 이유로 사이버공격을 수행하는 해커 활동가들, 다섯째, 비국가, 혹은 국가 지원의 형태로 사이버공격을 자행하는 테러분자들이다(Fischer, 2016: 2). 이러한 사이버위협이 끼칠 수 있는 대표적 피해는 사이버절취 혹은 사이버간첩활동을 통해 피해자가 종종 알지도 못하는 사이에 금전적, 자산적, 혹은 개인정보가 유용되고 탈취당하는 경우이다. 서비스의 거부(Denial-of-service) 공격은 정당한 사용자의 시스템 접근을 느리게 하거나 방해 하는 경우이다. 산업통제시스템에 대한 공격은 발전기나 펌프, 중앙가속기 등의 장비가 파손되거나 교란되는 피해를 입은 경우이다. 실제로 대부분의 사이버 공격은 제한적인 범위의 영향을 가지지만, 주요한 인프라의 일부에 대한 효과적인 공격은 국가 안보나 국가 경제 전체와 개인의 생명과 안전에 심각한 피해를 가져 올 수도 있다.

2. 사이버안보 정책 제도와 조직

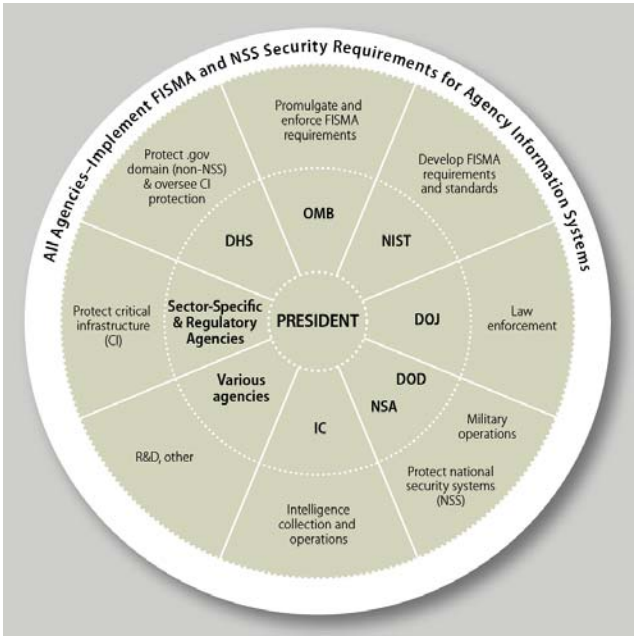
미국은 2001년 9·11 테러 이후 사이버테러의 가능성을 심각하게 인지하

고 이에 대한 국가정책을 추진하기 시작한다. 신설된 국토안보부(Department of Homeland Security)의 가장 중요한 임무중 하나로 사이버공격에 대비한 포괄적인 정책을 수립하는 것이 지정되어 2009년 “사이버 안보전략에 관한 국가사이버안보 종합계획(CNCI: Comprehensive National Cybersecurity Initiative)”을 발표한다(Henning and Rollins, 2009). 동시에 오바마 대통령은 취임 이후 사이버안보를 중요한 정부과제로 상정하고 “사이버공간 정책검토(Cyberspace Policy Review)”를 발표하여 단기, 중기 실행계획을 제시한다. 이 문서에 의하면 미국 정부가 정의하는 사이버안보 정책은 “사이버 공간과 그 내부의 운영에 대한 보안에 관계된 모든 기준과 정책, 전략을 포괄하며, 지구적 정보통신 인프라의 보안과 안정에 관여된 컴퓨터 네트워크 운영, 정보 보안, 법 집행, 외교, 군사, 첩보 활동 등을 포함하는 모든 범위의 위협축소, 취약성 감소, 억제, 국제 교류, 사고대응, 복원력, 복구 정책과 일체의 활동을 포괄한다(The White House, 2009: 2). 이 보고서에 따르면 미국은 사이버공간에 대한 심각한 위협과 미국이 가지는 취약성에 대비하기 위해 포괄적이고 장기적인 사이버안보 정책을 수립하여 시행해 나갈 것이며, 이를 위해 전 연방정부의 모든 부서가 이에 관한 문제의식을 공유하고 각자의 분야에서 대책을 수립하고 이를 수행할 조직과 지침, 예산을 확보할 것을 지시하고 있다. 또한 이러한 연방정부의 노력과 정책은 각 지방 정부와 민간 분야와의 협력 없이는 그 목적을 달성하기가 불가능하며, 따라서 정부와 민간, 중앙과 지방을 효과적으로 연결하는 제도와 조직, 법령 등이 필요함을 적시하고 있다.

오바마 행정부의 첫 사이버안보 정책 지침서인 2009년 “사이버공간 정책보고서”의 내용을 구체적으로 살펴보면 먼저 사이버안보의 중요성을 인식하여 연방정부의 최고 책임자인 대통령과 백악관이 직접 리더십 발휘할 것을 제시한다. 그리하여 대통령은 “사이버안보 정책관(Cybersecurity Policy Official)”을 별도로 임명하여 국가의 사이버안보 정책 및 활동을 총괄하고 조정하는 역할을 담당토록 할 것이 제시되었다. 사이버안보 정책관은 연방정부의 사이버 위기대응 능력을 강화하고 사이버안보 관련 기관들의 역할을 검토하여 변동사항을 제시하는 역할을 하며 대통령에게 국가사이버안보종합계

획(CNCI)의 평가 자료와 앞으로의 리더십 역할을 포함한 새로운 안보 전략을 보고한다. 또한 백악관 내의 국가안보회의(NSC)와 국가경제회의(NEC)와 동시에 소통하면서 행정부 내 부처 간 조정 프로세스를 이용하여 각 중앙정부 부처와 협업하고 사이버안보 정책의 조화를 유도할 것이 제시되었다(The White House, 2009: 7-9). 두 번째로, 백악관은 사이버안보 정책관을 통해 중앙부처의 사이버안보 담당 기관들에게 통일된 정책 지침을 제공하며, 연방정부의 각 기관에게 각자의 역할과 책임을 명확하게 분담한다. 이 과정에서 새로 시행되는 사이버안보 관련법과 정책이 시민의 자유, 개인정보 보호, 공공 안전, 국가 및 경제안보 이해와 조화를 이루도록 충분한 유통성과 다양성을 포용할 것이 요구되었다. 이를 위해 중앙정부는 의회와 긴말한 협력을 통해 적절한 법과 정책을 수립토록 노력해야 한다(The White House, 2009: 10). 세 번째로, 사이버안보에 대한 중앙 정부의 리더십과 책임을 강화하기 위한 방안으로 중앙정부의 각 부처와 기관이 사이버안보의 정책을 준수하도록 책임을 이양하여 부처별로 적절한 사이버안보 절차와 규정을 행하도록 제도화 한다. 네 번째로, 사이버안보 정책이 중앙정부 차원 뿐 아니라 각 미 연방의 50개 주와 각 지방, 그리고 소지역 단위의 행정기관이 자체적인 사이버안보 리더십과 역할을 개발토록 할 것이 제시되었다. 이를 위해 주, 지방, 소지역의 자치정부는 각각 사이버안보를 담당하는 리더를 지정하여 Chief Information Officers(CIOs), Chief Information Security Officers(CISOs), State Homeland Security Advisors(HSAs)들 차원에서 자신들의 관할 지역 안의 핵심 기간산업 보호 등에 관한 활발한 사이버 안보 협력을 촉진토록 하였다(The White House, 2009: 11).

또한 2009년 보고서는 디지털 국가로서의 역량 구축을 위해 디지털 안전, 윤리 및 보안에 관한 공공교육 등의 사이버안보에 대한 대중인식제고, 사이버안보 교육체계의 개선, 중앙 정부 내에 사이버안보 지식과 전문성을 갖춘 정보기술 인력양성, 민간부분 기업리더십의 새로운 주요 임무의 하나로 사이버안보 의식 고양 등의 정책과제를 제시한다. 특히, 이 보고서는 사이버안보의 강화를 위해서는 중앙과 지방의 협력뿐 아니라 정부와 민간 부분의 긴밀한 협력을 강조한다. 사이버안보 위협의 원천과 동기, 그리고 대상이 전통안



〈그림 1〉 미국 중앙 정부 사이버안보 담당 주요부서와 역할

보와 달리 국가부분에게만 국한되지 않고 오히려 민간분야의 취약성 및 상대적 역할과 참여가 더욱 중요한 경향을 보이기 때문이다. 따라서 기업의 개인정보보호에 대한 민감성, 기업의 민감 정보 공유 거부 경향 등을 충분히 인식하면서도 기업의 사이버공격 관련 정보공유와 협조가 그 어느 분야보다 중요함을 역설하고 있다(The White House, 2009: 17-19).

오바마 행정부는 2009년 사이버안보 정책 보고서 발표 이후 2013년 이후 주요 기반 시설 안보를 강화하기 위한 행정명령 제13636호(Executive Order 13636)와 대통령 정책지침 제21호(Presidential Policy Directive 21) 발표한다. 행정명령 13636호는 정보시스템 구축과 주요기반시설의 프레임워크 개발의 내용을 다루고 있으며 국토안보부에서 담당하는 정책지침 21은 주요기반시설 안보와 각 중앙 부처 및 기관의 업무를 제시하고 있다. 현재 미국의 중앙정부는 중앙정부의 시스템을 보호하는 사이버안보정책을 주관하며 동시에 각 주정부시스템 보호를 보조하는 역할을 동시에 수행한다. 현행법에 따르면 모든 중앙 정부조직은 자신들의 시스템을 보호할 사이버안보정책의 책

임을 지며, 이들 중 다수가 핵심 기간산업에 대한 특정분야의 책임을 가진다.

