사이버위기 대응을 위한 법적 과제
– 미국의 사이버위기 대응체계 현황과 시사점을 중심으로 –

김 도 승*

고도정보사회에서 사이버공격은 금융·교통·산업·방송·의료 등 사회 기반에 치명적인 영향을 끼칠 수 있음은 주지의 사실이다. 더욱이 사이버공격이 테러리즘 등 특정 목적과 결부될 경우에는 국가안전보장에 대한 위기를 초래하는 중대한 위협요인으로 등장하고 있다. 이러한 상황에서 최근 국가안보의 차원에서 사이버위기에 대한 관리 및 대응의 중요성이 부각되고 있어 주목을 요한다. 이와 관련하여 미국은 책임과 권한이 여러 부처에 분산됨으로 인해 발생하는 정책의 혼선을 방지하고 모든 역량을 한 곳에 집중하기 위해 국토안보부(DHS)의 창설로 대표되는 효율적인 대응체계를 마련하였고, 특히 최근 사이버위기 대응체계 확립을 위한 통합법제로서 소위 '2009 사이버보안법(안)'을 발의하는 등 '사이버안보 확립'에 가장 적극적으로 대응하고 있는 사례로 평가된다. 우리의 경우는 최근 소위 '7.7 DDoS 대란'으로 다시한번 사이버위기의 위험성과 그 대응 필요성을 깨닫게 되었으며, 아울러 사이버위기 대응을 위한 총괄전담기관의 부재로 인한 혼선, 사이버안보 확립을 위한 법제도적 기반 미비 등의 문제점이 제기되었다. 이 사건은 사이버공격으로 인한 국가위기상황을 대처하기 위한 법제도적 조치를 마련하는 것이 더 이상 지체될 수 없다는 준엄한 경고를 보내고 있는 것이다. 이에 본고에서는 사이버위기 대응을 위한 법제도적, 정책적 과제가 무엇인지에 대해 사이버안보의 선진사례로 평가되는 미국의 현황을 중심으로 시사점을 도출하고 향후 개선방안을 모색해 보았다. 즉, 우리나라의 사이버위기 대응을 위한 현행 체계의 문제점으로 지적되는 사이버위기 총괄전담기관의 부재를 극복하기 위해 국가정보원을 총괄전담기관으로 활용할 것과 공공부문과 민간부문을 아우르고 테러리즘의 양상으로 계획적 조직적으로 발생하는 사이버공격을 효과적으로 대응하기 위해 기존의 사이버위기 관련 법제를 통합·재정비하여 사이버위기 대응 기본법제를 마련할 것을 제안하였다.

* 법학박사/성균관대학교 법학연구소 선임연구원, (02)760-1288, dskim94@skku.edu

목 차

Ⅰ. 서 론

1. 사이버공간과 국가의 책무

우리 헌법은 인간의 존엄성과 가치, 불가침의 인권의 보장 및 자유와 권리의 본질적 침해금지 등을 천명함과 동시에 질서유지를 위하여 필요한 경우에 한해 자유와 권리를 법률로써 제한할 수 있으며, 아울러 안전의 확보가 국가존립 목적의 하나라는 것을 확인하고 있다. 따라서 기본권의 최대한 보장과 함께 안전과 질서를 확보하는 것도 헌법적 가치와 근거를 지니는 국가의 책무요, 목적이다.

현대인의 가장 큰 관심사는 자신의 생명과 신체 및 재산의 안전 확보에 관한 문제로 귀착되고 있다고 해도 과언이 아니다. 좋은 질서 상태가 유지되어야 할 우리 공동체에 안녕과 질서를 심각하게 훼손하는 경찰상의 위험이 일상화되고 내재화되고 있는 오늘날의 현실은 바로 고도 '위험사회(危險社會)'의 도래라고 할 수 있다. 위험사회의 요소로 공동체의 해체와 익명성 증가, 교통통신의 발달에 따른 국경붕괴, 자연재해 급증 등을 들 수 있으나, 정보사회로 특징되는 현대사회는 정보통신 기술의 발전에 따라 전통적인 물리적 공간을 뛰어넘는 공간의 등장, 즉 사이버공간의 등장으로 대표되는 정보통신기술 발전과 그에 따른 역기능에 주목할 필요가 있다.

이른바 사이버공간은 고도 정보사회의 진입에 따라 이미 현실공간의 필수적인 일부분으로 자리잡고 있으며, 해킹 등 사이버공격, 저작권 등 권리침해, 명예훼손 등 사이버 공간의 특수한 불법행위는 현실공간에 대한 막대한 파급력을 지니고 있다.

