미국의 사이버보안 분야 기술정책 및 투자 동향

National Cyber Security Policy and R&D Budget in the United States

김정태(J.T. Kim) 정보기반연구팀 연구원
이현우(H.W. Lee) 정보기반연구팀 책임연구원

미국은 자국을 향한 여러 테러 방법 중에서 사이버 테러리즘이 향후 치명적인 수단으로 발전할 수 있다는 것을 인지하고, 위협에 대비하여 이에 대응할 수 있는 보안기술을 확보하고 안보를 강화하는 데 노력을 기울이고 있다. 본 고에서는 9.11 테러 이후 최근 미국의 사이버보안 분야에 대한 기술정책과 연구개발 경향 및 예산 동향을 분석하고, 정책의 도입과정에서의 주요 쟁점 및 우리나라의 사이버보안 정책 수립에 참고할 만한 시사점 등에 대하여 살펴보고자 한다.

I. 서 론

근래 바이러스나 웜 등의 악성코드로 인한 피해의 확대로 인해 정보보호에 대한 관심은 꾸준히 증가하고 있다. 정보보호라는 분야가 나타난 이후, 정보보호에 대한 국제적인 의식을 한층 더 높이게 된 계기로 2001년 9월 11일의 테러사건이 있다. 그 형태가 사이버 테러리즘이 아니었음에도 불구하고 정보보호 분야의 중대한 전환점이 되었다. 이어 발생한 탄저균을 이용한 바이오 테러 이후, 사이버 기반시설에 대한 공격 또한 테러의 경로가 될 수 있다는 경고가 속속 나오기 시작하였다[1].

정보통신 분야의 선진국인 미국에서는 군사관련 시설이나 통신, 전력, 금융, 교통 등의 주요 기반시설이 지속적인 사이버 공격을 받아 지금까지 수많은 부정 침입사건이 발생하여 막대한 손해를 입어 왔는데, 이러한 사이버 공격은 경로의 다양화, 수준의 고도화가 급속히 진행되어 갈 것으로 예상된다. 이에 테러의 집중 대상이 되었던 미국은 사이버보안 분야에 막대한 연구개발 자금을 배정하기에 이르렀다.

미국의 경우, 사이버보안이나 정보통신 분야뿐만 아니라 여러 방면의 연구개발에 대한 연방 정부의 재정적 지원은 자국의 지식 기반과 기술 능력의 확충에 크게 공헌해 왔다. 특히, 정보기술 분야에서는 정부의 연구개발 프로그램이 산업계에 미친 영향이 미국 내에서 그치지 않고 전 세계로 펼쳐지고 있어, 미국의 사이버보안 분야의 동향을 파악하는 것은 우리나라의 정책 수립에 도움을 줄 수 있다. 본 연구에서는 연구개발의 규모나 기술수준에서 선도적인 위치에 있는 미국의 사이버보안 분야에 대한 기술정책과 이에 따른 연구개발 투자 동향을 살펴보고 시사점을 제시하고자 한다.

II. 기술정책 및 연구개발 경향

미국정부의 국토안보 영역 중 중요한 부분을 차지하고 있는 것은 사이버보안 부문이다. 정보 네트워크와 시스템들에 대한 중요한 전자 기반시설을 보호하는 사이버보안은, 기반시설의 동작을 보장하기 위한 새로운 사이버보안 도구와 기법들을 생산하고, 사이버 또는 물리적 테러위협에 대항하는 능력을 배양하기 위한 적극적인 연구개발의 대상영역으로 인식되고 있다. 이 장에서는 사이버보안과 관련된 최근의 정책과 연구개발 경향을 살펴보도록 한다.

1. 사이버보안 연구개발법

2002년 11월 27일, 미국 정부는 컴퓨터 및 네트

워크 보안에 관한 연구개발의 촉진과 인재육성을 목적으로 하는 '사이버보안 연구개발법(Cyber Security Research and Development Act, HR 3394/PL 107-305, 이하 HR 3394)'을 상정하였으며, 의회는 2003년 3월 4일에 이 법안을 승인했다. 이 법안은 컴퓨터 시스템이나 네트워크를 보호하기에 현재의 정보보호 기술이 충분하지 못하며, 새로운 방법을 개발하기 위한 연구개발의 규모가 다른 연구분야와 비교해 볼 때 크지 않다는 것에서 시작되었으며, 구체적으로 다음과 같은 문제점들을 제기하고 있다[2].

