전문가가 진단한 정보화법제도 쟁점과 과제- 2009-⑨

사이버테러 예방을 위한 법제도 개선방안

정준현(단국대학교 법과대학 교수)

목 차

제 1 장 서론 ····· 1

제 1 절 연구목적 ····· 1
제 2 절 연구범위 ····· 2

제 2 장 사이버테러와 문제점 ····· 4

제 1 절 사이버테러의 의의 ····· 4
제 2 절 사이버테러의 유형과 침해현황 ····· 16
제 3 절 몇가지 문제점 ····· 26

제 3 장 현행 대응법제와 문제점 ····· 28

제 1 절 개관 ····· 28
제 2 절 조직법상의 대응법제 ····· 29
제 3 절 작용법상의 대응법제 ····· 46
제 4 절 사견 ····· 57

제 4 장 주요외국의 입법례 ····· 59

제 1 절 오프라인 테러에 대한 국제동향 ····· 59
제 2 절 사이버테러와 관련한 주요국의 동향 ····· 63
제 3 절 시사점 ····· 75

제 5 장 맺는 말 ····· 79

<참고부록 : 2009년 사이버안보 법안> ····· 81

<참고문헌> ····· 110

표 목차

<표 1> 사이버테러형 범죄의 유형 ····· 19
<표 2> 사이버 범죄 발생 검거현황 ····· 20
<표 3> 사이버 공격 유형 기준 ····· 21
<표 4> 사이버 피해 유형 기준 ····· 22
<표 5> 사이버테러의 유형 ····· 23
<표 6> 2008년 공공기관별 침해사고 발생현황 ····· 24
<표 7> 2008년 민간부문 해킹사고 발생건수 ····· 25
<표 8> 국가기관별 대테러업무와 근거법제 ····· 40

그림 목차

<그림 1> 국가위기의 패러다임 변화 ····· 10
<그림 2> 1개의 개인 컴퓨터를 통한 사이버테러의 파급효과 ····· 17
<그림 3> 주요 국가를 대상으로 한 사이버공격 ····· 18
<그림 4> 현행 헌법상 국가안전보장의 체계 ····· 30
<그림 5> 사이버안전관리체계 ····· 35
<그림 6> 테러정보통합센터의 역할 ····· 37
<그림 7> 경찰의 비경찰화(행정경찰) ····· 52
<그림 8> 국토계획간 효력체계 ····· 56
<그림 9> 현행 정부조직상 경찰체제 ····· 58
<그림 10> 일본의 정보수집 평가체계도 ····· 73
<그림 11> 국가사이버위기관리법(안)의 주요내용 ····· 78

제1장 서론

제1절 연구목적

현대 정보화 사회는 인터넷을 기반으로 매체간의 융합을 통해 언제 어디에서나 개인에 관한 데이터를 수집·저장할 수 있는 유비쿼터스 컴퓨팅사회로 발전해가고 있으며, 이러한 기술적 기반을 복지사회의 이념과 연결할 경우에는 국민의 복지수요를 실시간으로 충족시켜 주는 순기능을 하는 반면, 개인정보의 오·남용을 통한 정보보유자의 개인감시 내지 개인테러 등의 위험과 함께 개인이나 사회 및 국가의 정보통신기반시설에 대한 의존도의 심화에 따라 정보통신망에 대한 테러가 특정 개인을 넘어서 전체 사회 내지 국가의 정상적인 기능의 마비로 이어질 위험 또한 상존하게 된다.

인간의 신경망과도 같은 정보통신망이 이러한 특성으로 인하여 향후의 사이버테러는 1·25 대란이나 7·7 DDoS공격 등 시간과 장소를 가리지 않고 상상하기 어려운 재난발생의 가능성을 내포(신경 뉴런스의 장애에 따른 전신마비의 위험)하고 있기 때문에 초공간적·초시간적 파급효과를 갖는 정보사회의 사이버테러에 대한 예방 및 대응체제의 입법적 구축 및 개선은 내부적인 국가·사회의 안정뿐만 아니라 국가의 대외적 안전을 위해서도 시급한 과제로 인식되고 있다.

이러한 이유로 미래 정보사회의 지속가능한 발전을 위해 사이버테러 발전양상에 능동적으로 대처하기 위한 선행조치로서 사이버테러의 개념

을 확정짓고 그에 상응하는 사이버테러의 예방과 발생된 사이버테러에 대한 대응의 조직법적 체계와 작용법상 체계를 검토하고 그 대안을 제시함으로써 국가사이버의 안전성을 담보할 필요가 있다.

제2절 연구의 범위

종래의 테러는 정치·신념(종교)·제도 등의 차이에 따른 반대세력의 제거를 위해 의도적이고 계획적으로 이루어진 결과 범죄의 단서를 추적하고 예측할 수 있는 요소를 어느 정도 탐지하는 것이 가능하였으나, 정보사회에서의 테러는 시소를 가리지 않고 호기심에 의해서도 이루어질 수 있고, 불순집단이나 적대국가의 치밀한 계획 하에 장기에 걸쳐 개인컴퓨터를 매개하여 드러나지 않는 상태로 사이버 테러가 자행될 수도 있는 결과 사이버테러는 그 예측이나 추적이 곤란하고, 정보화에 대한 국가·사회의 의존도가 높아질수록 그 파급효과 또한 예측하기 어려울 정도로 확산가능하다는 점에서 예방장치로서의 법제적 대응은 무엇보다도 중요하다.

다른 한편, 우리 헌법은 모든 국민의 인간으로서의 존엄과 가치 및 행복추구권을 보장하고 확인할 책무를 국가에 부여하는 한편(제10조), 정부를 구성하는 행정각부로 하여금 국가안전이 보장되고 질서가 유지되는 기반위에 적극적으로 공공복리를 실현하도록 의무지우고 있는 바(제37조), 정보화사회가 국민의 공적 및 개인적 수요를 실시간으로 충족하고자 하려는 의지가 크면 클 수록, 정보화에 대한 의존도가 크면 클수록, 정보통신망에 대한 부분적 침해조차도 전자정부의 국가기능 자체가 마비될 위험성을 안고 있다는 점에서 사이버테러에 대한 대응법제의 연구는 종

래의 질서유지차원에서의 규제가 아닌 국가의 위기관리 차원의 관점에서 검토되어야 한다.

이러한 연구의 목적을 위해 본고의 연구범위는 사이버테러의 개념 정립과 정립된 개념에 내포되는 보호법익 및 이를 보호하기 위한 현행 조직법제 및 작용법제의 현황과 문제점의 분석을 통한 법제개선방향의 한정하여 연구·검토를 수행하기로 한다.

제2장 사이버테러와 문제점

제1절 사이버테러의 의의

1. 전통적 테러

가. 전통적인 테러의 의의

본래 테러리즘은 정치 분야에서 폭력주의에 입각한 공포정치를 의미하는 것으로 등장하였다. 즉 정부 또는 소위 혁명단체에 의하여 조직적·집단적으로 행해지는 공포수단을 의미하는 것이었다. 그러나 오늘날에는 개인이나 단체가 정치·종교 기타 목적을 달성하기 위하여 행하는 폭력행위로까지 그 정의의 범위가 확대되었고, 이에 따라 형사법상 규제대상이 되는 테러범죄의 개념이 등장하게 되었다.

이 과제의 연구의 대상 및 범위를 확정하기 위해서는 먼저 테러범죄가 무엇인가에 관한 논의가 필요하다. 그러나 무엇이 테러범죄인지에 관해서는 관련 국가들의 상이한 이해관계나 시각에 따라 달리 이해될 수 있기 때문에 아직까지 테러범죄에 관하여 통일된 정의 없이, 개념을 정의하는 학자나 실무기관에 따라 또는 시대와 상황에 따라 각기 다양한 개념 정의가 있다.

예컨대, Thornton은 "폭력의 사용이나 그 위협을 수반하는 불법적인 수단에 의해 정치적 행동에 영향을 행사하려는 의도의 상징적인 행위"를

테러라고 하며,[1] Kaiser는 "정치적 권력투쟁의 폭력범적 형태"를 테러 범죄로 보았다.[2] 실무상으로는 미 중앙정보국(CIA)에서 "테러리즘이란 정치적 상징효과를 얻기 위한 폭력의 사용 또는 그 위협으로서 직접적인 피해자보다는 다수 대중에게 심리적인 충격을 가하려는 목적을 가진 것이며, 여기에는 국가 내에서 행하여지는 전복활동 또는 반란적 군사 활동을 모두 포함한다"고 정의하였으며[3], 국제형사경찰기구(ICPO) 결의에서는 "테러리즘이란 공포 또는 불안을 확산시켜 정치적인 목적을 달성하기 위해 계획된 조직집단에 의한 폭력적 범죄활동"이라고 규정하였다.[4]

우리나라에도 테러범죄에 관한 통일된 이론이나 법률적 정의조항은 없고, 훈령에서 규정하고 있는 것에 불과하다. 즉, 1982년 대통령훈령 제47호로 발하여지고 2008년 8월18일 대통령훈령 제223호로 일부 개정된 「국가대테러활동지침」 제2조에서는 "국가안보 또는 공공의 안전을 위태롭게 할 목적으로 행하는 ①국가 또는 국제기구를 대표하는 자 등의 살해·납치 등 「외교관 등 국제적 보호인물에 대한 범죄의 방지 및 처벌에 관한 협약」 제2조에 규정된 행위, ②국가 또는 국제기구 등에 대하여 작위·부작위를 강요할 목적의 인질억류·감금 등 「인질억류 방지에 관한 국제협약」 제1조에 규정된 행위, ③국가중요시설 또는 다중이 이용하는 시설·장비의 폭파 등 「폭탄테러행위의 억제를 위한 국제협약」 제2조에 규정된 행위, ④운항 중인 항공기의 납치·점거 등 「항공기의 불법납치 억제를 위한 협약」 제1조에 규정된 행위, ⑤운항 중인 항공기의 파괴, 운

---

1) T. P. Thornton, "Terror as a Weapon of Political Agitation", in H. Eckstein(ed.), Internal War : Problems and Approaches, 1964, p.73. 최인섭, "테러리즘의 실태에 관한 일 고찰," 국제법논총, 제6권, 1992, 35쪽에서 재인용.

2) G. Kaiser, Kriminologie : Eine Lehrbuch, 1988, S.658.

3) 국제문제조사연구소, 테러대책과 관련한 국내법상 미비점 검토, 1986, 15쪽.

4) 1986년 국제형사경찰기구(ICPO) 유고슬라비아 총회결의, "國際テロリズムの現狀と對策," 1989, 58쪽 참조.

항 중인 항공기의 안전에 위해를 줄 수 있는 항공시설의 파괴 등 「민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약」 제1조에 규정된 행위, ⑥국제민간항공에 사용되는 공항 내에서의 인명살상 또는 시설의 파괴 등 「1971년 9월 23일 몬트리올에서 채택된 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약을 보충하는 국제민간항공에 사용되는 공항에서의 불법적 폭력행위의 억제를 위한 의정서」 제2조에 규정된 행위, ⑦선박억류, 선박의 안전운항에 위해를 줄 수 있는 선박 또는 항해시설의 파괴 등 「항해의 안전에 대한 불법적 행위의 억제를 위한 협약」 제3조에 규정된 행위, ⑧해저에 고정된 플랫폼의 파괴 등 「대륙붕상에 소재한 고정플랫폼의 안전에 대한 불법적 행위의 억제를 위한 의정서」 제2조에 규정된 행위 및 ⑨핵물질을 이용한 인명살상 또는 핵물질의 절도·강탈 등 「핵물질의 방호에 관한 협약」 제7조에 규정된 행위"를 테러로 규정하고 있을 뿐[5] 별도의 법률적 정의규정은 존재하지 아니한 실정이다. 이와 관련하여 2001년 11월 26일 차관회의에서 의결되었으나 법률로 제정되지 아니한 "테러방지법(안) 제2조제1호에서도 테러의 보호법익을 국가안보 또는 외교관계 및 사회적 안정으로 규정하고 있는 유사한 정의규정을 두고 있다.

최근에는 정치적 목적보다는 경제적 이익에 집착하여 마약범죄와 연계하여 전개되는 마약테러범죄(Narco-Terrorism), 대규모 환경파괴를 위협하는 환경테러범죄(Environmental Terrorism), 컴퓨터 등을 이용한 정보·통신관련 테러범죄 등 새로운 형태의 테러범죄들이 등장하고 있다.

---

5) 현재의 대테러시스템은 법률이 없는 상태에서 1982년 대통령훈령 제47호에 의거한 '국가대테러 활동지침'에 기반하고 있다는 점에서 법률적 근거를 갖는 "테러방지법"의 제정이 시급한 실정이다. 현재, 해양경찰청 훈령 제696호인 「국가대테러활동 세부운영규칙」 제2조제1호에서도 동일한 개념정의조항을 두고 있다.

이렇듯 다양한 개념정의 가운데 공통된 요소들을 중심으로 테러를 이해하면 다음과 같이 정리할 수 있다.[6] 즉, 테러는 정치적, 종교적, 사회적 주장 등 일정한 목적을 위해(**목적지향성**), 생명이나 신체의 안전을 위협하는 폭력의 행사로서(**폭력성**), 충동적이거나 우발적이기 보다는 조직적으로 행하여지는(**조직성**) 결과 직접적인 범죄피해자뿐만 아니라 사회 전반에 대하여 공포 및 불안심리를 야기(**공포성**)하는 일련의 범죄행위를 의미한다고 하겠다.

나. 전통적 테러의 특성

앞에서 살펴본 바와 같이 테러는 목적에 있어 정치범죄와 관련되며,[7] 행위전략에 있어는 조직범죄와 유사한 면이 있고, 그 행위수단에 있어서는 폭력 범죄로서의 성격도 갖고 있으나, 테러는 이러한 범죄들과는 몇 가지 점에서 구별된다. 즉, 테러가 정치목적을 위해 행하여진다 하더라도 그 수법의 잔인성, 난폭성에서 정치범죄와는 구별되며, 조직적·계획적 범행이라는 측면에서는 조직범죄의 일면을 갖지만, 테러행위가 갖는 일정한 이념지향성을 볼 때 조직범죄와도 구별된다. 또한, 테러는 폭력범죄와도 구별되는 다음과 같은 특성을 갖고 있다.[10]

첫째, 동기 측면에서 폭력이 주로 개인적인 욕망에서 출발하나, 테러는 개인적인 동기보다는 이념적, 종교적, 민족적, 사회적 문제에서 기인

---

6) E. V. Badolato, Environmental Terrorism : A Case Study, Terrorism, vol. 14, 1991, 237-239 쪽 참조.

7) 이 때문에 국제법상 '정치범불인도 원칙'과 관련하여 테러범죄인의 인도에 관한 문제가 심각한 논란을 일으키고 있는 가운데, 국제협약으로 테러범죄의 정치범죄성을 부인하려는 노력이 있다. 波多野里望, "テロ犯人の引渡しをめぐる諸問題-ILA委員會の草案にそくして," 國際關係法の課題, 1987, 220-222 쪽 참조.

하는 경우가 많다. 둘째, 폭력의 경우 그 성공의 대가가 바로 범죄자에게 귀속되는데 비해, 테러는 범행에 성공한다 하더라도 그 효과는 행위자 개인에게 귀속되지 않고 소속단체나 이념을 같이하는 집단에 귀속되며 테러행위자의 희생은 순교자로 기억된다. 셋째, 테러의 궁극적인 목적과 테러대상 간에는 필연적 관련성을 갖지는 아니하나, 폭력의 경우에는 범행목적에 부합하는 범행대상을 선정하는 것이 보통이다. 넷째, 폭력의 경우 범죄의 실행에 의하여 범행의 목적이 달성되지만, 테러는 궁극적으로 표방하고 있는 목적 내지 정치적 주장의 달성을 위한 과정에 불과하다. 다섯째, 테러는 그 자체가 선전효과를 기대하는데 비해, 일반 폭력은 범죄사실이 알려지는 것을 기피하는 경향이 있다.

여섯째, 범죄 실행의 결의에 있어서 일반 폭력은 범행을 통한 이득과 그로 인한 위험을 比較衡量하여 결정하게 되는데 반하여 테러는 범행을 통해 달성하고자 하는 정치적 내지 이념적 이익과 범행에 수반되는 위험을 비교하여 결정한다. 끝으로, 범죄의 실행 방법이나 수단의 측면에서 일반 폭력은 가능한 최소한 침해를 통해 최대 효과를 노리는 것이 일반적인데 반하여 테러는 범행에 따른 손해정도를 불문하거나 혹은 그러한 손해의 극대화를 통해 정치적·이념적 목적달성에 최대의 효과를 줄 수 있는 수단을 선택하는 것이 일반적이다.

2. 사이버테러의 개념에 관한 논의

앞에서 살펴본 전통적 테러에 대한 개념을 전제로 컴퓨터 공격자의 의도에 관계없이 또는 공격자의 의도를 초과하여 특정 개인뿐만 아니라 사회전체 또는 국가의 기반 네트워킹 시스템에 장애를 야기할 수도 있는 온라인의 특성을 감안한 사이버테러[8]에 대한 개념을 별도로 정립할 필요

가 있다. 그 이유는 전통적인 테러에 대하여는 "정치적 목적으로 행하여지는 폭력을 수반한 각종 불법행위"로 그 공통점을 도출할 수 있지만, 사이버테러에 대하여는 일반적으로 받아들여지고 있는 정의도 현재 존재하지 않을 뿐 아니라 사이버공간의 특성을 고려하지 아니한 채 현실공간에서의 테러 개념을 그대로 도입할 수도 없기 때문이다.

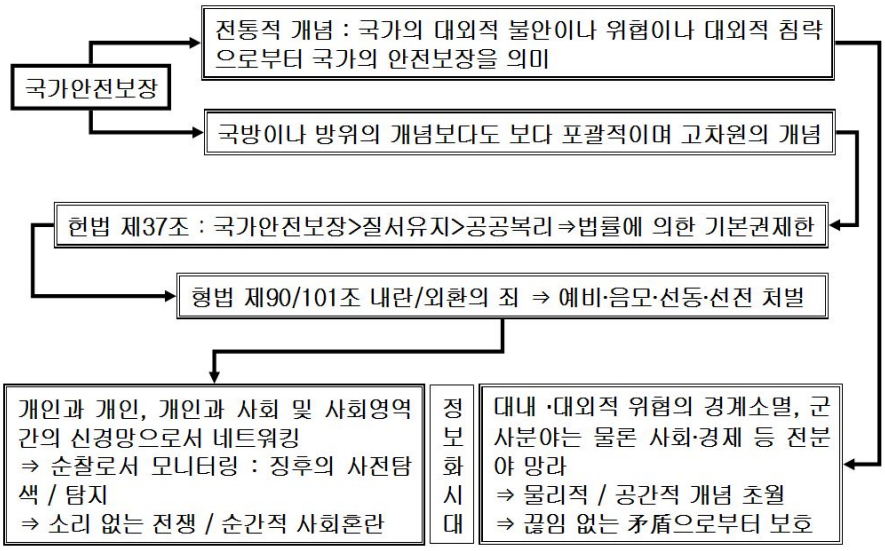
그렇다고 하여 단순히 컴퓨터 공격을 사이버테러로 규정짓는 것도 문제가 있다.[9] 왜냐하면, 아래의 <그림 1>에서 보는 바와 같이 정보화사회에 있어서의 사이버테러는 사건이 발생한 후 상당한 시간이 경과하지 아니하고는 컴퓨터 공격자의 의도, 동일인 여부 또는 정치적 동기나 목적을 확실하게 확정하기가 어렵기 때문이다.[10]

---

8) 테러리스트는 그들의 스타일상 사이버테러 보다는 현실의 물리적 공격을 선호한다면서 사이버테러에 대한 위협은 과장된 것이라고도 한다. "Cyber terror threat overrated", http://www.vnunet.com /news /1135876<2004.10.5. 접속>

9) 예컨대, 2004년 국가정보원이 발간한 백서의 목차 및 그 내용에 의하면 제1편 총론 제2장에서는 사이버침해 위협과 사례를 제시한 후 사이버테러에 대한 개념을 정의하지 아니한 채, 제2편 "제1장 국가정보보호체계" 제1절에서 사이버테러대응이라는 항목을 설정함으로써 "사이버위협 = 사이버테러"로 오인할 여지를 두고 있음은 큰 문제라고 할 것이다. 국가정보원, "2004 국가정보보호백서", 14-26쪽 및 35쪽 등 참조.

10) CRS Report for Congress(Oct. 17. 2003.), 4쪽 참조.



<그림 1> 국가위기의 패러다임 변화

그러나 사이버테러의 개념정의를 논의하기 위해 논의되고 있는 다음의 몇 가지의 개념을 참조해볼 필요는 있다. 첫째, 미국법전 제22권 제2656조에서는 테러리즘을 “통상 대중에게 영향을 미칠 의도로 하위 민족단체나 비밀결사에 의해 비전투원을 목표를 하여 범하여지는 계획적이고 정치적 동기를 가진 범행”으로 개념을 정의하고 있고, 국제테러는 한 국가 이상의 국민이나 영토와 관련이 있는 테러를 의미하는 것으로 이해되고 있다는 점이다. 이 경우 테러리스트 집단은 국제테러를 실행하는 집단이나 그 하부집단을 의미하게 된다.[11] 이와 관련하여, 미국의 국토안보부(The Department of Homeland Security) 내에 설치되어 있는 국가기간시설보호센터(NIPC)는 사이버 테러리즘을 “정부를 위협하여 정부정

11) 미국 정부는 1983년 이래로 테러리즘에 대한 이러한 개념정의를 채택하여 사용하고 있다. Patterns of Global Terrorism, 2003, <http: // www. state.gov/s/ct/rls/pgtrpt/ 2001/ html/ 10220.htm>.

책을 변경시킬 목적으로 컴퓨터를 통하여 폭력, 사망, 파괴를 초래하여 공포감을 생기도록 계획된 범죄행위"[12]로 개념을 정의하기도 한다.

둘째로, 정보화 사회가 고도화되면 될 수록 다중이 접하게 되는 공공시설의 통신기반 의존도는 커질 수밖에 없고 그만큼 정보화가 고도화된 사회는 곳곳에 전자적 아킬레스건(Electronic Achilles′ Heel)을 가질 수밖에 없다. 이러한 점에서 적대적인 국가나 세력이 이들 취약성을 악용하여 부실한 컴퓨터 네트워크에 침입하거나 주요기능을 와해시키거나 전복시키고자 획책할 것임을 상정할 수 있다. 따라서 사이버테러의 전제는 국가 주요기관 시설의 운용은 컴퓨터 네트워크에 의존할 수밖에 없고 그 의존도는 향후 더욱 점증하고 새로운 취약점도 발생할 것이라는 점에 착안해야 할 것이고, 이러한 착안점에서 출발할 때 사이버테러는 "에너지, 운송 및 정부기능 등 중대한 국가기간시설을 마비시키거나 정부나 일반대중을 협박 또는 강압하기 위해 컴퓨터 네트워크 도구를 사용하는 행위"[13][14]를 의미하는 것으로 새겨야 한다는 입장이다.

셋째로, 보안전문가의 보고서에 의하면[15] 컴퓨터의 공격이 물리적 테러리즘행위에 비견하는 파괴적 효과와 공포의 효과가 잠재해 있다면 사이버테러로 보아야 한다고 하면서, 이러한 효과의 엄격성을 전제로 사이버테러가 일정한 범위에 제한되어야 하겠지만 사망, 부상, 정전의 확산,

---

12) 2002 Director of NIPC. Scott Berinato, March 15, 2002, The Truth About Cyber terrorism, CIO.

13) James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber threats", CSIS, 2002.1쪽 참조.

14) 사이버테러라 함은 인터넷을 통하여 정부 등의 컴퓨터시스템에 침입하여 데이터를 파괴하는 등의 수단으로 사회를 마비시키는 테러행위라 하고 그 공격대상은 전기, 가스, 수도, 교통망, 의료기관 및 원자력발전소 등 사회의 중요기반시설이다.(www.urban.meijo-u.ac.jr/zchihru/ozawa001.file/frame.htm. 2004.11.24.접속)

15) Dorothy Denning, November 2001, Is Cyber War Next?.

비행기충돌, 물의 오염으로 이어지거나 경제에 대한 신뢰기반을 위축시키는 컴퓨터공격 또한 사이버 테러리즘으로 규정하여야 한다고 한다. 이러한 입장은 오늘날 인터넷이 생활의 중요한 터전이 됨에 따라 사이버공간은 더 이상 특정한 네티즌 집단에 한정되지 않고 디지털 소외층인 일반인을 포함한 일반 공중을 위한 생활의 터전이 되고 있는 점을 감안할 때, 인터넷상 공포감(Panic)을 확산하고 매체에 대한 불신을 야기할 정도의 사이버공격은 사회적 혼란을 야기할 우려가 있는 행위라는 차원에서 사이버테러리즘으로 간주하여야 한다는 견해와 흐름을 같이 하는 것이라고 할 것이다.

요컨대, 사이버테러 개념의 필요성과 관련하여서는 포괄적 사이버공격은 폭발물이나 생화학무기 또는 핵폭탄과 달리 단순한 생활상의 성가심(Annoyance)을 양산하는 것에 불과하다는 이유로 불필요하다는 견해도 있지만, 효과면에서 컴퓨터공격이 일반범죄로서 행하여진 경우라도 전통적인 테러에 상응하는 공포감을 조성하기에 충분한 결과를 야기하는 경우 또는 인터넷기반의 면에서 볼 때, 불법적 또는 정치적 동기에서 행하여진 컴퓨터공격이 정부나 대중을 협박하여 정치적 목적을 조성한다거나 심각한 경제적 피해를 야기한다면 사이버테러로 관념하여야 한다는 데에는 의견을 같이 하는 점[16]에 주목할 필요가 있다.

3. 현행 입법태도

현행법상 “사이버테러”에 대해 별도의 개념을 정의하지 아니한 채 그

16) John Rollins/Clay Wilson, "Terrorist Capabilities for Cyberattack:Overview and Policy Issues", CRS Report for Congress, Order Code RL33123, 2007.1. 22. CRS-3 참조.

용어만 답습하고 있는 예로는 “사이버테러신고·상담용 전화번호를 118”로 한다는 「전기통신사업법시행령」 제53조제3항제4호와 “수사국에 사이버테러대응센터를 둔다”는 「경찰청과 그 소속기관 직제 시행규칙」 제9조제1항을 들 수 있는바, 이와 같이 개념정의 없이 소관 전화번호나 업무를 분장한다는 것은 경계가 없는 상태의 업무분장으로 궁극적으로는 책임자가 존재하지 아니하고 이를 국가 전체적으로 통일성 있게 대응할 수 있는 추진체계의 부존재를 결과할 수도 있다는 비난을 피할 수 없을 것이다.