앞의 〈그림 1〉은 사이버안보 관련 중앙정부의 주요부서가 가지는 사이버안보 책임과 기능을 요약하여 보여준다. 먼저, 대통령과 백악관은 중앙정부 전체의 사이버정책을 총괄하며, 이 가운데 국립기술표준연구소(NIST: the National Institute of Standards and Technology)는 연방 정보보안 현대화법(FISMA: the Federal Information Security Modernization Act)에 의거하여 연방민간부분의 정보통신기술에 적용될 표준을 개발한다. 백악관의 예산처(OMB: the Office of Management and Budget)에서는 전체 시행을 감독하는 책임을 진다. 국방부의 주요 임무는 군 분야의 정보통신기술에 대한 보안과 사이버 공간에서의 국가 방어를 책임지며, 기밀정보를 관리하는 국가보안청(NSA: the National Security Agency) 을 통해 국가보안체계에 관한 보호책임을 진다. 한편 국가보안청은 첩보기관과의 연계를 통해 이들이 수행하는 사이버안보관련 정보수집과 정보활동에 함께 참여한다. 국토안보부(DHS: the Department of Homeland Security)는 연방정부 민간 시스템을 보호하는 동시에 민간분야의 핵심기간산업 분야를 보호하는 활동을 조정하는 주무부서이다. 또한 동시에 국립사이버안보 통신통합센터(NCCIC: National Cybersecurity and Communications Integration Center)를 통해 민간시스템을 위한 정보공유의 역할을 담당한다. 법무부(DOJ: the Department of Justice)는 관련법의 집행을 담당한다.

최근의 미국 정부의 사이버안보 촉진을 위한 활동으로 첫째, 민관 사이버안보 정보 공유 활성화를 목표로 하는 사이버 네트워크 보호 법안(PCNA: The Protecting Cyber Networks Act)이 2015년 4월 미국 하원을 통과하여 민간부문과의 협력을 촉진하기 위한 정보공유분석 조직(ISAO: Information Sharing and Analysis Organizations)이 설립되었다. 이 조직은 사이버범죄 활동에 대한 정보를 공유하며 산업별 기관들에게 정보 제공 강화. 또한 국토안보부 산하 국가사이버안보통신통합센터(NCCIC)와 ISAO와의 협력 체제를 간소화 하여 정보공유 활성화를 지원한다. 둘째, 연방정부의 사이버 안보 거버넌스 체계를 재정립하기 위해 이-거브 사이버(E-Gov Cyber)을 설립을 위한 예산을 수립한다. 이를 통해 정부 전반에 걸친 사이버안보 프로그램에

대한 감독을 강화하고 연방정부의 핵심 사이버안보 관련자간의 협의를 통해 연방정부의 사이버안보가 보다 높은 수준의 관심과 감독, 관리의 대상이 되도록 하였다. 셋째, 2015년 오바마 행정부는 국가정보국(DNI: the Director of National Intelligence)산하에 사이버위협 정보종합센터(CTIIC: Cyber Threat Intelligence Integration Center)를 설립하여 전체 중앙연방정부 조직을 가로지르는 국가이익에 관한 사이버안보 위협과 사고를 종합적으로 분석하여 각 유관기관에 정보를 제공하는 임무를 부여하고 민관 사이버안보 정보공유를 촉진토록 유도하고 있다(Fisher, 2016: 3-4). 넷째, 2015년 12월에는 사이버 정보공유법(CISA: Cybersecurity Information Sharing Act)을 공식 발효 하여 정부가 사이버안보를 위해 필요한 경우 민간분야가 소유한 방대한 양의 개인 정보를 연방정부 관련기관에 자발적으로 공유토록 권한을 부여하였다. 이는 사이버공격의 소지가 있거나 의심되는 개인의 관련 정보와 활동들을 정부가 미리 요구하지 않더라도 민간 분야가 유관 정부기관에 제공토록 함으로써 민관 정보공유를 활성화 하고 날로 지능화 되는 사이버공격의 추가 피해를 막기 위한 취지에서 시행되었다. 그러나 법안이 최초 발효된 2009년 이후 4년이 넘도록 개인의 프라이버시를 침해를 우려하는 정치권과 시민사회의 반대의견과 개인정보 침해에 대한 책임 소재를 우려하는 기업들의 반발에 의해 법안 통과가 지연되었다. 그러는 사이 사이버공격 기술은 더욱 진화하여 정작 뒤늦게 통과된 법안이 과연 실질적인 효과가 있을지에 대한 의심이 제기되었다. 한편 구글이나 페이스북과 같은 거대 개인정보를 취급하는 민간 분야로부터는 여전히 개인의 사생활 정보 보호에 대한 우려의 지적이 나오고 있다(Sanger and Perlrothoct, 2015).

그 중요성에 더불어 지난 10년간 사이버 안보관련 예산도 꾸준히 증가하였다. 아래의 〈표 1〉은 미국 연방정부의 IT 예산과 그 중에서 사이버안보 예산의 증가와 비중을 정리하여 보여준다. 표에 따르면 2009년까지는 사이버안보예산의 비중이 전체 통신기술 비중의 8퍼센트 남짓에 머물렀으나 오바마 행정부의 2009년 사이버안보 보고서 이후 그 비중이 두 배 남짓 증가하여 최근에는 16~17퍼센트에 이르고 있다. 그런데 이러한 높은 비중은 최근 5년간 예산의 규모가 가장 큰 국방부 IT 예산에서 사이버예산이 22에서 30

〈표 1〉 미국 사이버안보와 IT 예산(십억 불)

회계연도	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
사이버안보	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3	12.7	13.1
전체 IT예산	66.2	68.2	72.8	76.1	80.7	76.0	75.0	73.2	75.6	80.4
전체 IT 예산대비 사이버안보 비중 (%)	8.3	8.7	8.5	8.9	14.9	17.5	19.3	14.1	16.8	16.3

퍼센트를 차지하게 된 것에 기인한다. 실제 국방부를 제외한 여타 연방정부 부서의 사이버안보 관련 예산은 전체 IT 예산의 평균 6~7퍼센트이며, 이는 민간기업의 4~9퍼센트 예산 평균과 비슷한 수치이다(Painter and Jaikaran, 2016). 한편 2017년 예산에는 전체 연방정부 IT 예산 816억 불 가운데 190억 불이 사이버안보 관련 예산으로 책정되어, 그 비중이 22.3퍼센트로 전년도에 비해 가파른 상승을 보이고 있다(Fischer, 2016: 6).

3. 사이버안보와 국가안보

2013년 제임스 클래퍼 국가정보국장은 사이버 위협을 미국이 당면한 최고의 안보 위협으로 정의한다. 이는 2001년 9·11 테러 이후 테러 이외의 안보 위협이 미국에 가장 위험한 안보위협으로 인식된 초유의 사건이었다(Boyd, 2016). 사이버안보는 전통적 안보 개념을 넘어서는 다른 차원의 복합적인 성격을 가지며 미국의 국가안보정책에서 새로운 도전과 접근을 요구한다. 이는 특히 전통적인 안보개념에 바탕을 둔 국방 정책 분야에서 많은 과제를 제시한다. 실제 미국 군은 전군에 15,000여 개의 네트워크, 700여만 대의 컴퓨터 기기, 9만 명의 관리인원을 보유하고 군수, 지휘통제, 정보, 작전 등 모든 분야에서 정보통신기술의 활용도 및 의존도가 가장 높은 조직이다. 따라서 사이버공격의 위협으로부터 이 거대한 조직과 시스템을 보호하는 것 자체가 가장 중요한 임무의 하나로 부상하였다. 미국은 사이버공간을 육, 해, 공의 전통적 물리적 공간에 준하는 새로운 전장으로 인식하고 2009년 이전까지 느

슨한 합동 태스크포스 형태로 유지되던 사이버 대응 조직을 대신하여 독자의 사이버 사령부(US Cyber Command)를 전략사령부(US Strategic Command) 산하에 신설하고 4성 장군을 사령관에 임명하여 그 중요성을 반영하였다 (Jackson, 2009).

신설된 사이버 사령부는 크게 세 가지의 임무가 부여되었다. 첫째는 사이버공간에서의 모든 일상적 방어 체계 구축 및 지원, 관리; 둘째는 전군에 걸친 사이버전 자원 관리로 이를 위한 단일 지휘계통 수립(대통령-장관-전략사령관-사이버사령관-전군 각급부대)하고, 각 군의 사이버 훈련 감독관(육군 사이버 사령부, 해군 제10함대, 제24공군, 해병대 사이버 사령부)를 신설; 셋째, 대내외 협조체제구축으로 FBI, 국토안보부, 법무부의 사이버 안보관련 주요 부처와 사기업 및 민간단체를 아우르는 대내외 협조체제를 구축하는 한편 Defense Info. Systems Agency와 NSA에 실시간 검색 및 경보 시스템을 구축하여 인트라넷과 인터넷의 인터페이스 관리하는 임무를 주로 맡고 있다 (Lynn, 2010). 이 세 가지의 주요임무를 달성하기 위한 구체적 작업으로 먼저 단순 해커와 정보 절도 및 첩보활동, 정부에 대한 심각한 공격의 구분에 따른 사이버 교전 수칙을 수립하기 위해 노력하고 있다. 동시에 동맹국과의 연계를 통한 예방능력 강화 방안, 민간의 주요 방위관련 분야, 특히 군수산업에 대한 사이버 보호망 확대, 사이버전사를 훈육시키기 위한 DARPA내에 사이버 전투훈련장 설립을 통한 실전 대비, 군내 시스템의 신형 하드웨어 및 소프트웨어 개발을 통한 공격자 우위 상쇄, 사이버보안 관련 인력양성을 통해 “ethical hacking”을 통한 취약점 개선 등의 과제에 노력을 기울이고 있다.