- 민간 부문은 신속함과 편리함만을 중시하므로 사이버보안에 투자하는 비중이 작음
- 연방 정부의 사이버보안에의 투자가 부족함
- 강력한 사이버보안 연구를 수행할 행정 부처가 존재하지 않음
- 사이버보안 연구가 부족하여 사이버보안에의 기본적 대응이 어려움
- 자금과 연구자가 적어 사이버보안에 관심을 가지는 학생이 적음

이러한 사항들을 해소하기 위해, 국립과학재단(NSF)과 국립표준기술원(NIST)은 새로운 연구 및 교육 프로그램을 신설하였다. 이 프로그램의 목적은, 정부 또는 민간의 컴퓨터에 대한 테러리스트로부터의 공격을 예방하거나 차단하기 위해, 사이버보안 분야에서의 혁신적인 연구를 촉진하며 이 분야로 새로운 인력을 유도하거나 육성해 나가는 것이다. 이에, NSF는 다음과 같은 목적을 지닌 프로그램을 실시하기 시작하였다.

- 대학이 단독 또는 타 대학이나 산업계나 정부 연구소와 협력해, 복수의 학술 영역에 걸치는 컴퓨터 및 네트워크보안 연구 센터를 설립함
- 대학이 사이버보안에 관한 학사 및 석사 프로그램을 개설 또는 개선함
- 박사 과정의 학생이 네트워크보안 전공으로 학위를 취득하기 위한 연구 지원금을 지급함
- 대학원 학생이 박사 학위 취득 직후 사이버보안 분야의 학문적 발전을 추구할 수 있도록 능력향상을 위한 연습생 과정을 마련함

또한, NIST에서도 다음과 같은 목적을 달성하기 위한 프로그램을 개설중이다.

- 산학 제휴에 의해 산업계의 관심에 응하기 위한 연구 센터를 설립함
- 관련 분야의 상급 연구자가 사이버보안에 관한 연구를 실시함
- Post-Doc이 사이버보안에 관한 연구의 기회를 이용함

2. 국토안보법

2002년 7월 16일, 미국 정부는 국가안보의 약점을 보완하기 위해 '국토안보법(Homeland Security Act, HR 5005/PL 107-296, 이하 HR 5005)'을 발표하였고, 2002년 11월 19일, 의회에서 통과되었다. 이 법률에 의해 국토안보부(Department of Homeland Security, 이하 DHS)가 설립되게 되었다.

DHS는 지난 1947년에 국방부가 창설된 이후 가장 큰 정부조직 개편을 통해 신설된 부처로, 산하에 22개 연방정부기관과 18만 명의 직원을 거느리는 초거대 부처로 설립과정에서 반대도 적지 않았다. 개인 사생활을 침해하고 개인에 대한 정부의 부당한 개입여지가 넓어진다는 의견이 나왔고 부처의 신설보다는 기존의 부처간 효율성을 높이는 방식을 모색해야 한다는 주장도 있었으나, 이러한 의견들은 행정부의 강력한 테러방지 의지에 묻혀 크게 반영되지 못한 것으로 보인다.

HR 5005에 의해 중요한 기반시설의 보호를 담당하고 있던 기존의 여러 조직들이 DHS에 통합되었다. 통합된 조직은, 연방 수사국(FBI)의 국가 기반시설 보호 센터(NIPC), 국방부의 국가 통신 시스템(NCS), 상무성의 중요 기반시설 보전국(CIAO), 에너지성의 분석 센터, 연방 컴퓨터 사건 대책 센터(FedCIRC) 등이다. 또한, 국방부(DoD) 산하의 고등연구 계획국(DARPA)을 표본으로 하는 국토안전 고등연구 계획국(HSARPA)이 설립되었다. HSARPA의 역할은 국토안전에 공헌하는 신기술의 혁신을 재촉하고 기술개발을 진행시켜, 국가의 취약성을 보완하는 기술의 실용화와 도입을 촉진하는 것이다.