그밖에 사이버테러라는 용어를 사용하지는 않지만 그 범주에 속하는 것으로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상의 “침해사고”나 「정보통신기반보호법」 상의 “전자적 침해행위”를 들 수 있다. 전자에 대하여는 “해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태”(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제7호)로, 후자에 대하여는 “정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위”(「정보통신기반보호법」 제2조제2호)로 각각 정의하고 있지만, 단어의 배열은 다르지만 동일한 의미를 가질 뿐만 아니라 그 보호법익 “정보사회의 안전성”이라는 공통점을 가지고 있어 입법적인 정비가 필요하다.

아울러, 사이버테러는 사회의 안전성만을 보호하는 것이 아니라 헌법상 국가기관의 마비를 통해 형법 제87조의 내란에 준하거나 동등한 사태를 야기할 수도 있다는 점에서 국가사무의 정상적인 기능에 대한 침해를

포함하는 개념이 되어야 할 것이고, 추가적으로는 사이버공격의 비정형성을 고려할 때 그 도구를 위의 규정과 같이 예시하면서 그 결과에 있어서는 사회 또는 국가의 정상적인 기능의 마비를 초래하는 일체의 불법행위로 설정함이 타당하다.[17]

4. 사이버테러에 대한 법적 정의개념의 제안

전술한 개념을 종합해보면, 사이버테러는 좁게는 "특정한 집단이나 개인이 자신의 정치적 목적이나 이념을 관철시킬 목적으로 대중, 정부요인 또는 정부기관이나 공공기반시설 등에 대해 위협을 가할 수 있는 무기로서의 정보통신망 또는 그 기반시설에 대한 일체의 공격적 행위"로 파악할 수 있다.[18]

넓은 의미에서의 사이버테러는 오늘날 정보통신기반이 정보화사회의 아킬레스 건으로 기능한다는 점에 착안하여 정보통신기반 시스템 전반에 대해 장애를 초래하는 물리적 또는 소프트웨어적 불법행위 일체로서 전기, 가스, 수도, 교통망, 의료기관 및 원자력발전소 등 국가나 사회의 중요 기반시설 뿐만 아니라 개인을 대상으로 네트워크 시스템에 침입하여 데이터를 파괴하는 등의 수단으로 개인을 포함하여 사회 및 국가를 마비시킬 수 있는 잠재적인 행위를 포함하는 사이버 테러행위로 개념을 정의할

17) 「국가사이버위기관리법(안)」 제2조제3호에서는 "사이버공격으로 인한 사이버경보의 심각단계에 도달한 상태에서 정보통신망의 장애 또는 마비나 정보의 절취·훼손 등의 피해가 대규모로 발생하여 국가·사회기능에 심각한 지장을 초래하거나 피해가 전국적으로 확산될 가능성이 현저한 경우"를 "사이버위기"로 개념정의하고 있음에 주목할 필요가 있다.

18) 이와 관련 중국의 경우에는 '제4군' 사이버 부대를 창설하여 "點穴(급소)전략"이란 이름으로 해킹전술을 개발하고 있음은 주지하는 바이다. 중앙일보, "중국 '제4군' 사이버부대 유학파 등 2000명 활약",중앙일보, 2004. 7. 16. 3쪽.

필요가 있다고 할 것이다.[19]

요컨대, 사이버테러의 개념정의에 있어서는 다음의 사항이 고려되어야 한다. 즉, 인터넷이 제공하는 가상공간이 갖는 특성상 특정 개인에 대한 컴퓨터공격이 사회전체의 법익을 침해할 수도 있고, 이러한 공격은 개인이나 특정 집단에 의해서 야기될 수 있다는 점, 데이터간의 막힘없는 네트워킹을 특징으로 하는 유비쿼터스 컴퓨팅 사회에 있어서는 부분사회의 불안감일지라도 그 전파속도 및 파급효과가 매우 크기 때문에 국가적 위기로 전이될 수 있기 때문에 사회일반인의 건전한 사이버이용관계를 보장해야 한다는 점 및 그렇기 때문에 사회 및 국가보호의 차원에서 매개자로서 일반 개인을 포함하되 개인적 보호법익에 대한 테러는 제외하여야 한다는 점 등을 고려하여 입법적으로는 사이버 테러의 개념을 오프라인의 경우와 달리 사회 내지 국가전체에 대한 공포감의 조성이라는 관점에서 다소 폭넓게 정립할 필요성이 있다.

이러한 관점을 정리해보면, 첫째, 보호법익은 정보통신망을 매개로 하는 사회 및 국가기관을 포함하는 공공기관의 정상적인 기능으로 하여야 할 것이다. 둘째, 행위의 주체는 사회적 또는 국가적 공포감을 조성할 목적을 가진 개인 또는 단체를 대상으로 하여야 한다. 셋째, 수단에 대한 예측가능성을 갖기 어렵다는 점에서 예시적으로 하되 국가 및 사회의 정상적인 기능을 해치는 결과에 대해 상당인과관계가 있는 것으로 한다. 이러한 요소를 포섭하여 개념정의를 해보면, 사이버테러라 함은 “정보통신이용자에 대해 정보통신을 매개로 하는 각종 서비스나 국가기관이나 공공기관의 정상적인 사무수행의 안전성을 해칠 목적으로 사이버를 매개로

19) http://www.urban.meijo-u.ac.jr/zchihru/ozawa001.file/frame.htm. <2004.11.24. 접속>

하여 이루어지는 일체의 불법행위(Act of Vandalization of Cyber)"로 개념을 정립할 수 있다.[20]

이러한 개념의 정립을 토대로 사이버테러의 침해의 심각성에 따라 사회적 및 국가적 테러로 개념을 재분류하고 그 법익에 따라 국가안전을 사무로 하는 기관과 사회안전을 사무로 하는 국가기관에 각각 그 기능을 분장하는 것이 타당할 것으로 생각된다.[21]

제2절 사이버테러의 유형과 침해현황

1. 정보사회에 있어서 사이버테러 전망

---

20) 공성진 의원안에 의하면, "정치적·이념적·인종적·종교적·민족적 또는 그밖에 유사한 목적을 추구하거나 그 주의 또는 주장을 널리 알리기 위하여 계획적으로 테러단체 또는 그 구성원이 행하는 다음 각목의 폭력행위"로, 조성태 의원안에 의하면, "다음 각목의 어느 하나에 해당하는 행위로서 국가안보 또는 공공의 안전을 위태롭게 하는 행위"로 그리고 정형근 의원안에 의하면, "동기나 목적을 불문하고 유엔이 지정한 테러단체와 연계하여 계획적으로 실행되는 범죄행위로서 국가안보 또는 공공의 안전을 위태롭게 하려는 다음 각목의 행위"로 규정하고 있는바(각 안의 특성에 대하여는 강대출, "테러방지법안에 관한 입법적 검토", 「대테러정책연구논총」, 2009.1. 59쪽 이하 참조), 공성진 안은 사이버테러의 현실과 합치되지 아니하는 목적을 지나치게 세부적으로 나열하고 법익에 침묵하고 있는 점에서 취할 바가 되지 아니하고 그 밖의 두 개의 안은 국가안보 또는 공공의 안전을 보호법익으로 한 점에서 공감을 가질 수 있으나 행위를 오프라인 테러의 개념에 치우친 나머지 열거하고 있어 사이버공격의 다양성을 외면하여 바람직하지 않다.

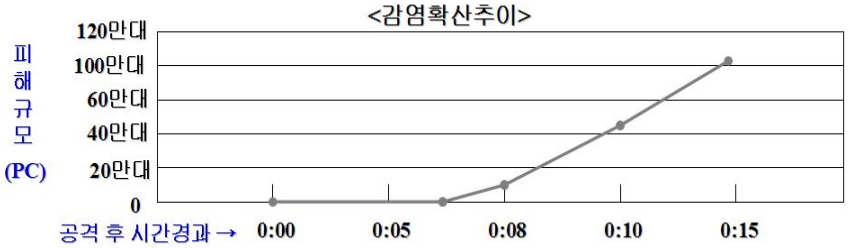
21) 이와 관련하여 사이버테러와 사이버범죄를 구별할 필요가 있는가에 대하여는 의문이다. 실제로 사이버 테러리스트는 다국적 범죄조직에 의하여 개발된 사이버 범죄기술을 이용하기 때문에 사이버 범죄공격이 단순한 사이트 범죄공격인지 아니면 국제 테러집단에 의한 사이버테러 탐지공격인지 여부를 판단하기가 매우 어렵다고 사이버 범죄공격이 사이버테러 탐지공격으로 보도되는 일도 왕왕 있다고 한다. http://www.acap보안. com/html/c_terror.html. <2004.11.7. 접속>

정보사회에 있어서 특정개인에 대한 것이든 사회에 대한 것이든 간에 컴퓨터망을 이용하여 데이터베이스화되어 있는 군사, 행정, 인적 자원 등 국가적인 주요 정보를 파괴하거나 국가기관의 정상적인 기능을 저해하는 사이버테러의 양상을 띨 것으로 예상되며, 국가간의 분쟁 또한 군사시설에 대한 직접적이고 물리적인 타격보다는 정부기간통신망, 군사통신 또는 금융망에 대한 사이버테러 양상을 띨 가능성이 높다. 특히, 사이버를 통한 공격은 아래의 <그림 1>에서 보는 바와 같은 파급효과를 통해 물리적 전쟁이나 테러와는 달리 언제 어디에서나 인적 자원의 낭비 없이 조용하면서도 그 파급효과는 핵공격에 상응한다는 점에서 향후의 전쟁이나 테러는 <그림 2>에서 보는 바와 같이 국지적이 아니라 전지구촌을 상대로 이루어질 것으로 전망된다.

- 가상시나리오 -

• 1개의 PC를 숙주로 하여 공격을 시작한 웜 바이러스가 자동탐색 및 공격기능을 이용해 15분만에 백만대의 PC를 감염시키고 공격대상국가의 사회혼란 초래가능

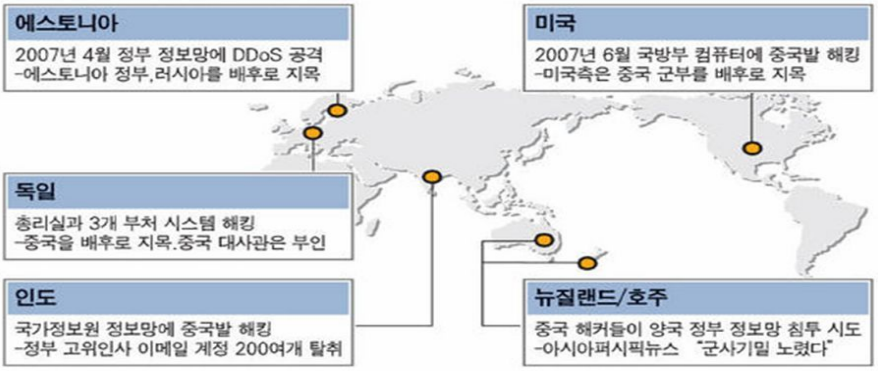
<감염확산추이>



• 15분 후 피해상황

- 컴퓨터시스템 파괴 : CIH
- 네트웍 과부하로 통신장애
- 특정사이트에 대한 분산서비스 거부 공격 : Code Rode
- 항공/에너지/수자원/철도 등 디지털데이터를 사용하는 국가 및 사회주요시설의 정보장애 발생

<그림 2> 1개의 개인 컴퓨터를 통한 사이버테러의 파급효과



출처 : http://www.hankyung.com/news/app/newsview.php?aid= 2007113078561

<그림 3> 주요 국가를 대상으로 한 사이버공격

2. 기관별 사이버테러 유형

현행법상 사이버테러에 근접하는 개념으로서 “침해사고” 내지 “전자적 침해”의 종류로는 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의한 공격 등이 열거되고 있고, 국가기관에 따라서 그 유형과 수단에 대해 아래와 같이 분류를 달리하고 있는바, 그 이유는 입법적 정의의 부재에서 비롯하며, 이로 인하여 겪게 되는 것은 국가기관간의 시각차이로 인한 사회와 일반국민의 혼란이라고 할 것이다.

가. 경찰청

경찰청은 사이버범죄를 아래의 <표 1>에서와 같이 사이버테러형 범

죄와 일반사이버범죄로 구별하고[22], 전자는 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 있는 정보통신망 자체를 통해 이루어지는 것으로 정의함으로써「정보통신기반보호법」상의 "전자적 침해행위" 내지 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상의 "침해사고"에 포섭되는 반면, 후자는 전자상거래 사기, 프로그램 불법복제, 불법사이트 운영, 개인정보침해 등과 같이 사이버공간이 범죄의 수단으로 이용된 유형으로 정의하여 주로 형법상의 사기죄나 지적재산권에 대한 침해 및 개인의 명예 등을 그 대상으로 하여 구별하고 있다.

22) http://www.netan.go.kr/ <2009.9.3. 접속>

<표 1> 사이버테러형 범죄의 유형

단순침입	**단순침입**	정당한 ① 접근권한 없이 또는 허용된 접근권한을 초과하여 ② 정보통신망에 침입 하는 것
	사용자도용	정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 것
	파일 등 삭제와 자료유출	정보통신망에 침입한 자가 행한 2차적 행위의 결과로, 일반적으로 정보통신망에 대한 침입행위가 이루어진 뒤에 가능함
	폭탄메일	서버가 감당할 수 없는 양의 메일을 일시에 보내거나 메일내부에 수신자 컴퓨터에 과부하를 일으킬 실행코드 등을 송신(서비스공격 유형)
악성프로그램	**트로이목마**	프로그램에 미리 입력된 기능을 능동적으로 수행, 외부 해커에게 정보를 유출하거나 원격제어기능 수행/ 유용한 유틸리티로 위장/확산(감염사실 알아채기 어려움)
	인터넷 웜	시스템 과부하를 목적 이메일 첨부파일 등 인터넷 이용하여 확산. 확산 시 정상파일에 이메일에 첨부되기 때문에 개인정보 유출의 위험 내포
	스파이웨어	공개프로그램, 셰어웨어, 평가판 등의 무료 프로그램에 탑재되어 정보를 유출시키는 기능이 있는 모든 종류의 프로그램

아래의 <표 2> 최근 5년의 사이버범죄 현황에 의하면, 사이버테러형 범죄보다는 일반사이버범죄가 2배 이상 증가하고 있어 문제의 심각성을 간과할 수 있으나 일반범죄 능력은 사이버 테러능력으로 발전할 수 있다는 점에 경각심을 가질 필요가 있다.

<표 2> 사이버 범죄 발생 검거현황

구분 / 연도	총계		사이버테러형 범죄		일반사이버범죄	
	발생	검거	발생	검거	발생	검거
2004	77,099	63,384	15,390	10,339	61,709	52,391
2005	88,731	72,421	21,389	15,874	67,342	56,547
2006	82,186	70,545	20,186	15,979	62,000	54,566
2007	88,847	78,890	17,671	13,037	71,176	64,853
2008	136,819	122,227	20,077	16,953	117,742	105,274

출처 : http://www.netan.go.kr/)

나. 국가사이버안전센터

국가사이버안전센터 역시 사이버테러에 대한 개념을 별도로 정하지 아니한 채 2004년 7월부터 사이버 공격 및 피해 유형을 최근의 사고 유형에 맞추어 아래의 <표 3>에서 보는 바와 같이 사이버 공격 유형 기준을 웜·바이러스, 스캐닝, 취약점이용, 기타로 분류하고 있다.

<표 3> 사이버 공격 유형 기준

대분류	내용	유형 예시
웜 / 바이러스	시스템에 침투하여 악성코드를 삽입/ 시스템 파괴와 확산을 시도 하는 공격	웜·바이러스, 트로이목마, AD-ware, Spyware 등
스캐닝	해킹하기 전 대상 네트워크나 시스템의 취약점 수집 작업, DoS 공격	각종 포트 스캐닝, DoS 취약점 이용
취약점 이용	S/W 오류, 설정상 오류, 프로그램 취약점 등을 악용한 공격이나 취약점을 이용한 권한 획득	Buffer Overflow, ActiveX 및 Java 악성 코드, SQL 주입, 권한 설정 취약, 보안설정 오류 등
기타	시스템 공격목적이 아닌 시위나 사기, 명예훼손 등을 위한 공격으로 위 항목에 정의되지 않는 공격 유형과 공격시도가 없는 상태	홈페이지 접속 장애, 사이버 시위, 쇼핑몰 사기, 물리적 보안 취약, 사회공학 등

출처 : 국가사이버안전센터, Monthly 사이버시큐리티 2004.7, 18면

피해유형을 기준으로 할 경우에는 아래의 <표 4>에서 보는 바와 같이 경유지 이용, 웜·바이러스피해, 홈페이지 변조, 자료훼손 및 유출, 단순 침입시도, 기타로 분류할 뿐이 결과적으로는 정보통신기반보호법」상의 “전자적 침해행위” 내지 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상의 “침해사고”에 따른 분류에 의존하고 있는 것으로 추정된다.

<표 4> 사이버 피해 유형 기준

대분류	내용	유형 예시
경유지 이용	해킹 피해를 당한 뒤 다른 사이트를 공격하는 경유지로 활용되는 피해	해킹 경유지, 스팸 릴레이
웜/ 바이러스	웜·바이러스 감염시도 및 전이	감염시도, 감염 후 전이, 시스템 장애, 네트워크 부하 등
홈페이지 변조	홈페이지의 메인 페이지가 변조되거나 사용하지 않는 페이지가 삽입되는 피해	홈페이지 변조, 삽입, 삭제
자료훼손 및 유출	FTP, 서버 및 PC 등의 권한이나 공유 설정의 취약으로 자료가 변조, 삭제, 유출	자료삭제, 자료유출, 자료변조, 자료열람, 백도어, 루트킷
단순침입 시도	스캐닝 기법 등으로 시스템이나 네트워크의 취약점 점검 및 계정추측 등의 침입시도만 이루어진 피해	패스워드 추측 시도, 침투시도, 스캐닝
기타	사이버상 시위나 단순사기, 명예훼손 등의 사건이나 위 항목에 정의되지 않는 피해유형	-

다. 기타

참고로, 미국의 국립표준기술연구소가 권고하는 컴퓨터 보안사고처리 가이드 초안(DRAFT Computer Security Incident Handling Guide)에서 분류한 컴퓨터 보안사고의 유형은 아래의 <표 5>와 같이 서비스거부, 악성코드, 웜·바이러스, 비인가자접근, 강탈, 협박 등으로 구별하고 있다.

<표 5> 사이버테러의 유형

분 류	상 태
서비스거부	특별 제작된 패킷을 웹서버에 보내 정상적인 서비스를 방해
악성코드-웜	웜 조직 내 수백 개의 컴퓨터를 빠르게 감염
악성코드 - 바이러스	신종바이러스가 인터넷 전체에 확산
인가 없는 접근	시스템의 패스워드에 접근하기 위한 공격툴(Exploit tool) 실행
강탈	시스템 관리자 권한을 취득 후 취득방법 공개 위협
부적절한 이용	파일공유 서비스를 통해 불법 복제된 소프트웨어를 타인에게 제공
협박	이메일을 통한 타인 위협

출처 : 국가사이버안전센터, Monthly 사이버시큐리티 2004.7, 19면

3. 침해현황

가. 국가·공공부문

2009년의 국가정보보호백서에 의하면, 2008년 국가사이버안전센터에서 접수·처리한 침해사고를 분석한 결과 아래의 <표 6>에서 보는 바와 같이 공공부문 침해사고는 전년 7,588건 대비 4.96%가 증가한 7,965건이 발생하였다. 국가·공공부문 침해사고 유형들을 살펴보면 전년과 같이 웜·바이러스 감염 유형이 대부분의 건수를 차지하고 있으며, 전체 침해사고의 71%를 차지하고 있다. 이러한 결과에 비추어 볼 때 웜·바이러스에

의한 사이버공격의 수법은 향후 보다 치밀해지고 포괄적으로 행하여질 가능성이 높을 것으로 예상된다.

<표 6> 2008년 공공기관별 침해사고 발생현황

구분	합계	웜/바이러스 감염	경유지 악용	홈페이지 변조	자료훼손 및 유출	기타
국가기관	1,187	813	67	23	204	80
지자체	3,067	2,443	224	64	283	53
연구소	818	698	31	6	65	18
교육기관	1,867	1,210	454	82	73	48
산하기관	672	418	104	36	92	22
기타	354	73	104	17	72	88
합계	7,965	5,655	984	228	789	309

출처 : 2009국가정보보호백서 (단위 : 건)

나. 민간부문

2009년의 국가정보보호백서에 의하면, 2008년 한국정보보호진흥원에서 접수·처리한 민간부문 침해사고 통계를 분석한 결과 해킹사고 접수·처리는 총 15,940건으로 2007년 21,732건에 비하여 26.7% 감소한 것으로 드러났다. 침해사고유형별로는 스팸릴레이, 단순침입시도, 홈페이지변조가 전년대비 44.4%, 26.4%, 3.9% 감소하였으며, 피싱경유지, 기타 해킹은 각각 6.2%, 23.2% 증가한 것으로 나타났다.[23)]

<표 7> 2008년 민간부문 해킹사고 발생건수

구분	'07 총계	2008년												'08 합계
		1	2	3	4	5	6	7	8	9	10	11	12	
스팸 릴레이	11,668	592	597	530	565	636	574	464	423	631	697	474	307	6,490
피싱 경유지	1,095	88	117	110	94	116	131	76	62	111	109	74	75	1,163
단순침입 시도	4,316	386	289	350	291	206	226	247	240	202	261	242	235	3,175
기타해킹	2,360	239	226	235	227	231	218	242	220	228	254	255	333	2,908
홈페이지 변조	2,293	47	287	135	85	281	369	107	245	139	132	200	177	2,204
합계	21,732	1,352	1,516	1,360	1,262	1,470	1,518	1,136	1,190	1,311	1,453	1,245	1,127	15,940

출처 :2009 국가정보보호백서

4. 시사점

사회 또는 국가의 정상적인 기능을 방해하여 사회의 혼란을 야기할 수 있는 공공기관에 대한 사이버침해사고 건수는 2008년을 기준으로 총 7,965건인데 반하여, 주로 개인의 인격침해나 재산권침해를 목적으로 하고 있는 민간부문의 침해사고는 21,732건으로 약 3배에 달하고 있다. 이는 앞의 <표 5>에 의한 사이버테러형 범죄 발생건수(2007년 17,671건; 2008년 20,077건)가 일반사이버범죄의 발생건수(2007년 71,176건 ; 2008년 117,742건)에 비해 약 1/4 내지 1/5 수준에 머물고 있어 국가정보백서와

23) 국가정보원・방송통신위원회, 「2009 국가정보보호백서」, 60쪽.

는 상당한 괴리를 보이고 있는바, 그 주된 원인의 하나가 통계처리에 있어 기본이 되는 분류기준으로서 사이버테러의 개념 부재로 판단된다.

아울러, 일반범죄로 분류된 사이버범죄라 할지라도 그것이 일반대중을 상대로 동시다발적으로 행하여질 때는 사회적 불안을 야기할 뿐 아니라 개인이 사이버공격의 경유지 등으로 사용될 시에는[24] 테러가능성이 항상 잠재하게 된다는 점에서 양자는 불가분의 관찰대상이 된다고 할 것이다.

제3절 몇가지 문제점

민간 및 공공영역에 있어서의 모든 서비스가 정보통신망에 의존하게 될 수밖에 없는 정보사회에 있어서는 이용자가 원하는 서비스만이 실시간으로 이루어질 뿐만 아니라, 각종 유언비어나 바이러스 프로그램 또한 실시간으로 전파되는 결과 주요 웹사이트에 설치되어 있는 방화벽의 기능적 한계상 - 이용자의 일정한 패턴에 착안한 외관상 이상 징후에 대한 통제만 수행할 뿐 오프라인의 검색대처럼 위험한 물건 등에 대한 검색이 이루어지는 것은 아니다 - 부분적 마비가 전체적 마비로 될 수 있는 위험은 상존하게 된다. 이러한 사이버의 특징으로 인해 사이버테러의 개념은 종전의 테러개념을 그대로 차용할 수는 없다는 점은 앞에서 살펴본 바와 같다.

---

24) 인터넷 탄생 후 발생한 온라인 보안 위협 사례 가운데 가장 악명 높은 사례 10가지 중에는 지난해부터 확산돼 지금까지 위협이 되고 있는 '컨피커' 웜 바이러스가 포함됐다. 이 바이러스는 좀비PC를 만든 후 스팸메일 발송과 악성프로그램 배포에 이용되는데 현재 전 세계 460만개 IP 주소에 컨피커가 심어진 것으로 추산되고 있다. 디지털타임스, "악명 떨친 보안위협 '톱10'은?", 2009. 9. 7.

문제는 이러한 사이버테러에 대응할 수 있는 정부기관으로서 갖추어야 할 기능으로 일반적으로 요구되는 것이 “대테러 업무의 기획 및 조정기능”, “정보수집기능” 및 “수사기능” 등이 있으며, 테러를 전담하는 기관이 갖추어야 할 핵심적 기능은 “정보의 통합적 분석과 평가”를 할 수 있는 능력이라고 할 수 있다.[25] 예컨대, 2004년 6월 발생한 변종 피프(Peep)에 의한 국가기관 해킹에 대해 국가정보원과 경찰청 사이버테러대응센터는 중국 해커들의 소행으로 규정한 바 있으나, 실제로 이에 따른 피해사례나 피해가 어느 정도나 되는지에 대해서는 파악조차 하지 못한 경험이 있는 점에서도 통합적 기능의 필요성을 재확인할 수 있다.

오늘날 주요 국가는 사이버테러에 효율적으로 대처하기 위해 기능의 분담과 국가안보기관 통합 그리고 기획·조정기능과 정보수집·수사기능의 통합화가 시도되고 있지만, 우리의 경우에는 그러하지 아니한바, 정부조직법상의 권한분장의 형태와 이를 뒷받침하는 작용법제의 현황을 살펴보고 그 대안을 모색할 필요가 있다.

---

25) 이호용, “효율적인 국가 대테러조직의 위상과 기능”, 「대테러정책 제6호」, 국가정보원, 2009.1. 15-17쪽.

제3장 현행 대응법제와 문제점

제1절 개관

정보기술이 사회전반에 사용됨으로 인하여 다양한 새로운 분야에서 취약성이 발생하고 있다. 불법접근, 바이러스확산과 서비스거부 공격 등과 같은 정보시스템에 대해 미리 계획된 악의적 공격이 다양하게 발생할 수 있는 것이다. 즉, 공격은 대상과 장소에 상관없이 언제라도 발생할 수 있다. 다시 말해 사회는 전혀 새로운 보안문제에 직면하고 있는 것이다.