미 국방부에 의하면 사이버위협은 재래식 군사위협과 다른 세 가지의 특징적 도전을 제시한다. 먼저 사이버 공격은 재래식 전쟁에서는 일반적으로 방어자가 유리한 경우가 많은 것에 비해 공격자가 비대칭적 우위를 점하는 특징을 보인다. 이는 사이버공격의 특성상 방어자가 공격자체를 인지하지 못하는 공격의 양태 때문이다. 따라서 냉전식의 억제모델을 적용하기도 불가능하다. 대신 끊임없는 대비책 강구 및 강화를 통해 보복이 아닌 예방에 중점을 두는 접근법이 필요하다. 두 번째로 사이버공격은 전통적인 전쟁에 비해

민-군의 구분이 어렵고 오히려 다양한 행위자와 위협의 원천을 통해 기간산업 등의 물리적 파괴뿐 아니라 지적재산권 및 정보 유출 등 네트워크뿐만 아니라 하드웨어와 소프트웨어를 통한 공격이 가능하다는 점이다. 마지막으로 사이버 공격은 그 예측의 어려움으로 인해 이를 대비함에서 유연성과 적응성의 극대화가 필요하다는 점이다. 이러한 특징은 재래식 전쟁 개념에 익숙한 군의 사이버안보 강화노력에 다른 차원의 도전을 제시한다.

미 국방부는 2015년 보다 종합적이고 구체적인 사이버안보 대응 전략을 담은 “국방부 사이버 전략”을 발표한다. 2015 사이버안보 전략은 사이버 영역에서 국방부의 세 가지 임무를 다음과 같이 보다 구체적으로 명시한다. 1) 국방부자체의 네트워크, 시스템과 정보 방어, 2) 심각한 결과를 초래할 수 있는 사이버 공격으로부터 미국의 국토와 국익을 수호, 3) 필요시 사이버 군사작전과 비상사태 대책을 지원하기 위한 통합적인 사이버 역량 제공이다(US Department of Defense, 2015: 4-5).

이를 위해 5대 전략목표가 제시되다. 첫째는 사이버공간에서의 작전수행 준비태세와 역량을 갖춘 군사력의 건설과 유지를 위한 인력 훈련, 자원 유지, 준비태세 및 장비의 첨단화를 위해 향후 5년간 군사 및 인력 충원, 훈련, 장비에 대한 구체적 목표를 설정하고 실행할 것. 둘째는 국방부 정보 네트워크 방어, 데이터 안보, 임무 위험 감소를 위해 지나치게 광범위한 국방부 네트워크 전선에서 단계별로 중요한 네트워크를 식별, 우선순위 설정, 방어를 통해 효과적 임무 수행을 가능토록 할 것이 제시된다. 이를 위해 국방부의 네트워크와 데이터, 특히 작전운영과 비상계획 수립에 필요한 핵심 기반시설이 공격당한 경우 악화되고 교란된 환경에서도 운영이 가능하도록 계획과 훈련이 필요하다. 특히 합동정보환경(JIE)에서 더 뛰어난 방어능력을 갖춘 네트워크 구조를 구축하고 활용하는 등 사이버 방어 능력을 강화함으로써 기술과 혁신을 선도하기 위한 기준을 높일 요구된다. 더불어 민간부문과 협력하여 방위산업 거래 데이터를 보호하고 다른 유관 기관과 협력하여 사이버 공격과 정탐에 대한 대비토록 하고 있다. 셋째는 심각한 결과를 초래할 수 있는 파괴적 사이버공격으로부터 미국 국토와 핵심 이익을 보호하기 위한 준비태세 마련이다. 그 구체적 임무로 정부, 민간, 동맹국과의 협력을 통해 공격을 미연

에 격퇴, 방지, 미국의 이익에 영향이 발생하기에 앞서 정교한 악의적 공격을 무력화하기 위한 정보, 경보, 작전 능력 개발, 세계 네트워크와 시스템, 적의 역량, 밀거래 시장에 대한 자세하고, 예측 가능하며, 행동 가능한 정보 수집이 요구된다. 넷째, 분쟁 격화를 통제하고 모든 단계에서 분쟁 환경 형성을 주도할 수 있는 가용한 사이버 작전의 수립과 관리이다. 여기에는 사이버 공격의 긴장 고조 혹은 분명한 적대행위 발생 시 대통령에게 제시할 수 있는 다양한 위기관리 계획을 제시하고 사이버 작전을 통한 적군의 지휘통제 네트워크 및 군사 역량을 교란토록 해야 한다. 또한 각 군의 긴밀한 공조 하에 연계되어 실제 전장에서의 작전과 동조화할 수 있는 사이버 공간에서의 작전 수립을 통해 행동의 통일성을 부여할 것과 사이버 가상 적군을 활용한 훈련으로 실제 적에 대한 폭넓은 작전 수행 역량 육성이 제시된다. 마지막으로 다섯째, 공통의 위협 저지, 국제 안보 및 안정 증진을 위한 건실한 동맹과 동반자 관계의 수립과 유지이다. 국방부 사이버 전략 목표의 하나가 동맹국과의 긴밀한 협조인데 사이버 역량에 대한 높은 수요와 상대적 공급 부족으로 인해 반드시 미국의 핵심 이익이 걸린 분야에 대해서는 공조역량 강화가 필요하다는 것이다. 이를 위해 향후 5년간 중동, 아태 지역 및 나토 동맹국 지역에서 공조 능력 강화를 추진하고 이 과정에서 지속적으로 국제 환경을 평가하고 새로운 과제 및 기회에 대응하기 위한 혁신적 동반자 관계를 구축할 것이 제시된다(US Department of Defense, 2015: 13-15).

4. 향후 주요과제와 전망

현재 미국 정부가 중점을 두고 있는 사이버 안보 과제는 사이버공격에 기인한 재앙적 상황이나 간첩피해 방지, 치명적인 사이버공격의 충격 축소, 주요 적용 대상 분야 내 혹은 분야 간 공조 향상, 중앙정부부처의 역할과 책임 소재 명료화, 사이버범죄 격퇴 등이다. 그러나 이러한 당면과제와 더불어 설계(design), 보상(incentives), 공감대(consensus), 환경(environment)의 네 가지 요소를 의미하는 DICE 와 관련된 장기적 도전에 대한 대비 또한 요구

된다. 먼저 전문가들에 의하면 효과적인 사이버보안은 정보통신기술의 설계 단계부터 하나의 기본 구성으로 구상되어야 한다. 그러나 지금까지 정보통신 기술의 개발은 보안보다는 경제적인 목적을 위한 상품성에 주로 초점이 맞추어져 왔다. 더욱이 설사 보안을 설계단계에서 부터 구상하고 싶어도 미래에 필요한 보안의 수요를 미리 알기도 어렵다. 두 번째, 사이버안보를 진작하기 위한 경제적 보상의 구조자체가 왜곡되거나 역작용을 하는 경우가 많다는 것이다. 사이버범죄의 경우는 비용도 적고, 수익성이 높으며, 상대적으로 안전한 반면 사이버보안은 비싸고, 본질상 불완전하며, 투자의 보상이 불투명한 것이 현실이다. 세 번째, 사이버안보, 혹은 보안문제에 관해 각각의 이익상관자마다 그 의미나, 시행방법, 위험에 대해 다르게 해석되거나 공감대 형성이 어렵다는 점이다. 이러한 문제는 다른 분야나 기관들 사이뿐 아니라 같은 조직 내에서도 종종 나타난다. 안보에 관한 전통적 접근이 엄청난 연결망을 가진 사이버공간의 환경에서는 적용하기 어려우면서도 그 대안에 대해서도 여전히 증명된 것이 없는 현실이다. 마지막으로 사이버 공간은 그 크기와 내용에 있어서 인간역사상 가장 빠르게 진화하는 기술공간이다. 소셜 미디어, 모바일 컴퓨팅, 빅데이터, 클라우드 컴퓨팅, 인터넷 사물 등의 새로이 등장하는 내용과 응용기술 들은 진화하는 위험 환경을 더욱 복잡하게 만든다. 하지만 동시에 클라우드 컴퓨팅이나 빅데이터 분석에 의한 규모의 경제와 같은 경우는 사이버안보에 새로운 기회로 작용할 수도 있다. 따라서 이제 그 중요성이 부각되기 시작한 사이버안보 정책의 장기적 성공을 위해서는 이상의 도전과 기회를 적극적으로 인식하고 대비해 나가려는 접근이 필요하다(Fischer, 2016: 9).