DHS의 주요 임무는 미국에 대한 테러공격을 예방하고 국민을 보호하는 것이며, 이를 위해 △정보분석과 기반시설 보호 △화학·생물·방사능·핵 등에 대한 대응조치 △국경 및 수송부문 보안 △비상시 대처 및 대응조치 △연방 주 지방 정부 부서 및 민간부문과 공조 등 5가지 기능을 수행한다. 다음과 같은 구체적 조항이 HR 5005에 포함되어 있다[3].

- 정보기술, 금융 네트워크, 위성 등을 포함한 미국의 중요 자원 및 기반시설을 보호하기 위한 포괄적인 국가 계획을 작성함
- 컴퓨터 범죄를 수사하기 위한 도구, DNS 인증 등을 취급하는 기술분야의 기관을 설립함
- 컴퓨터 범죄의 방지에 임하는 주 경찰이나 지방 경찰을 지원하기 위한 도구의 개발자금을 제공함
- 중앙정보국(CIA), 국방부(DoD), 국가 안전 보장국(NSA)을 포함한 모든 정부기관에 대해, 미국의 기반시설의 취약성에 관한 정보를 DHS에 제공하는 것을 의무화함
- 개인 사생활보호 및 인권문제를 담당하는 부서를 설치해, DHS에 대해 개인정보의 이용, 수집, 개시에 있어서의 개인 사생활보호를 철저하게 함
- DHS는 중요한 정보 시스템을 운영하는 기업에 대해 기술 지원을 제공하여 취약성에 대해 경고함
- 지역사회가 정보 시스템 및 통신 네트워크에의 공격에 대처해 복구를 꾀하는 것을 지원하기 위해서 전국에서 자원봉사 단체를 조직함
- 시스템 및 취약성 분석, 전화망이나 인터넷 등의 기반시설의 취약성에 대해 시뮬레이션과 모델링을 수행하는 국토 안전 연구소(Homeland Security Institute)를 설치함

3. 사이버보호를 위한 국가전략

2003년 2월 14일, 미국정부는 '사이버보호를 위한 국가전략(The National Strategy to Secure Cyberspace, 이하 NSSC)'의 최종안을 발표하였다[4]. 2002년 9월에 발표한 전략의 초안을 중심으로 사회 각 분야의 의견을 수렴하여 일부 수정을 가한 것이다.

NSSC의 5개의 중점 항목은, △사이버공간의 보안 대책 시스템의 개발 △위협 및 취약성 경감 프로그램의 확립 △보안 트레이닝 및 보안 의식의 향상 △미 정부의 시스템의 보안 확보 △보안 문제 해결을 향한 국가간의 협력이다. 이 전략에서는 정부주도의 규제보다는 정부와 민간의 협력을 통해 인터넷 보안 문제를 해결하도록 호소하고 있다. 이 전략의 또 다른 핵심은 사이버공격에 대한 조기 경보와 방지이다. 인터넷의 상태를 감시하고 큰 피해를 야기할 수 있는 사이버공격과 바이러스의 창궐을 감지하기 위한 네트워크 운영센터의 설립을 요구하고 있다. 또한 부대조항의 계획을 지지하고 있는데, 주요 인터넷 노드가 마비될 경우를 대비해 재해 복구 계획의 설립을 포함하고 있다.

NSSC에는 DHS가 미국의 중대한 자원 및 기반시설의 안전확보에 대한 포괄적인 국가 계획을 책정하도록 정해져 있다. DHS는 긴급사태에의 대응, 정부 및 민간기업으로의 기술 지원, 각 정부기관의 대처현황에 대한 통계, 국토안전을 위한 연구의 실시 및 자금 제공도 담당한다. DHS 이외의 정부기관과 민간기관의 역할에 대해서는 다음과 같이 기술되어 있다.

- NIST: 연방기관과 민간기업에게 사이버보안에 대한 요구사항과 보안시스템의 성능 평가를 위한 지침과 도구를 제공함
- NSA: 암호화에 대한 중요한 연구 프로그램들을 운용함
- CERT-CC: 보안 침해 사고 대응, 경보 발령, 취약성과 침입 행위에 대한 추정 정보 등을 제공함

또한, 9.11 테러 직후의 대통령 행정명령을 통해 신설된 바 있는 대통령 주요 기반시설 보호위원회(President's Critical Infrastructure Protection Board)의 폐지가 이 전략을 통해 결정된 바 있다.