이 가운데 가장 심각한 문제는 다른 나라나 단체가 사회의 주요기능을 마비시킬 목적으로 조직적이고 체계적으로 정보통신망에 대한 공격을 감행할 수 있다는 것이다. 특정한 목적을 가진 세력들에 의해 조직적이고 체계적으로 행하여지는 정교한 악의적 공격 이외에도 정보통신망의 보안 취약성과 사용자의 부주의나 무지가 결합된 우발적이고 의도되지 아니한 정보통신망의 마비 또한 야기될 수 있다는 것이다.[26] 이와 같은 정보통신망의 취약성은 위험의 범위에 영향을 줄 수 있는 홍수나 뇌우와 같은 혹독한 일기 조건 때문에 증가할 수도 있는 바, 이러한 일들은 국가의 위기를 구성하는 가장 중요한 속성으로 제시되고 있는 ①시간적 절박성, ②위협의 크기 및 ③기습성의 3가지[27] 모두를 충족한다는 점에서 국가위기관리의 관점에서 전자정부의 신경망인 국가정보통신기반시설에 대하여 계

26) 무지로 인한 경우에는 온라인상의 피해는 개인적 법익에 대한 침해를 넘어서 사회적 혼란을 야기할 수 있음에도 불구하고 오프라인적 패러다임에 의한 형법상 고의나 과실 등을 인정하기 어려워 처벌의 한계로 기능할 수 있다.

27) 허태회, “국가위기관리차원에서의 사이버안보 및 위기관리 향상 프로그램연구”, 국가보안기술연구소, 2004.5. 11쪽.

획적 또는 우발적으로 행하여질 수 있는 사이버테러에 대한 전방위적 고찰을 통한 조직법상의 역할구분에 합당한 및 작용법적 대응이 요구된다.

참고로 국가안전보장회의가 2004년 7월 대통령훈령으로 제정한 「국가위기관리기본지침」은 국가위기를 "국가의 주권 또는 국가를 구성하는 정치·경제·사회·문화체계 등 국가의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태"로 정의하고, 위기관리는 "국가위기를 사전에 예방하고 이에 대비하며 위기 발생시에는 효과적인 대응 및 복구를 통하여 위기상황으로부터 야기될 수 있는 영향을 최소화하고 위기이전으로 복구하고자 하는 제반활동"으로 규정하고[28] 있으며, 이러한 구도에 따라 현행법상「재난관리기본법」과 같이 위기발생 이후의 통합적인 조치에 관한 법은 있으나 위기의 사전예방을 위한 기관별 역할의 분담과 통합을 위한 위기관리기본법은 없다는 점에서 국가안전보장입법체계의 결함이 지적될 수 있다.

제2절 조직법상의 대응법제

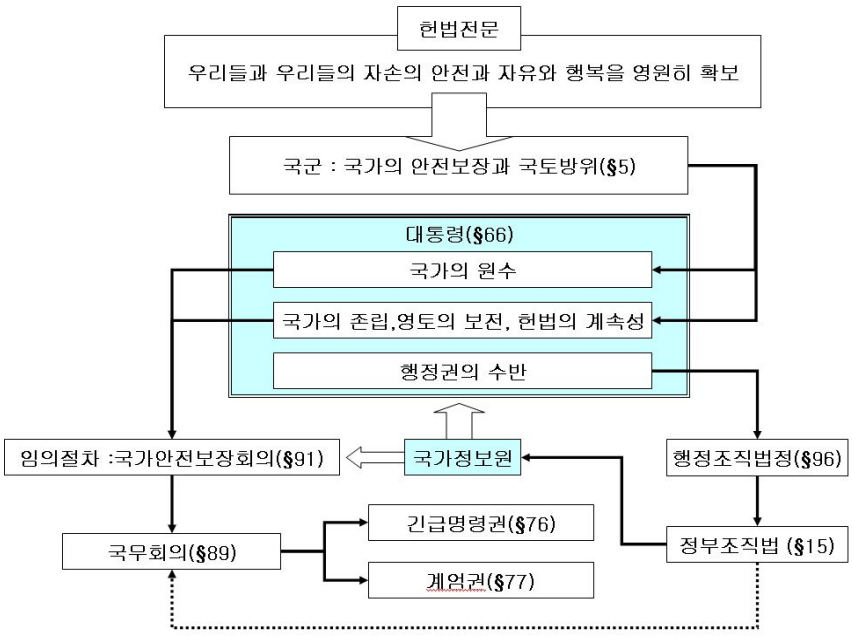
1. 헌법

현행 「헌법」은 "대한민국은 통일을 지향하며, 자유민주적 기본질서에 입각한 평화적 통일정책을 수립하고 이를 추진한다"고 규정(제4조)하는 한편, 국민으로부터 위임받은 국가권력을 입법·행정 및 사법으로 분장하여 상호견제를 통한 국가권력간 균형(Check and Balance)을 유지하

28) 행정자치부, 「국내·외 위기관리 제도 연구」, 2006.12. 86쪽.

도록 하도록 하면서, 대통령에 대하여는 국가원수로서 국가의 독립·영토의 보전·국가의 계속성과 헌법을 수호할 책무를 부여하고(제66조), 법률이 명한 바에 따라 행정의 수반이자 군통수권자로서 국가안정보장의 책무를 수행하도록 하고 있다(제69조, 제74조, 제5조제2항).

국가원수로서 대통령의 국가보위임무의 수행을 위해 아래의 <그림 4>에서 보는 바와 같이 대통령에 대해 내우·외환·천재·지변 또는 중대한 재정·경제상의 위기에 있어서 국가긴급조치권(제76조) 및 계엄선포권(제77조)을 부여하는 한편, 국가안전보장에 관련되는 대외정책·군사정책과 국내정책의 수립에 관하여 국가정보원의 보고를 받아 국무회의의 심의에 앞서 국가안전보장회의의 자문을 구할 수 있도록 하고 있다(제91조).



<그림 4> 현행 헌법상 국가안전보장의 체계

2. 헌법상의 기관(국가안정보장회의)

헌법 제91조제1항에 의거하여 “국가안전보장에 관련되는 대외정책·군사정책과 국내정책의 수립에 관하여 국무회의의 심의에 앞서 대통령의 자문에 응하기 위하여 국가안전보장회의가 설치되고, 이러한 자문의 실효성을 담보하기 위해 「국가안전보장회의법」은 국가정보원장에 대해 국가안전보장에 관련된 국내외정보를 수집·평가하여 이를 대통령의 임의적 자문기관인 국가안정보장회의에 보고하여 심의에 제공할 의무를 부여(제10조)하도록 하고 있다.

국가안전보장회의는 헌법상 대통령의 자문기관이라는 점에서 볼 때 이를 정책의 수립 및 집행기관으로 보아서는 아니 되기 때문에 국가안정보장회의는 별도의 작용법은 요구되지 아니한다고 할 것이다.

3. 정부조직법상 기관

「정부조직법」은 대통령을 수반으로 하는 행정권한을 15부17청으로 분장(제22조)하고, 대통령 소속하에 국가안전보장에 관한 사무를 수행할 국가정보원의 설립(제16조)을 규정하고 있다. 이러한 점에서「정부조직법」은 행정권한을 15부 17청 1원(5개 위원회)에 분장하여 행정권한 또한 기관 상호간의 존중과 견제를 유지하고 있는 것으로 새겨지며, 방송통신위원회는 부칙으로 행정권한의 일부를 갖게 된 것으로 볼 수 있다.

이하에서 그 개략적인 내용을 살펴보되, 사이버테러로부터 사회의 안전과 국가의 안전을 보호하여야 한다는 점에서 국가안전을 사무로 하는 국가정보원 이외에 「정부조직법」제28조상 “국방과 군사에 관한 사무”

를 장리하는 국방부 및 제29조제1항에 의거하여 “전자정부 및 정보보호에 관한 사무”를 장리하는 행정안전부의 관계가 매우 중요하다고 할 것이고, 이러한 범행행위에 대한 수사와 관련하여서는 같은 법 제27조제1항에 의거하여 “검찰·출입국관리 그 밖에 법무에 관한 사무”를 장리하는 법무부와의 관계를 중심으로 살펴볼 필요가 있다.

가. 「정부조직법」

(1)「정부조직법」의 개정이유 2008년2월에 개정된 「정부조직법」은 디지털 기술의 발달에 따른 방송과 통신의 융합현상에 능동적으로 대응하고, 방송의 자유와 공공성 및 공익성을 보장하며, 방송과 통신의 균형발전과 국제경쟁력을 높이기 위하여, 그동안 방송위원회와 정보통신부[29]로 이원화되어 있던 방송통신 관련 기능을 통합하여 대통령 소속의 방송통신위원회를 설치하고 그 운영에 관하여 필요한 사항을 정하려는 목적으로 이루어졌으나, 제한된 시간일정으로 종래 정보통신부의 권한을 외견상으로는 분장하였으나 실질적으로는 행정기관 상호간 정합적인 업무분장이 이루어지지 못하여 대통령령인 직제로써 법률상 명시하지 아니한 권한을 재분장하는 문제점을 야기하였다.[30]

---

29) 종전의 정보통신부의 사무는 지식경제부(IT산업정책 기능), 행정안전부(전자정부 및 정보보호 기능), 문화부(디지털콘텐츠 기능) 등 3개 부처와 대통령 소속하에 신설되는 방송통신위원회(통신시장 조정 및 규제정책 기능)로 그 기능이 각각 분산되었다.

30) 예컨대,「정부조직법」제29조제1항은 “전자정부 및 정보보호”를 행정안전부의 소관사무로 정하는 반면, 「방송통신위원회의 설치 및 운영에 관한 법률」제11조제1항은 방송위원회의 소관 사무를 “방송, 통신, 전파 연구 및 관리에 관한 사항, 그 밖에 이 법 또는 다른 법률에서 위원회의 사무로 정한 사항”으로 하고 민간부문의 개인정보보호에 관련하여 침묵하였다가, 대통령령인 「방송통신위원회와 그 소속기관 직제」제13조의2 제2항에서는 네트워크정책국에 ‘개인정보보호윤리과’를 두도록 하여 개인정보보호를 방송통신위원회에서 관장하도록 하는 기현상을 보이고 있다. 물론, 해석상으로는 통신에 관한 사무에는 통신경찰로서 개

그밖에 정부조직의 개편과 관련하여 “대부처주의에 따른 통제의 폭에 관한 사항”이 논의되어 대부처주의는 조직 세분화에 따른 낭비요소를 제거하고 조직할거주의를 최소화할 수 있다는 장점에도 불구하고, 통제의 폭(Span of Control)이 너무 넓어 내부 통제기능이 제대로 작동하지 않을 경우 상당한 문제가 발생할 가능성이 있다는 점에서 외국의 사례 및 과거의 경험 등을 참고하여 조직규모와 통제범위 간의 적정성 여부, 복수차관제의 확대 필요성 여부 등에 대한 검토 필요성[31]이 논의되었음에도 불구하고 행정안전부의 비대화를 결과하여 행정권한의 분장에 있어서는 균형과 견제의 원리가 이루어지지 못하였다는 문제를 남기고 있는 것이다.

⑵ **사이버공격과 관련한 권한분장** 행정각부와 청은 소관사무별로 요구되는 질서의 예방과 위험의 제거를 위해 「행정조사기본법」과 다종다양한 소관 작용법령에 근거하여 필요한 정보를 수집·분석하여 필요한 행정조치(자료제출명령이나 차단명령 등 경찰조치)를 취할 수 있도록 하고 있다.

나. 국가정보원

헌법 제96조의 정부조직법정주의 원칙에 따라 제정된 현행 「정부조직법」은 제15조는 국가의 원수이자 행정의 수반인 대통령 소속하에 “국가안전보장에 관련되는 정보·보안 및 범죄수사에 관한 사무”를 담당할 국

인정보보호사무가 포함되는 것으로 볼 수는 있다.

31) 대부처주의를 택한 일본의 2001년 정부조직 개편에 따라 우리의 보건복지부 격인 후생성과 노동부 격인 노동성이 통합되어 발족한 후생노동성의 경우 내부조직에 대한 통제가 부실해져 2007년 7월 연금납부기록 5000만 건이 누실되는 사건이 발생하였음. 1994년 경제기획원과 재무부가 통합되어 탄생한 재정경제원이 내부통제의 미비로 인해 외환위기를 가져왔다는 점을 참고할 필요가 있음.

가정보원을 둘 수 있도록 하고, 이를 구체화하고 있는 「국가정보원법」 제3조는 국가정보원의 사무를 “국외정보 및 국내보안정보(대공·대정부전복·방첩·대테러 및 국제범죄조직)의 수집·작성 및 배포”, “국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무(다만, 각급기관에 대한 보안감사는 제외)”, “형법 중 내란의 죄, 외환의 죄, 군형법 중 반란의 죄, 암호부정사용죄, 군사기밀보호법에 규정된 죄, 국가보안법에 규정된 죄에 대한 수사” 및 “정보 및 보안업무의 기획·조정”으로 규정하고 있지만, 이러한 소관사무의 집행에 필요한 국가정보원 소관 개별 작용법은 「국가보안법」, 「형법」 상 국가안전에 관한 죄, 「보안업무규정」 및 「보안업무기획조정규정」 등에 불과하고 국가위기에 관한 정보의 수집과 분석을 위한 통합기능법제는 없는 형편이다.

나-1. 「국가사이버안전관리규정」에 의한 조직

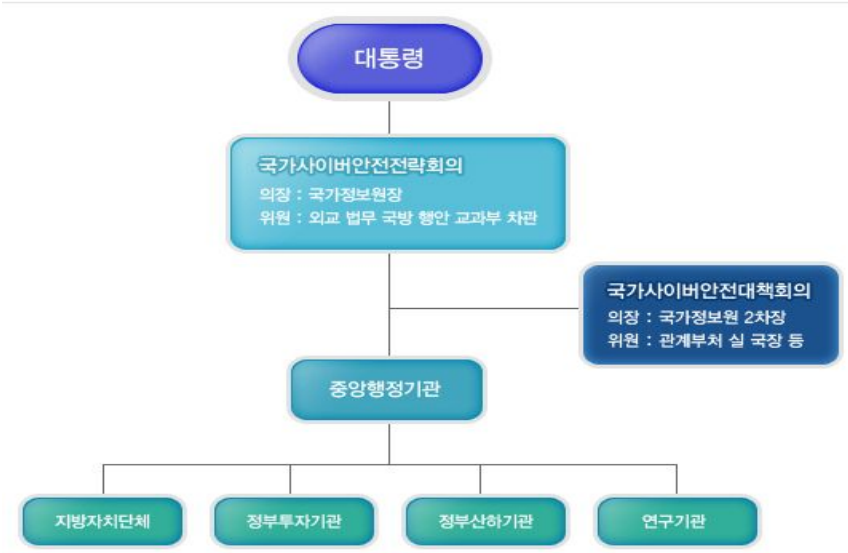
“국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적”으로 하여 2008. 8.18. 대통령훈령 제222호로 제정된 「국가사이버안전관리규정」에 근거하여 설치된 조직으로서는 국가사이버안전전략회의와 국가사이버안전센터가 있다.

전자는 “국가사이버안전체계의 수립 및 개선에 관한 사항, 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, 국가사이버안전 관련 대통령 지시사항에 대한 조치방안, 그 밖에 전략회의 의장이 부의하는 사항”을 심의하기 위한 기관으로서 국가정보원장 소속하에 설치(제6조)[32]된

32) 사이버공격으로부터 국가정보통신망 보호하기 위해 「정보통신기반보호법」 상의

다.

후자는 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 설치되어 “국가사이버안전정책의 수립, 전략회의 및 대책회의의 운영에 대한 지원, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가사이버안전매뉴얼의 작성·배표, 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, 외국과의 사이버위협 관련 정보의 협력”등의 사무를 수행하게 된다.



출처 : 사이버안전센터

<그림 5> 사이버안전 관리체계

정보통신기반보호위원회와 유사한 기능을 수행하는 국가사이버안전전략회의는 훈령상의 기관이라는 점에서 「정보통신기반보호법」에 의한 “정보통신기반보호위원회”와 권한충돌이 발생할 경우에 국가사이버안전전략회의의 권한이 무력화될 소지가 크다는 문제점을 안고 있다.

그러나 이들 기관은 행정조직법정주의를 명시한 헌법 제96조 및 이를 구체화한 정부조직법 제4조에 근거하여 최소한 대통령령으로 설치되어야 함에도 불구하고 행정규칙인 대통령의 훈령을 근거로 한다는 점에서 조직법체계상의 문제를 내포하고 있다.

나-2. 「국가대테러활동지침」에 의한 조직

국가의 대테러 업무수행을 위하여 필요한 사항을 규정함을 목적으로 시행 2008. 8. 18. 대통령훈령 제223호로 제정된 「국가대테러활동지침」은 아래의 <그림 5>에서 보는 바와 같이 "국내외 테러 관련 정보의 통합관리 및 24시간 상황처리체제의 유지, 국내외 테러 관련 정보의 수집·분석·작성 및 배포, 테러대책회의·상임위원회의 운영에 대한 지원, 테러 관련 위기평가·경보발령 및 대국민 홍보, 테러혐의자 관련 첩보의 검증, 상임위원회의 결정사항에 대한 이행점검, 그 밖에 테러 관련 정보의 통합관리에 필요한 사항"을 임무(제12조)로 하는 테러정보통합센터를 국가정보원에 두도록 규정하고 있다(제11조).

그림 6 > 테러정보통합센터의 역할(출처 : 테러정보통합센터)

그러나 앞에서 살펴본 바와 같이 행정조직법정주의에 반하는 것으로서 현행 정부조직법 제4조에 의하더라도 최소한 대통령령에 의한 입법적 근거가 마련되어야 하는 사항이라고 할 것이다.

다. 국방부(국군기무사령부)

국방에 관련된 군정 및 군령과 그 밖에 군사에 관한 사무를 관장하는 국방부장관 소속하에 사이버공격에 대응하는 조직으로는 대통령령인 「국군기무사령부령」에 근거한 "국군기무사령부"와 「국방정보보호훈령」에 근거한 "국방정보전대응센터"가 있다. 전자의 경우는 「정부조직법」제4조와의 관계에서 문제가 없으나 "국방정보전대응센터"는 대통령령인 「국방부와 그 소속기관 직제」상 편성된 조직이 아닌 국방부장관의 훈령에 의한 조직이라는 점에서 법체계상의 문제점이 있다.

다-1. 국군기무사령부

국방부는 정보화추진을 위해 정보화관련 조직, 제도 및 절차를 정비하여 정보화를 촉진할 수 있는 환경을 조성하고, 정보전 및 사이버전에 대비하여 우리 실정에 맞는 국방차원의 사이버전 교리발전 및 사이버전을 수행할 수 있는 인력확보와 조직정비를 추진하고 있다. 국방부의 경우 사이버테러에 대한 대응은 주로 국군기무사령부를 통해 이루어진다고 할 수 있는데, 정부조직법 제4조에 근거하여 2002.10.23. 대통령령 제17762호로 발하여진 「국군기무사령부령」 제1조제4호에 따라 국군기무사령부는 정보통신기반보호법 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대한 동법 제7조제1항 각호의 기술적 지원 가운데 국방 분야에 관한 사항을 수행하고 있다.

다-2. 국방정보전대응센터

국방부장관이 「정보통신기반보호법」, 「공공 기관의 정보보호 및 개인정보보호에 관한 법률」, 「전자정부법」, 「국가사이버 안전관리규정」 및 「국방전력발전업무훈령」에서 위임된 사항을 구체화하고 국방정보체계의 안정적 운영을 위하여 국방정보 보호에 필요한 제반 업무와 절차에 대하여 규정함을 목적으로 제정된 「국방정보보호훈령」 제53조제3항에 따라 설치되는 '국방정보전대응센터는 정보수집기관 및 다양한 채널을 통해 국방망 등 주요기반통신망에 대한 위협정보를 수집하여 국·내외 공조기관과의 협조를 통해 분석·전파하는 사무를 관장한다.

라. 행정안전부

행정안전부는 종전의 행정자치부에 중앙인사위원회 및 국가비상기획

위원회의 사무를 통합한 것으로서 개정된 「정부조직법」 제29조에 의하면, "… 전자정부 및 정보보호, … 안전관리정책 및 비상대비·민방위·재난관리제도에 관한 사무"를 관장하게 됨으로써 전자정부 기능의 통합을 통해 권한 다툼으로 인한 갈등을 해소 및 전자정부의 효율적인 구현과 분산된 국가안전관리 정책의 총괄·조정기능이 강화될 것이라는 기대를 부여받고 있다.[33]

라-1. 경찰청

「정부조직법」 제29조제4항에 따라 치안에 관한 사무를 관장하기 위하여 행정안전부장관소속으로 설치된 경찰은 국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압 및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 사무로 한다(「경찰법」 제4조). 특히 사이버침해에 의한 일반범죄의 예방 및 수사를 위해 경찰청은 1995년 해커수사대를 시작으로 1997년 컴퓨터범죄수사대, 1999년 사이버범죄수사대, 2000년 7월 사이버테러대응센터(CTRC) 등의 사이버범죄 수사조직을 두고 있다. 사이버테러대응센터는 「경찰청과 그 소속기관 직제 시행규칙」 제9조제1항에 의하여 수사국에 설치되며, "사이버테러의 탐지·추적 수사 및 경보 등 조치, 사이버테러 관련 수사기법의 연구·개발 및 국제경찰기구 등과의 협력, 사이버범죄의 수사 및 지도 및 디지털매체 등 증거분석 업무" 등의 사무를 수행한다(제9조제9항).

마. 법무부(검찰청)

「정부조직법」 제27조상 검찰·행형·인권옹호·출입국관리 그 밖에

33) 이하의 사항은 "정부조직법 전부개정법률안 심사보고서"(2008. 2. 행정자치위원회)에 근거한 것임.

법무에 관한 사무를 관장하는 법무부의 소관사무와 관련하여서는 개인적 및 사회적 법익에 대해서뿐만 아니라 국가적 법익의 침해에 대한 범행의 수사지휘권 및 기소권을 독점하고 있는 검찰의 사이버테러에 대한 수사 및 기소권이 관심의 대상이 된다.

현재 검찰의 경우에는 사이버범죄에 대응하기 위해 대검창청과 지방검찰청, 차장검사가 있는 지청 등 22개 검찰청에 컴퓨터범죄 수사부서를 설치하여 운영하고 있다. 검찰의 사이버범죄 관련 조직은 대검찰청 컴퓨터수사과, 서울지검 컴퓨터수사부, 일선청의 컴퓨터수사반 등이 있다.

사. 그밖에 기관과 소관사무

그밖에 테러사무를 관장하는 국가기관과 그 근거법령은 아래의 <표 8>과 같다. 주목해야 할 것은 이들 모두는 법률이나 대통령령에 의한 사무분장이 이루어지고 있다는 점이다.

<표 8> 국가기관별 대테러업무와 근거법제

기관	담당업무	근거법령
해양경찰청	해상 테러예방 및 진압, 해양테러사건 대책본부설치·운영	「해양경찰청과 그 소속기관등 직제」, 대통령훈령 제47호
중앙안전대책위원회	국민의 생명이나 피해를 주는 재난의 예방이나 수습	「재난관리법」
중앙통합방위협의회	테러행위를 포함하는 것으로 해석되는 통합방위사태에 대응하기 위하여 군과 경찰, 국가기관과 지방자치단체, 향토예비군, 민방위대, 일정한 범위의 직장 등 국가의 모든 방	「통합방위법」

중앙통합 방위협의회	위요소를 통합하고 지위체계를 일원화하여 관리할 수 있도록 체계구축 및 권한부여	
국토해양부	항공기테러사건 대책본부의 설치·운영 철도공안원의 대테러예방업무 철도재산 및 대테러대책에 관한 사항	대통령 훈령 제47호 「국토해양부와 그 소속기관직제」 「국토해양부와 그 소속기관직제」
관세청	총기류·폭발물 등 테러관련 물품의 반입금지	「관세청과 그 소속기관 직제」
외교통상부	국외테러사건 대책본부 설치·운영	대통령 훈령 제47호
금융위원회	테러자금 차단	
교육과학 기술부	방사능테러사건 대책본부 설치·운영	
환경부	화학테러사건 대책본부 설치·운영	
지식경제부	기간 및 산업시설 대테러·안전관리 및 방호대책수립	
보건복지 가족부	생물테러 사건대책본부의 설치·운영	
국무총리실	관계기관 소관사항 협의·조정	
대통령실	국가위기관리체계에 관한 기획·조정	
대통령 경호실	경호대책 수립·시행	

출처: 이호용, “효율적인 국가대테러조직의 위상과 기능”

4. 작용법에 근거를 둔 조직

공공 및 민간부문의 정보통신질서와 관련한 주요 작용법으로는 「국가정보화기본법」, 「정보통신기반보호법」,「정보통신망 이용촉진 및 정보보호등에 관한 법률」 및 「재난 및 안전관리기본법」등이 있는바, 그 주요사무와 기능은 다음과 같다.

가.「국가정보화기본법」(국가정보화전략위원회 및 한국정보화진흥원)

(1) **국가정보화전략위원회** 국가정보화전략위원회는 대통령 소속하에 국회사무총장, 법원행정처장, 헌법재판소사무처장과 중앙선거관리위원회 사무총장, 중앙행정기관의 장과 지방자치단체의 장 중 대통령령으로 정하는 사람 및 국가정보화에 관한 전문지식과 경험이 풍부한 사람 중에서 대통령이 위촉하는 사람으로 구성되며(제9조), "기본계획 및 시행계획의 수립, 기본계획 및 시행계획 중 대통령령으로 정하는 중요한 사항의 변경, 부문계획의 작성지침, 국가정보화 정책이나 사업 추진의 조정, 기본계획 및 시행계획의 주요 시책에 대한 추진실적 분석 및 점검, 지식정보자원의 지정, 정보문화의 창달 및 정보격차의 해소를 위한 사업의 우선순위 결정, 「전자정부법」과 그 밖의 다른 법령에서 위원회의 심의사항으로 정한 사항, 중장기 지식정보자원 관리계획, 그 밖에 국가정보화의 추진과 관련하여 위원장이 필요하다고 인정하는 사항" 등을 심의한다(제10조).

「국가정보화기본법」제5조 제1항은 "국가정보화의 추진에 관한 다른 법률을 제정하거나 개정할 때에는 이 법의 목적과 기본이념에 맞도록 노력하여야 한다"고 하여 국가정보화의 헌법적인 의미를 부여하면서 같은

조 제2항에서는 “국가정보화의 추진에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다”고 규정하여 국가정보화에 관한한 일반법의 성격을 갖고 있음을 명시하고 있다.

법 제5조 제1항과 관련할 때, 국가정보화와 관련한 기본계획은 최고상위계획으로서의 성격을 갖는다고 할 수 있으나, 정보화는 “정보를 생산·유통 또는 활용하여 사회 각 분야의 활동을 가능하게 하거나 그러한 활동의 효율화를 도모하는 것”(제3조제2호)을 의미하는 점에서 국가정보화 기본계획은 조성 내지 복리적인 측면에서의 우위성을 갖는 것이지 정보통신망의 안전과 관련한 질서의 측면에 대하여도 다른 국가계획이나 정책에 대하여도 우위성을 갖는 것으로 보기는 어렵다.