III. 사이버안보와 국제협력

1. 국제전략: 목표와 원칙, 행동강령

국제협력은 다양한 국내 정책과 더불어 미국 사이버안보 전략의 다른 중요한 축을 이룬다. 무한대로 열리고 연결된 사이버공간의 특성상 국내와 국외의 구분이 어렵거나 존재하지 않는 것이다. 2009년 보고서에서 미국은 국제 사이버안보 정책을 위한 미국의 역할을 확립하고 국제 파트너십 관련 역량을 강화할 것을 제시한다. 그러나 효율적인 국제사회와의 협력이 중요하면서도 어려운 이유는 먼저 사이버범죄나 위협은 국경을 초월하는 반면 이에 대응하는 사이버 범죄의 수사 및 기소, 데이터 보존, 개인 정보 보호에 관한 법률이 국가마다 다르기 때문에 안전한 디지털 환경을 유지하기 어려운 점이 지적된다. 따라서 미국은 다른 국가와 협력하여 사이버 범죄나 위협에 대한 관할권 허용 기준, 국가의 책임, 무력 사용에 대한 기준에 관하여 상호 협력하며 공동 대응을 할 수 있는 국제환경 조성에 노력할 것이 제시되었다. 이를 위해 미국과 동맹국들은 공통의 정책 목표를 설정하고 국제전기통신연합(ITU: International Telecommunication Union), 국제표준화기구(ISO: International Organization for Standardization)와 같이 현존하는 사이버안보 관련 국제기구 및 지역 포럼에서의 중복되는 역할을 조정하며 포괄적 국제협력체계 구축을 위한 노력을 해 나갈 것을 제안한다(The White House, 2009).

2011년 오바마 행정부는 “사이버공간의 국제전략(International Strategy for Cyberspace)”이라는 보고서를 펴내고 국제사이버안보 정책을 위한 미국의 역할을 확립하고 국제파트너십 관련 역량 강화를 위한 보다 구체적인 국제협력의 기본 원칙과 전략을 제시한다(The White House, 2011). 미국이 제시하는 기본원칙은 크게 3가지이다. 첫째는 미국이 추구하는 근본적 자유(fundamental freedom)로 표현의 자유와 집회, 결사의 자유를 진작하는 모

든 사이버 공간의 활동을 진작하면서도 동시에 아동 포르노나 테러 활동 등이를 악용하는 것에는 관용하지 않는다. 둘째, 사생활의 존중으로 개인에 대한 정보 노출을 지양하며 개인의 권리를 법률에 의거 일관성 있게 보호한다. 셋째, 혁신과 표현의 자유를 위한 정보의 자유로운 흐름 진작하기 위해 자유무역과 보다 폭넓은 정보의 흐름을 저해하지 않는 각종 국제 사이버안보 조치와 기준을 위해 노력한다는 것이다(The White House, 2011: 6).

국제사이버안보 협력을 통해 미국은 궁극적으로 국제적으로 열린, 상호 호환이 가능하고, 안전한, 그리고 신뢰할 수 있는 정보 기반을 추구하여 국제무역과 통상을 지원하며, 국제 안보를 강화시키고, 표현의 자유와 혁신을 촉진시키는 목표를 추구한다. 이러한 목표를 달성하기 위해, 책임감 있는 사이버공간의 규범(norms)이 국가의 정책을 제시하고 파트너십을 유지하고 사이버 공간의 법규를 지지하는 환경을 만들 것을 제시한다. 여기서 미국이 의미하는 사이버 규범이란 받아들여질 수 있는 행동에 대한 국가들 간의 공통된 합의가 사이버공간의 안정성을 강화시키며 국제 행동의 기반을 마련으로 것으로 이는 다음의 다섯 가지 원칙에 의거한다. 첫째, 오프라인은 물론 온라인에서의 근본적 표현의 자유 지향, 둘째, 지재권이나 특허, 저작권 같은 재산권 존중, 셋째, 인터넷을 사용함에서 국가의 간섭으로부터 사생활 보호, 넷째, 사이버범죄에 대한 색출과 처벌을 위한 국제협력을 통한 사이버 범죄로부터의 보호, 다섯째, 유엔 헌장에 보장된 자위권의 원칙에 의거한 사이버 공격으로부터 국가의 안보를 지킬 자위의 권리이다. 이를 위해 각 국가는 구체적 행동 강경으로 1) 인터넷 접근에 대한 상호 보장, 2) 국제적으로 연결된 인터넷 정보의 자유로운 소통, 3) 개인의 인터넷 접근성에 대한 불간섭을 통한 네트워크 안정성 보장, 4) 정부를 넘어선 다양한 이해당사자에 의한 인터넷 거버넌스의 필요성 인식, 5) 각자 자국의 정보 인프라와 국가적 정보 시스템을 공격이나 피해로부터 보호할 사이버공간의 기본책무 수행을 제시한다(The White House, 2011: 9-10).

2. 양자협력

앞에서 제시된 목표와 원칙, 행동 강령을 중심으로 미국은 주요 동맹국들과의 국제사이버안보 협력외교를 벌이고 있다. 먼전 미일 협력외교로 미국은 일본과 2013년 5월 동경에서 처음으로 각 정부부처의 사이버안보관련 담당자들이 참여하는 “사이버 문제 관련 대화”를 개최하고, 협력 강화 확인 공동성명 발표한다(US Department of State, 2013a). 이는 양국의 사이버 문제에 대한 최초 회의로 사이버 공격 등에 관한 정보 교환 강화 및 중요한 인프라를 사이버 공격으로부터 지키기 위한 대책 마련, 국제적인 규범을 만들기 위한 협력 강화 등의 내용을 다룬다. 이듬해인 2014년 4월에는 미일 방위협력지침을 개정하면서 사이버 안보 부문에서 공조를 강화한다. 2015년 5월에는 세 번째 “사이버 문제 관련 대화”를 통해 미국이 일본에게 이른바 전통적인 “핵우산”에 대응하는 개념의 “사이버 우산”을 제공하기로 합의한다. 공동성명에 따르면 미국은 일본의 군 기지와 사회기반시설에 대한 사이버 공격 위협에 대처할 수 있도록 지원하기로 동의 한다(The Ministry of Defense of Japan, 2015). 이는 아직 일천한 일본의 사이버안보 방위 인력에 대한 미국의 지원을 약속한 것으로 일본 방위성에 따르면 일본 자위대 가운데 사이버 안보군은 90명에 불과. 반면 미국은 6,000명이 넘는 것으로 보도되었다(Kelly, 2015).

미국은 영국과도 사이버안보를 위한 영미 협력외교를 진행하고 있다. 미국은 영국과 사이버 안보 강화를 위해 정보공유와 컴퓨터 네트워크 방어 업무의 파트너십을 지속적으로 강화해 왔다. 2015년 1월 사이버 보안 강화를 위한 협력 논의를 통해 양국 정상은 주요 인프라의 사이버 보안 강화, 사이버 방어의 연계 강화, 사이버 보안 분야의 학술 연구 및 인재 육성에 관한 협력을 약속하고 주요 인프라 대상의 사이버 공격에 관한 정보 교환 실시 및 공동 대응 훈련을 전개할 계획을 수립하였다(The White House, 2015). 이어서 2015년 11월에 양국은 합동 사이버 훈련을 실시하였다. 리질리언트 쉴드

작전(Operation Resilient Shield)으로 명명된 합동 훈련은 미국 CERT (Computer Emergency Response Team)와 영국 CERT가 공동으로 주관하여 영국의 영란은행과 미국의 상대은행에 대한 가상의 사이버공격 모의 훈련을 통해 시스템과 관련한 정보 공유 및 사건 대응 과정에서의 약점을 찾아내는 데에 집중하였다(Wallace, 2015). 2015년 8월에는 인도와의 협력을 위해 공동 노력을 펼치기로 하였다.

한국과의 협력외교의 경우 2013년 9월 국방사이버정책실무협의회 설치를 위한 약정을 체결하고 사이버안보 관련 논의를 진행하였다. 양국군은 2015년 7월과 10월 2차례에 걸쳐 합참과 주한미군사령부 주관으로 사이버 공격에 대응한 토의식 연습을 통해 전술지휘통제자동화체계(C4I)에 대한 사이버 공격이 발생했을 경우에 대비한 공동 대응 절차를 논의하였다. 이어서 2015년 10월 한미 국방 사이버 정책회의를 개최하여 북한의 사이버 공격 위협에 대한 공동 대응 방안을 논의하고 한미 간 공조체계를 강화하고 사이버 위협 관련 정보를 공유키로 하였다(이영재, 2015). 한편 미국 국부무는 한국의 미래창조부와 2013년부터 2016년 3차에 걸쳐 한미 ICT 정책포럼을 개최하여 한국 측과 회담을 갖고 양국이 사이버보안 분야 협력 강화를 위해 공동 기술개발, 글로벌 사이버위협 정보공유 강화, 사이버보안 정책 공조를 위해 노력하키로 합의 하였다(미래창조과학부, 2016).

3. 미중 협력과 과제

미중 간의 양자협력과 논의는 양국의 사이버안보뿐 아니라 양국관계 전반, 나아가 국제사이버 안보 공조노력과 거버넌스에 중요한 함의를 가진다. 미중의 사이버 안보 대화는 먼저 양국이 서로를 가장 위험한 사이버위협의 대상으로 삼는 것에서부터 시작한다. 2000년대 후반부터 미국 정부와 언론은 중국 해커들의 공격이 미국의 경제와 국가안보의 근간을 뒤흔드는 위협을 초래하고 있다는 소위 '중국해커 위협론'을 펼치기 시작한다. 앞서 살펴보았듯이 미국은 중국의 해커들이 중국 정부와 군의 지원받아서 미국의 물리적 인프라

와 지식정보 자산을 심각하게 침해하고 있다고 판단해왔다. 특히 2010년대에 이후 중국의 해커 공격에 대한 미국 측의 비난의 목소리가 높아지면서 미국과 중국 간의 사이버 갈등이 증폭되기 시작한다.