NSSC에서는 정부기관이 스스로 자신의 시스템을 보호하는 것으로 사이버보안의 실례를 보이기를 요구하고 있으나, 사설 기간시설 운영자들이 자신의 자산을 어떻게 보호해야 할 것인가에 대해서는 정리하지 못하고 있다. 주로 정부기관에서의 변화에 초

점을 맞추고 개별 영역을 위한 보안 권고안만을 담고 있으며, 민간기업이 행동을 취할 동기를 부여하지 못하고 있다. 정부기관에서도, 보안 업무는 명확하게 정의되거나 설명되지 않고 있다. 또한, 이를 뒷받침하고 운용되도록 해줄 전반적인 정치적 지지를 얻고 있지 못한 상황이다.

가. IAIP의 설립

HR 5005와 NSSC가 연이어 발표된 이후, DHS는 연구개발 활동에 중점을 맞춘 사이버보안 연구개발 센터인 정보분석 및 기반시설보호(Information Analysis Infrastructure Protection, 이하 IAIP) 부문을 설립하였다. IAIP는 △사이버보안에 관련된 연구 및 평가 촉진 △공공 및 사설기관과의 의견교환과 조율, 확고한 사이버 기반시설을 마련하기 위한 국가적·국제적 협력 촉진 △IAIP의 운용 상의 요구 지원 △참여 대학과의 교육 프로그램 개설을 촉진하기 위한 NSF와의 협력 등 네 가지 주요 기능과 역할을 담당한다. IAIP 부문이 설립되기 이전에는 사이버보안과 관련된 연구개발 활동이 과학 및 기술(Science & Technology) 부문에서 수행되어 왔으나, IAIP 부문 신설 이후에는 모두 IAIP 부문으로 이전되었다.

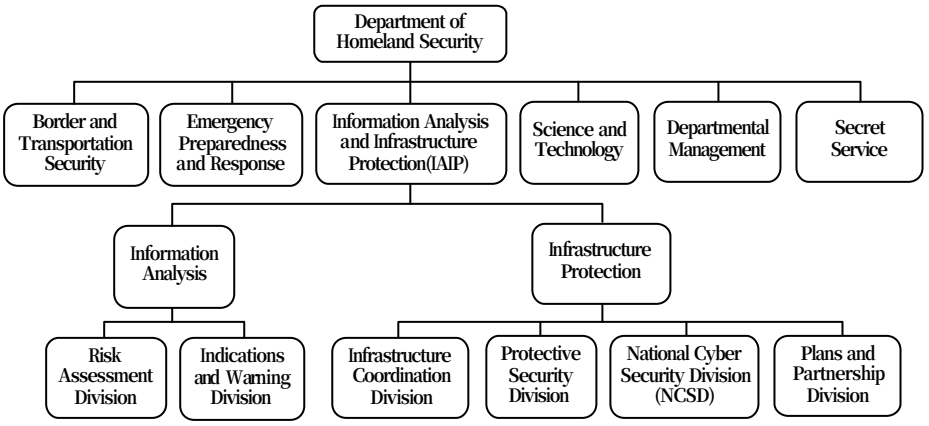
IAIP는 2004년에 주요 자산을 식별하고, 취약점을 파악하고, 위험 분석을 수행하는 데 초점을 두고 있다. 중요한 기반시설은 정부에 의해 소유되거나 운용되고 있지 않으며, 효과적인 보호를 위해 정부와 사설업체의 협력을 요구한다. 따라서, IAIP는 중요한 기반시설의 보안담당자, 소유자, 운용자와 함께 작업한다. 그리고, 2005년에는 주요 자산의 식별과 측량을 지속할 것으로 보인다. IAIP 산하의 팀들은 기반시설의 소유주와 운영자를 돕기 위해 현장을 방문하여 취약성을 식별하고 감소시키는 일을 수행해 나가며, 주요한 자산을 사이버 테러리스트의 공격으로부터 보호하기 위한 취약점 파악과 대처방안을 권고하는 역할을 지속할 것이다.

나. NCSD의 설립 및 운영

2003년 6월 6일, DHS는 모든 정부 부처의 정보보호 기능을 집중시키기 위해 범국가적 사이버보안 센터인 NCSD(National Cyber Security Division)를 설립하였다. 이 조직은, NSSC에 의거해 설립된 것으로 IAIP의 감독 아래 놓여진다.