⑵ **한국정보화진흥원**　국가기관등의 국가정보화 추진과 관련된 정책의 개발과 건강한 정보문화 조성 및 정보격차 해소 등을 지원하기 위하여 설립된 한국정보화진흥원(「국가정보화기본법」 제14조제1항)은 “기본계획과 시행계획의 수립·시행에 필요한 전문기술의 지원, 국가기관등의 정보통신망 관리 및 운영의 지원”, “국가기관등이 보유한 주요 정보의 원활한 유통과 공동이용을 위한 시스템의 구축·운영 및 표준화의 지원”, “국가기관등의 정보자원 관리 지원, 국가기관등의 정보화사업 추진 및 평가 지원”, “국가기관등의 정보통신 신기술 활용 촉진과 이에 따른 전문기술의 지원”, “정보문화의 창달과 인터넷 중독의 실태조사, 예방 및 해소 지원”, “정보격차의 해소를 위한 지원”, “건강한 정보문화의 확립 및 정보격차의 해소를 위한 교육 및 홍보”, “국가정보화, 정보문화 및 정보격차 해소와 관련된 정책 개발을 지원하기 위한 동향 분석, 미래예측 및 법·제도의 조사·연구”, “국가정보화, 정보문화 및 정보격차 해소와 관련된 국제협력 및 홍보”, “다른 법령에서 정보화진흥원의 업무로 정하거

나 정보화진흥원에 위탁한 사업” 및 “그 밖에 국가기관등의 장이 위탁하는 사업” 등을 수행하게 된다(제14조제3항).

「국가정보화기본법」 제14조 제3항에 의할 때 한국정보화진흥원은 정보화와 관련한 조성·급부 내지 복리행정에 관한 사무수행을 보조하는 기관으로서의 성격을 갖는 점에서 정보통신침해 등 정보통신질서와 관련한 사무수행을 보조하는 한국인터넷진흥원과는 그 성격을 달리 함을 알 수 있다.

나.「정보통신기반보호법」(정보통신기반보호위원회)

전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 하는 「정보통신기반보호법」 제 3조에 의한 조직으로서 국무총리소속하의 “정보통신기반보호위원회”는 “주요정보통신기반시설 보호정책의 조정에 관한 사항, 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항, 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항, 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항 및 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항”에 관한 심의를 관장하게 된다(제4조).

따라서 “정보통신기반보호위원회”는 사이버테러와 관련한 국가의 중요정책심의기관임을 알 수 있고, 「정보통신기반보호법」이 다른 법률과의 관계에 대해 별도의 규정이 없으나 국가의 주요정보통신기반시설의 안전과 관련한 보호계획은 일단 다른 정보통신계획에 우선한다고 할 수

있다.

나.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(한국인터넷진흥원)

한국인터넷진흥원은 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 하는 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 제52조에 의해 설치된다.

한국인터넷진흥원은 " 정보통신망의 이용 및 보호, 방송통신과 관련한 국제협력·국외진출 등을 위한 법·정책 및 제도의 조사·연구, 정보통신망의 이용에 따른 역기능 분석 및 대책 연구, 정보보호 안전진단, 정보보호 관리체계의 인증, 정보보호시스템 평가·인증 등 정보보호 인증·평가 등의 실시 및 지원, 정보통신망 침해사고의 처리·원인분석 및 대응체계 운영" 등의 사무를 비롯하여 "법령에 따라 인터넷진흥원의 업무로 정하거나 위탁한 사업이나 행정안전부장관·지식경제부장관·방송통신위원회 또는 다른 행정기관의 장으로부터 위탁받은 사업"을 수행한다. 따라서 한국인터넷진흥원은 민간부문에 있어서 정보통신망 침해사고 등 정보통신질서와 관련된 사무수행을 보조하는 기관으로 볼 수 있다.

다. 「재난 및 안전관리기본법」(중앙안전관리위원회)

에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비 등으로 인한 피해로부터 국토를 보존하고 국민의 생명·신체 및 재산을 보

호하기 위하여 국가 및 지방자치단체의 재난 및 안전관리체제를 확립하고, 재난의 예방·대비·대응·복구 그 밖에 재난 및 안전관리에 관하여 필요한 사항을 규정하고 있는 「재난 및 안전관리기본법」 제9조에 의하여 국무총리산하에 설치되는 중앙안전관리위원회는 안전관리에 관한 중요정책의 심의 및 총괄·조정, 국가안전관리기본계획안 및 집행계획안의 심의, 중앙행정기관이 수행하는 재난 및 안전관리업무의 협의·조정, 국가기반시설 지정사항의 심의, 재난사태 선포 및 특별재난지역 선포에 관한 건의사항의 심의와 재난사태 선포의 사후승인 등을 권한을 수행하는 등 기본적으로 통신 등 국가기반체계의 마비 등에 대한 예방적인 조치를 주목적으로 하기 보다는 발생된 위기의 사후관리를 위한 통합법제의 성격을 갖는다.

제3절 작용법상의 대응법제

1. 논의의 실익

시간적 물리적 한계를 초월하여 전자정부의 기반위에 있는 국가와 사회의 기능을 마비시키고자 하는 사이버테러 내지 전자적 침해는 사회나 국가에 대해 불만을 갖고 있거나 적대적 관계에 있는 자나 세력들이 사회 또는 국가의 기능을 마비시키는 주된 수단으로 범하여지고 있음은 주지하는 바이다. 이와 같이 사회 및 국가의 정보시스템을 파괴하여 그 기능을 마비시키는 신종 테러는 정보화시대의 산물로, 컴퓨터망을 이용하여 데이터베이스화되어 있는 민간기업이나 공공기관을 비롯하여 국가 및 사회의 안전을 책임지는 국가기관 등 의 정상적인 기능을 해칠 가능성 내지 결과를 내포하는 것이다.

이 점에서 21세기의 테러는 사이버테러를 중심으로 이루어질 것으로 예측되며[34], 이에 대한 대비를 하지 아니할 경우에는 7·7DDoS 사태와 같이 '호미로 막을 일을 가래로도 막지 못하는 촌극'을 야기할 수도 있다는 점에서 현행법제에 의한 작용법적 대응가능성을 살펴볼 실익이 있다고 할 것이다.

2. 주요기관별 사이버침해 대응 작용법(권한행사법)

사이버상의 생활관계와 관련한 작용법으로는 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것을 목적으로 하는 「전자정부법」, 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 하는 「공공기관의 개인정보보호에 관한 법률」이 있다.

그밖에, 전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전

34) 유엔은 만약 3차 세계대전이 일어난다면 사이버전이 될 수 있으며 전쟁 발발시 어떤 국가도 성역으로 남을 수 없다고 경고했습니다. 국제전기통신연합의 하마둔 투레 사무총장은 스위스 제네바에서 열린 회의에서 사이버상에서 일어나는 세계대전은 '재앙'과 같을 것이라며 이 같이 말했습니다. 투레 사무총장은 핵심 네트워크들이 파괴된 국가는 곧바로 통제 불능 상태가 될 것이며 어떤 국가도 사이버 공격의 위협을 피할 수 없다고 지적했습니다. 투레 사무총장은 특히 각국이 상업과 금융, 식량 거의 전 분야를 기술에 의존하는 상황에서, 사이버 전쟁에서 이기는 방법은 오로지 전쟁이 일어나는 것을 미리 막는 것이라고 강조했습니다. http://www.ytn.co.kr/_ln/0104_200910071239178192

성과 신뢰성을 확보함과 아울러 전자금융업의 건전한 발전을 위한 기반 조성을 함으로써 국민의 금융편의를 꾀하고 국민경제의 발전에 이바지함을 목적으로 하는「전자금융거래법」, 전자상거래 및 통신판매 등에 의한 재화 또는 용역의 공정한 거래에 관한 사항을 규정함으로써 소비자의 권익을 보호하고 시장의 신뢰도 제고를 통하여 국민경제의 건전한 발전에 이바지함을 목적으로 하는 「전자상거래 등에서의 소비자보호에 관한 법률」등이 있다.

그러나 사이버테러로부터 사회와 국가의 안전성을 사전적으로 담보하는 기능을 가진 대표적인 법률로는 공공부문에 있어서의 「정보통신기반보호법」과 민간부문에 관련한 「정보통신망 이용촉진 및 정보보호등에 관한 법률」이라고 할 수 있다. 이하에서는 이러한 관점에서 이들 두 개의 작용법을 비롯한 소관기관별 관련 법령을 간단하게 살펴보기로 한다.

다만, 국가통신재난과 관련한 「재난 및 안전관리기본법」이나 적의 침투·도발이나 그 위협에 있어서 국가총력전의 개념에 입각하여 국가방위요소를 통합·운용하기 위한 통합방위대책을 수립·시행하는데 필요한 사항을 규정함을 목적으로 하는 「통합방위법」에 의한 통합방위사태는「재난 및 안전관리기본법」에 의한 통신재난과 마찬가지로 발생된 사태에 대응하여 기능회복을 목적으로 하는 것이라는 점에서 이하에서는 고려의 대상에서 제외하기로 한다.

가. 국가정보원

국가안전보장을 주된 사무로 하는 국가중앙행정청으로는 국가정보원은J「형법」,「군형법」,「군사기밀보호법」,「국가보안법」상의 국가적

범죄에 대한 수사권을 행사할 수 있도록 법적 조치가 되어 있지만, 그밖에 국가안전보장을 위한 국내외 보안정보의 수집·작성 및 배포 및 국가기밀에 속하는 보안업무 등에 대한 권한행사를 뒷받침할 수 있는 작용법(권한행사법)은 보이지 않고 있어, "음지에서 양지를 지향한다"는 국가정보원의 특징을 감안하더라도 헌법 제37조의 법률유보원칙과 관련하여 많은 문제를 내포하고 있다.

그밖에 국가안전보장을 위한 예방적 사무로서 "국외정보 및 국내보안정보(대공·대정부전복·방첩·대테러 및 국제범죄조직)의 수집", "국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무(다만, 각급기관에 대한 보안감사는 제외)" 및 "정보 및 보안업무의 기획·조정"을 총괄적으로 집행하기 위한 작용법은 전무한 상태이다. 물론, 조직법인 국가정보원법에 근거한 작용법령으로서 「보안업무규정」 및 「보안업무기획조정규정」등이 있으나, 이들은 효력면에서 법률 하위에 있기 때문에 다른 국가기관의 소관법률과 저촉될 경우에는 그 효력이 형해화되어 규범력을 상실할 우려가 있다.

나. 국방부

국방에 관련된 군정 및 군령과 그 밖에 군사에 관한 사무를 관장하는 국방부의 소관법률로는 2009년 10월 현재 54개의 법률이 있으며, 그 중 국가안전과 관련한 작용법적 성격을 갖는 주요한 법률로는 「계엄법」, 「군사기밀보호법」, 「군사기지 및 군사시설 보호법」,「국방·군사시설사업에 관한 법률」, 「군수품관리법」, 「군용전기통신법」, 「군형법」 및 「군 책임운영기관의 지정·운영에 관한 법률」 등 소관사무의 수행에 필요한 작용법을 갖추고 있다.

다. 행정안전부의 사무와 소관 작용법(권한행사법)

“전자정부 및 정보보호,…안전관리정책 및 비상대비・민방위・재난관리제도에 관한 사무”를 소관하는 행정안전부의 소관법률로는 2009년 10월 현재 105개의 법률이 있으며 질서와 관련한 법률로는 「공공기관의 개인정보보호에 관한 법률」, 「공공기관의 정보공개에 관한 법률」, 「공공기록물 관리에 관한 법률」,「국가정보화 기본법」,「비상대비자원관리법」, 「재난 및 안전관리기본법」,「전자서명법」, 「전자정부법」, 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」,「정보통신기반보호법」, 「집회 및 시위에 관한 법률」 및 「화염병사용 등의 처벌에 관한 법률」등 다양한 작용법을 갖고 있다.

그 중에서「정보통신기반보호법」은 “전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여, 국가의 안전과 국민생활의 안정을 보장하는 것을 목적”으로 하는 법률로서 국무총리 소속하의 정보통신기반보호위원회는 주요정보통신기반시설의 보호에 관한 사항을 심의하며(제3조, 제4조), 행정안전부장관과 국가정보원장 등은 주요 정보통신 기반시설 보호대책의 이행여부를 확인하기 위하여 필요한 자료를 관계중앙행정기관의 장에게 요청할 수 있고, 행정안전부장관과 국가정보원장 등은 확인한 주요 정보통신기반시설 보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있도록 규정하고 있다(제5조의2).

이와 달리,「재난 및 안전관리기본법」은 “각종 재난으로부터 국토를 보존하고 국민의 생명・신체 및 재산을 보호하기 위하여 국가 및 지방자치단체의 재난 및 안전관리체제를 확립하고, 재난의 예방・대비・대응・

복구 그 밖에 재난 및 안전관리에 관하여 필요한 사항을 규정함을 목적"으로 국민의 신체나 재산 및 국가에 피해를 줄 수 있는 국가통신기반체계의 마비(제3조제1호 다목) 등에 대한 국가안전관리기본계획안은 국가안정보장회의와 협의 하에 국무총리 소속의 중앙안전관리위원회에 의해 수립되고(제10조), 이러한 통신재난에 대한 예방・대비・대응・복구는 행정안전부장관을 본부장으로 하는 중앙재난안전대책본부가 하도록 되어 있어(제14조), 국가의 원수로서 대통령 소속하에 국가안전보장을 주된 사무로 하는 국가정보원의 참여가 배제된 입법의 모순점을 발견할 수 있다.

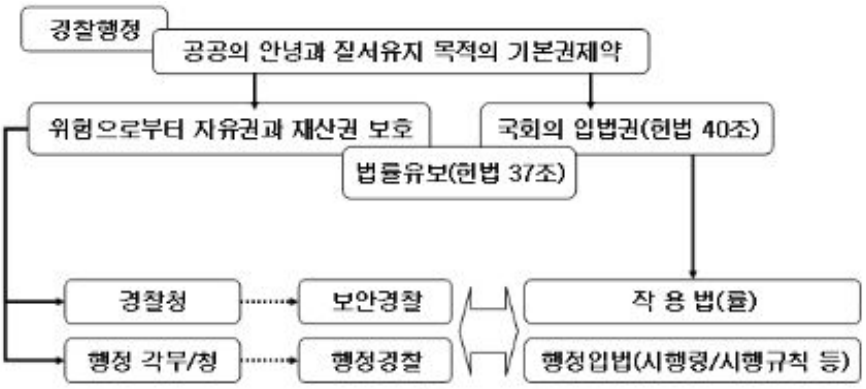
라. 법무부

검찰·행형·인권옹호·출입국관리 그 밖에 법무에 관한 사무를 관장하는 법무부의 소관법률은 2009년 10월 현재 133개의 법률이 있으며, 그 중 각종 범죄의 수사와 처벌 등에 관련한 작용법으로는 「형법」,「형사소송법」,「공무원범죄에 관한 몰수특례법」,「범죄수익은닉의 규제 및 처벌 등에 관한 법률」, 「보건범죄단속에 관한 특별조치법」, 「특정 범죄자에 대한 위치추적 전자장치 부착 등에 관한 법률」 및 「특정강력범죄의 처벌에 관한 특례법」등의 법률에 대한 집행을 책임지며, 각종 범죄에 대한 수사권한을 행사할 뿐 아니라 모든 범죄에 대한 기소권을 독점적으로 보유한다.

마. 그밖에 국가기관

앞에서 언급한 국가기관 이외의 중앙행정기관도 자신의 소관 사무를 수행하기 위해 부수적으로 요구되는 질서(행정경찰)작용에 필요한 작용법을 갖고 국민의 권리나 자유를 제한하고 있다. 예컨대, 보건복지부의

「전염병예방법」, 문화체육관광부의 「게임산업진흥에 관한 법률」 및 지식경제부의 「산업기술의 유출방지 및 보호에 관한 법률」, 「화학·생물무기의 금지 및 특정화학물질·생물작용제 등의 제조·수출입규제 등에 관한 법률」,「민·군겸용기술사업 촉진법」 등 사회안전 뿐만 아니라 국가안전과도 관련이 있는 작용법들이 소재하고 있다.



<그림 7 > 경찰의 비경찰화(행정경찰)

3. 사이버테러와 작용법제의 문제점

가. 경찰의 비경찰화와 행정경찰

경찰을 의미하는 'Police'는 그리스어의 'Politeia'에서 유래하는 것으로 고대부터 중세에 이르기까지는 '이상적인 상태, 국가·헌법 또는 국가 활동' 등 다양한 의미를 내포하고 있었다. 15·16세기에 이르러서는 교회활동에 대응한 국가작용의 일체를 가리키는 말로 사용되다가 17세기에는

국가작용의 분화와 더불어 국가작용 중에서 외교·재정·군정 등이 분리되고 남은 오늘날의 내무행정(치안작용과 복리작용을 합한 것)으로 한정되어 18세기 전반까지 경찰은 보안경찰과 복리경찰을 의미하게 되었다.

18세기 중엽 이후 근대 시민적 법치국가의 성립과 더불어 국민의 자유로운 활동을 보장하려는 경찰국가사상으로부터 경찰권을 소극적 치안유지만을 임무로 하는 보안작용에 한정시키기에 이르러 근대 법치국가적 경찰개념의 성립을 보게 되었고, 그 후 19세기 말부터 20세기에 걸쳐 "시장의 자동조정기능"이 아닌 국가에 의한 국민복리 증진의 요구가 광범위하게 전개됨에 따라 근대 법치국가적 경찰개념 외에 복리증진에 수반하는 질서유지를 위한 권력적 활동을 다시 경찰의 임무로 요구하게 되었다. 그 결과 아래의 <그림 6>에서 보는 바와 같이 경찰사무가 다른 행정기관의 사무로 이관되는 소위 "탈경찰화" 내지 "비경찰화"의 과정을 겪게[35] 되어 우리의 행정각부 또한 건축경찰, 영업경찰, 경제경찰 등 자신의 소관 사무를 수행함에 있어 부수적으로 요구되는 행정경찰권을 보유하고 있다.

나. 사이버테러의 특징과 경찰기능의 분담과 통합

현대 정보화기술은 새롭게 등장하는 다양한 미디어기기와 융합하여 방송과 통신의 구별을 곤란하게 할 뿐만 아니라 전자식별장치(RFID)를 통해 인간과 동·식물을 비롯한 모든 물건과도 전자적인 소통을 가능하게 하는 IT기술(특히, 시멘틱 웹의 개발)[36]과 위치정보기술(Global

35) 김남현/김형훈, 경찰행정법, 경찰공제회, 2005, 18·20쪽 참조.

36) 현재의 컴퓨터처럼 사람이 마우스나 키보드를 이용해 원하는 정보를 찾아 눈으로 보고 이해하는 웹이 아니라, 컴퓨터가 이해할 수 있는 웹을 말한다. 즉 사람이 읽고 해석하기에 편리하게 설계되어 있는 현재의 웹 대신에 컴퓨터가 이해할

Position System)의 결합에 힘입어 미래 고도정보사회는 언제·어디에서나 인간의 수요를 실시간으로 충족할 수 있는 "거침없이 원활한 전자적 소통사회"(seamless networking society) 내지 "유비쿼터스 사회"(Ubiquitous Society)[37]로서 "사생활이 없는 사회"(Zero Privacy Society)[38]에 대한 두려움[39]과 공공적 내지 비공공적 수요에 대한 실시간의 충족을 매개하게 되는 될 것으로 기대되는 사회이다. 이 처럼 개인과 개인, 개인과 사회, 사회와 사회 및 개인·사회와 국가 상호간 "거침없이 원활하게 소통"하는 정보통신망이 하나의 신경망처럼 연결되어 의존하는 사회에서는 부분적 마비는 전체적 마비로 전이될 위험을 항상 안

수 있는 형태의 새로운 언어로 표현해 기계들끼리 서로 의사소통을 할 수 있는 지능형 웹이다. 원리는 사람들이 이해할 수 있도록 자연어 위주로 되어 있는 현재의 웹 문서와 달리, 정보자원들 사이에 연결되어 있는 의미를 컴퓨터가 이해할 수 있는 형태의 언어로 바꾸는 것이다. 이렇게 되면 컴퓨터가 정보자원의 뜻을 해석하고, 기계들끼리 서로 정보를 주고받으면서 자체적으로 필요한 일을 처리하는 것이 가능해진다. 2004년 현재 시멘틱 웹과 관련된 연구는 RDF(Resource Description Framework)를 기반으로 한 온톨로지 기술과 국제표준화기구(ISO) 중심의 토픽 맵(Topic Map) 기술이 주류를 이루고 있다. http://100.naver.com/100.nhn?docid=780515 <2008.8.1. 접속>

37) USN사회로 진입하게 됨에 따라 "인간의 요구사항을 고도로 적용하는 환경", "모든 이에게 가장 기본적인 서비스제공", "어떤 콘텐츠, 기기, 포맷이라도 언제나 접속 가능한 환경" 및 "스팸, 정크메일, 해킹, 바이러스 등이 존재할 수 없는 환경(Digital Dystopia)" 등 4대 미래 인터넷 시나리오가 제시되기도 한다. Smart Internet Technology CRC, "Smart Internet 2010", 2005. 9.(한국전산원, "통계로 본 2010년 유비쿼터스사회 조망", 2005.9.30. 5쪽에서 재인용).

38) "현대 고도정보사회에 있어서는 사생활에 대해 조의를 표하여야 하며, 카메라나 데이터베이스의 침해를 방지하기엔 너무 늦었다. 이미 쏟아진 물이다. 아무리 많은 입법이 행하여진다고 하더라도 입법으로 새로운 감시도구와 데이터베이스를 제거할 수는 없다"고 한다. D.J. Solove, Marc Rotenberg, "Information Privacy Law", Aspen. 2002. p.507.

39) 바람난 남편이나 가출한 자녀를 찾기 위해 이들이 조난을 당했다고 허위로 신고할 경우 GPS를 작동해 이들의 위치를 파악하는 것이 개인 프라이버시 문제와 어떻게 상충될지 등에 대한 연구가 필요할 뿐 아니라 정치인이나 저명인사의 동선이 파악돼 엉뚱한 용도로 악용될 가능성에 대한 우려의 시각도 있다. 졸고, "位置認識 및 通信事實確認資料 등의 個人情報與否에 관한 小考", 토지공법연구 제24집, 2004.12. 494쪽.

고 있는 것으로 평가할 수 있다.

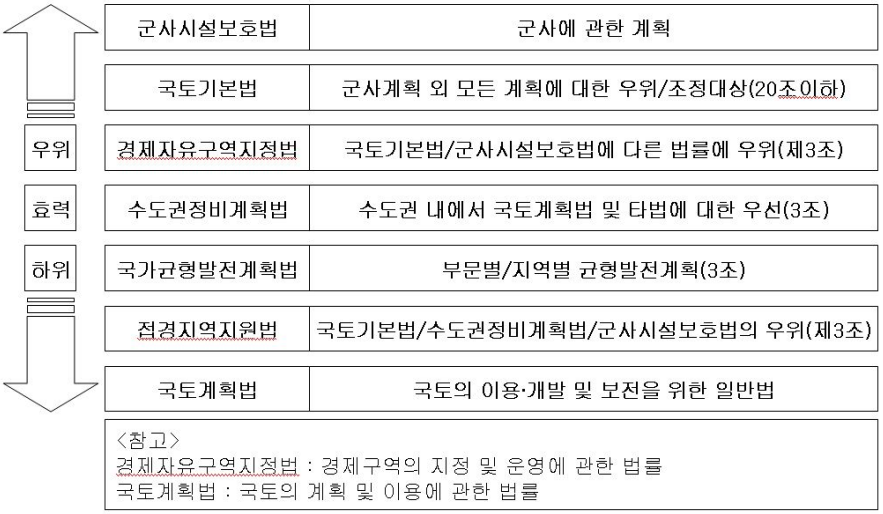
따라서 오프라인의 테러와 달리 물리적 제약을 받지 아니하는 사이버테러는 국부적인 경찰작용과 전체적 경찰작용은 조직법 및 작용법의 측면에서 상호 분리되어 있다고는 하더라도 사이버테러가 갖는 파급효과의 “seamless networking”을 고려할 때, 개인 및 사회적 위험이 국가적 위험으로 전이되는 것을 예방하기 위해 개별 위험에 대한 원정보의 공유를 전제로 한 통합적 통제기관 및 보안계획을 입법적으로 조치할 필요성이 있음을 알 수 있다.

다. 문제점

현행 조직법 체계에 의하면, 국가정보원은 대통령의 직접적인 지휘·감독 하에 국가안전보장사무를 관장하고 있으며, 전자정부법을 주관하는 행정안전부의 행정내부경찰사무(전자정부경찰사무)를 비롯하여 행정각부·청은 사회의 안전을 위한 보안경찰사무 및 행정경찰사무를 관장하고 있음을 확인할 수 있다. 이와 관련한 문제로는 전자정부는 국가기능의 안전이라는 측면에서는 국가정보원과 전자정부에 기반을 둔 전자행정부의 안전이라는 측면에서는 행정안전부와 사무의 중첩이 발생할 수밖에 없다는 점이다.

다음으로 작용법상 사이버의 안전과 관련된 개별 작용법에 의한 계획간의 효력우위 문제를 들 수 있다. 예컨대, 국토계획과 관련하여서는 개별 작용법이 효력에 관련한 개별규정을 통해 아래의 <그림 7>과 같이 국토계획간 효력체계를 설정할 수 있으나, 「정보통신기반보호법」에 의한 정보통신기반시설보호계획,「국가정보화기본법」에 의한 국가정보화

기본계획, 「재난 및 안전관리기본법」상의 국가안전관리기본계획 및 「국가사이버안전관리규정」에 의한 국가사이버안전정책은 효력과 관련하여서는 별도의 규정이 없어 계획상의 총괄 또한 어렵다는 비난을 면하기 어려울 것으로 생각된다.