이렇듯 위험사회에서는 불안전과 위

험을 완전하게 제거할 수 없기 때문에 최악의 상황을 예방하는 것이 무엇보다 중요하며 이러한 점에서 공공의 안녕과 질서유지를 위한 예방적 활동으로서 국가의 역할, 즉 경찰(警察)에 대한 재조명이 필요한 시점이다.[1] 특히 최근에는 이러한 국가작용이 이른바 국가위기관리의 일환으로 활발하게 논의되고 있다. 국가위기란 "국가의 주권 또는 국가를 구성하는 정치·경제·사회·문화 체계 등 국가의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태"라고 정의할 수 있으며,[2] 국가위기관리(대응)는 "국가위기를 효율적으로 예방·대비하고 발생시에는 효과적으로 대응·복구하기 위하여 국가가 가용 자원을 기획·조정·통제하는 과정"이라고 정의할 수 있다. 과거에는 국가위기 사태가 주로 군사적인 범주에 국한되었지만 최근에는 테러, 대량 살상무기 확산, 마약 밀거래, 환경 파괴, 에너지 문제, 사이버공격[3] 등 준군사, 또는 비군사적인 분야까지 포함하는 추세로 바뀌었다. 이러한 포괄적 안보 개념 하에서 국가 위기의 개념 또한 과거와 달리 새로운 환경의 변화에 대응하여 변화하게 되었다.[4]

현대사회는 정보통신 기술의 발달과 인터넷의 급속한 보급으로 인해 소위 유비쿼터스 환경이 점차 고도화되고 있다. 그러나 이러한 발전과 동시에 컴퓨터 웜·바이러스

1) 더욱이 이러한 불법행위는 인터넷의 기술적 특성상 다수의 관계자가 연계되어 복합적인 책임문제를 발생시키며, 이는 인터넷의 특성과 그에 대한 자유주의적 사상과 맞물려 매우 복잡한 이해관계를 표출한다. 컴퓨터 보급의 확대와 정보통신기술의 발전은 국민 생활의 편의성을 향상시키지만, 동시에 공공의 안녕과 질서에 대한 위험을 가져오기도 한다. 즉, 인터넷으로 대표되는 사이버공간은 행위자의 익명성, 중앙통제조직의 부재, 정보유통의 신속성과 파급효과의 광범위성 등의 특성을 갖추고 음란물의 유포, 명예훼손적 유언비어의 유포, 해킹이나 컴퓨터바이러스 유포를 통한 업무 마비, 개인정보의 유출 등 다양한 형태의 위험발생 가능성을 갖는다. 이는 경찰법상 위험발생 영역의 확장을 의미할 뿐만 아니라, 물리적 공간을 전제로 한 종래의 경찰법 규정과 이론에 한계가 있음을 의미하기도 한다. 사이버공간에서 경찰작용의 법적 구조와 특수성에 관한 보다 상세한 내용은 졸고(2009), 참조.

2) 국가위기관리기본지침(대통령훈령 제124호) 참조.

3) 「사이버공격」에 대한 법적 정의로는 국가사이버안전관리규정 제2조제2호에서 "해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위"라고 정의하고 있다.

4) 이재은 외(2006); 안철현(2005).

의 창궐과 사이버공격이 급증하고 있으며, 사이버공격 기법은 갈수록 지능화되어가고 있다. 특히, 최근의 사이버 공격 형태는 단순 자기과시에서 벗어나 금전적인 이득추구로 본격화되고 있으며 정보유출을 목적으로 한 악성코드가 크게 증가하고 있고, 피싱 등 여러 사회공학적 방법과 유기적으로 결합한 사이버 공격 수법이 나날이 증가되고 있다. 또한, 다양해진 공격수법은 과거 웜 바이러스 등의 악성코드에 집중된 경향에서 벗어나 봇넷 구성, 방문자가 많은 홈페이지 해킹, 백신 등 정보보호제품의 취약점 공격 등으로 진화하고 있다.[5] 이처럼, 향후 국가사이버위기는 고도화, 다양화, 은밀화를 지향할 것으로 예상되며, 그 피해는 전산망 장애에 국한되지 않고, 국가기관이나 기업의 중요자료유출 내지 개인정보유출로 이어질 것으로 우려된다. 또한 사이버공격은 금전적인 목적을 갖는 해킹은 물론 소위 사이버전쟁의 형태로 나타나기도 한다.[6] 이처럼 정보통신망에 대한 사이버 공격은 최악의 경우 금융·교통·산업·방송·의료 등의 마비로 국가 전체의 위기를 초래할 수 있으므로 사이버위기관리의 중요성이 부각됨과 동시에 각 국가는 자국의 사이버 위기관리에 심혈을 기울이고 있다. 즉, 사이버공격의 급증으로 국가차원에서 사이버공간에서의 극도의 경찰위험인 사이버위기를