NCSD는 DHS 창설 당시 DHS로 이관되었던 NIPC, NCS, CIAO, FedCIRC 등의 조직들의 기능을 총괄하고 있으며, 다음의 역할들을 담당하는 3개의 부문으로 나누어져 있다.

- 정부나 민간 부문의 사이버 자산의 취약성 파악 및 대응
- 인터넷상에서 발생하는 사건들의 검지 및 대응, 사이버공간에서의 잠재적 위협과 취약성 추적, 여러 협력 기관들과의 공조 등의 통합된 기능을



(그림 1) DHS의 조직 구성도

담당하는 CSTARC(Cyber Security Tracking, Analysis, and Response Center)에 대한 감독
- 관련 기관들과 공동으로 사이버보안 경고 발령 및 교육 프로그램 개발

2004년 1월, NCSD는 사이버보안 관련정보 및 경고를 국민에게 제공하는 National Cyber Alert System(이하 NCAS)의 운용을 시작하여, 미국의 일반 시민이나 기업 및 정부조직의 기술자에게 보안 관련문서나, 지침서, 위협에의 대응책 등을 제공하고 있다. NCAS는 컴퓨터의 취약성이나 보안상의 문제에 대해 분석 및 분류를 실시하며, 관리 및 운영은 NCSD와 민간기업의 협력 조직인 US-CERT가 담당하고 있다. NCAS가 제공하는 정보는 Cyber Security Tips, Cyber Security Bulletins, Cyber Security Alerts 등의 3종류로 다음과 같은 내용을 담고 있다.

- Cyber Security Tips: 일반의 컴퓨터 유저를 대상으로, 보안 문제의 대책 정보를 격주 단위로 송신함
- Cyber Security Bulletins: 보안 문제, 취약성의 정보, 피해 상황과 향후를 간파해, 리스크 관리 정보 등을 격주의 뉴스 메일로 보안 전문가에게 제공함
- Cyber Security Alerts: 신속한 대응이 필요한 보안 정보를 실시간으로 전달함

4. 네트워킹·정보기술 연구개발

미국에서는, 정보기술을 포함한 과학 및 공학 분야에 있어서 십여 개의 연방 정부기관이 연구개발 프로그램을 조성할 책임을 지니고 있다. 10여 년간 여러 연방 정부기관에서 실시되어온 정보기술 분야의 전체적인 정책방향은 '네트워킹 정보기술 연구개발(Networking and Information Technology Research and Development, 이하 NITRD)' 프로그램을 통해 살펴볼 수 있다.

2003년도 NITRD 보고서는 2002년도의 보고서와 비교해 내용면에서 크게 바뀐 부분은 없으며, 보고서에 기술된 사이버보안과 관련된 활동들을 살펴보면 다음과 같다[5],[6].

국방부(DoD) 산하 조직인 DARPA는 미국 국가안보에 해를 끼칠 수 있는 기술적인 위협에 대응하기 위해 다양한 프로그램들을 수행한다. 그 중에서도 Information Assurance and Survivability 프로그램에서는 사이버 공격에 대한 강력한 방벽을 구축하고 다양한 사이버 공격을 발견, 대응, 처리하기 위한 기술을 갖춘 지휘관을 육성하고 있다. 기초과학 연구를 주로 담당해 오던 NSF는 국토안보와 테러에 관련된 연구를 지원한다. 9.11 테러 이후의 임무를 재검토하고, 생화학적 위협과 사이버보안 등과 관련한 연구에 연방기금을 사용하며, 이 중에서 사이버보안 분야에 대해서는 국가적 사이버보안 연구 방향에서 문제를 파악하고 연구의 경향을 검토해 나가게 된다.

2004년도 NITRD 보고서에서는, 2002년 2월에 가동을 개시한 일본의 '지구 시뮬레이터(地球シミュレ-タ)'에 의해 지금까지 미국이 선도적 입지를 고수해 오던 최첨단 컴퓨팅(high-end computing) 분야에서의 우위성이 없어진 것과 같은 일련의 요인들로 인해 내용면에서 일부 변화가 있었다. 최첨단 컴퓨터 기술은 NITRD 정책뿐 아니라 국가 안전보장 정책에서도 불가결한 요건이므로, 이 기술의 재구축은 매우 중요한 과제로 생각되고 있다[7].