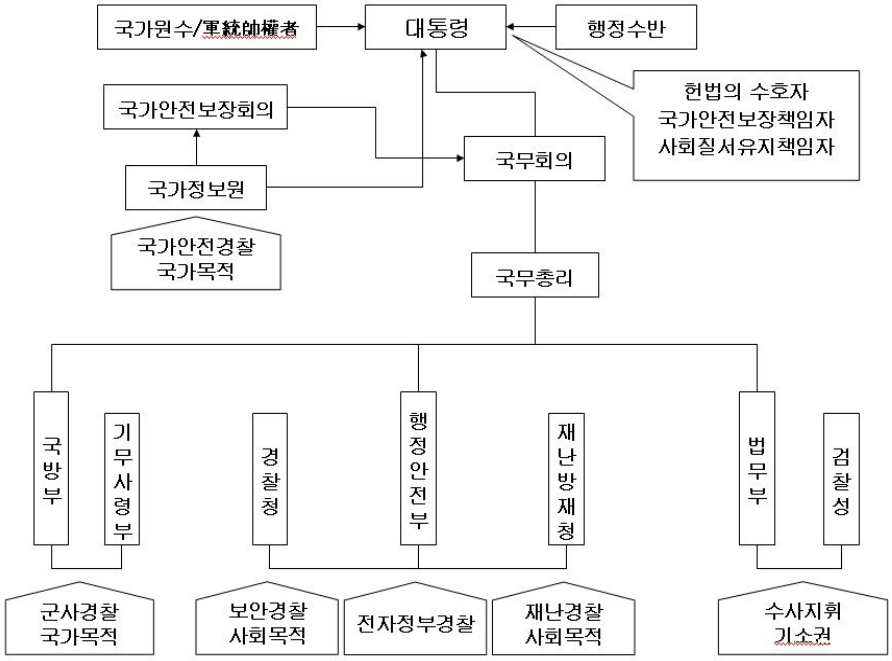
<그림 8> 국토계획간 효력체계

조직법상 대통령 소속하에 국가안전사무를 소관하는 최고 중앙행정기관이 국가정보원이라는 점에서는 「국가사이버안전관리규정」에 의한 국가사이버안전정책이 최고의 효력을 갖는 것으로 볼 수 있지만, 이 정책은 훈령에 의한 것이라는 점에서 법률에 의한 계획에 우선한다고 할 수는 없다. 그리고 작용법적인 측면에서 보자면, 정보화의 기본이 되는 「국가정보화기본법」에 의한 국가정보화기본계획이 최고 상위의 효력을 갖는다고 할 것이지만, 국가안전이 사회나 개인의 안전에 우선한다는 점

에서는 군사시설보호법에 의한 군사계획이 국토기본법에 의한 국토계획에 우선하도록 한 것과 마찬가지로 「정보통신기반보호법」에 의한 정보통신기반시설보호계획 및「재난 및 안전관리기본법」상의 국가안전관리기본계획이나 「국가사이버안전관리규정」에 의한 국가사이버안전정책에 우선한다고 하기도 어렵다.

제4절 사견

아래의 <그림 8>에서 보는 바와 같이 국가안전보장의 체계는 대통령을 수반으로 하여 국가정보원은 국무총리의 통할 없이 대통령의 직접적인 지휘·감독 하에 국가안전보장사무를 총괄하는 국가최고행정기관으로서의 지위를 갖고 국방부는 군사적 위협으로부터 국가안전사무를 수행하는 국가최고행정기관으로서의 지위를 각각 갖는다는 점, 앞에서 살펴본 바와 같이 군사시설보호법에 의한 군사계획은 다른 국가계획에 우선한다는 점, 행정안전부는 전자정부와 관련한 행정기관의 전자적 안전사무를 총괄하는 내부경찰기능을 가진 국가최고행정기관이라는 점, 끝으로 행정각부와 청은 소관사무의 수행에 부수적으로 요구되는 사회목적적 행정경찰권을 갖는 점 등을 종합할 때 조직법상의 사무분장과 사무의 국가목적성 여부에 합치되는 작용법체계 및 국가사이버 관련 계획간의 효력우위를 정비함으로써 국가사이버의 안전을 총합적이고 체계적으로 담보할 수 있도록 법제정비에 착수할 필요성이 있다.



<그림 9> 현행 정부조직상 경찰체제

제4장 주요외국의 입법례

제1절 오프라인 테러에 대한 국제동향

1. 오프라인 테러에 대한 일반적 동향

현실공간에서 발생하는 다양한 테러범죄에 대한 대응법제는 크게 두 가지 형태로 구분해 볼 수 있다. 첫째, 유럽국가나 이스라엘 등과 같이 테러단체에 의한 테러범죄가 빈발하는 경우 형사법 개정이나 대테러특별법의 제정을 통하여 일정한 범죄유형을 테러범죄로 정의하거나 분류한 후 이에 대해 형사절차상의 특별한 취급을 규정하는 경우이다.[40] 둘째, 일본이나 우리나라와 같이 국내외 테러범죄가 빈번하지 아니한 국가에서는 적극적인 대응방식 대신에 기존의 형사법체계를 유지하면서 테러행위가 형법상의 범죄행위를 구성하게 되는 경우 해당 규정에 따라 처벌하고 있다. 이 경우 테러범죄의 처벌을 위한 형사절차법상 특별한 규정은 존재하지 않으므로, 테러범죄도 일반범죄와 동일한 절차에 의하여 처리된다.

2. 오프라인 테러에 대한 국제조약 등

오늘날 국제범죄로서 그 심각성을 더해 가고 있는 국제테러범죄에 대

---

40) 미국의 경우에는 국내테러범죄에 비해 미국 또는 미국민에 대한 국제테러가 월등히 많이 발생함에 따라 형사법상 역외관할권이 인정되는 각종 국제테러범죄의 포괄적 규제를 위한 특별규정들을 마련하는 한편, 1995년 4월 오클라호마시티 폭발테러사건을 계기로 국내테러사건에 대해서도 보다 철저한 대책을 강구하고 있다. Newsweek, 1995. 5. 3., pp.31-32; TIME, 1995. 5. 1., pp.38-42.

하여는 국가간의 정보교환 및 경찰수사상의 협력이나 범죄인인도조약 또는 국제형사사법공조 등과 같은 국제사회의 공동대응노력을 비롯하여 국제테러범죄를 차단하고 테러범죄인의 인도를 의무화하기 위한 각종 협약이 존재한다. 1937년 '테러방지와 처벌을 위한 협약'[41]을 비롯하여, 1960년부터 빈발하기 시작한 항공기납치와 항공기사보타지를 규율하기 위해 1963년에 '항공기내에서 범한 범죄 기타 행위에 관한 협약'(동경협약)[42], 1970년에 '항공기납치 억제를 위한 협약'(헤이그협약)[43], 그리고 1971년에 '민간항공의 안전에 대한 불법행위의 억제를 위한 협약'(몬트리올 협약)[44]이 체결되었다. 외교관 등에 대한 암살, 납치, 유괴, 상해, 폭행, 협박

41) 이 협약은 1934년 10월 마르세이유에서 유고슬라비아 알렉산더 왕과 프랑스 외상 Croatie가 마케도니아 출신 테러리스트들에 의해 살해된 사건을 계기로 국가원수나 기타 공직자에 대한 테러행위를 금지하고 국가간 협력의무 등을 규정한 최초의 국제테러 규제를 위한 협약이었으나, 발효되지 못하였다. 정형근, 전게서, 101면 이하 참조.

42) 전문 7장 26조로 구성된 이 협약은 항공기의 안전, 항공기상의 인명과 재산의 보호 등 민간항공의 안전을 증진하기 위하여 항공기내에서 일어나는 범죄에 대한 처리방법을 규정한 것으로 우리나라에 대해서는 1971. 5. 20. 발효되었다. 형법상의 범죄행위뿐만 아니라 항공기 자체나 승객의 안전을 위협하거나 기내의 질서 유지를 위협하는 행위에 대한 처벌의 관할권에 주안점을 두어, 기내에서 발생한 범죄에 대한 항공기등록국의 관할권을 규정하고(제3조), 자국민 혹은 상주하는 주민에 의한 범죄에는 적극적 속인주의를, 이들에 대한 범죄에는 소극적 속인주의를, 안전보장에 관계되는 범죄에는 "당해국 보호주의"를, 그리고 영토상에 영향을 미치는 범죄에 대하여는 속지주의를 택함으로써 관할권을 확대하였다(제4조).

43) 이 협약에서는 항공기의 납치, 점거 및 동 행위의 기도와 그 공범행위를 범죄행위로 규정하는 한편(제1조), 이에 대한 처벌을 입법화할 의무를 체약국에 부과하고 있다(제2조). 특히 범죄가 당해국에 등록된 항공기내에서 행해진 경우, 범죄가 행해진 항공기가 범죄혐의자를 싣고 그 영토 내에 착륙한 경우 등에는 범죄행위를 기소할 수 있도록 적절한 입법조치를 하도록 하였다(제4조 1항). 관할권을 행사할 수 있는 국가로서는 항공기 등록국가, 납치범을 태운 채 항공기가 착륙한 국가, 항공기 임차인의 주요 사업지나 상주지 국가, 납치범이 발견된 국가 등을 규정하여 관할권의 경합을 인정하고 있다(제4조 3항). 뿐만 아니라 항공기 납치행위를 '인도 아니면 기소'하도록 규정하였고(제7조), 체약국은 형사처벌 또는 인도를 위해 납치범을 반드시 구금하도록 하고 있다(제6조). 우리나라에서는 1973. 2. 17. 발효되었다.

등 가해행위에 관련되는 조약으로는 1973년 '외교관 등 국제적 보호인물에 대한 범죄의 방지 및 처벌에 관한 협약'[45]이 있으며, 외교관은 물론 일반사인의 인질억류의 규제를 위하여서도 '인질억류방지에 관한 국제협약'[46]이 체결되었다. 1988년에는 '항해의 안전에 대한 불법행위의 억제를 위한 협약'(로마협약)[47]이 체결되었다.

---

44) 이 협약은 항공기에 대한 폭력과 사보타지를 규율하기 위하여 체결되었는데 범죄의 범위를 항공기의 불법납치 뿐만 아니라 지상에서의 공격, 비행시설물에 대한 공격까지도 포함하는 것으로 확대시켰으며 미수와 공범까지도 포함시켰다. 헤이그협약과 마찬가지로 '인도 아니면 기소'원칙을 확립하였으며(제7조), 재판관할권 역시 이와 동일하다. 다만 순수한 국내범인 경우에는 이 협약의 적용을 받지 않으나 범인이 외국으로 도피한 경우에는 적용을 받는 것으로 하였다(제4조 2항). 우리나라에서는 1973. 9. 1. 발효되었다.

45) 전문 12개조로 이루어진 이 협약은 국제적 보호인물의 범위(제1조) 및 이들에 대한 범죄행위(제2조)를 규정하고 각국은 이러한 범죄를 예방하기 위해 모든 조치를 취할 것은 물론 이와 관련된 정보교환, 행정조치의 상호조정 등 국제협력을 도모하도록 하고 있다(제4조). 또한 형사관할권의 성립요건을 정하고(제3조), 당해국은 이들을 적절한 형벌로 처벌할 것을 규정하고 있다(제2조 2항). 이를 위하여 범죄혐의자를 관할권을 갖는 국가에 인도하든지 아니면 사법처리를 위하여 관계당국에 회부하도록 하고 있다(제7조, 제8조). 우리나라에서 는 1983. 6. 24. 발효되었다.

46) 이 협약은 인질범죄를 "국가, 국제기구, 개인 등에 어떤 행위를 강제하기 위하여 인질의 신체적 손상을 위협하며 신체적으로 구속하는 것"으로 정의하고(제1조), 이러한 범죄의 예방 및 처벌을 위한 제 규정을 마련하고 있다. 동 범죄에 대한 관할권(제5조), 혐의자의 체포, 구금의 의무화(제6조), 혐의자의 공정한 취급(제8조), 사법공조의무(제11조) 등을 규정하고 있다. 우리나라에서는 1983. 6. 3. 발효되었다.

47) 1985년 팔레스타인 해방전선(PLF)에 의한 이탈리아 여객선 Achille Lauro호 납치사건을 계기로 1988년 3월 1일 체결된 이 협약은 폭력 기타 협박에 의한 선박 납치, 승선중인 자에 대한 폭행으로 운항의 안전을 해할 가능성이 있는 경우, 선박파괴 기타 운항의 안전을 해할 가능성이 있는 선박·화물의 손괴행위, 해운시설의 파괴와 중손괴, 선박의 안전운항을 해할 위험성이 있는 업무방해행위, 허위정보를 제공하여 선박의 안전운항을 위협하거나 사람을 사망 또는 상해에 이르게 한 경우를 범죄로 규정하고 있다(제3조). 또한, 각 당사국은 자국국적의 선박 및 영토 내에서의 범행이나 자국국민에 의한 경우는 '의무적 관할권'을 갖고, 자국에 거주하는 무국적자의 범행인 경우 또는 자국민이 피해를 입은 경우, 자국에게 일정한 작위나 부작위를 강요하기 위한 범행인 경우 등에는 '재량에 의한 임의적 관할권'이 인정되고 있다(제7조 1, 2항). 이외에도 범죄인인도의무 및 형사사법공조의무도 규정하고 있다(제12조).

그밖에 1971년 '국제 요인에 대한 대인범죄와 강요의 형태를 취하는 테러행위의 방지와 처벌에 관한 협약'[48]이 미주기구(OAS)의 주관 하에 체결되었고, 1976년에는 유럽국가간에 '테러리즘의 억제에 관한 유럽협약'이 채택되어 지역적 차원에서 테러범죄에 대하여는 범인을 관계국가에 인도하거나 국내법에 따라 처벌할 것을 의무화하고 있다.

그러나 국가간의 시각 내지 이해의 차이로 인하여 어떠한 테러범죄를 정치범죄로 보고 국제법상 정치범 불인도원칙을 내세워 범죄인인도를 거부한다거나 국가간의 실정법 차이로 인하여 관할권을 부인하는 등의 문제로 인하여 테러범죄의 규제에 있어 국가간 공조가 잘 이루어지지 아니하는 경우가 발생할 뿐 아니라, 테러범죄를 규율하는 국제조약의 법적 구속력으로 인하여 국제테러규제 조약에 가입하지 아니거나 조약상의 의무를 이행하지 않은 경우에도 그것을 강제할 수 있는 방법은 없는 등 테러에 대한 국제사회의 실효적이고 포괄적인 규제 방안의 정착은 거의 불가능한 것이 현실이다.

이러한 사정은 테러의 행위지와 불법결과의 발생지가 일치하는 오프라인 테러와 달리 사이버테러의 경우에는 행위자의 행위지 내지 행위자의 소재지, 사이버테러의 효과발생지 및 사이버테러의 도구로 사용된 사이트의 소재지 등이 각각 달리하기 때문에 국제사회의 공조적인 협조체계의 구축은 더욱 불가능하고 해당 국가 스스로가 보안 및 방어체계를 확립할 수밖에 없을 것으로 생각된다.

---

48) 이 협약은 1971년 2월 2일 워싱턴에서 서명되었는데, 주로 외교관 납치의 방지에 주목적을 둔 것으로서 기타 살인이나 암살의 방지 및 처벌규정도 두고 있다. 1989년 말 현재 체약국 수는 9개국이다.

제2절 사이버테러와 관련한 주요국의 동향

1. 미국의 사이버안전센터와 관련 주요법률

가. 국가사이버보안센터

미국의 국토안보부는 사이버공격으로부터 네트워크 시스템을 보호하기 위하여 2004년 국가사이버보안센터를 설립하여 사이버 기간시설 보호를 위한 효과적인 사이버공간 대응체제의 구축·유지와 중요기간기설의 보호를 위해 '국가사이버공간 대응시스템(National Cyberspace Response System, NCRS)'과 '사이버위험관리 프로그램'을 실행하도록 하고 있다. 전자는 컴퓨터사용자가 국가사이버공간 대응시스템에 등록하여야 최신정보를 수신 받을 수 있도록 함으로써 1차적으로는 국가컴퓨터위기대응팀이 사이버위협과 취약성을 분석, 감소시키거나 사이버위협 경고정보를 유포하는 등 사이버위협에 대한 효율적인 대책을 세우게 하고, 종국적으로는 13명의 연방정부기관으로 구성되는 국가사이버대응조정단(National Cyber Response Coordination Group)으로 하여금 사이버사건에 대한 연방차원에서의 대응을 취할 수 있도록 하고 있다.

후자는 국가사이버보안센터에 의하여 운영되는 것으로 사이버 위험을 관리·평가하고 사이버 기간시설의 안전 확보를 위한 보호수단을 취하는 기준으로 기능한다. 이 프로그램의 중요한 내용으로는 2년에 한번씩 국가중요시설에 대한 사이버사건들에 대응하기 위한 준비능력을 평가하기 위하여 시행되는 국가차원의 사이버보안 훈련(또는 사이버폭풍), 매년 10월 州·대학·민간부문의 참여하여 이루어지는 국가사이버보안 인식행사 및 소프트웨어의 취약성을 감소시키고 불법이용을 최소화하며 신뢰할 수 있

는 소프트웨어의 개발과 설치를 향상시킬 수 있는 방안구축을 위한 소프트웨어 보장프로그램 등으로 구성되어 있다.

나. 주요관련 법

1) 국토안보법(Homeland 보안 Act of 2002)

2001년 9·11테러 이후 미국 국내에서의 테러에 대응하기 위하여 2002년 6월6일 부시 대통령은 국토안보부의 창설을 제안하였다. 부시 대통령은 연방재난관리국, 해안경비대, 세관국, 이민국, 국경경비대, 비밀경찰국 등 국가안보와 관련된 각 연방기관의 통합과 이를 총괄하는 부서로서 국토안보부 설립을 내용으로 하는 법안을 제출하였고, 2001년 11월 25일 서명함으로써 성립되었다. 국토안보부로 하여금 국토안전보장업무를 총괄하도록 하고, 정보기술을 유효하게 활용하여 사이버공격이나 물리적 공격으로부터 미국국토를 방위함을 목적으로 제정된 「국토안보법」은 주요기반시설의 보호를 국토안보의 핵으로 전제하여 주요기반보호를 위한 '정보분석 및 기반보호국'을 설치하고, 주요기반 보호와 사이버 위협에 대한 대응을 위해 설립되었던 주요기반보호센터, 주요기반보장국, 국가통신시스템, 컴퓨터비상대응팀 등의 기구를 통합하였다.

「국토안보법」은 포괄적 테러로부터 미국의 국가기반을 보호하고자 제정된 법으로써 총 17장으로 구성되어 있으며, 특히 사이버보안과 관련된 규정으로는 "2장 정보분석 및 기반시설 보호에 관한 규정", "제10장 정보보호에 관한 규정"이 대표적이다. 이 법에서 규정하고 있는 국토안보부의 주요임무로는 다음과 같다. ①미국 내에서의 테러리스트 공격을 억제하고 테러리즘에 대한 미국의 취약성을 감소시키며 미국 내에서 테러리스트의 공격으로 인한 피해를 최소화한다. ②복구 지원시 자연적·

인위적 위기와 비상계획에 관한 업무를 포함하여 이관된 기관의 모든 직무를 수행하며 국토안보를 목적으로 하는 모든 노력과 활동 및 프로그램을 수행한다. 이와 동시에 ③미국의 경제안전을 보장하고 불법 마약거래와 테러리즘간의 연계를 감시·차단한다.

2) 애국자법(Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act; USA Patriot Act)

2001년 9월 11일 테러공격과 관련된 입법 중 가장 대표적인 법률인 「2001년 테러방지 방안수립을 통한 미국통합 및 강화법」 또는 그 약칭인 「애국자법」은 테러용의자의 수사와 테러조직에 대한 자금원과 지원을 차단하기 위한 목적을 가진 다양하고 복합적인 형사처벌조항을 담고 있다. 그 주요 내용을 살펴보자면, 종래 법집행기관의 용의자 관련된 전화번호 기록 권한을 인터넷이나 휴대전화를 포함한 전자통신으로 확대하고 DCS1000(통칭 '카니보어(Carnivore)')[49] 등에 의한 IP 주소 등의 기록(통신내용의 기록은 불허)을 인정함과 아울러 사람의 생명 등에 관한 긴급사항 발생시 인터넷 통신사업자가 법집행기관에 대한 고객통신기록(통신 내용을 포함)의 공개를 합법화함으로써 컴퓨터 해킹과 같은 전산망 침입자의 감시에 필요한 피해자(컴퓨터 소유자)의 법집행기관에 대한 통신감청 의뢰요구를 수용하였다.[50]

그리고 사이버테러의 억제와 예방을 위하여 관련 처벌을 강화(동법

---

49) DCS-1000기술은 연방법집행기관에게 미국뿐만 아니라 외국에 위치한 테러조직에 대한 광범위한 감시를 가능하게 하는 것으로 인터넷과 기타 전자통신 "전송"을 통하여 이루어지는 테러조직원 사이의 통신을 추적하는 기술이다. 컴퓨터네트워킹시스템에 대한 공격을 예방하기 위해 매우 필요한 테러방지대책으로 평가된다.

50) 그 결과 「애국자법」은 인터넷상 모든 종류의 사생활에 대한 감시를 허용하고 있으며, 심지어는 법집행기관으로 하여금 개인이메일을 통해 전달되는 사적 정보의 수집을 가능하게 하였다고 한다.

제814조)하여 보호되는 컴퓨터에 손해를 가한 해커에 대한 최고 형량을 초범에게는 10년, 상습범에게는 최고 20년형으로 상향·조정하는 한편, 고의범 이외에도 미수범을 처벌할 수 있는 근거를 마련하여 해커가 1년 이내에 야기한 모든 사건의 피해규모를 합산하여 처벌할 수 있도록 하였다. 나아가 국방이나 국가안전보장과 관련된 컴퓨터에 대하여 피해를 야기한 경우에는 그 피해에 대한 입증이 없는 경우에도 처벌이 가능하도록 하였다. 그러나 「애국자법」의 대부분 조항은 기존의 연방 법률을 수정하거나 증보한 것이기 때문에[51], 해당 조항이 실효성을 가질지 여부에 대하여는 회의적인 입장이 많다.

어쨌거나, 「애국자법」에서 가장 논란이 되는 조항 중 하나는 연방기관에게 법원에 영장을 청구할 만한 적정한 사유가 있을 경우 사전통지 없이 사후통지에 의한 비밀수색을 할 권한을 부여한 제213조이다. 이 조항에 대하여는 "통지 없이 개인의 재산과 사업기록의 압수를 가능하게 할 뿐만 아니라, 全國단위 수색영장의 발부를 가능하게 하고 중앙정보부(CIA)와 국가안보국(NSA)이 국내에서 활동할 수 있게 한다"는 비판이 있기는 하지만, 사후통지의 수색(sneak and peak searches)은 중립적이고 독립된 판사에 의한다는 점과 수사기관으로 하여금 "계획을 누설"하지 않고서 증거를 수집할 수 있게 하므로 "은둔중인" 테러리스트나 테러단체의 임시거소로부터 가치가 있는 정보를 적시에 실효적으로 수집할 수 있도록 한다는 점에서 긍정적인 평가가 이루어지고 있다.

---

51) 예컨대, 애국자법 제203조는 기타 이해관계기관과 국외정보와 관련된 기소정보를 공유할 수 있도록 연방형사소송법(Federal Rules of Criminal Procedure)을 수정하고 있고, 제219조는 테러사건에 대한 연방단위 수색영장을 허용하도록 연방형사소송법을 수정하고 있으며, 제213조는 "sneak and peak"로 알려진 수색영장집행의 사후통지를 용인하기 위하여 연방법률집(United States Code) 제18편 제3103조의a에 하위항목을 증보하고 있다.

3) 사이버보안강화법

「사이버보안 강화법(Cyber 보안 Enhancement Act of 2002)」은 2002년 하원에서 통과 후 상원에서 폐기되었으나, 그 주요내용은 「국토안보법」 제2장 제225조로 수용되어 있다.

4) 「해외정보감시법」(Foreign Intelligence Surveillance Act)

「해외정보감시법」은 일반 법집행기관의 감청수사를 규제하고 있는 미국 연방법령집 제3권(Title 3. 「감청법」(the Wiretap Statute)과 달리 미국의 대외정보 수사를 강화를 위해 "해외정보"에 대한 미국정부의 수집을 규율하고 있다. 이 법은 본래 전자적 감청과 도청에 대해서만 규제하였으나, 1994년의 개정법에 의하여 보안수사와 연계한 물리적 비밀 잠입 수사를 허용하는 규정을 포함하게 되었고, 1998년에는 법원의 "pen/trap 명령"[52]을 허용하는 개정이 있었다. 동 법에 의하여 영업 기록에 대한 획득도 가능하게 되었으며 이로 인해 수사 영장의 발부 기준인 '상당한 이유'의 규정이 완화되었고 그 대상에 있어서도 미국인에 대한 최소한도 규정하였다. 또한 FISA에 의한 수사 절차 및 승인에 관한 구체적 내용이 규정되었다.

5) 「법집행기관을 위한 통신지원법」(Communications Assistance for Law Enforcement Act)

1994년에 제정된 「법집행기관을 위한 통신지원법」은 급변하는 통신기술 환경에 직면하여 법집행기관의 전자적 수사 능력을 지속적으로 보유하도록 함에 그 목적이 있다. 즉, 통신사업자들로 하여금 법 집행 당국이 법원의 명령 또는 다른 법적 권한에 의하여 전자수사를 실시할 경우

52) 밖으로 나가는 주소정보(pen register)와 안으로 들어오는 주소정보의 기록(trap and trace) 명령을 의미한다.

에는 법집행기관을 지원할 의무를 법률로 규정하여 국가안보와 공공안녕을 보호함을 목적으로 하고 있는 것이다.

6)「연방정보보안관리법」(Federal Information 보안 Management Act)

「연방정보보안관리법」은 「전자정부법」(E-Government Act of 2002) 제3편으로 제정된 것으로, 연방의 주요 정보자원에 대한 보호 및 통제를 위해 포괄적인 프로그램을 제공하는 한편, 고도로 네트워크화된 국가기반 환경의 보호를 위해 민간을 비롯하여 국가안보와 관련이 있는 기관과 법집행 기관 전체의 정보보호사무를 조정함과 동시에 사이버위협에 대해 효과적으로 대응할 수 있도록 함을 목적으로 하고 있다. 정부 전체에 대한 관리감독은 국토안보부에 부여하고 있으며 연방을 지원하는 정보자원에 대한 정보보호 통제의 효과를 보장하기 위한 기본적 틀을 제공함과 아울러 연방정보 및 정보시스템을 보호하는데 필요한 최소한의 통제장치의 개발 및 유지를 제공하고, 연방 정보보호 프로그램의 감독 및 개선을 위한 메커니즘을 규정하고 있다.

2. 일본의 대응체계

가. 개관

1999년에 책정된 "경제신생대책"에서 일본정부는 2003년까지 전자정부의 기반을 구축과 관련하여 컴퓨터 네트워크에 접속된 정부기관과 민간중요분야 등의 시스템은 항상 해커와 사이버테러의 위협에 노출되어 있다는 정책적 판단을 전제로 2000년 "정보보안 관계성·청·국장회의"(의장 : 내각관방부장관)에서 "해커대책 등의 기반정비 관련 행동계획"을

책정하였다. 동 행동계획에서는 해커대책을 위한 방안으로, 정부기관의 방호기술의 개발과 감시·긴급대처체제의 강화, 민간중요분야 등에서의 방호강화의 촉진 등이 제시되어, 해커에 대한 근본적인 대책을 정부전체에서 추진하기로 합의하였다.