5) 참고로 사이버테러대응센터에서는 사이버범죄를 사이버테러형 범죄와 일반사이버범죄로 구분하고 있다. 사이버테러형범죄란 해킹, 악성프로그램 유포 등과 같이 고도의 기술적 요소가 포함되어 정보통신망 자체를 통해 공격이 이루어지는 것을 말하며, 일반사이버범죄란 사기(통신, 게임), 불법복제(음란물, 프로그램), 불법 유해사이트(음란, 도박, 폭발물, 자살), 명예훼손, 개인정보침해, 사이버스토킹, 사이버성폭력, 협박·공갈 등 사이버공간이 범죄의 수단으로 사용되는 유형을 말한다. 최근 유형별 발생건수를 살펴보면 아래 표와 같다.

구분	총계	해킹·바이러스	인터넷사기	사이버폭력	불법사이트운영	불법복제판매	기타
2008	122,227	16,953	29,290	13,819	8,056	32,084	22,025
2007	78,890	14,037	28,081	12,905	5,505	8,167	10,195
2006	70,545	15,979	26,711	9,436	7,322	2,284	8,813
2005	72,421	15,874	33,112	9,227	1,850	1,233	11,125

자료: 사이버테러대응센터(http://www.netan.go.kr/)(2009. 5. 30 방문)

6) 대표적인 예로 2007년 5월에는 러시아 해커들이 에스토니아 전산망을 공격해 에스토니아가 3주간 마비상태에 빠진 일이 있었으며, 2008년 8월에는 러시아가 사이버 공격을 통해 그루지야의 정부·언론·금융·교통 전산망을 무너뜨려 그루지야가 초토화된 사건이 있었다. 보안 전문가들은 이런 공격이 익명으로, 비교적 적은 비용으로, 그리고 세계어디서나 이뤄질 수 있다는 점에 주목하고 있다. 김민식 외(2009), p.30.

효율적으로 관리하고 극복할 수 있는 사이버위기 대응체계에 대한 관심이 집중되고 있는 것이다.[7]

한편 사이버침해 및 사이버테러로 인한 사고를 표현하는 용어로 '디지털재난'을 제안하고 이에 대한 관리필요성을 제기하는 주장이 있다.[8] 사이버보안 사고는 국가적 재난으로 안전한 정보사회 구축을 위해서는 사이버보안 대책의 강구, 사이버보안사고를 대응하기 위한 이른바 '디지털 위험관리'가 필요하다는 견해로 그 취지에 공감한다. 다만, 이를 위해 사이버보안 사고를 대처하기 위한 개념적 징표로 '디지털재난'을 설정하는 것은 현대 사이버위기의 특성과 '통신 재난'을 규율하는 현행 법체계를 고려할 때 적절하지 않은 측면이 있다. 즉, 현행법상 통신, 에너지, 교통 등 국가기반체계의 마비로 인한 재난에 대하여는 「재난 및 안전관리 기본법」이 우선 적용된다.[9] 허나 이번 '7.7DDoS대란'[10]에서 보는 바와 같이 현대의 사이버위기 내지 사이버보안 사고는 고의적이고 계획적인 사이버공격이 중대한 위협요인으로 지적되는 바, 과연 이를 대응·관리하기 위한 체계로 '재난'의 개념을 차용하는 것이 타당한지는 의문이다. 왜

7) 최근에 발생하는 국가적 위기의 일반적인 특성으로서 첫째, 그 발생 양상이 점차 다양화·대형화되고 있으며, 둘째, 각종 위기는 도발적·가변적이어서 불확실성이 점차 증가하고 있고, 셋째, 위기에 대한 대응 조치를 취하는 시간이 극히 적어서 위기관리에 대한 평상시 예방의 필요성이 강력하게 대두된다. 박동균(2004).

8) 정국환·유지연(2009).