사이버 안보는 오바마 행정부 취임직후부터 2009년 이후 양국 간에 진행된 전략경제대화의 의제 중의 하나로서 다루어졌으며, 좀 더 구체적으로는 미·중 사이버 보안 실무그룹의 협의가 진행되어왔다. 그러나 이러한 협력의 노력에도 불구하고 물 밑에서는 미·중 사이버 갈등은 계속 진행되었다. 대표적으로 미국의 정부, 국제기구, 기업, 연구소 등 72개 기관에 침투한 "Shady RAT" 공격은 중국의 미국에 대한 해킹 사례로 대량의 자료 복제 및 유출이 이루어졌다(Gross, 2011). 그 결과 미국 정부의 2011년 국가 방첩 보고서(National Counterintelligence Executive Report)는 중국을 "가장 적극적이고 지속적인" 사이버 침투 세력으로 지목하게 된다(Office of National Counter Intelligence Executive, 2011: 5). 이후 2013년 2월 미국의 컴퓨터 보안회사인 맨디언트는 76쪽에 걸친 보고서를 통해 그동안 간헐적으로 탐지된 중국군의 사이버 테러와 공격의 실태를 종합적이고 자세하게 보고한다. 이들 공격이 정보통신·항공우주·행정·위성·통신·과학연구·컨설팅 분야에 집중되었으며, 주로 지적재산권과 연구개발의 내용을 훔치는 데 주안점을 두었다는 점이 보도된다. 당시 백악관 국가안보보좌관 토머스 도닐런(Thomas Donilon)은 중국에 해킹을 중단하라고 촉구하기에 이른다(The White House, 2013). 맨디언트는 2014년에도 비슷한 내용의 보고서를 냈는데, 미국 정부의 요구에도 불구하고 중국이 지속적으로 해킹을 벌이고 있다는 내용이 폭로되었다. 보고서는 여전히 미국 기업들이 보유한 첨단기술과 정보에 대한 중국의 해킹이 심각하다고 밝힌다. 2014년 5월 미국 법무부는 급기야 이와 관련하여 그 배후에 있을 것으로 추정되는 중국군 61398 부대 장교 5명에 대한 정식 기소를 단행하여 양국 간의 외교적 마찰이 정점에 달하는 사건이 벌어진다. 중국은 이에 즉각 반발하며 미국과의 정부대화를 중단하는 동시에 중국 시장에 진출한 미국 IT 기업들에 대한 규제의 고삐를 죄는 조치를 취한다(Schmidt, 2014).

한편 중국은 오히려 자국이 미국으로부터의 사이버 공격에 더 취약하다고

주장한다. 미국해커에 의한 복제 소프트웨어가 만연한 가운데 매년 미국으로부터 34,000건으로 추산되는 사이버 공격 시도된다고 주장한다. 중국은 미국의 비대칭적 우위로 세계 전체 인터넷 운영에 필요한 13개의 루트 서버 중 10개가 미국에 소재하고 인터넷 프로토콜 주소를 관리하는 ICANN은 미국 정부의 지침에 따라 설립되었다는 점 등을 들어 미국이 사이버공간에서의 기술 및 자산에서 여전히 절대적인 비대칭적, 구조적 우위에 있으며, 이를 근거로 개인과 국가의 사이버공격이나 해킹 능력이 중국에 비해 뛰어날 수밖에 없다고 의심한다(Lieberthal and Singer, 2012: 4-5).

양국 간의 사이버공격과 위협에 대한 우려가 심각해지면서 이를 논의하기 위한 노력도 지속되었다. 2015년 9월 시진핑 주석과 오바마 대통령의 백악관 정상회담에서 양국은 "어떤 국가의 정부도 무역 비밀을 포함한 지적 재산권 등에 대한 사이버 절도를 지원하지 않는다"고 합의하고 사이버 안보와 관련해 양국이 사이버 범죄 및 관련 문제 등에 대처하기 위한 고위급 공동대화 메커니즘을 설치키로 한다. 또한 사이버 해킹을 막기 위한 제도적 기반을 마련키로 합의 한다(Bejtlich, 2015). 이어서 2015년 12월에는 정상간 합의에 대한 구체적 논의를 위해 궈성쿤 중국 공안부장이 미국을 방문하여 제이 존슨 미국 국토안보부 장관과 사이버 안보와 해킹 문제 해결을 논의한다. 이는 사이버안보에 관한 미중간의 최초의 실무 장관급 회동으로 미국 측은 중국에 미국 기업에 대한 해킹 방지와 미국의 지적재산권 등에 대한 적극적인 보호 조치를 취해 줄 것을 요청한다. 회담에서 양국은 정부 주도로 사이버 공격을 통해 기업 기밀을 훔치거나 해킹을 지원하지 않기로 합의하고 중국 공안부·국가안전부·사법부와 미국 국토안보부·사법부 등 관련 부처 수장이 향후 정기적인 만남을 통해 보다 논의를 진작 시킬 것을 합의하였다. 또한 양측은 미중 '사이버 안보 대책 핫라인 설치'에 합의하며 2015년 일련의 사이버 공격 사건으로 악화한 양국 관계의 회복에 노력한 것으로 보도 되었다(Risen, 2015). 실제로 보도에 의하면 미국의 기업과 기관 등에 대한 중국군의 사이버 공격이 2015년 5월 이래 급격히 감소했다고 전해진다. 미국 당국자들에 의하면 사이버 공격을 통해 미국 대기업의 비밀을 훔친 혐의로 중국군 장교 5명을 사법당국이 작년 5월 기소한 후 중국군의 해킹 공격이 크게 줄었다는

것이다. 다만 여전히 중국 정보기관인 국가안전부가 미국 기업 등을 겨냥한 사이버 공격을 계속하고 있는 흔적을 포착되고 있다는 점에서 중국 발 해킹 행위가 완전히 중단되지는 않고 있음이 지적된다(Nakashima, 2016).

미중 간의 사이버안보 협력은 사이버공간이 가지는 익명성과 다양한 행위자, 공격자 우위 특성, 양국 간 점증하는 전략경쟁과 관련한 정보요구증가 등이 가지는 요소에 의해 어려운 것이 현실이다. 또한 양국 정부가 사이버안보에 대해 가지는 기본적인 개념과 원칙의 근본적인 입장 차이는 양국 간 대화 노력에도 불구하고 이 분야의 협력을 더욱 어렵게 만든다. 미국이 추구하는 정보의 자유로운 흐름과 개인의 정보활동과 의사표현의 자유, 사생활 보호 등은 공산당 독재에 대한 반정부 선동, 정부의 통제 약화, 외부의 불순 사상과 문화의 유입 등 현 체제자체를 위협하는 행위로 이해된다. 그럼에도 불구하고 미중 간 사이버안보 분야의 대화노력과 협력은 향후 미중의 사이버 문제 뿐 아니라 양국의 전반적인 관계와 국제 사이버안보의 협력을 위해서는 중요한 함의를 가지며, 따라서 향후 협력을 위한 다음의 고려사항이 제시된다.

첫째, 양국은 다른 분야와 달리 사이버공간 기술적의 특성으로 인해 가지는 협력의 어려움을 상호 인식해야 한다. 또한 사이버안공간에서의 정보의 자유에 관해 양국의 정치체제가 가지는 근본적인 접근의 차이도 솔직히 인정할 필요가 있다. 둘째, 이러한 기술적, 개념적 차이에 대한 인정을 바탕으로 여전히 양국이 공유하는 사이버안보 문제, 즉 정치적 함의가 없는 사이버범죄나 사이버테러 활동에 대한 공조를 확대해 추구해야 한다. 셋째, 이를 위해 환경이나 기후분야, 금융, 비확산 등 여타 분야에서 양국이 이룩한 다양한 협력 모델의 적용을 논의할 수 있으며, 넷째, 지구적 차원의 인터넷의 순조로운 기능을 위한 다양한 기술적 규범에 대한 합의와 명문화 노력, 애매한 책임소재 식별에 대처하려는 노력, 양국이 서로 중대한 갈등을 야기시킬 수 있는 “마지노선”이나 “적색선”에 대한 상호 인식 노력 등을 시도해야 한다. 마지막으로 이러한 논의를 위해 보다 다양하고 책임 있는 당국자 간의 협의 채널을 구축하여 상호신뢰와 협력을 증진해야 한다(Lieberthal and Singer, 2012: 23-31).