경찰은 종래부터 고도기술범죄대책을 추진하고, 컴퓨터 네트워크상의 치안유지에 노력하여 왔다. 또 경찰 자신이 보유한 정보통신시스템에 대하여 보안대책을 실시하는 외에, 산업계와의 연대를 강화함과 동시에, 고도기술범죄 및 사이버테러대책에 관한 홍보·계발활동 등을 실시하고 있다. 향후 경찰의 정보보안시책을 반석 위에 올려놓기 위하여, 법집행방호대책의 실시·산업계와의 연대 등 다방면에서 정보보안시책을 강화함과 동시에 그 기반이 되는 기술, 지식 등을 관계기관과 공유하고 있다.

나. 정보보안대책 현황과 고도기술범죄·사이버테러의 위협

종래 컴퓨터와 그 내부정보를 해커와 사이버 테러로부터 보호하기 위한 여러 가지 대책이 검토·실시되어 왔던바, 기술 및 운용면에서의 보안대책이 강조되고 실행되고 있지만, 네트워크의 공간적·시간적 무제약성과 익명성의 특징상 완전한 보안대책은 현실적으로 어렵다는 입장이다. 방화벽의 설치 등의 조치가 되어 있더라도, 보안구멍이 기술면 또는 운용면에서 발생하고 있어, 결과적으로 보안대책이 불완전하게 되는 경우가 발생할 수 밖에 없음도 시인되고 있다. 즉, 보안대책의 실시를 통해 위험을 감소시키는 것은 가능하나, 위험을 완전히 제거할 수는 없다는 인식이 전문가 사이에서는 일반적이다.

2000년 과학기술청, 총무청을 비롯한 8개의 중앙성・청 등이 인터넷상

개설하고 있는 홈페이지가 마음대로 변경·소거된 사건이 연이어 발생하였다. 피해를 입은 홈페이지에서는 해외의 성인잡지의 홈페이지에 접속하는 창이 설치되고, 문서가 영어·중국어로 바뀌었다. 그 외에 일부 성·청에서 침입성공까지는 이르지 못하였으나, 시스템에 부정침입하려고 하였던 흔적도 발견되고 있다. 이들 사안은 동시다발적으로 발생하고 있고, 향후의 사이버테러발생의 징후를 보여주는 일본에서는 최초의 사례라고 할 수 있다.

일본의 고도기술범죄에 대하여는, 컴퓨터·전자적 기록을 대상으로 한 사안은 감소하고 있는 반면, 인터넷의 급속한 보급에 따라 컴퓨터 네트워크를 매개로 하는 범죄가 급격히 증가하고 있고 그 태양도 타인·가공명의에 의한 서비스제공자(ISP)와의 계약과 은행구좌의 개설 등을 수법으로 하는 사안, 이른바 타인 사칭 사안이 다발하는 등 교묘화하는 경향에 있다.

다. 전자정부의 실현을 향한 cyber terror대책의 추진

안전하고 신뢰받는 전자정부를 실현하기 위하여 경찰의 정보통신시스템m에서의 정보보안대책을 추진함과 동시에 이를 통하여 취득한 지식·기술과 함께 정부기관과 민간중요분야를 대상으로 하는 사이버테러대책에 이바지할 정보제공 등을 행하는 등 다음의 제시책을 추진하고 있다.

(1) 정보수집체제 등의 강화

사이버테러를 미연에 방지함과 동시에 사이버테러가 발생한 경우에 정확하게 이에 대처하기 위하여 사이버테러를 감행할 우려가 있는 국내외의 테러조직 등에 대한 정보수집과 민간 중요분야 등의 관리자와의 연

대강화 등을 위한 인적·물적 체제의 강화를 도모한다.

⑵정보보안수준의 향상

사이버테러는 정보통신시스템이 취약한 부분을 노려 공격하여 올 것으로 예상되므로, 높은 보안을 확보한 전자정부를 실현하기 위해서는, 시스템 전체의 보안수준을 일정수준 이상으로 하여야 한다. 또 경찰의 정보통신시스템에 있어서 보다 고도의 보안을 실현하기 위한 연구개발의 성과, 사이버테러대책에 관련된 연구개발의 성과 등 중에서 정부기관 및 민간중요분야 등에서 유효하게 활용할 수 있는 정보를 사이버테러의 사전 예방이라는 관점에서 제공한다.

⑶감시·긴급대처체제의 정비·강화

경찰의 정보통신시스템의 안전성을 더욱 높이기 위하여, 고도기술범죄, 부정접근수법에 관한 분석 등을 활용하는 등 기존의 감시·긴급대처체제의 강화·확충을 행한다. 또 전자정부 전체에 중대한 영향을 미칠 가능성이 있는 사태에 정확하게 대처하기 위한 체제에 대하여 검토한다. 나아가 정부기관 및 중요 민간분야와의 긴급정보연락체제를 확립한다.

⑷정보보안정책의 책정

경찰이 정보보안의 종합적·체계적 대책의 기본이 되는 보안정책의 검토에 있어서, 미국을 비롯한 해외의 대응방안 마련 동향 등을 조사하고, 국제규격에 준거한 신뢰할 수 있는 보안정책을 책정한다. 또한 높은 수준의 보안을 갖는 전자정부를 실현하기 위하여 정보보안관계 성·청·국장 등 회의에서 책정된 “정보보안 정책에 관한 지침”의 검토에 이바지할 정보를 제공한다.

⑸ 평가·검증시스템의 검토

경찰의 정보통신시스템에 대한 부정접근과 사이버테러에 의한 공격에 대하여 강력한 방호력을 갖추기 위하여 부정접근대책과 사이버테러대책에 관한 지식·기술을 활용한 “penetration test” 등에 의하여 평가·검증을 행하는 것을 검토한다.

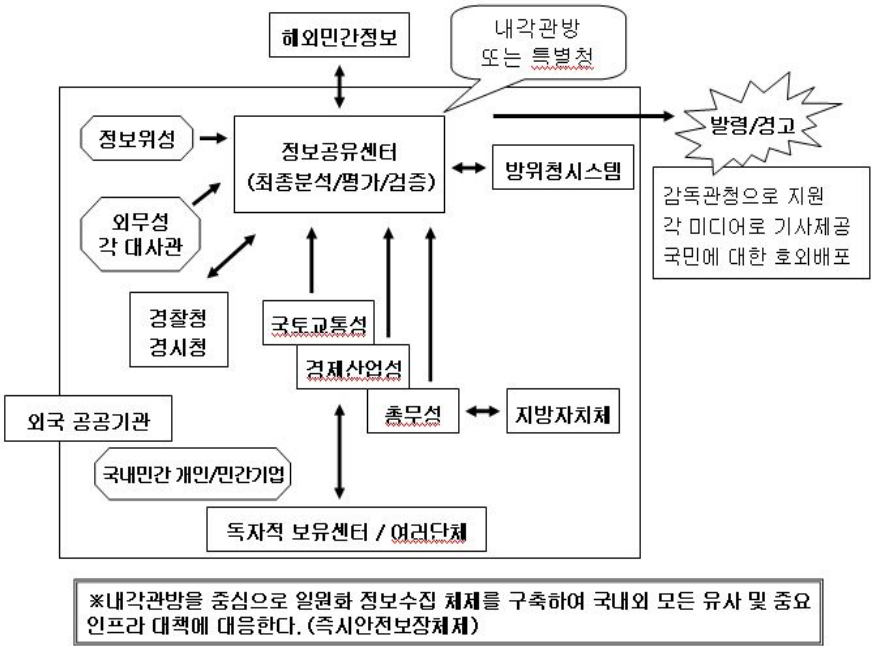
라. 일본의 대테러정책의 결정과정(‘내각결의’의 개정)

일본의 경우 한국의 국가정보원과 같은 특별한 별도의 국가정보기관은 없다. 그러나 내각관방, 법무성, 외무성, 경찰, 국가공안위원회, 방위청 등에서는 각자의 필요에 의하여 정보수집·분석업무를 수행하는 부서를 설치하고 있다. 각 기관에서는 다른 기관의 협력요구에 응해야할 법적 의무는 없다. 그러나 각 기관에서는 수집·분석된 정보를 행정상의 지휘계통에 의하여 국정최고책임자인 내각의 수상에게 전달하게 된다. 이렇게 각 기관으로부터 정보를 수집·분석하고 분석된 정보를 종합하여 내각수상에게 보고하는 업무를 담당하고 있는 것이 ‘내각정보조사실’이다.

유기적이고 효율적인 테러정책 추진을 위해 가장 중요한 것은 테러와 관련된 정확한 정보를 수집하고 다른 기관과의 유기적인 협조 하에 수집된 정보에 대한 철저한 분석과 동시에 이에 대한 대응방안을 신속히 마련하는 일이다. 이러한 측면에서 일본의 정보 수집·분석기관은 효율적인 정보수집능력을 가진 중앙기관이 존재하지 않기 때문에 기관 상호간의 협조가 원활하지 않을 경우에는 자칫 매우 큰 문제가 발생할 수 있다.

일본에서는 이러한 문제점을 인식하고 9·11테러 이후 각 기관간의 정보독점을 위한 ‘기관이기주의’를 배제하고 효율적인 결정을 하기 위하

여 '중대테러 등 발생시의 정부의 초동조치에 대하여'라는 내각결의(각의)를 개정한 바 있으며, 9·11 이후에는 이 '각의'에 의하여 대테러정책이 결정·수행되고 있다(아래의 <그림 10> 참조).[53]



<그림 10> 일본의 정보수집 평가체계도

중대한 테러 행위가 발생할 경우에는 관계 성·청에서는 사전에 정비된 정보연락체계에 의해 '내각정보조사실'을 거쳐 신속히 내각 총리대신, 내각관방장관, 내각관방부장관 및 내각위기관리감에게 보고·연락을 함과

53) 조성용, "전게논문", 2003, 20-22쪽 참조. 조성렬, "9·11 사태 이후 일본의 대테러전 전력", 「Strategy 21」, 제5권 제2호, 2002 가을·겨울, 100-127면.

동시에 대응체제를 확립하여야 한다. 한편, 일본에서는 중대테러에 대처하기 위하여 내각총리대신의 판단에 의해 내각에 내각총리대신 또는 내각관방장관을 본부장으로 하고, 내각관방장관이나 필요한 경우 본부원 가운데 국무대신인 자 중에서 본부장이 지칭하는 자를 부본부장으로 하는 대책본부를 설치하는데, 여기에서는 관계기관의 구체적 대응조치가 원활하게 진행될 수 있도록 중요사항에 대해 협의·결정하게 된다. 이러한 대책본부체계를 통하여 일본에서는 관계 성청이 테러에 대응하여 일치단결하여 협력함으로써 법질서와 국가의 안전을 유지할 수 있는 시스템을 마련하고 있다.

마. 일본의 대테러관련 법제

9·11테러 이후 일본에서는 2개의 국제적인 조약이 시행되었으며, 이에 대해 구체적인 입법을 한 바 있다. 그 중 하나는 「폭탄테러방지조약」의 시행입법인 「테러리스트에 의한 폭탄사용의 방지에 관한 국제조약의 체결에 따른 관계법령의 정비에 관한 법률」이다. 이법이 제정됨에 따라 「폭발물단속벌칙」, 「방사선동위원소에 의한 방사선장애 방지에 관한 법률」 등 관련 규정에 국외범에 대한 처벌규정을 신설하게 되었다. 둘째로 일본에서는 「생물병기금지법」을 개정하여 생물병기 또는 독소병기를 사용하여 생물제, 독소로 국민을 위협하는 행위나 독극물을 발산시키는 행위 이외에도 이러한 독극물을 부주의하게 발산시켜 생명 등에 위험을 발생하게 한 행위에도 가벌성을 인정하고 있다.

셋째로 「화학병기금지법」을 개정하여 화학병기를 사용하여 독성물질 등을 발산시키는 행위와 아울러 이것을 부주의하게 발산시켜 생명 등에 위험을 발생하는 경우에도 처벌하도록 규정하고 있으며,「핵원료물

질」·「핵연료물질」·「원자로 규제에 관한 법률」 등을 개정하여 핵원료물질과 핵연료물질에 오염된 물질을 함부로 취급함으로써 방사선을 방사시켜 생명·신체·재산에 위협을 발생시킨 행위 역시 처벌하도록 하고 있다.

그 밖에도 「테러자금공여방지조약」의 시행입법으로 「금융기관본인확인법」과 「테러자금공여처벌법」을 제정함과 아울러 「외환 및 외국무역법」을 개정함으로써 테러단체에 자금이 전달되는 것을 원천적으로 차단하고 있다. 즉 이 법들에 의하여 공중이나 국가를 대상으로 한 테러를 위한 자금의 제공·수집을 처벌하고 제공자금을 몰수할 수 있도록 하고 있다.[54]

제3절 시사점

미국을 비롯한 일본은 기본적으로 가상공간은 "우리의 주요기간망을 작동하게 해주는 무수히 많은 상호 연결된 컴퓨터, 서버, 루터, 스위치, 광섬유케이블로 구성된 우리나라의 통제시스템이기 때문에 가상공간의 건전한 기능은 우리의 경제와 국가안보에 필수적인 것이다"는 인식을 전제로 포괄적인 사이버테러정책 및 입법을 허용하고 있음을 볼 수 있다. 특히, 미국의 경우에는 9·11 테러를 계기로 많은 테러법이 제정되었으며, 그 중 「애국자법」에 대해 갖는 전체주의국가화 경향에 대한 비판은 별론으로 「국토안보법」과 같이 각각의 목적을 달리하는 정보기관의 개별적 역량을 극대화하면서도 통합적인 관리시스템을 갖추도록 한 것은 "原

54) 이상 일본의 대테러관련 법제에 관해서는 조성용, "일본의 테러관련 법제연구", 「대구법학」 제6호, 2003, 22-23면 참조.

데이터"는 각각의 정보기관이 자체적으로 보유하고 있는 정보를 기초로 다른 의미를 가질 수 있고, 이러한 원데이터에 대한 기관별 분석·평가가 가해진 인식대상으로서의 정보(Information)는 기관마다 다를 수 있지만 국가안전을 위해서는 통합적인 판단대상으로서의 지식(Knowledge)으로 구축되어야 한다는 점에는 우리에게 시사하는 바가 크다고 할 것이다.

구체적으로 말하자면, 우리 헌법 제37조제2항이 법률유보원칙으로 천명하고 "국가안전보장"을 최우선의 법익으로 출발하여 "질서유지>공공복리"의 관점에서 이들 법익의 보호를 위해 필요한 경우 필요한 최소한의 범위에서 법률로써 기본권을 제한할 수 있다고 규정하여, 국가 없는 국민이 존재할 수 없고, 국가가 존재한다면 질서를 토대로 모든 국민이 자신의 기본권을 대등하게 향유할 때 공공복리 또한 가능하게 되고, 그 점에서 법률에 의한 기본권의 일부제한 또한 정당화된다는 헌법적 질서를 표현하고 있다는 점, 헌법은 국가권력의 구성에 있어 "상호견제를 통한 균형의 원리"에 입각하여 국가권력을 입법·행정·사법으로 분장할 뿐 아니라 행정권한 또한 정부조직법을 통해 분장하여 개별 기관의 "Synergy Effect"를 통한 국가전체적인 "Synergy Effect"를 도모하고 있는 점 등을 감안할 때, 정부조직법에 의한 기관별 소관사무에 대한 전문적 판단능력을 전제로 한 사이버데이터의 공유와 해당 데이터에 대한 기관별 정보화를 토대로 이를 통합하는 기관에 의해 행정에 의한 정보의 국가전체를 위한 지식화를 도모할 필요가 한 것으로 보아야 한다는 것이다.

그러나 우리의 경우에는 정부는 분산서비스거부(Distribute Denial of Service·DDoS) 공격을 계기로 국가사이버안전 전략회의에서 국가사이버위기 종합대책[55]을 최종 확정한 것과 관련하여, "사이버위기′ 빌미로 과

55)주요 내용은 평시 국가기관간 사이버위기관리 기능을 명확히 하고, 민간분야의

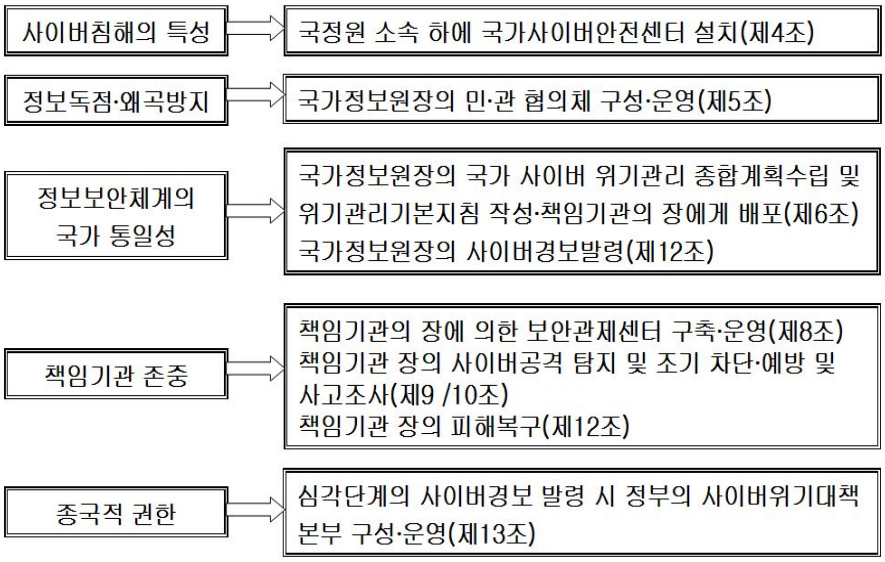
도 규제하나, 정부 '종합대책' 기본권 침해 우려… 책임도 국민의식에 떠넘겨"라는 언론보도[56]에서 보는 바와 같이 이성적이기보다는 감성적인 정책비판이 주류를 이루는 결과 통합적인 정보관리체제에 대해 지극히 부정적인 입장을 보이고 있다.

이러한 부정적인 요소를 극복하고 현재 국회에 계류 중에 있는 아래의 <그림 11>과 같은 내용을 가진 "사이버위기관리법"을 맹목적으로 반대할 것이 아니라 법의 필요성여부를 먼저 논하고 다음으로 필요하다면 헌법상 보장된 국민의 기본권과 국가의 책무와의 비교형량을 통해 개별조문에 대한 검토를 통해 전자정부를 통해 국제사회가 하나로 "연결된 사회"(Connected Society)의 구성요소로서 우리의 사이버안전을 능동적으로 보호할 필요가 있다고 할 것이다.

부언하자면, 장기적으로는 정보화 예산 대비 정보보호 예산을 단계적으로 확대하고, 정보 보호 설비투자 제고를 위한 조세감면정책이나 전력·통신 등 국가기능유지 핵심시설의 보안체계의 고도화 등 21세기 사이버환경에서 주도권을 확보하고 안보위협에 대비하기 위한 정부차원의 대책이 필요한 시점이라고 할 것이다.

사이버안전 수준을 높이기 위해 학교·직장 및 민방위 훈련시 사이버보안교육을 확대하는 것 등이다. 아울러 자동차·조선 등 산업별 협회에 보안관제센터(ISAC)를 세워 사이버침해 차단 및 산업기밀 보호 활동을 강화키로 하였으며, 국가 사이버위기 때 구성될 민·관 합동 범정부 대책기구는 위협분석 및 경보발령, 외국과 공조체계 가동 등을 총괄하며, 기구의 언론창구는 방송통신위원회로 일원화하는 것을 내용으로 하고 있다.

56) "미디어 오늘", 2009.9.13.



<그림 11> 국가사이버위기관리법(안)의 주요내용

제5장 맺는 말

“다음 세계대전은 사이버 공간에서 시작될 수도 있다. 이런 전혀 새로운 전쟁의 시작은 전통적인 외교의 영향력에서 벗어나는 일이 될 것이라며, “사이버 공간에서는 슈퍼파워와 같은 통제자가 없고, 모든 시민이 슈퍼파워이기 때문이다. … 특히 봇넷 군단이나 감염된 컴퓨터, 그리고 이에 대한 통제권만 있으면, 누구라도 사이버 전쟁에서 엄청난 전투력을 휘두를 수 있다”는 ITU 사무총장 하마둔 뚜레의 경고[57]가 시사하는 바와 같이 사이버전은 일정한 지역에서 물리적 힘의 행사에 의한 살상을 매개로 상대방을 무력화하는 종전의 전쟁개념과 달리 현대 정보사회 및 국가의 기반을 이루는 인터넷에 대한 공격을 통해 사람에 대한 살상 효과 없이도 특정한 집단이나 사회 및 국가를 무력화하는 전쟁의 양상을 띠게 된다. 이러한 사회적 국가적 혼란의 효과는 대규모의 군인과 장비의 도움 없이, 자해불순세력이나 불순국가가 양성하거나 보유한 전문적인 해커를 통해 시간적 공간적인 제약 없이 이루어질 수 있음을 의미한다.

정보사회가 고도화를 거듭할수록 정보통신망을 매개로 개인과 사회의 안전이 융합하고 사회의 안전과 국가의 안전 또한 융합하여 개인보호와 사회보호 및 국가보호의 경계 또한 매우 어렵게 될 것이라는 점에서 다음과 같은 제언을 한다.

첫째, 국가사이버위기관리법을 법제화하여 사이버위기 내지 사이버테러에 대한 법적 개념정의를 두고, 이상 패턴에 대한 국가기관 상호간 데

57) ITU 사무총장, “세계 3차 대전은 인터넷에서 발생”, 투데이뉴스, 2009.10.06

이터의 공유를 제도화한다.

둘째, 정부조직법에 의해 분장된 사무별 개별 국가중앙행정기관간의 전문역량(Synergy Effect)을 통한 데이터의 정보화와 개별 정보의 국가적 통합관리에 의한 지식화를 통한 국가적 시너지효과(Synergy Effect)를 도모한다.

셋째, 국가사이버위기의 예방과 대응을 위해 현행법상 상호모순 충돌하는 사이버위기와 관련한 계획 또는 정책간 효력 우선순위(예컨대, “국가 사이버위기 관리 종합계획”과 “국가정보보호 종합계획”간의 효력우위 문제 등)를 법정화한다.

넷째, 현행 법령은 “데이터(Data)”와 “정보(Information)” 및 “지식(Knowledge)”에 대한 명백한 개념정의 조항을 두고 있지 않아, 앞에서 지적한 바와 같이 최소의 인식단위를 담고 있지 않아 공유되어야 할 데이터가 공유되지 못하는 문제점과 동일한 데이터에 대해 사무주관 기관이 보유하고 있는 다양한 데이터나 정보 및 지식과 결부하여 창출하게 되는 특정 데이터의 정보화 내지 지식화가 이루어지고 있지 못한 문제점을 빨리 해소하여야 할 것이다.

참고부록

< 2009년 사이버안보 법안 (상원의 제안) >

제 2 조 조사 결과

국회는 다음의 조사 결과를 밝힌다.

(1) 미국의 사이버안보 실패는 국가가 직면한 가장 긴급한 안보 문제들 중 하나이다.

(2) 오늘날 대부분의 지적 재산들은 디지털 형태로 저장되기 때문에 사이버안보의 취약점을 노리는 산업스파이는 우리의 기술발전투자를 저해한다. 이에 반해 외국의 경쟁사들은 연구와 발전을 거듭하고 있다. 국력의 주 평가 요인으로 경제력과 기술 선도력이 부각되는 글로벌 경쟁시대에 사이버 안보의 실패는 우리에게 큰 불이익을 가져다 줄 것이다.

(3) '2009년 연례 위험 평가'에 따르면 주요 금융 서비스 기관을 겨냥한 사이버 공격은 국가 경제에 심각한 손상을 입힐 것이다. 또한 전력 송전망이나 기름 정제소과 같은 곳을 겨냥하여 컴퓨터 시스템의 물적 인프라를 통제하는 사이버 공격을 행해진다면 몇 시간 혹은 몇 주 동안 서비스가 중단될 가능성이 있다. 정부와 민영 조직의 정보 통신망은 산업 분야에서의 경쟁적인 이점을 취하기를 원하는 국가 규모의 범죄자들의 표적이 될 수도 있다.

(4) 국가정보국은 2009년 2월 19일, 국가와 비국가적인 적들은 인터넷과 전화 통신망, 컴퓨터 시스템, 중앙 연산처리장치, 제어장치, 주요 정보 인프라에 대한 침탈과 잠재적인 분열이나 파괴를 목표로 삼고 있으며 이러한 추세는 계속될 것으로 보인다고 국회에서 증언하였다.

(5) 2009년 3월 2일, 국가안보국과 대테러 보좌관인 존 브레넌(John Brennan)은 우리 국가의 안보와 경제적 번영이 통신 수단의 안보와 민간 소유의 국제 운영 기업의 정보 인프라의 견고함과 무결성에 달렸다고 기술하였다.

(6) 굿하버컨설팅회사(Good Harbor Consulting LLC)의 파트너겸 운영사무소장이며 버락 오바마 정권인수위회의 고문(顧問)인 폴커츠(Paul Kurts)는 최근 미국의 '사이버 카트리나'에 대하여 정부와 민영간의 적절한 공조체제 없이는 장기간의 충격과 붕괴를 가능성도 몰고 올 수 있는 막대한 사이버 분열사태에 대비할 수 없다고 말한다.

(7)국가안보국의 임원진이 주최하고 부즈 알렌 헤밀턴(Booz Allen Hamilton)이 진행한, 2008년 사이버 전략 구상(The Cyber Strategic Inquiry)에서는 사이버안보의 문제에 대하여 국가가 하나의 목소리를 가지고 행동하는 것이 중요하고, 사이버안보라는 독특한 상황에 맞는 리더십 방법론을 가질 필요가 있다는 결론을 내렸다.

(8) SANS 연구소의 연구팀장인 알렌 팔러(Allen Paller)는 국회에서 '사이버범죄와의 전쟁은 시시각각 방어자들은 새로운 벽을 세우고 공격자들은 그 벽을 부수기 위해 새로운 무기를 만들어내는 군비 전쟁과 비슷하다'고 말하였다. 이러한 분석에서 특히나 주의할 점은 사이버범죄와의 전쟁이 병력의 배치에 시간과 돈이 드는 가시적으로 전개되는 전통전쟁들과는 달리, 공격자들이 새로운 무기를 찾아내어 몇 시간 혹은 며칠 내에 자신을 드러내지 않은 채로도 수백만 개의 컴퓨터들을 공격하여 감염시킬 수 있다는 사실이다.

(9) 2003년 2월, 국가 사이버 안보전략에 따르면 국가의 주요 인프라들은 공공부문과 민영부문으로 이루어져있다. 이는 농업식품, 식음료, 공중보건, 응급 서비스, 정부, 방어 기반 산업, 정보와 원격 통신, 에너지, 교통, 은행, 화학물과 독성물질, 우편과 해운등으로 구성된다. 사이버

공간은 미국의 시스템을 통제하는 뇌의 신경체계와 같고 미국의 사이버 안보전략의 토대는 현재에도 그리고 미래에도 공공부문과 민영부문의 협력으로 이루어 질 것이다.