Ⅲ. 연구개발 투자 동향

과거 연방 정부의 연구개발 동향을 살펴보면, 연구개발 전략의 구성이 시대와 함께 변화하였고, 필요에 따라서는 국책의 우선순위의 변화를 반영해 왔다는 것을 알 수 있다. 이러한 국가의 우선 과제의 변화는 과학기술 분야의 각 기관에 대한 예산의 증감으로 나타난다. 예산관리국(OMB)에서 발표하는 국방부(DoD), 에너지부(DOE), 법무부(DOJ), 보건복지부(HHS), 항공우주국(NASA) 등의 20여 정부기관들에 할당된 정보기술 분야와 정보기술 보안분야에서의 지출액 합계를 나타낸 <표 1>을 살펴보

<표 1> 연방 정부 기관의 정보기술 및 정보기술 보안분야의 지출액 (단위: 10억 달러)

	FY 2001	FY 2002	FY 2003(예상)	FY 2004(예상)	FY 2005(예상)
정보기술	46.1	48.6	52.6	59.3	59.8
정보기술 보안	1.3	2.7	4.2	4.7	N/A
보안 비중	2.81%	5.56%	7.98%	7.93%	N/A

<자료>: 예산관리국

면, 9.11 테러 이후 정보기술 보안 분야의 비중이 2.81%에서 5.56% 수준으로 급증하여 정보기술 보안 분야에 적극적으로 투자가 이루어지고 있음을 알 수 있다.

그리고, 2003년부터 정보기술 분야의 지출액이 두드러지게 증가한 것은 2002년 말에 신설된 DHS에 대한 정보기술 분야의 예산 규모가 확대되었기 때문으로 보인다.

HR 3394의 발표로 인해 미국 정부는 대학들의 보안센터 설립과 연구비 보조를 위해 2003년부터 5년간 약 9억 달러를 지원하게 되었다. HR 3394에 대한 2003~2007년도 예산으로 인가된 액수는 항목별로 다음과 같다[8].

- Computer and Network Security Research: 암호기술, 사생활보호, 무선보안이나 지적 재산권의 침해를 포함한 사이버 범죄의 검지, 수사, 기소 등의 법집행 능력의 강화 등 보안과 관련된 9분야의 연구 보조금(2억 3,300만 달러)
- Computer and Network Security Research Centers: 컴퓨터 및 네트워크보안의 연구자나 전문가의 양적 증가와 질적 향상을 꾀하기 위한 컴퓨터 및 네트워크보안 연구센터의 설립(1억 4,400만 달러)
- Computer and Network Security Capacity Building: 대학들이 컴퓨터 및 네트워크보안에 관한 학사 및 석사 프로그램을 창설 개선하기 위한 보조금(9,500만 달러)
- Graduate Traineeships in Computer and Network Security Research: 컴퓨터 및 네트워크 보안 연구를 실시하는 대학원생을 위한 실습 프로그램의 개설(9,000만 달러)
- Cyber Security Faculty Development: 대학원생에 사이버보안으로 학위를 취득하게 하는 것에 의해 학술적 성과를 추구하는 것을 장려하기 위한 실습 프로그램(2,500만 달러)
- NIST Extramural Research: 컴퓨터시스템 보안 연구를 위한 Post-Doc 및 상급 연구자에게로의 연구 지원금(2억 7,500만 달러)
- Computer Security Review, Public Meetings, and Information: 컴퓨터보안, 사생활보호, 암호 등에 관한 새로운 논점 검토, 회의 소집, 보고서 발간(215만 달러)
- Intramural Security Research: 여러 구성요소로 이루어진 네트워크 컴퓨터의 보안 유지를 위한 연구, 실시간 컴퓨팅의 보안 능력 향상에 대한 연구, 컴퓨터시스템 보안의 개선방법에 관한 복수의 학술 영역에 걸치는 장기적 연구(3,200만 달러)
- National Academy of Sciences Study on Computer and Network Security in Critical Infrastructures: 하드웨어 및 소프트웨어의 구조적 취약성과 주요 기반시설의 상호의존성에 대한 기존의 연구와 관련된 자료를 재검토, 견고한 기반 네트워크의 보안을 위한 기술적 능력의 격차 파악 및 연구 우선순위나 요구사항에 대한 권고, 기타 컴퓨터 및 네트워크 보안의 중요한 요소를 재검토(70만 달러)

이상과 같이, HR 3394의 성립으로 인해 미국은 사이버보안에 관한 연방정부 지출을 기존의 연간 약 6천만 달러 수준으로부터 급격히 증가시켜, 연구개발과 인재육성 부문에 많은 노력을 기울이기 시작하였다.