IV. 지역 및 글로벌 거버넌스 전략

미국은 당면한 사이버안보 도전에 대응하기 위한 다양한 양자외교를 벌임과 동시에 자신이 추구하는 사이버공간의 가치와 안보이익을 보호하기 위한 국제 규범과 통치제도의 창출을 위한 지역협력과 지구적 차원의 거버넌스 형성에 노력을 경주하고 있다. 이를 위해 가치와 이익을 공유하는 기존의 동맹국들과 협력하여 다음의 전략을 추구한다. 첫째, 사이버 공간과 인터넷 표현의 자유, 개방, 신뢰 등 기본 원칙이 존중되어야 한다. 둘째, 사이버 공간을 사용하고 있는 개인, 산업계, 시민사회 및 정부기관 등 다양한 구성원들의 의견이 수렴된 국제적 규범을 제정해야 한다. 셋째, 기존의 국제법이 인터넷 및 사이버 공간에도 규범 원칙을 설정함에서 그 출발은 기존의 국제법을 토대로 하며, 따라서 유엔헌장 등이 사이버 공간을 규율하는 국제규범의 모태가 되어야 한다. 넷째, 상호간 사이버 공간상의 위협 요소 감축 및 신뢰 증진을 위한 사이버 공간에 적용 가능한 신뢰구축조치(CBMs: Confidence Building Measures)의 이행이 필요하다(김소정, 2013).

1. 지역협력외교

미국의 국제 전략은 지역차원에서 기존에 존재하는 지역안보기구를 통한 협력체계 구축에 힘쓰고 있다. 유럽안보협력기구(OSCE: Organization for Security and Cooperation in Europe)는 그 대표적인 예이다. 냉전시기 동서간의 신뢰구축을 통해 유럽의 공동안보와 협력을 추구한 OSCE의 경험을 살려 사이버공간에서의 위협요소 감축과 신뢰구축에 활용하려 한다. 2012년 4월 이래 미국은 비공식 워킹 그룹(Informal Working Group)을 설립하고 자신들이 의장으로 역할을 하면서 유럽회원국과 미국을 포함한 국가 간 정보통

신과 사이버 분야의 신뢰구축방안에 관하여 논의를 해오고 있다(OSCE, 2014). 2013년 12월에는 첫 번째 조치로 회원국 간에 사이버안보 분야의 신뢰구축을 위한 기본 11개 원칙에 합의안을 내기도 하였다(OSCE, 2013). 한편 군축과 사이버 안보는 본질적인 측면에서 다르기 때문에 일방적인 군축 개념을 사이버 안보분야에 적용시키기 어렵다는 회의적인 시각도 존재한다. 특히 핵무기 등 전통적 안보개념에서는 억지력 확보 및 신뢰구축조치 향상으로 인한 예측성 강화가 결정적인 요소였으나 인터넷과 사이버 분야의 특성상 억지력 확보와 예측성 강화가 불가능할 것이라는 비판적 시각이 있다.

한편, 미국은 유럽의 나토(NATO) 동맹국들과 함께 나토 내에 사이버안보에 관한 협의체를 설치하고 사이버공간에서의 안보위협에 전통 군사동맹인 나토가 함께 대응해 나갈 전략과 방안을 수립코자 노력한다. 2008년 NATO 동맹국을 주축으로 이를 처음 제안한 에스토니아의 탈린에 나토 사이버방위협력센터(NATO Cooperative Cyber Defence Centre of Excellence: CCDCOE)를 설립하고 사이버방위에 관한 회원국들 간의 정보교환, 공동연구, 협력방안 등을 중점적으로 추구해왔다. 특히 2009년부터 탈린메뉴얼과정(Tallinn Manuel Process)을 시작하여 3년여에 걸쳐 20명의 국제법 학자들이 참여한 사이버전쟁에 관한 기존 국제법에 기준한 일종의 사이버전쟁에 관한 국제법 지침서를 발간한다. 미국 해군대학의 국제법 교수인 마이클 슈미트가 편집 책임을 맡은 이 지침서는 302페이지에 달하는 문건을 통해 주권 개념, 국가책임, 전쟁의 시작에 관한 국제법(jus ad bellum), 국제인권법, 중립에 관한 법 등의 핵심적인 전쟁과 관련한 문제에 관하여 이미 수립된 전통 국제협약이나 관습법이 어떻게 사이버공간과 사이버전쟁에 적용될 수 있는지의 문제를 논의한다(NATO CCDCOE, 2013). 이 지침서에 의하면 사이버공간에서도 전통의 교전수칙이 적용될 수 있으며, 이러한 원칙에 따라 특정 국가나 개인에 대한 사이버 공격도 그에 상응하는 대응과 조치를 기존 전쟁의 교전 수칙이나 전쟁법에 의거 취할 수 있다고 제시한다.

아세안지역포럼(ARF: ASEAN Regional Forum)은 아시아지역의 사이버안보 분야의 다자적 지역협력을 위해 미국이 노력을 기울이는 기구이다. 동남아의 아세안회원국 10국가와 한중일, 미국, 러시아, 유럽연합 등의 27개국

이 참여하는 대표적인 다자안보협의체인 ARF는 2012년 사이버안보진작을 위한 공동선언을 채택한 이 후 지역의 각종 사이버 안보 현안에 관한 논의가 주로 벌어지는 곳이다. 아세안을 위주로 한 회원국 장관들은 2013년에 사이버안보관련 정보공유와 능력배양에 관하여 함께 협력할 것을 약속하였다. 이러한 ARF에 대해 미국의 케리 국무장관은 미국이 아시아 국가들의 사이버 안보로부터 우리 모두를 보호하고 사이버위협의 위험을 줄이기 위한 능력배양 노력을 매우 적극적으로 도울 의사가 있음을 밝히기도 하였다. 그리하여 미국은 이들을 대상으로 사이버공간에서의 가짜 도용자를 대응하는 세미나를 개최하고 아세안 국가들 간의 사이버신뢰구축을 위한 사이버 워크숍, 아세안 사이버범죄 대응능력강화방안, 첨단범죄수사와 디지털 유전분석 프로그램 워크숍 등을 조직하는 등 아시아 지역의 사이버안보 다자협력 증진에 적극적인 지지를 보내고 있다(US Department of State, 2013b).

2. 글로벌 거버넌스

사이버공간과 사이버안보에 관한 지구적 차원의 국제규범과 제도를 만들려는 시도는 아직은 시작단계에 있다. 미국은 당연히 새로이 형성될 사이버공간의 국제규범을 주도하고, 이 과정에서 미국이 추구하는 사이버안보 관련 규범, 원칙, 가치를 실현코자 한다. 문제는 미국이 주도하는 사이버공간의 국제규범과 거버넌스에 대해 모두가 동조하지 않는다는 것이다. 특히 사이버위협과 공격 행위를 규제할 국제규범과 원칙 설립을 놓고 미국과 영국으로 대표되는 서방측과 중국과 러시아로 대표되는 비 서방측은 크게 다른 입장을 보인다. 미국이 추구하는 국경을 초월한 정보 접근과 소통의 자유, 개인의 사생활과 지적재산권의 보호 등에 대해 러시아와 중국을 위시한 국가들은 사이버 공간에서도 국가주권은 인정되며 필요시 정보 통제를 허용해야 한다고 주장한다. 이러한 주장의 이면에는 중국 및 러시아 등이 자신들 체제의 안정성 확보를 위해 인터넷 등에서 언론의 자유를 통제하는 것을 미국과 서방측이 저지하려는 의도가 있다는 이들의 이해를 반영한다. 또한 이들은 기존의 인

터넷 체계를 구성하고 주도해 온 서방측의 의도대로 인터넷과 사이버 공간을 규율하는 체제를 수용할 수 없으며, 사이버 공간의 신뢰구축조치 수립이나 이행보다는 국가의 인터넷 통제 강화 등을 내용으로 한 국제정보보안 행동수칙에 대한 합의가 시급하다는 입장이다(김소정, 2013).

부다페스트 사이버범죄 조약은 미국이 그동안 적극적으로 참여해온 국제협약의 하나이다. 2001년에 시작하여 인터넷을 사용한 사이버범죄 행위에 대한 국가 간의 공조와 협력을 통한 대응을 추구하는 이 조약은 2016년 현재 미국과 유럽, 일본 등을 포함한 55개국이 가입하고 있다. 미국은 이 조약을 통해 날로 심각성과 위험성이 증가하는 사이버범죄에 대해 효과적인 대응을 위해서는 각 국이 사이버범죄에 관한 공통의 규정과 법을 만들고 이를 통해 증거수집, 범죄인 인도 등에서 공조할 것을 제안한다. 또한 이 협약이 각국이 사이버범죄 관련 법률을 만들고 현 법률을 개선하는데 도움이 될 것으로 기대한다. 그러나 러시아나 중국은 여기에 미온적인 반응을 보이고 가입하고 있지 않다(Council of Europe, 2016).

한편 UN를 중심한 국제사이버 규범 형성 노력이 러시아에 의해 시도된 사례도 있다. 1998년 러시아는 “Developments in the field of information and telecommunications in the context of international security”라는 결의안을 UN에 제출하고 이를 총회에서 채택한 후, 유엔의 군축 및 국제안보 위원회에서 사이버 안보가 논의되기 시작하였다. 그러나 동 결의안에 대해 미국은 처음부터 동조하지 않았고, 이후로도 소극적으로 사이버 안보 관련 국제협력에 대응해왔다. 이후 동 위원회는 국제안보 차원에서의 사이버 안보 문제를 논의하기 위해 2004년부터 “국제안보 맥락에서의 IT 분야 개발에 관한 UN 정부전문가그룹(Group of Government Experts on Developments in the Field of Information and Telecommunications In the Context of International Security)” 회의를 지속해오고 있다. 지금까지 4회에 걸쳐 열린 사이버안보 관련 정부전문가그룹(GGEs) 회의를 통해 유엔은 러시아는 물론 미국과 중국, 일본 등의 국가들 간에 사이버안보에 관한 국제 규범 확립에 관한 공동의 입장을 확인하고 이견을 좁히려는 노력을 하고 있다.