(10)국가정보국(National Intelligence)의 전 국장이었던 “National Journal” 지의 마이크 멕코넬(Mike McConnell)은 2007년 5월 부시 대통령에게 다음과 같이 말했다. 만약 9/11테러범들이 비행기대신 컴퓨터를 그들의 무기로 사용하여 미국의 은행들에 대규모 공격을 하였다면, 세계무역센터에 대한 물리적인 공격보다 훨씬 더 강한 경제적인 파장을 몰고 왔을 것이다.

(11) 전략국제문제연구소는 미국 44대 대통령의 사이버 안보에 대해 다음과 같은 결론을 내린다. (A) 사이버안보는 현재 미국의 중요 국가안보 문제이다. (B) 이에 대한 결정들과 행동들은 개인과 시민의 자유를 존중해야 한다. (C) 사이버안보에 있어서 국내외를 포괄하는 전면적인 국가 안보 전략만이 더 나은 안보를 가능하게 할 것이다. 이 보고서는 현재 미국이 사이버공간에서 '외국 정보국들과 군대, 범죄와 다른 것들로부터 장기적인 도전에 직면하고 있으며, 이러한 투쟁에서 지는 것은 미국의 경제와 국가안보에 심각한 손상을 입히는 것이라고 말한다.

(12) 국제적인 전략을 연구하는 기관인 기술 공공 정책 프로그램의 선임연구원장인 제임스 루이스(James Lewis)는 국제 전략 연구 센터를 대표하여 미국의 사이버안보분야가 잘 정비되지 않았고 국가전략의 일관성이 부족하다고 지적하였다.

(13) 2008년 7월 16일, 오바마 제 44대 미국 대통령은 퍼듀대학교(Purdue University)에서의 연설에서, 모든 미국인들은 직접적 혹은 간접적으로 정보네트워크 시스템에 의존하고 있다고 말하였다. 이러한 정보네트워크는 우리 경제와 사회 기반 시설, 국가안보와 개인의 안녕에

필수요소인데 현재 테러범들이 미국의 컴퓨터 네트워크를 사용하여 국가를 무력화시킬 수 있다는 것은 공공연한 사실이다. 사이버 첩보 활동과 일반 범죄는 이미 그 수가 증가하고 있는데, 중국과 같은 나라들은 이미 이러한 변화를 빠르게 감지하고 있는 반면 미국은 여전히 주춤하고 있다. 또한 오바마 대통령은 '우리는 모든 사이버 공격을 감지하고 분리하여 대응할 수 있는 능력을 갖추어야한다'고 말하였다.

(14) 대통령의 정보 기술 자문 위원회[58]의 2005년 연례 보고에 따르면, 소프트웨어 부분은 가장 공격받기 쉬운 분야이며 기준이 되었던 소프트웨어 발달 기술은 IT시설이 요구하는 양질의 믿을만한 소프트웨어를 제공하는 것에 실패하였다. 암세포와 같이 공격받기 쉬운 소프트웨어는 쉽게 공격의 대상이 되고 변이를 일으켜 건강한 다른 소프트웨어에 해를 입힐 수 있다. 또한 감염된 소프트웨어는 자기 복제하며 네트워크를 통하여 이동하여 다른 소프트웨어까지도 망가트릴 가능성이 크다.

제 3 조 사이버안보 자문위원회

(a) 총칙 - 대통령은 사이버안보 자문단을 설립 혹은 지정할 것이다.

(b) 필요조건

(1) 대통령은 산업계, 학계, 비영리조직, 이익 집단 대표들과 변호사 집단의 대표들로 자문위원단을 임명하여야 한다. 또한 사이버 안보의 연구, 발달, 증명, 교육, 정보전달, 상업분야 적용 또는 사회적, 시민적인 자유권에 대하여 조언과 정보를 제공할 수 있는 국가와 지방 정부를 사이버안보 자문위원회로 임명해야 한다.

---

58) The President's Information Technology Advisory Committee

(2) 또한 대통령은 의회, 산업, 사이버안보 단체, 변호 단체, 주 정부와 지역 정부와 같은 다른 해당 조직들의 의견을 참작하여야 한다.

(c) 의무 - 자문위원단은 국가 사이버안보 프로그램과 전략에 관한 자문을 하고, 이하의 사항들을 평가하여야 한다.

(1) 사이버안보 과학의 연구와 발전의 흐름 및 발달

(2) 전략의 이행과 관련된 진행사항

(3) 전략 개선에 필요한 사항

(4) 프로그램들 간의 자금 관리를 포함한 국가 전략 사항들 간의 균형

(5) 전략과 선 이행 사항들, 목표들이 미국의 리더십과 사이버 안보방어에 도움이 되는지의 여부

(6) 전략의 관리와 조정, 이행과 활동

(7) 그리고 사회의 자유와 시민의 자유가 적절히 검토되었는지의 여부

(d) 보고서 ; 자문위원들은 (c)항에 나와 있는 사항들의 평가와 전략을 향상시킬 수 있는 방법에 대하여 최소한 2년에 한번 씩 대통령에게 보고해야 한다.

(e) 국외 체류 자문위원에 대한 항공 비용 - 국외의 자문위원들 국내에서 무보수 정부를 위해 일하는 개인을 위한 미국코드(USC:United States Code)의 제 5 절 5703조에 따라 실제 경비와 항공비를 제공받을 것이다. 이는 자문위원회 회의 참가 시, 혹은 국외 체류 중이거나 출장 중 자문단 의장의 요청에 의해 일을 할 때를 포함하며 이는 자문위원이 공무원에 준하는 대우를 받을 것을 의미한다.

(f) 연방자문위원회 행정개혁 촉진법[59]으로의 면제 - 국가자문위원회법 (5 U.S.C. App.) 제 14조는 자문위원에게 적용되지 않는다.

---

59) FACA SUNSET (Federal Advisory Committee Act, Sunset law)

제 4 조 사이버안보 실시간 정보시스템

상무부장관은 (1) 예산관리국[60]과의 협의아래 법안 제정 후 90일 내에 적극적이며 포괄적인 실시간 사이버안보 체계를 제공하기 위하여 상무부와 함께 취약성을 가진 모든 연방정부의 정보 시스템과 네트워크 계획을 고안하여야 한다.

(2) 법안 제정일 1년 내에 이 계획을 실행하여야 한다.

제 5 조 국가와 각 지역의 사이버안보 향상 프로그램

(a) 사이버안보 센터의 창설과 지원 - 상무부 장관은 사이버안보 기준을 진작시키고 실행하기 위한 지역 사이버안보 센터에 대한 창설과 지원에 대한 보조를 제공하여야 한다.

(b) 목적 - 센터의 목적은 미국의 중·소 사업장의 사이버 안보를 향상시키는 것에 있으며 이는 다음의 방법을 통해 한다.

(1) 국립표준기술연구소[61]에서 개발된 사이버안보의 기준과 과정, 기술을 기관들에게 전수하고, 기관은 미국 내 모든 중소기업에게 위의 사항을 전달한다.

(2) 산업과 대학, 정부와 연방 정부와 해당 참여 기관과 협력하여 기술을 전달한다.

(3) 미국의 중소기업에서 이용 가능한 새로운 사이버보안 기술, 기준, 절차를 고안한다.

(4) 사이버보안에 관한 과학, 기술, 관리정보를 중소기업을 포괄하는 회사들에 배포한다.

(5) 연구기관들뿐만이 아니라 연방 연구소 또한 적절히 이용한다.

(c) 활동 - 센터는 (1) 연구기관에 의한 연구결과를 토대로 한 기술 전이

---

60) OMB : The Office of Management and Budget

61) The National Institute of Standards and Technology

를 목적으로 사이버보안 기술, 기준, 과정을 보급해야한다. (2) 회사와 기업, 특히 중소기업들을 겨냥한 사이버 공격의 위협에 대한 보안을 위해 적극적으로 사이버보안 전략과 최선의 실행방법과 기준, 기술들을 전이시키고 유포해야 한다. (3) 직원이 100명 이하인 작은 사업체를 선별하여 최신식 사이버안보제품들을 대여해준다.

(c) 지원 분양과 지원 기간 ; 프로그램 설명 ; 적용 범위 ; 장점 ; 보조 평가에 대하여

(1) 재정적인 지원 - 장관은 연간 운영비용의 50 퍼센트가 넘지 않는 범위 내에서 6년 이하로 모든 센터에게 재정적인 지원을 제공해야 한다. ((5)(D)에 예외사항 명시)

(2) 프로그램 개괄 - 이 법의 제정 후 90일 이내에 장관은 연방 관보에 설립되는 기관의 프로그램에 대한 사항을 공포해야 한다. 30일 간의 의견 수렴일을 갖고 프로그램에 대한 최종안을 공포한다. 이는 다음의 내용을 포함하여야 한다.

(A) 프로그램에 대한 설명

(B) 지원자가 따라야 하는 절차

(C) 지원자 선별기준

(D) 적격한 지원자 중 이 조항에 명시된 재정적인 지원을 받는 지원자의 선택 기준 ((4)항의 내용을 포함한 기준)

(E) 이 조항에 따라 4년에서 6년까지 보조를 받는 기관의 지원 상한선

(3) 지원과 지원 대리 - 비영리 기관이나 비영리 기관의 조합은 이 조항에 명시된 재정적 지원을 위한 지원서를 장관이 정한 절차에 따라 장관에게 제출해야 한다. 이 조에 따라 지원을 받기 위해 지원자는 기관에 첫 3년간과 그 다음 3년간 적절한 보증을 제공해야 한다.

(4) 지원 기준 - 지원은 경쟁공채로 이루어질 것이다. 이 조항에 따라 지원을 승인하거나 재정적인 지원을 제공하는 결정은 다음의 최소 요

건들의 충족 후 이루어 질 것이다.

(A) 기술 전이와 훈련, 교육, 사이버안보 기술, 특히 필수적 산업부문에 이를 적용했는지 여부

(B) 제공한 서비스의 질

(C) 서비스 지역의 범위의 지리적인 다양성

(D) 다른 자원의 현물지급공적 양과 자금의 비율

(5) 3년 후의 평가

(A) 총칙 - 이 조항에 따라 재정적인 지원을 받는 센터들은 시행 후 3년이 되는 해에 장관에 의해 임명된 평가단으로 부터 평가받을 것이다.

(B) 평가단 - 평가단은 개별 전문가들로 구성될 것이고 해당 기관이나 연방 공무원과 관계없는 자이어야 한다. 각각의 평가단은 이 조에 명시된 지침에 따라 기관의 수행 상황을 평가할 것이다.

(C) 지속적인 자금지원을 위해서는 긍정적 평가가 필요 - 만일 평가가 좋지 않을시 장관은 차후 4년에서 6년까지 자금을 지원하지 않을 것이다. 평가가 긍정적이라면 장관은 점차 감액한다는 조건아래 6년까지 자금을 지원할 것이다.

(D) 시행 6년 이후의 자금 지원 - 시행 6년 이후에 설립 기관이 연구소가 확립한 절차에 따fms 독립적인 검토를 통해 긍정적인 평가를 받게 된다면, 장관은 기관에 추가 재정지원을 제공할 것이다. 추가 독립 평가는 시행 6년 이후 매 2년마다 행해질 것이다. 이 조항에 따라 6년의 운영 후에 회기년도에 받는 자금은 기관의 연간 운영비용에 1/3을 넘지 않을 것이다.

(6) 발명에 대한 특허권 - 미국 코드(USC : United States Code) 35조 18장의 규정들은(이 조항에 일치하는 범위 내에서) 이 조항에 따라 기관에 의한 연구 기술 증진에 적용된다. 단 특정 기술 확대나 이전

서비스는 대통령이나 대통령이 임명한 자에 의한 법규에 의해 명기된다.

(d) 다른 연방 부서와 기관으로부터의 자금의 승인 - 센터의 운영을 위해 장관이나 대통령, 대통령이 임명한 자에 의해 인가받고 정식화된 자금은 다른 연방 부서나 기관에 의해 기관의 지원을 위해여 연방에 제공되는 것을 목적으로 한 자금으로 인가될 것이다. 연방 부서나 기관으로부터 지원된 자금을 받은 기관은 이 조항에 따라 선택되어 운영될 것이다.

제 6 조 미국 국립 표준 기술원(NIST, National Institute of Standards and Technology)의 표준 확립과 수용

(a) 총칙- 이 법의 제정 후 1년 내에 미국 국립 표준 기술원은 연방정부와 정부 계약 도급자, 혹은 다음과 같은 중대 기반 정보 시스템과 네트워크들에 대한 수혜자에게 측정에 가능하고 감시 가능한 사이버안보 기준을 확립하여야한다.

(1) 사이버안보 계량법 연구 - 미국 국립 표준 기술원은 사이버안보 계량법을 발전시키기 위한 연구 프로그램과 사이버안보의 경제적 파장을 평가하는 표준을 확립하여야 한다.

(2) 보안 통제 : 국립표준기술원은 잘 알려진 공격요인들을 공격하거나 공격을 완화시키는 일련의 보안통제 순위를 매겨 지속적인 효율성 평가 기준을 확립해야 한다.

(3) 소프트웨어 보안 - 연구소는 공격당할 가능성이 있는 취약한 소프트웨어들에 대한 우선순위를 매겨 소프트웨어 보안을 측정하는 기준을 확립해야 한다. 또한 연구소는 보안 측정을 위한 산업 통제 시스템에서 볼 수 있는 소프트웨어들의 구분 기준을 확립하여야 한다.

(4) 소프트웨어 구성 세목 용어 - 연구소는 연방정부와 정부 계약 도급자들과 보증인들, 민간 소유의 주요 시설 정보시스템과 네트워크에서 폭넓게 사용되는 컴퓨터 시스템 소프트웨어의 구성에 사용되는 컴퓨터 해독 가능 언어(computer-readable language)의 기준을 확립해야 한다.

(5) 표준 소프트웨어의 구성 - 연구소는 운영 체제 소프트웨어를 구성하는 표준 구성과 연방정부와 정부 계약 도급자들과 보증인들, 민간 소유의 주요 시설 정보시스템과 네트워크에서 폭넓게 사용되는 소프트웨어 유틸리티에 대한 기본 구성을 확립해야 한다.

(6) 취약 부분 언어 - 연구소는 소프트웨어의 특별 취약부분에 대한 컴퓨터 해독 가능한 언어 기준을 확립해야 한다. 이는 소프트웨어 판매자가 소프트웨어 사용자와 취약한 데이터에 대한 통신을 가능하게 하기 위함이다.

(7) 모든 소프트웨어에 대한 국가의 요구 기준

(A) 프로토콜 - 연구소는 연방정부와 정부 계약 도급 자들과 보증인들, 민간이 소유한 주요 시설 정보시스템과 네트워크에서 폭넓게 사용되는 소프트웨어에 관한 프로토콜 시험 인증 기준을 확립해야한다. 이것은 다음의 사항들을 보증하기 위함이다.

(i) (2)항에 나와 있는 소프트웨어 보안기준을 충족시키기 위하여.

(ii) (4)항에 나와 있는 기준 구성요인들에 다른 변화사항들을 요구하거나 발생시키지 않기 위하여.

(B) 권고 사항 - 연구소는 다음의 사항들을 증명하기 위한 과정을 만들어야한다.

(i) 소프트웨어 발달 기관들은 소프트웨어 발달 과정동안에 (A)항에 나와 있는 프로토콜에 따라야한다.

(ii) 적절성 시험과 결점감소 증거를 보여주는 시험결과는 소프트웨어 활용 전에 연방정부에게 제공되어야한다.

(b) 표준 기준 - 이 조항에서 만들어지는 기준들은 (어떠한 행정명령을 포함한) 다른 법규, 규칙, 규정 혹은 가이드라인에도 불구하고, 연구소는 정보 시스템 네트워크를 국가보안 체계 또는 정보 분류, 보안물로 간주하지 않을 것을 것이다. 또한 위험 정책에 기초하여 기준을 만들 것이다.

(c) 국제 기준 - 연구소와 해당 연방기관의 감독은 사이버 보안에 대하여 미국을 대표할 것이다. 또한 국제 사이버보안 기준과 관련하여 기국의 입지를 극대화하는 방안을 고안하여 이행할 것이다.

(d) 강제적인 권고 사항 - 감독은 (1) 소프트웨어 제작자, 배포자, 판매자들이 이 조항에 나와 있는, 연구소에 의해 만들어진 기준들을 따르게 해야 한다. (2) 각각의 연방 기관과 정보 시스템 네트워크에 관하여, 주요 시설 정보시스템 네트워크로 대통령이 선정한 운영자가 이 조항에 나와 있는 기준들을 주기적으로 따르도록 촉구해야한다.

(e) 연방 통신 위원회의 국가 광역통신망 계획 - 2009년 경기부양법[62]의 제 6001 조 (k)항에 따라 연방 통신 위원회(FCC)는 상업 광역통신망 네트워크의 사이버안보에 가장 효율적이고 효과적인 수단을 보고해야 한다. 이는 소비자 교육과 봉사프로그램을 포함한다.

제 7 조 사이버안보 전문가 자격 취득과 증명

(a) 총칙 - 이 법의 제정 후 1년 안에 상무부장관은 사이버보안 전문가들에 대한 국가 자격증과 정기적인 자격갱신프로그램을 발달시켜 이를 조정하며 통합해야 한다.

---

62) American Recovery and Reinvestment Act

(b) 의무 요건 사항 - 이 법의 제정 후 3년 후에 이 프로그램 아래 자격이 증명되지 않은 개인이 사이버안보서비스 제공자로서 미국 내에 혹은 미국정부에 고용되어, 연방정부나 정보시스템 혹은 네트워크의 제공자로 중요 시설 정보 시스템이나 네트워크에서 대통령에게 임명되거나 피지명자로 고용되는 것은 불법이다.

제 8 조 미국통신정보관리청(NTIA, National Telecommunications and Information Administration)의 도메인 이름 계약에 대한 검토

(a) 총칙 - 인터넷할당번호(Internet Assigned Numbers Authority, IANA)의 실행과 관련사항의 미 법안의 제정 이후, 정보와 통신에 관한 상무부 차관보가 행하는 어떠한 결정도 자문단이 다름과 같은 사항을 충족시키지 않을 시에는 최종안으로 추정되지 않을 것이다.

(1) 자문단의 검토.

(2) 자문단이 사안에 대하여 연관된 상업적, 국가 안보적 사안 고려.

(3) 자문단의 승인.

(b) 승인 절차 - 약 자문단이 이러한 사안을 승인하지 않았을 때, 차관보는 즉시 비승인 사유에 대하여 서문으로 통지받아야 한다. 자문단은 차관보에게 사안을 승인을 위한 필요요건사항을 담은 수정 권고사항을 통지해야한다.

제 9 조 도메인 이름 어드레싱 시스템 보안

(a) 총칙 - 이 법의 제정 후 3년 이내에 정보와 통신에 관한 상무부 차관보는 도메인이름 어드레싱 시스템 보안을 실행하기 위한 전략을 구상해야 한다. 차관보는 연방의 이행 일정과 대통령과 대통령이 임명한 자에 의해 지정된 정보 시스템 네트워크의 주요 시설 정보 시스템

네트워크들에 대하여 시스템요구사항들에 대한 공지를 연방관보(Federal Agency)에 실어야 한다.

(b) 요구 사항 - 대통령은 각각의 연방과 시스템 네트워크들이 보안된 도메인 이름 어드레싱 시스템이 차관보에 의해 공포된 이행 절차에 따라 실행되고 있는지 확인할 것이다.

제 10 조 사이버안보에 대한 인식 증진

상무부 장관은 국가적인 사이버안보 인식 증진 캠페인을 발전시키고 실행할 것 이다. 이에 대한 사항은 다음과 같다.

(1) 사이버 보안 문제 자각을 위한 대중의 인식 증진

(2) 인터넷과 관련된 활동에 관한 인터넷과 개인의 자유 보호와 시민자유에 대한 보호, 그리고 연방 정부의 역할에 대한 상호 교류

(3) 공공서비스 통지를 포함한, 정보를 공공에게 알리는 수단으로의 공적 부분과 사적 부분의 이용

제 11 조 연방의 사이버안보 조사 및 발전

(a) 사이버안보의 기본 조사 - 국가과학재단[63]의 국장은 컴퓨터와 정보과학에 우선권을 부여하고 실질적인 보조를 보증하기 위한 공학 분야 연구를 제공한다. 이는 이하의 사이버안보의 과제를 충족시키기 위함이다.

(1) 초기 개발 기에 신뢰감 있고 안정적인 복합 소프트웨어 내장 시스템을 설계하고 고안하는 방법.

(2) 지역적으로 개발되고 제 3자에 의해 얻어진 소프트웨어가 널리 알려진 안보 오류의 주요사항으로부터 자유로운지에 대해 검사하고 증명하는 방법.

---

63) NSF : The National Science Foundation

(3) 제 3자로부터 얻어진 소프트웨어가 기능적으로 실행될 수 있는 지에 대한 검사와 증명

(4) 분산된 시스템을 통하여 저장되거나 네트워크를 통하여 전송될 때 개인의 신원사항과 정보 혹은 법률 처리의 개인 정보 보호 방안.

(5) 인터넷이 주 기능 중 하나로 강력한 보안을 가능하게 하는 새로운 프로토콜을 구축하는 방법.

(6) 인터넷을 통해 전송된 메시지의 출처를 확인하는 방법.

(7) 개선된 보안과 함께 개인정보보호를 지원하는 방법.

(8) 내부 위협으로부터 증가하는 문제에 대처하는 방법.

(b) 코딩 연구의 보안 - 감독관은 선별된 코딩교육이나 개선 프로그램 보안을 평가하는 연구를 지원할 것이다. 감독관은 또한 보안 코딩 향상을 주요 컴퓨터공학 프로그램 교육사항에 통합시키고, 졸업생들이 졸업 후에도 실질적인 소프트웨어를 발전시킬 수 있는 다른 분야의 연구 프로그램에 대한 연구를 지원할 것이다.

(c) 대학의 보안 코딩 교육 평가 - 이 법의 제정 후 일 년 내에 감독은 산업, 과학, 교통 미 상원위원회와 과학 기술 미 하원대표위원회에 회계 연도 2008동안 국립과학재단에서 1.000.000달러 이상을 지원받은 미국의 대학에서 보안 코딩 교육 현황에 대하여 보고하여야 한다. 이러한 보고는 다음의 사항을 포함해야 한다.

(1) 컴퓨터 공학이나 졸업생들이 졸업 후에 소프트웨어 분야에 종사할 실질적인 가능성이 있는 다른 프로그램에서 학사학위를 받은 학생의 수.

(2) 학사과정동안 독립된 보안 코딩 교육이나 증진 프로그램을 이수한 학생의 비율.

(3) 보안 코딩 설계를 학생들이 마스터하게 할 수 있는 것을 교육하고 장려하는 프로그램과 이러한 프로그램의 효율성을 측정하는 것에 대한 범위와 내용.

(d) 사이버보안 모형과 시험 - 감독은 높은 교육과 실시간 사이버 공격과 방어의 실제적인 모형을 만들어 사이버보안 실험을 가능하게 한 연구소에게 상을 수여하는 프로그램을 만들어야 한다. 이 프로그램의 목표는 실제적인 세계 환경에서 최신 기술을 이해하고 평가하는 것을 증진시켜 새로운 사이버보안 방어와 기술, 실행과정에 대한 빠른 발전을 지원하기 위함이다. 실험은 실제 네트워크 환경의 규모와 복잡성을 구현할 수 있을 정도로 충분한 크기를 갖추어야 한다.

(e) 미국과학재단(National Science Foundation, NSF) 컴퓨터와 네트워크 보안 연구 수용 범위 - 사이버 안보 연구 발전법 4조 (a)(1)의 내용(15 U.S.C. 7403(a)(1))은 다음과 같은 방법으로 수정된다.

(1) 세부 항 (H)의 세미콜론(;) 뒤에 'and'를 입력함으로써

(2) 세부 항 (I)에 '자산(property)'을 입력하여 삽입함으로써

(3) 다음의 사항을 문미에 첨가함으로써

'(J) 네트워크간의 통신이나 정보의 교환의 심장부인 기반 프로토콜의 보안

'(K) 다음의 사항을 포함한 소프트웨어의 기술과 확실성을 보안

'(i) 기초 보안 특징들을 포함한 프로그래밍 언어와 시스템

'(ii) 다양한 환경에 배치되어 보안이 유지되는 휴대 혹은 재사용이 가능한 코드

'(iii) 필요사항과 개별사항들이 실행을 보증하기 위한 증명과 유효성

'(iv) 요구 기준을 충족을 보증해주는 비교 계량 모델들

'(L)전체 시스템 보안

'(i) 신빙성의 입증이 가능한 혹은 가능하지 않은 부분들에 대한 보안 시스템 구축 착수
'(ii) 취약점 감축을 위한 사전 대책 강구
'(iii) 내부 위협요소들 대처
'(iv) 보안능력 향상과 함께 개인정보보호의 지원
'(M) 감시와 탐지
'(N) 피해 최소화와 즉각적인 복구 방법

(f) 미국과학재단[64] 컴퓨터와 네트워크 보안 승인- 사이버 안보 연구 발전법 4조 (a)(3)의 내용(15 U.S.C. 7403(a)(1))은 다음과 같이 수정된다.
(1) 세부 항 (D)의 세미콜론(;) 뒤에 'and'를 입력함으로써
(2) 세부 항 (E)에 '2007'을 입력하여 삽입함으로써
(3) 다음의 사항을 문미에 첨가함으로써
'(F) 회계연도 2010년 : 150,000,000달러
'(G) 회계연도 2011년 : 155,000,000 달러
'(H) 회계연도 2012년 : 160,000,000 달러
'(I) 회계연도 2013년 : 165,000,000 달러
'(J) 회계연도 2014년 : 170,000,000 달러

(g) 컴퓨터와 네트워크 보안 기관 -사이버 안보 연구 발전법 4조(b)(7)의 내용(15 U.S.C. 7403(b)(7))은 다음과 같이 수정된다.
(1) 세부 항 (D)의 세미콜론(;) 뒤에 'and'를 입력함으로써
(2) 세부 항 (E)에 '2007'을 입력하여 삽입함으로써
(3) 다음의 사항을 문미에 첨가함으로써
'(F) 회계연도 2010년 : 50,000,000 달러
'(G) 회계연도 2011년 : 52,000,000 달러

64) NSF:National Science Foundation,

'(H) 회계연도 2012년 : 54,000,000 달러
'(I) 회계연도 2013년 : 56,000,000 달러
'(J) 회계연도 2014년 : 58,000,000 달러.

(h) 컴퓨터와 네트워크 보안 능력 구축 보조금 - 사이버 안보 연구 발전법 5조 (a)(6)의 내용(15 U.S.C. 7404(a)(6))은 다음과 같이 수정된다.