9) 동법에 따르면 국무총리가 위원장으로 되는 중앙안전관리위원회가 국가안전보장과 관련된 사무의 경우에는 국가안전보장회의와 협의를 거쳐, 안전관리에 관한 중요정책의 심의 및 총괄·조정, 국가안전관리기본계획안 및 집행계획안의 심의, 중앙행정기관이 수행하는 재난 및 안전관리업무의 협의·조정하며(제10조제1항), 인명 또는 재산의 피해정도가 매우 크거나 재난의 영향이 사회적·경제적으로 광범위하여 주무부처의 장 또는 법 제16조제2항의 규정에 의한 지역재난안전대책본부의 본부장의 건의를 받아 법 제14조제2항의 규정에 의한 중앙재난안전대책본부의 본부장이 인정하는 재난(같은 법 시행령 제13조) 등 대통령령이 정하는 대규모 재난의 예방·대비·대응·복구 등에 관한 사항을 총괄·조정하고 필요한 조치를 하기 위하여 행정안전부에 중앙재난안전대책본부를 두고 있다.

10) 2009년 7월 7일부터 10일까지 악의적으로 유포한 좀비PC의 악성코드를 활성화해 미국과 한국의 주요 정부기관, 포털 사이트, 은행 사이트 등을 분산서비스거부공격(DDoS: Distributed Denial of Service attack)하여 해당 사이트 접속 장애 및 서비스를 지연시킴으로써, 정보보호의 중요성을 재확인시킨 사건이다. 이 사건에 대한 자세한 내용은 정국환·유지연(2009).

냐하면 행정안전부장관이 관장하는 '통신재난'은 「재난 및 안전관리 기본법」의 성격상 자연적 재해이거나, 인재(人災)라도 특정 의사가 없이 발생한 일반적 재난을 의미하며, 동법의 제반규정 또한 이에 대한 사후적 복구의 의미를 가지기 때문이다. 요컨대, '통신재난관리'와 정보통신상 야기될 수 있는 위험의 예방과 제거를 의미하는 소위 '정보통신질서(경찰)업무'와는 구별되며, 현대의 사이버위기 대응을 위한 국가작용은 후술하는 바와 같이 국가안전보장 및 질서 확립의 영역으로 보고 그에 대한 법제정립의 과제로 설정하는 것이 타당하다고 본다.

2. 사이버위기의 현황과 특징

사이버공간은 정보통신기술의 비약적인 발전과 더불어 정보기기와 컴퓨터 그리고 인터넷 등의 네트워크로 연결된 가상의 공간으로 이미 국민 생활의 보편적인 영역으로 자리매김하였고, 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있음은 주지의 사실이다. 이러한 특수성으로 말미암아 복잡·고도화되며, 시공간의 제약을 벗어나 발생하는 모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있다. 게다가 사이버공격으로 초래되는 사이버위기는 현실세계의 물리적 질서혼란과 달리 특정개인에 대한 것일지라도 국가전체의 위기로 확대될 수 있는 위험성을 가지고 있다. 2003년 소위 '1·25 인터넷 대란'[11]과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터 조직적인 사이버공격으로 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대하고 있다. 2004년 들어서는 중국의 조직적 해커집단으로 추정되는 세력이 한국의 국회, 국방연구원, 원자력연구소 등 주요 국가

11) 1. 25 인터넷 대란은 2003년 1월 25일에 마이크로소프트(MS)의 SQL서버취약점을 집중 공격한 슬래머웜으로 대량의 네트워크 트래픽으로 망에 과부하가 발생되어 9시간 동안 국가 인터넷 접속이 마비됨으로써 사회적 혼란을 야기한 사건이다. 불과 수분 만에 전세계 75,000여개 시스템이 접속 불능상태에 놓여 인터넷뱅킹과 트레이딩, 전자상거래 등 일부 주요 사이트뿐만 아니라 국가 인터넷망이 마비되어 막대한 피해를 발생시킨 대표적 사례로 언급된다. 이에 대한 자세한 내용은 정국환·유지연(2009).