2015년 7월에 열린 회의에서 미국, 러시아, 중국, 영국, 프랑스, 독일, 브

라질 등 20개국이 합의한 내용은 사이버 공간에서 국가들이 지켜야 할 규범, 규칙, 원칙에 대한 기본 원칙과 신뢰구축방안, 사이버안보 능력배양에 대한 지지이다. 이들이 합의한 원칙을 살펴보면 각 국가는 정보통신기술을 사용함에서 국제법과 국가주권, 평화적 방법에 의한 분쟁해결과 내정불간섭의 원칙을 준수할 것이며, 동시에 각국이 정보통신기술 사용함에서 기본 인권과 근본적인 자유를 존중할 의무를 가진다고 규정한다. 또한 국가는 가짜 프락시를 정보통신기술 활용에 사용하지 않을 것과 자신들의 영토가 비국가행위자들의 그러한 행위에 이용되도록 허용하지 않을 것을 합의하였다(UN Office of Disarmament Affairs, 2016). 한편, 유엔은 2006년부터 인터넷 거버넌스 포럼(IGF: Internet Governance Forum)을 개최하여 인터넷 안보는 물론 지속가능성, 성장, 개발과 안정성 등 인터넷과 관련된 종합적인 문제에 대해 정부는 물론 이해 당사들이 모여 인터넷 관련 국제 거버넌스 이슈에 대한 정책적 대화를 나누는 장으로 사용되고 있다.

V. 결론: 정책적 함의

지금까지 살펴본 미국의 국내 및 국제 사이버안보 전략이 가지는 정책적 함의는 다음과 같다. 첫째, 사이버공간 및 사이버안보가 가지는 기술적 특수성으로 인한 정부차원 대응의 어려움에 대한 인식이다. 사이버 공간은 그 익명성으로 인해 다양한 공격의 목적과 행위자 그리고 공격 목표를 가진다. 가장 일반적인 사이버범죄나 공격의 목적과 행위자가 금전적 이득을 위한 것이 현실이지만, 동시에 단순한 정보의 탈취나 과시성 해킹도 빈번하게 벌어지며, 이것은 종종 국가에 의한 사이버 공간의 간첩활동이나 사이버 공격과 구분이 어렵고 경계가 모호한 경우가 많다. 또한 민간과 정부의 구분이 어렵고, 공격속도에 비해 훨씬 더딘 의사결정과정, 소수의 해커조직이나 한 개인의 일사불란하고 민첩한 공격에 대해 분산되고 파편화 되어 있는 정부 조직, 책임소재의 불명확성 등은 사이버안보를 위한 중앙정부 차원의 정책과 전략 마련

에 근본적인 도전을 제기한다.

둘째, 사이버공간에서의 공격의 특수성은 공격보다 이에 대응하는 방어를 더욱 어렵게 만든다. 사이버공격의 경우는 재래식 공격과 반대로 공격자우위의 성향을 가지며, 이는 방어대책 마련과 억제의 어려움으로 직결된다. 재래식 전쟁에서는 방어가 보통 공격자에 비해 3배의 우위를 가지는 것으로 여겨진다. 그러나 사이버공간에서는 공격자 식별의 어려움, 은밀성, 속도의 우위, 기술진화의 빠른 전개 등에 의해 공격자가 유리하다. 이는 실제로 공격과 방어 우위 이론에 의하면 선제공격에 대한 인센티브를 강화하는 결과를 초래한다.

셋째, 전통 안보개념 적용의 어려움이다. 전투원과 민간의 구분이 어려움, 공격의 출처 식별의 어려움, 현실세계의 국경과 전장구분에 비해 그 경계가 존재하지 않는 사이버공간의 특수성, 금전적 목적과 국가안보 위협 구분의 모호성, 민간 핵심 기간 시설의 사이버 공격에 대한 취약성으로 인한 공격과 피해의 비대칭성 등은 재래식 전쟁이나 안보개념에 의한 사이버안보 접근법의 한계를 극대화한다.

넷째, 따라서 사이버안보 정책은 국방부나 특정 안보관련 부분만이 아니라 전체 유관 정부 부처 간의 통합적 소통과 공조를 바탕으로 한 민, 관, 군의 긴밀한 협조와 공동의 대응을 요구하지만, 현실은 그 시행이 가장 어렵다는 것이다. 사이버안보상의 민간의 협조를 위한 조치가 개인의 사생활 침해나 기업의 이윤추구나 소비자 보호 책임에 반하는 결과를 초래하여 정부와 민간, 시민사회 간에 갈등과 논쟁을 불러일으키는 사례가 대표적인 경우이다.

다섯째, 사이버안보는 국경을 초월하는 개방성과 연결성으로 인해 국내정책 못지않게 국제적 협력의 중요성도 강조된다. 그러나 각 국가별로 사이버안보에 대한 접근 방식과 조직, 능력에 많은 차이를 가지는 것이 현실이며 이는 국제공조의 어려움을 야기한다. 더욱이 미중의 경우와 같이 사이버안보의 근본적인 목적과 원칙에 대한 대조적 접근법은 이들 간 사이버안보 협력의 필요성과 중요성이 증가함에도 불구하고 사이버안보를 위한 공동규범의 창출이나 국제 거버넌스 형성을 더욱 어렵게 만든다.

여섯째, 그럼에도 불구하고 미국은 영국, 일본 등 전통적인 동맹국들과 연

합하여 사이버공간에서 미국이 추구하는 목표와 가치를 구현하기 위한 국제 규범과 제도, 거버넌스 형성을 위해 지역적, 지구적 차원의 노력을 기울이고 있다. 인터넷 공간의 자유로운 정보의 흐름과 개인의 정보 접근의 자유, 개인의 의사표현의 자유 및 지적 재산권 등의 보호를 추구하는 미국은 유엔 등에 확립된 전통적 국제규범과 원칙을 토대로 사이버공간에서 이를 구현할 지역 협력 및 국제 거버넌스 창출을 주도하기 위해 노력하고 있다.

미국은 사이버공간의 가장 큰 기술적 리더이자, 수혜자이며, 또한 각종 사이버 공격의 가장 큰 대상이기도 하다. 미국은 정보의 자유로운 소통과 접근, 개인의 의사표현과 정보 습득 권한 보장, 열린 사이버 공간을 통한 개인과 민간, 국가 이익의 증진 등을 목표로 사이버범죄로 부터 이들 가치와 원칙을 지키기 위한 국내정책, 국제협력, 국제규범 창출에 노력하고 있다. 이러한 노력은 사이버 공간이 가지는 기술적 특성으로 인해 기존의 여타 안보정책과 다른 많은 도전과 과제를 제시한다. 또한 국제적 규범 확립을 위한 노력은 이에 대한 다른 이해관계와 접근을 추구하는 중국이나 러시아와의 갈등을 야기하기도 한다. 그럼에도 여전히 사이버안보 관련 정책과 제도, 기술개발, 국제규범 설립 등에서 선도적 역할을 추구하는 미국의 사이버안보 전략은 향후 한국을 비롯한 각국의 사이버 안보 전략은 물론 국제사이버 질서 확립에서도 많은 시사점을 가질 것이다.

투고일자: 2016-10-21 심사일자: 2016-12-08 게재확정: 2016-12-23

참고문헌

김소정. 2013.「사이버 안보 국제협력과 국가전략」. JPI PeaceNet No. 2013-17. 제주평화연구원. http://www.jpi.or.kr/kor/regular/policy_view.sky?code=papermorgue&id=5033(검색일: 2016. 9. 10).

김형우·이광호. 2015.「미국의 주요 기반시설 사이버 보안 위협과 정책 소개」.『국방과 기술』441호. pp. 132-139.

미래창조과학부. 2016.「미래부, 미국과 차세대 ICT 협력 가속화한다; 2차관, 한-미 ICT 정책 포럼에서 포괄적 협력을 위한 공동선언문 채택」. 9월 11일.

http://m.msip.go.kr/mobile/cms/contentsView.do?cateId=mssm15_12&artId=1311843&pageNum=1(검색일: 2016. 9. 15).

민병원. 2015.「사이버공격과 사이버억지의 국제정치: 규제와 새로운 패러다임을 중심으로」.『국가전략』21권 3호. pp. 37-61.

배병환·송은지. 2014.「주요국 사이버보안 전략 비교·분석 및 시사점: 미국, EU, 영국의 사이버보안 전략을 중심으로」.『정보통신방송정책』26권 21호. 통권 589. pp. 1-27.

장노순. 2013.「사이버 안보와 미중관계」. JPI PeaceNet(June 14, 2013). 제주평화연구원. pp. 1-3.

장노순·김소정. 2016.「미국의 사이버전략 선택과 안보전략적 의미」.『정치정보연구』19권 3호. pp. 57-91.

장노순·한인택. 2013.「사이버안보의 쟁점과 연구 경향」.『국제정치논총』53권 3호. pp. 579-618.

이영재. 2015.「한미 국방사이버정책 실무협의, 북 사이버공격 대응 논의」.『연합뉴스』10월 27일 http://www.yonhapnews.co.kr/bulletin/2015/10/27/0200000000AKR20151027072351014.HTML(검색일: 2016. 9. 10).