(1) 세부 항 (D)의 세미콜론(;) 뒤에'and'를 입력함으로써
(2) 세부 항 (E)에 '2007'을 입력하여 삽입함으로써
(3) 다음의 사항을 문미에 첨가함으로써
'(F) 회계연도 2010년 : 40,000,000 달러
'(G) 회계연도 2011년 : 42,000,000 달러
'(H) 회계연도 2012년 : 44,000,000 달러
'(I) 회계연도 2013년 : 46,000,000 달러
'(J) 회계연도 2014년 : 48,000,000 달러

(i) 과학 발전 기술 보조금 - 사이버 안보 연구 발전법 5조 (b)(2)의 내용(15 U.S.C. 7404(b)(2))은 다음과 같이 수정된다.

(1) 세부 항 (D)의 세미콜론(;) 뒤에 'and'를 입력함으로써
(2) 세부 항 (E)에 '2007'을 입력하여 삽입함으로써
(3) 다음의 사항을 문미에 첨가함으로써
'(F) 회계연도 2010년 : 5,000,000 달러
'(G) 회계연도 2011년 : 6,000,000 달러
'(H) 회계연도 2012년 : 7,000,000 달러
'(I) 회계연도 2013년 : 8,000,000 달러
'(J) 회계연도 2014년 : 9,000,000 달러

(j) 컴퓨터 네트워크 보안 훈련졸업생 - 사이버 안보 연구 발전법 5조 (c)(7)의 내용(15 U.S.C. 7404(c)(7))은 다음과 같이 수정된다.

(1) 세부 항 (D)의 세미콜론(;) 뒤에 'and'를 입력함으로써

(2) 세부 항 (E)에 '2007'을 입력하여 삽입함으로써

(3) 다음의 사항을 문미에 첨가함으로써

'(F) 회계연도 2010년 : 20,000,000 달러

'(G) 회계연도 2010년 : 22,000,000 달러

'(H) 회계연도 2010년 : 24,000,000 달러

'(I) 회계연도 2010년 26,000,000 달러

'(J) 회계연도 2010년 28,000,000 달러

(k) 사이버보안 교수진 발전 훈련 프로그램- 이 법의 (15 U.S.C. 7404(e)(9)) 제 5조 (e)(9)은 '2010'년에서 '2014'년까지 '2007'을 입력하여 삽입함으로서 수정된다.

(l) 네트워크와 정보 기술조사, 그리고 발전 프로그램 - 1991년 고성능 정보처리법[65](15 U.S.C. 5524(a)(1)) 제 204(a)(1)조는 다음과 같이 수정된다.

(1) 세부 항 (B)의 세미콜론(;) 뒤에 'and'를 입력함으로써

(2) 다음의 사항을 (C)항 뒤에 삽입함으로써

'(D) 컴퓨터 네트워크와 일반 사용자 인터페이스 시스템의 사이버보안을 향상시키기 위하여 기준과 지침을 발전시키고 제안하며, 측량 기술과 시험방법을 발전시킨다.

제 12 조 연방의 사이버 장학 프로그램

(a) 총칙 - 국가 과학 기금 장은 다음세대의 연합 정보 기술 노동자와 공안 경찰을 채용하고 훈련시키기 위하여 연합 사이버 장학재단을 설립해야 한다.

---

65) High-Performance Computing Act

(1) 장학금은 교육비 전액, 각종 비용들을 포함하며 사이버안보 분야의 학부나 대학원에 재학 중인 학생들 중 연간 1,000명 범위 내에서 한 차례 장학금을 제공해야 한다.

(2) 장학금 대상 학생들에 대한 요구사항 : 장학 프로그램을 지원받은 학생은 졸업 후에 학위를 받은 기간 동안 연방 정보 기술 인력으로써 연방 관청이 제안하는 분야에서 근무해야 한다.

(3) 학생들에게 방학기간동안 연방 정보 기술 작업 인턴으로 채용에 준하는 일시적 임용을 받도록 기회를 제공해야한다.

(4) 미래적 가치가 있는 K-12학생들을 선별하기 위하여 연방 정보 기술 작업 인턴에 평가기준을 확립하고, 학생들에게 미래에 채용가능성을 확대하도록 진작시키는 여름 인턴십 프로그램에 참여시켜야 한다.

(5) 2, 3학년 학급들에게 컴퓨터 보안 지식을 증진하기에 유용한 프로그램을 시청하도록 하고 이러한 지식의 함양을 권고하여야한다.

(c) 고용 권한 - 연방 시민 서비스와 관계된 일에 개인이 종사하도록 관장하는 이 법의 목적에 따라, 프로그램을 성공적으로 이수하여 학위를 받은 학생들은 연방법규[66] 213.3102(r) 제 5절에 따라 임명될 것이며 경쟁채용으로부터 면제될 것이다. 서비스 수료기간의 완료시 학생이 직위에 필요한 요구사상을 충족한다면 다른 지원자와의 경합 없이 정규직으로 전환될 것이다.

(d) 적격성 - 이러한 조건의 장학금을 수령하기 위하여 개인에게 요구되는 사항은 다음과 같다.

(1) 미국 시민일 것

(2) 국가 사이버 방위 향상을 위한 노력을 증명할 것

(e) 고려사항 및 우선권 - 이 조항의 장학금을 선별하는 것에 있어서 감독은 (1) 가능한 한 사이버 안보 기술 분야뿐만 아닌 사회과학분야

66) Code of Federal Regulations

출신 등 다양한 지원자들을 선발한다. (2) 제 13조에 명시된 경진대회에 참가하였던 학생에게 우선권을 부여한다.

(f) 평가보고 - 감독은 장학금 수령자의 선발 평가 후 이를 산업, 과학, 교통 미 상원위원회와 과학 기술 미 하원대표위원회에 보고해야한다.

(g) 적절성 인가 - 이 조항을 실행에 옮기기 위하여 국립 과학 재단에서 정식인가를 받아야 한다.

(1) 회계연도 2010년 : 50,000,000 달러

(2) 회계연도 2011년 : 55,000,000 달러

(3) 회계연도 2012년 : 60,000,000 달러

(4) 회계연도 2013년 : 65,000,000 달러

(5) 회계연도 2014년 : 70,000,000 달러

제 13 조 사이버안보 경진대회

(a) 총칙 - 연방의 적절한 인준에 따라 국가표준기술원장은 상금이 주어지는 '사이버안보경진대회'를 개최할 것이다. 이의 목적은 다음과 같다.

(1) 연방정보기술 인력으로 능력 있는 인재를 모으고 발굴하며 평가하여 채용할 수 있는 기회를 확대하기 위하여

(2) 기반기술혁신을 진작시켜 사이버안보 연구와 기술발전, 연방정부의 연방 정보 기술 활동에 적용 본보기로 사용한다.

(b) '사이버안보경진대회'의 형태 - 감독은 이하와 같이 동등한 조건의 그룹을 구별하여 각각의 대회를 개최하여야한다.

(1) 고등학생 대상

(2) 대학생 대상

(3) 대학원생 대상

(4) 학회와 연구소 대상

(c) 주제 - 대회의 주제 선정에 있어서 감독은 연방정부의 안팎에 폭넓은 자문을 구하고 자문위원회를 심사위원에 포함시켜야한다.

(d) 광고 - 감독은 대회에 관하여 제 10조 이하의 사항에 따라 인식 증진과 참여를 독려하는 다양한 광고를 해야 한다.

(e) 자격과 등록 - 각각의 대회에 감독은, 대회의 주제와 대회에 참가하기위한 자격과 상금, 수상 기준에 대하여 연방관보에 게재한다.

(f) 자격 - 이 조항에 따라 수상자에 선정되려면 개인이나 단체는

(1) (d)항의 감독에게 공표된 규칙에 따라 대회에 참가등록을 해야 한다.

(2) 이 조항에 나와 있는 요구사항들을 준수해야한다.

(3) 사 기관의 경우 직장이 미국 내에 있어야 하고, 개인의 경우, 단독이든 여러명이든 간에 미국 시민이거나 영주권자이어야 한다.

(4) 직업이 연방에 소속되어 있거나 고용되어 있지 않아야 한다.

(g) 심판 - (h)항에 따라 합의하에 선출된 감독은 각각의 대회에 우승자를 가리기 위한 적격한 심판을 소집해야 한다. 각각의 대회에 심판은 개개인으로 선출 될 것이다. 심판은 아래의 사항에 해당되지 않아야 한다.

(1) 사적인 금전이익을 취하거나 대회의 참가자로 등록된 자의 고용인, 간부, 감독 또는 대리인이어서는 안 된다.

(2) 참가자와 친족관계이거나 금전관계가 있어서는 안 된다.

(h) 대회의 운영 - 감독은 이 조항에 따른 대회의 운영을 위해 사설의 비영리 협회에 등록해야 한다.

(i) 자금

(1) 상금 - 이 조항에 따르는 상금은 연방승인자금으로 나올 것이며, 상금은 민간 부문에서 조달될 것이다. 감독은 상금을 위해 다른 연방기관으로부터 예산 자금을 승인할 것이다. 감독은 어떠한 참가자에게도 기부의 답례로 특혜를 주어서는 안 된다.

(2) 지출되지 않은 자금의 사용 - 다른 법 조항이 존재한다고 할지라도 이 조항에 따라 상금을 위해 조성된 자금은 지출이 완료될 때까지 사용가능하고, 처음 자금이 조성되었던 해로부터 회계연도 10년이 지나 만료된 이후에만이 다른 용도로 전환되거나 재구성되어 사용할 수 있을 것이다. 이 조항의 규정들은 채무불이행방지법[67](31 U.S.C. 1341)을 위반하여 채무를 지거나 자금을 지출하여서는 안 된다.

(3) 상금이 발표되기 전의 자금의 조성 - 민간의 출처에 의해 지불되어야 하는 상금의 액수가 적합하게 알려지지 않기 전에는 어떠한 상금도 발표되지 않을 것이다. 감독은 만약 (A) 처음 공지된 상과 같은 방식으로 공지가 이루어졌을 때 (B) 사적인 재원에 의해 서면으로 공지된 액수의 증가가 필요할 때 (d)항에 의한 최초의 발표가 있은 후에 상금의 액수를 증액할 수 있다.

(4) 규모가 큰 상에 대한 요건 - 이 조항에 나와 있는 대회의 어떠한 상도 산업, 과학, 교통 미 상원위원회와 과학 기술 미 하원대표위원회에 서면으로 공지한 후 30일이 경과하지 않고서는 5,000,0000달러를 초과할 수 없다.

(5) 특별상에 대한 감독의 승인 요구 - 이 조항에 따른 어떠한 상도 감독의 승인 없이는 1,000,000달러를 넘지 못한다.

(j) 연방 기장(記章)의 사용 - 이 조항에 따라 대회에 등록된 참가자는 감독에 의한 검토와 서면의 승인을 받은 후 연방 기관의 이름과 첫 글자, 기장을 사용할 수 있다.

(k) 타 조항의 적용 - 연방정부는 자격, 수출통제, 확산 방지법과 관련규정들을 포함한 연방법에 대회의 등록된 참가자의 적용 책임을 지지 않을 것이다.

---

67) Anti-Deficiency Act

(l) 세출 예산 인가 - 국가 표준 기술 위원회는 2010년부터 2014년까지 매년 이 조항에 따라 15,000,000달러를 인가해야한다.

제 14 조 공공과 민간의 상호 교류

(a) 지명 - 상무부는 사이버안보 위협과 연방 정부와 중대 시설 정보 시스템 네트워크를 보유한 사인간의 정보의 취약점에 대하여 정보기관으로서의 역할을 할 것이다.

(b) 목적 - 상무부 장관은 (1) 법률과 규정, 규칙, 또는 접근 권을 제한 규정과 관계없이 네트워크 시스템과 관련된 모든 관계 사항들에 대한 접근권한을 가질 것이다. (2) 연방 정부와 다른 중대 시설 위협에 대한 연방 정부와 사인간의 책임의 공유를 조율할 것이다. (3) 의회에 연방 정부에 의해 제기된 네트워크 관계사항 운영 유지에 대한 책임을 가진 사람에게 비공개된 정보 위협에 대하여 정기적으로 보고해야 한다.

(c) 정보 공유 규칙과 절차 - 법 제정 후90일 이내에 장관은 연방관보에 어떠한 방법으로 연방 정부가 사이버보안 위협을 사 기관의 주요 시설 정보 체계와 네트워크 소유자와 공유할 것인지에 관한 규칙과 절차의 초안을 게재하여야 한다. 30일의 정보공유기간 이후에 장관은 규칙과 절차에 대한 최종안을 공포하여야 한다. 그러한 최종안은 다음의 사항을 포함하여야 한다.

(1) 어떻게 연방정부가 사이버보안 위협과 정보의 취약성을 사 기관의 주요 시설 정보 체계와 네트워크 소유자와 공유할 것인지,

(2) 사 기관의 주요 시설 정보 체계와 네트워크 소유자가 소송을 제기할 수 있는 정보보안 위협과 취약한 정보, 그리고 연방 정부와 관계된 정보를 공유할 것인지,

(3) 주요 시설 정보 체계와 네트워크의 사 기관 소유자와 연방정부 간에 사이버보안 위협과 정보의 취약성의 공유를 강화할 수 있는 다룬 규칙과 절차.

제 15 조 사이버안보 위험 관리 보고서

법안 제정 후 1년 이내에 대통령 혹은 대통령이 임명한 자는, 산업, 과학, 교통 미 상원위원회와 과학 기술 미 하원대표위원회에 다음 사항의 이행가능성에 대해 보고하여야 한다.

(1) 시민의 책임체계기준과 보험(정부 보증 포함)과 관계된 사항을 포함한 사이버안보 위험 관리 시장 도입

(2) 채권과 관련된 사항에 대한 사이버안보의 요구

제 16 조 법률 기준 검토와 보고

(a) 총칙 - 법 제정일 1년 이내에 대통령 혹은 대통령이 임명한 자는 적절한 독립기구를 통하여 연방 법령과 법률의 토대에서 사이버와 관련된 활동에 관한 포괄적인 검토를 완료해야 하고, 위의 사항은 다음의 법률을 포함하여야 한다.

(1) 1980년 사생활 보호법 (42 U.S.C. 2000aa)

(2) 1986년 전자 통신 사생활법 (18 U.S.C. 2510)

(3) 1987년 컴퓨터 보안법 (15 U.S.C. 271 et seq.; 40 U.S.C. 759)

(4) 2002년 연방 정보 보안 관리법 (44 U.S.C. 3531 참조)

(5) 2002년 전자정부법 (44 U.S.C. 9501 참조)

(6) 1950년 방위생산법 (50 U.S.C. App. 2061 참조)

(7) 사이버 활동과 관계된 다른 연방 법률

(8) 다른 연관된 행정 명령 또는 긴급 명령, 규정, 지침

(b) 보고 - 법안의 검토 후에 대통령 또는 대통령이 임명한 자는 산업, 과학, 교통 미 상원위원회와 과학 기술 미 하원대표위원회 혹은, 다른 적절한 의회위원회에 조사 결과와 결론, 그리고 조언들에 대한 보고서를 제출하여야 한다.

제 17 조 신원 증명과 시민의 자유에 대한 보고

이 법의 제정이후 1년 이내에 대통령 혹은 대통령이 임명한 자는 신원관리와 입증 프로그램이 미 정부의 주요 시설 정보 시스템과 네트워크의 이행에서 시민의 자유와 개인정보 보호에 얼마만큼의 적절성을 가지고 있는지 대하여 검토한 후 의회에 보고하여야 한다.

제 18 조 사이버안보의 책임과 이에 대한 입증

대통령은 다음과 같은 직무를 수행하여야 한다.

(1) 대통령은 이 법률의 제정일로부터 1년 이내에, 이행 가능한 국가 사이버안보 전략을 발전시켜 적용하여야 하며, 이는 (A) 국가의 미래 사이버 보안의 장기적인 비전과 (B) 민영부문참여, 주요 시설 관리자와 운영자, 그리고 전 분야의 안전을 고려하는 내용을 포함하여야 한다.

(2) 대통령은 권한을 가진 모든 연방 정부와 미 정부의 주요 시설 정보 시스템과 네트워크에 사이버안보 긴급 상황에 이를 발표하거나 인터넷 트래픽의 차단과 제한을 명령할 수 있다.

(3) 대통령은 (2)에 따른 사이버보안 긴급 상황 발표의 효과에 따른 연방 정부와 미 정부의 주요 시설 정보 시스템과 네트워크의 복구가 필요할 시 중재자를 지정하여 이를 해결하게 한다.

(4) 대통령은 적절한 기관이나 혹은 중개자를 통하여 사이버안보 공격 후에 필요한 장비의 검토와 취득, 보관 및 주기적인 교체에 대한 전략을 발전시켜야 한다.
(5) 대통령은 연방 정부와 미 정부의 주요 시설 정보 시스템과 네트워크는 주기적인 조사에 대한 감독의 책임을 맡고 실질조사과정의 효과적인 평가기준을 확립해야한다.
(6) 대통령은 국가 안전을 위해 연방 정부와 미 정부의 주요 시설 정보 시스템과 네트워크의 중단을 명령할 수도 있다.
(7) 대통령은 과학기술정책 부서를 통하여 모든 연방 사이버 기술 조사 및 투자개발의 검토를 1년마다 정기적으로 감독하여야 한다.
(8) 대통령은 국가 사이버 보안 증진을 위해, 적절한 연방 공무원에게 분류에 관한 일에 권한을 위임할 수 있다.
(9) 대통령은 적절한 부서 혹은 중개자를 통하여 사이버안보에 관하여 연방 전문가들에 관한 법률을 공표하여야 하며, 이 법률에 대한 연방 중개자의 승낙 보고서를 매년 의회에 제출하여야 한다.
(10) 대통령은 연방공무원에 대한 교정활동을 감독하고, 연방 법률의 위반에 시 계약을 종료시키며, 대통령은 추가적인 보상을 보류하며 이러한 행하여진 모든 활동을 기밀 되지 않은 상태에서 48시간 안에 의회에 보고하여야 한다.
(11) 미국 시민에게 국가공인 사이버 관련 자격증의 수여할 시 48시간 내에 의회에 통보하여야 한다.

제 19 조 4년 주기의 사이버 보고

(a) 총칙 - 2013년을 시작으로 매 4년마다 대통령 혹은 대통령이 임명한 자는 미국의 사이버 현황 중 기밀사항이 아닌 것의 규칙과 임무, 성과, 계획, 프로그램들에 대하여 철저히 검토해야한다. 이러한 검토는

국가 사이버 전략과 의무 사항, 업데이트 계획, 제반 시설, 예산 계획, 사이버 긴급 상황에서 국가의 회복능력과 사이버 프로그램과 정책에 대한 미국의 사이버전략의 결정 관계 요인들, 이후 4년을 위한 개정된 사이버 프로그램의 설립에 대한 조망과 같은 포괄적인 검토를 그 내용으로 해야 한다.

(b) 사이버안보 자문단의 포함

(1) 대통령 혹은 대통령이 임명한 자는 제 3조에 의해 설립된 사이버보안자문단에게 검토의 결과로 착수된 일에 대한 기초 진행 사항에 대하여 통보해야 한다.

(2) 검토의 완료 후 1년 내에 자문단의 의장은, 대통령 혹은 대통령이 임명한 자에게 검토 에 따른 자문단의 평가에 대하여 제출하여야 한다. 또한 평가서와 함께 검토 중 지적된 문제들의 개선방안을 함께 제출해야 한다.

(c) 검토안 평가 - 검토안의 작성에 있어서 자문단의 의장은 자문단의 대표하여 대통령 혹은 대통령이 임명한 자에게 (d)항의 내용을 담은 평가서를 제출해야 한다.

(d) 보고 - 2013년 9월 30일 전까지 매 4년 마다 대통령 혹은 대통령이 임명한자는 검토사항에 대한 전반적인 보고서를 관계 의회 위원회에게 제출해야 한다. 이 보고서는 다음의 사항을 포함하여야 한다.

(1) 사이버안보에 대한 전반적인 쟁점사항들을 포함한 검토안과 이에 대한 결과물, 공공과 민간의 협력을 위한 가장 적합한 이행 전략

(2) 위협요소들을 평가를 목적으로 한 검토안과 시나리오

(3) 검토 안에 명기 된 수용 가능한 위험과 다른 국가와의 협력과 관계된 사항들

(4) 자문단의 평가서

제 20 조 정보 위협 평가 협력

국가 정보국과 상무부 장관은 의회에 사이버안보 위협요인들과 주요 국가 정보 통신과 데이터 네트워크 시설의 취약성에 대한 연례평가보고를 제출해야 한다.

제 21 조 국제 규범과 사이버안보 억제 수단

대통령은 (1) 정부 기관 대표와 협력한다. 이는 (A) 사이버 안보를 향상시키기 위하여 국제교류를 활성화하고 사이버안보 관련 용어와 정의, 조직들과 다른 협력 사항들을 발전시키기 위해서, (B) 국제적인 사이버 안보를 증진시키기 위한 국제 공조를 진작시키기 위함이다. (2) (A)항에 따라 국제 발의권 도입을 위한 연례보고서를 의회에 제출해야 한다.

제 22 조 연방 안보 물과 서비스 획득 위원회

(a) 제정 - 보안 재화와 서비스 취득 위원회가 설치되어 있다. 위원회는 연방정부의 소프트웨어 유효성에 관한 적절한 기준을 확립하기 위하여 국립표준기술연구소와 협력하여 사이버보안 검사와 양질의 상품과 서비스 획득을 위한 책임을 진다. 국립표준기술연구소 소장은 검사 과정을 도입하고 위원회 규칙을 마련한다. 이 조항에 따른 소프트웨어의 검사에서, 위원회의 승인은 필수적이며, 이에 따라 독립적인 보안 소프트웨어는 효력을 취득한다고 여겨진다.

(b) 취득 기준 - 감독은 예산관리부가 타 해당 연방 기관과 공동으로 재화와 서비스 승인의 전제조건으로 (1) 위원회의 검토와 (2) 연방 취득 기준 획득 조건을 충족시켜야 함을 확인시켜야한다.

(c) 취득 요건- (a)항의 공시 후에 연방 기관의 요청에 따라 허가되었던 재화와 서비스는 이들이 사이버보안의 전반적인 요건의 충족하였다는 보증을 받는 절차를 거쳐야 한다.

제 23 조 정의

이 법안에서 쓰는 용어의 정의는 다음과 같다.

(1) 자문위원회 - '자문위원회'는 제 3조에 의해 설립되거나 임명된 사이버암보 자문단원을 의미한다.

(2) 사이버 - '사이버'라는 용어는 다음의 사항들을 의미한다.

(A) 인터넷과 인트라넷, 자동 정보 처리나 전송, 또는 인터넷이나 인트라넷을 통한 원격 통신과 관련된 어떠한 과정이나 프로그램, 또는 프로토콜

(B) 컴퓨터 혹은 네트워크의 사용과 관련된 문제

(3) 연방 정부와 미 정부의 주요 시설 정보 시스템과 네트워크 - '연방 정부와 미 정부의 주요 제반 정보 시스템과 네트워크'는 다음과 같은 사항들을 포함한다.

(A) 연방 정부의 정보 시스템과 네트워크

(B) 대통령에 의해 주요 시설 정보 시스템과 네트워크라 지정된 미국의 주, 지방, 비정부 정보 시스템과 네트워크

(4) 인터넷 - '인터넷'이라는 용어는 제4조 제4항의 의미로 해석된다.

(5) 네트워크 - '네트워크'라는 용어는 1991년 고성능컴퓨터법(15 U.S.C 5503(4)) 제 4조 제5항(15 U.S.C 5503(5))의 의미로 해석된다.

<참고문헌>

국내 문헌

강대출, “테러방지법안에 관한 입법적 검토”, 「대테러정책연구논총」 제6호, 국가정보원, 2009.1.

김윤덕, 「국가정보학」, 박영사, 2007.

김남현/김형훈, 「경찰행정법」, 경찰공제회, 2005.

이호용, “효율적인 국가 대테러조직의 위상과 기능”, 「대테러정책연구논총」,제6호, 국가정보원, 2009.1.

조성렬, “9·11 사태 이후 일본의 대테러전 전력”, 「Strategy 21」, 제5권 제2호, 2002 가을·겨울

조성용, “일본의 테러관련 법제연구”, 「대구법학」 제6호, 2003.

정준현, “位置認識 및 通信事實確認資料 등의 個人情報與否에 관한 小考”, 토지공법연구 제24집, 2004.12.

최인섭, ″테러리즘의 실태에 관한 일 고찰,″ 국제법논총, 제6권, 1992.

한희원, 「국가정보체계 혁신론」, 법전출판사, 2009.

허태회, 「국가위기관리차원에서의 사이버안보 및 위기관리 향상 프로그램 연구」, 국가보안기술연구소, 2004.5.

국가정보원·방송통신위원회, 「2008 국가정보보호백서」, 2009.3.

한국전산원, “통계로 본 2010년 유비쿼터스사회 조망”, 2005.9.

한국정보화진흥원, 「2009 상반기 정보화 법제」, 2009. 7.

행정자치부, 「국내·외 위기관리 제도연구」, 2006.11.

행정자치위원회, “정부조직법 전부개정법률안 심사보고서”, 2008. 2.

국외 문헌

波多野里望, "テロ犯人の引渡しをめぐる諸問題-ILA委員會の草案にそくして," 「國際關係法の課題」, 1987.

D.J. Solove, Marc Rotenberg, "Information Privacy Law", Aspen. 2002.

T. P. Thornton, "Terror as a Weapon of Political Agitation", in H. Eckste-in(ed.), Internal War : Problems and Approaches, 1964.

James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Oth-er Cyber threats", CSIS, 2002.

John Rollins/Clay Wilson, "Terrorist Capabilities for Cyberattack:Overview and Policy Issues", CRS Report for Congress, Order Code RL33123, 2007.1. 22.

디지털타임스, "악명 떨친 보안위협 '톱10'은?", 2009. 9. 7.

미디어 오늘, " '사이버위기' 빌미로 과도 규제하나 정부 '종합대책' 기본권 침해 우려…책임도 국민의식에 떠넘겨", 2009.9.13.

일본경찰청, "日本警察廳情報保安政策大系", 2000.8.16.

중앙일보, "중국 '제4군' 사이버부대 유학파 등 2000명 활약", 2004. 7. 16.

Patterns of Global Terrorism, http: // www. state.gov/s/ct/rls/pgtrpt/ 2001/ html/ 10220.htm.

"Cyber terror threat overrated", http://www.vnunet.com /news /1135876

사이버테러 예방 및 대응체계 구축을 위한 법제도 개선방안

2009년 12월 인쇄
2009년 12월 발행

발행인 : 김 성 태
발행처 : 한국정보화진흥원
서울시 중구 무교동 77번지
전화 : (02) 2131-0114
인쇄처 : 호정씨앤피
전 화 : (02) 2277-4718

<비매품>