한편 DHS 및 DHS의 산하 조직인 IAIP와 NCSD의 예산을 살펴보면, DHS의 경우 부처가 설립된 2003년을 기점으로 예산이 급증한 것을 알 수 있다. 증가된 예산은 다른 부처로부터 관련 프로그램의 예산이 이관되

기 이전인 2002년에 비해서 80% 가량 증가한 것인데, 이러한 증가의 원인은 DHS 내에 신설된 HSARPA의 예산 배정에서 기인한 것이다(<표 2> 참조).

IAIP의 경우에도, 부문이 설립된 2004년부터 편성된 금액이 급증하였다. IAIP가 설립되어 연방기관을 통한 기반시설 보호 활동을 조정하고, 테러로부터 국가의 기반시설에 대한 취약점을 줄이기 시작한 2004년에는 예산이 전년대비 350% 가량 대폭 증가하였으며, 2005년 예산은 9.11 테러 이전의 7배에 달하는 8억 6500만 달러를 요구하고 있다[9]. 특히, IAIP에 대한 예산 중에서 주요 기반시설을 감정하고 이러한 시설에서의 보안이 향상되는 것을 보장하기 위해 필요한 단계를 지원하는 부분에 5억 달러 이상이 할당되어 있다. IAIP 산하의 NCSD에 대한 재원은 2005년 예산에서 증가하여, 7980만 달러가 요청된 상태이다(<표 3> 참조).

<표 2> 2003~2007년도 HR 3394 예산 편성액 (단위: 100만 달러)

프로그램		FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	합계
NSF Research	Computer and Network Security Research	35	40	46	52	60	233
	Computer and Network Security Research Centers	12	24	36	36	36	144
	Computer and Network Security Capacity Building	15	20	20	20	20	95
	Community Colleges	1	1.25	1.25	1.25	1.25	6
	Graduate Traineeships in Computer and Network Security Research	10	20	20	20	20	90
	Cyber Security Faculty Development	5	5	5	5	5	25
NIST	NIST Extramural Research	25	40	55	70	85	275
	Computer Security Review, Public Meetings, and Information	1.06	1.09				2.15
	Intramural Security Research	6	6.2	6.4	6.6	6.8	32
	National Academy of Sciences Study on Computer and Network Security in Critical Infrastructures	0.7					0.7
합계		110.75	157.54	189.65	210.85	234.05	902.85

<자료>: GOP.gov

<표 3> DHS 및 산하 조직의 예산 편성액 (단위: 100만 달러)

	FY 2001	FY 2002	FY 2003(예상)	FY 2004(예상)	FY 2005(예상)
DHS	15,000	17,500	31,200	36,500	40,200
IAIP	108	153	185	834	865
NCSD				N/A	79.8

<자료>: DHS, 밑줄 친 금액은 조직이 통합 이관되기 이전의 각 세부 기관들의 예산 합계임

<표 4> NITRD 예산 편성액 (단위: 100만 달러)

	FY 2000	FY 2001	FY 2002	FY 2003(예상)	FY 2004(예상)
LSN	299.8	322.4	333.5	328.1	373.3
HCSS	92.0	163.1	132.2	142.3	128.1
기타 부문	1154.2	1442.9	1364.0	1505.6	1645.6
합계	1546.0	1928.4	1829.7	1976.0	2147.0

<자료>: 과학기술심의회

최근 기반시설의 안정성 강화에 우선 순위를 두고 있는 NITRD의 6대 기술 개발 분야 중에서, 사이버보안과 관련된 직접적인 연구가 수행되어 오고 있는 분야로는 대규모 네트워킹(Large Scale Networking, 이하 LSN)과 고신뢰 소프트웨어 및 시스템(High Confidence Software & Systems, 이하 HCSS) 부문이 있다. 그러나, <표 4>와 같이 최근 NITRD의 연구자금 조성의 추이를 살펴 보면, LSN과 HCSS 부문 모두에서 뚜렷한 증가세가 나타나고 있지는 않음을 알 수 있다. 이는 NITRD 보고서에서 대부분의 연구 프로그램이 사이버보안을 고려하여 수행되고 있다고 밝히고 있으나, 실제 사이버보안에 대한 집중적인 예산 편성은 부족했음을 알 수 있다.