Bejtlich, Richard. 2015. “To hack, or not to hack?” Brookings Institute (September 28, 2015). http://www.brookings.edu/blogs/up-front/posts/2015/09/28-us-china-hacking-agreement-bejtlich (accessed 10 September 2016).

Boyd, Aaron. 2016. “DNI Clapper: Cyber bigger threat than terrorism.” *Federal Times* (February 4, 2016). http://www.federaltimes.com/story/government/cybersecurity/2016/02/04/cyber-bigger-threat-terrorism/79816482/ (accessed 5 September 2016).

Center for Strategic and International Studies(CSIS). 2014. “Net Losses: Estimating the Global Cost of Cybercrime.” http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf?cid=BHP028 (accessed 2 September 2016).

Council of Europe. 2016. “Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime.” https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XTRqwS6d (accessed 10 September 2016).

Davis, Julie Hirschfeld. 2015. “Hacking of Government Computers Exposed 21.5 Million People.” *New York Times* (July 9, 2015). http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?action=click&contentCollection=Politics&module=RelatedCoverage&region=Marginalia&pgtype=article (accessed 2 September 2016).

Sanger, David E. “U.S. Decides to Retaliate Against China’s Hacking.” *New York Times* (July 31, 2015). http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?action=click&contentCollection=Politics&module=RelatedCoverage&region=Marginalia&pgtype=article (accessed 2 September 2016).

Filkins, Barbara. 2016. "IT Security Spending Trends." SANS Institute (February 2016). https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697 (accessed 5 September 2016).

Fischer, Eric A. 2016. "Cybersecurity Issues and Challenges: In Brief." CRS Report No. R43831 (August 12, 2016).

Gross, Michael Joseph. 2011. "Exclusive: Operation Shady Rat – Unprecedented Cyber-Espionage Campaign and Intellectual – Property Bonanza." *Vanity Fair* (August 2, 2011). http://www.vanityfair.com/news/2011/09/operation-shady-rat-201109 (accessed 15 September 2016).

Harris, Shane and Nancy A. Youssef. 2016. "Pressure Grows on Obama to Name DNC Hackers." *Daily Beast* (July 30, 2016). http://www.thedailybeast.com/articles/2016/07/29/pressure-grows-on-obama-to-name-dnc-hackers.html (accessed 2 September 2016).

Jackson, William. "DOD creates Cyber Command as U.S. Strategic Command subunit New post will defend .mil domain." *FCW* (June 24, 2009). https://fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx?Page=1 (accessed 5 September 2016).

Jennings, Peter. 2013. "Rise of the cyber-men in Asia." *The Strategist*. The Australian Strategic Policy Institute (July 5, 2013). http://www.aspistrategist.org.au/rise-of-the-cyber-men-in-asia/ (accessed 10 September 2016).

Kelly, Tim. 2015. "U.S. to bring Japan under its cyber defense umbrella." *Reuters* (May 20, 2015). http://www.reuters.com/article/us-japan-us-cybersecurity-idUSKBN0OF0EL20150530 (accessed 10 September 2016).

Korte, Gregory and David Jackson. 2015. "Obama sanctions North Korea for movie hacking." *USA TODAY* (January 2, 2015). http://www.usatoday.com/story/news/politics/2015/01/02/obama-north-korea-sanctions-interview-movie/21195385/ (accessed 2 September 2016).

Knowlton, Brian. 2010. "Military Computer Attack Confirmed." *New York Times* (August 25, 2010). http://www.nytimes.com/2010/08/26/technology/26cyber.html (accessed on 2 September 2016).

Lichtblau, Eric and Eric Schmitt. 2016. "Hack of Democrats' Accounts Was Wider Than Believed, Officials Say." *New York Times* (August 10, 2016). http://www.nytimes.com/2016/08/11/us/politics/democratic-party-russia-hack-cyberattack.html?_r=0 (accessed 2 September 2016).

Lieberthal, Kenneth and Peter W. Singer. 2012. "Cybersecurity and US-China Relations." *Brookings Institute* (February 2012). https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf (accessed 10 September 2016).

Lynn, William J. III. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* (September/October 2010).

McAfee. 2009. “Unsecured Economies: Protecting Vital Information.” https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf (accessed 2 September 2016).

Nakashima, Ellen. 2016. “Chinese hacking activity down sharply since mid-2014, researchers say.” *The Washington Post* (June 20, 2016). https://www.washingtonpost.com/world/national-security/chinese-hacking-activity-down-sharply-since-mid-2014-researchers-say/2016/06/20/089703e6-36fd-11e6-9ccd-d6005beac8b3_story.html (accessed 10 September 2016).

NATO CCDCOE. 2013. “Tallinn Manuel Process.” https://ccdcoe.org/tallinn-manual.html(accessed 10 September 2016).

Office of the National Counter Intelligence Executive. 2011. “Foreign Spies Stealing US Economic Secretes in Cyberspace: Report to the Congress on Foreign Economic Collection and Industrial Espionage 2009-2011” (October 2011). https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed 15 September 2016).

OSCE. 2013. “Decision No. 1106, Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologie” (December 3, 2013). http://www.osce.org/pc/109168?download=true (accessed 10 September 2016).

OSCE. 2014. “Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna” (November 7, 2014). http://www.osce.org/cio/126475 (accessed 10 September 2016).

Painter, William L. and Chris Jaikaran. 2016. “Perspectives on Federal Cybersecurity Spending.” CRS Report No. R44404 (February 25, 2016).

Perez, Evan. 2016. “Sources: US officials warned DNC of hack months before the party acted.” CNN (July 26, 2016). http://www.cnn.com/2016/07/25/politics/democratic-convention-dnc-emails-russia/ (accessed 2 September 2016).

Peterson, Andrea. 2014. “The Sony Pictures hack, explained.” *Washington Post* (December 18, 2014). https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/ (accessed 2 September 2016).

Risen, Tom. 2015. “Hotline Bling: China, U.S. Work to Further Cybersecurity Pact; The two countries aim to set up a ‘hotline mechanism’ for cybersecurity concerns and are taking other steps to discourage criminal hacking.” *US News & World Report* (December 3, 2015). http://www.usnews.com/news/articles/2015/12/03/hotline-bling-china-us-work-to-further-cybersecurity-pact (accessed 10 September 2016).

Sanger, David E. and Nicole Perlrothoct. 2015. “Senate Approves a Cybersecurity Bill Long in the Works and Largely Dated.” *New York Times* (October 27, 2015). http://www.nytimes.com/2015/10/28/us/politics/senate-approves-cybersecurity-bill-despite-flaws.html?_r=0 (accessed on 5 September 2016).

Schmidt, Michael S. and David E. Sanger. 2014. “5 in China Army Face U.S. Charges of Cyberattacks.” *New York Times* (May 19, 2014). http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html (accessed 10 September 2016).

The Ministry of Defense of Japan. 2015. “Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group” (May 30, 2015). http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf(accessed 10 September 2016).

The White House. 2008. “National Security Presidential Directive/NSPD-54 Homeland Security Presidential Directive/HSPD-23” (January 8).

The White House. 2009. “Cyberspace policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.” https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 5 September 2016).

The White House. 2011. “International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World.” https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 10 September 2016): 6, 9-10.

The White House. 2013. “Remarks By Tom Donilon, National Security Advisor to the President: “The United States and the Asia-Pacific in 2013”.” During the Asia Society held in New York (March 11, 2013). https://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an (accessed 15 September 2016).

The White House. 2015. “FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation” (January 16, 2015). https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation (accessed 10 September 2016).

UN Office of Disarmament Affairs. 2016. “Developments in the field of information and telecommunications in the context of international security.” https://www.un.org/disarmament/topics/informationsecurity/(accessed on 10 September 2016).

US Department of Defense. 2015. “The DoD Cyber Strategy.” http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed 5 September 2016).

US Department of State. 2013a. “Joint Statement on US-Japan Cyber Dialogue” (May 10, 2013). http://www.state.gov/r/pa/prs/ps/2013/05/209238.htm (accessed 10 September 2016).

US Department of State. 2013b. “U.S. Engagement in the 2013 ASEAN Regional Forum.” Press Release (July 2, 2013). http://www.state.gov/r/pa/prs/ps/2013/07/211467.htm (accessed 15 September 2016).

Wallace, Tim. 2015. “Bank of England and US authorities to simulate cyber-attack.”

The Telegraph (November 1, 2015). http://www.telegraph.co.uk/finance/bank-of-england/11968470/Bank-of-England-and-US-authorities-to-simulate-cyber-attack.html (accessed 10 September 2016).

Obama Administration's Cyber Security Policy and Challenges

Seong-ho Sheen
Professor, Graduate School of International Studies,
Seoul National University

The United States has been the biggest leader and beneficiary of cyber space. Yet, it has been also the biggest target of cyber attack. The US government has worked hard to promote free exchange and free access of information, guarantee of individual right of free expression and acquiring information and open cyber space. For this, the US government pursues various policies in domestic and international arena. Especially, under the Obama administration, the United States initiated a comprehensive policy review and published two major reports on cyber security policy: "Cyberspace policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2009)" and "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World (2011)." This paper discusses the US efforts to deal with cyber security issues, challenges, and its implications in ever more complex and rapidly changing environment of cyber space in the 21st century.

Keywords: the Obama Administration, US, Cyber Security, US-China, Global Governance

신성호. 서울대학교 국제대학원
서울특별시 관악구 관악로 1
E-mail_ssheen@snu.ac.kr