Ⅳ. 결 론

사이버보안은 기반시설 보호의 중요한 요소 중 하나로, 사이버공격의 결과는 여러 기반시설을 통해 전파될 수 있으며 경우에 따라서는 경제에 위해를 줄 뿐만 아니라 공공 안전까지 위험하게 만든다. 테러의 집중적인 대상이 되었던 미국에서는 자국민에 대한 '안전'과 '자유'의 균형보다는 국토안보가 최우선적으로 고려되기에 이르렀고, 이를 위해 사이버보안 분야에서 전략적 정책수립과 연구개발을 촉진하고 있다.

미국의 사이버보안 전략에 대한 국가적인 추진 전략은 적극적인 대응 측면에서 높은 점수를 받을 수 있겠으나, 대부분의 정책에서 정부의 리더십이 제대로 발휘되고 있는 것인가에 대한 의문이 뒤따르고 있다. 규제를 마련한다고 하더라도 보안수준의 향상은 보장될 수 없으며 새로운 규제에 따른 비용의 증가만이 뒤따르게 된다. 따라서 미국 정부의 매년 증가되고 있는 사이버보안 분야의 투자액이 실효를 거두기 위해서는 주도적인 입장을 취하고 여러 부처들간의 협력을 이끌어내어야 할 것이다.

또한, 침해로 인해 유발되는 피해의 규모와 파장을 고려하면 주요 기반시설이 최우선시 되어야 하나, 사이버보안이 필요한 대상은 주요 정부 관리하의 기반시설 이외의 민간 부문이 양적으로 압도적이다. 다양한 정책을 통해 정부와 민간 부문이 얼마나 협력해 인터넷 보안을 확보해 나갈까를 강하게 밝히고 있으나, 민간 기업이 어떻게 자신의 시스템을 관리해 나가는가 하는 점에는 부족함이 느껴진다. 비록 미국 정부가 자신의 시스템의 보안을 확보하고 민간과 협력해 공공 인터넷 기반시설의 보안 개선에 임했다고 해도, 민간기업이 자신의 시스템의 보안에 허술했다면 전체적인 대처로서는 실패일 것이다. 따라서, 민간의 참여를 유도하는 것에서 그치지 말고 정책적 지원이 뒷받침 되어야 할 것이다.

아직 우리나라에서 사회 또는 경제불안을 초래한 사이버공격이 나타나진 않았으나, 미국을 포함한 세계 어느 곳에서라도 조만간 발생하더라도 이상하지 않을 만큼 급박한 상황에 놓여있다. 우리도 미국의 사례를 참고하여 우리의 사정에 적합한 구체적 대처 방안을 모색하고 실제로 적용해 보며, 잇따르는 문제점을 수정해나가는 작업을 조속히 시작하여야 할 것이다.

참 고 문 헌

[1] The White House, "National Strategy for Homeland Security," 2002. 7.

[2] House Committee on Science, "Summary of H.R. 3394-The Cyber Security Research and Development Act," 2001.

[3] Homeland Protection Institute, "Key CBR Technology-Related Provisions of House Bill HR5005," 2002.

[4] The White House, "The National Strategy to Secure Cyberspace," 2003. 2.

[5] National Science and Technology Council, "Supplement to the President's Budget for FY 2002," 2001.

[6] National Science and Technology Council, "FY 2003-Supplement to the Presidents' Budget," 2002. 7.

[7] National Science and Technology Council, "FY 2004-Supplement to the President's Budget," 2003.

[8] GOP.gov, "H.R. 3394-Cyber Security Research and Development Act," 2002.

[9] Office of Management and Budget, "Budget of the United States Government, Fiscal Year 2005," 2004.