기관을 대상으로 보안시스템을 무력화시키는 공격을 감행하여 국가기밀과 주요인사의 이메일 등이 유출되는 사건이 발생하기도 하였다.[12)]

경찰청 사이버테러대응센터에 의하면, 사이버테러형 범죄인 해킹·바이러스는 2003년도에 1,323건, 2004년 3,970건, 2005년 4,549건으로 계속적으로 증가하는 추세이다. 2006년부터 그 증가율의 약세를 보이고는 있지만, 국가정보원 국가사이버안전센터의 자료에 의하면, 2007년의 공공분야 사이버 침해사고가 2배 가까이 늘었고 지방자치단체와 교육기관들의 보안 취약성은 오히려 악화된 것으로 나타났다. 국가사이버안전센터가 매달 발표하는 2007년도 공공분야 사이버 침해사고 건수를 취합한 결과, 전체 공공기관에서 발생하는 사이버 침해사고 건수는 총 7,588건으로 전년도의 4,286건에 비해 크게 증가한 것으로 나타났다. 최근 2008년 2월 공공기관에서 발생한 침해사고는 768건으로, 그해 1월에 나타난 634건에 비해 21%(134건) 증가하였는바, 이는 2007년 12월 발생했던 524건에 비해서는 46.6%나 늘어난 수치이다.[13)] 2008년 10월의 국정감사에서 공공기관이 지난 5년 간 사이버사고가 12배나 증가했다는 발표가 있는데, 국가사이버안전센터의 2008년 9월 통계자료에 의하면 침해사고는 웜 바이러스 감염사고의 증가로 인해 8월보다 63.1%(277건) 증가한 716건을 기록했고, 악성코드 감염사고는 지난 1년간 월평균 432건이 발생했는데 이번 달에는 전월대비 186% 증가한 572건이 발생하는 등 공공기관의 사이버침해사고가 여전히 증가추세를 보이고 있음은 심각한 문제로 지적된다.[14)] 특히, 최근 발생한 소위 '7.7 DDoS 대란'은 다

12) 이 사태의 대응과정에서 국가정보의 취약점과 국가 사이버위기에 대한 대응체계상의 문제가 노출되어 이에 대한 개선책이 필요하다는 주장이 제기되었다. 뚜렷한 목적과 장기적인 계획을 가지고 시도하는 특정세력의 조직적·전면적 사이버공격에 국가 주요 시스템과 기밀정보가 무차별적으로 피해를 입고 있어 보다 강력한 보안조치가 필요하다는 점을 일깨워 준 사건으로 평가된다. 하옥현(2004).

13) 침해사고율은 지방자치단체가 308건으로 가장 많았으며, 교육기관(208건)과 산하기관(139건) 순이다. 2008년 2월에 비해 사고율이 가장 많이 늘어난 곳은 산하기관(총 139건)이며, 악성코드 감염사고는 전월 대비 26.3% 증가한 634건이 발생하여 지난 1년 동안 월 평균 464건 발생했던 것과 비교할 때 높은 수치를 보였다. 이러한 악성코드 감염사고 기관별로 발생비율을 살펴보면, 지방자치단체가 300건으로 전체 감염사고의 47.3%를 차지하고 있어 지방자치단체에 대한 보안 확보가 시급하다는 점을 알 수 있다. 기타 상세한 내용은 국가사이버안전센터(2008) 참조.

시 한번 사이버위기의 위험성과 그 대응 필요성을 일깨워주는 사건이었으며, 이러한 사이버공격으로 인한 국가위기상황을 대처하기 위한 법제도적 조치가 더 이상 지체될 수 없다는 준엄한 경고를 보내고 있다.

사이버위기는 전 세계에 그물망처럼 연계된 인터넷망을 통해 매우 빠른 속도로 전개되며 소요시간도 그동안에 있었던 일반적인 위기와는 달리 수분이내에 끝나면서도 피해규모에 있어서는 일반의 상상의 초월하고 심지어는 국가의 안보에 심각한 위협으로 나타날 수 있다. 또한 사이버공격은 최소의 인원으로 최대의 피해를 가할 수 있는 가능성을 지닌다. 과거의 테러행위 등 물리적인 공격이 대규모 혹은 소규모라도 다수의 인원을 필요로 하는 것에 비해 사이버공격을 위한 인원은 다른 어떤 물리적인 테러를 수행하기 위한 인원에 비해 적은 것이 일반적이다. 그러나 이러한 경우에도 타격대상이 되는 정보통신 시스템을 파괴 또는 마비시키는 것에 따른 경제적 사회적 파급효과는 정보통신기반시설이 더욱 선진화되고 의존도가 높은 국가일수록 비례하여 커지며, 또한 이러한 위협행위는 반복 가능성, 영속성의 속성이 있으므로 한 번의 범죄행위는 그 규모나 피해가 작을 지라도 계속적으로 자동적인 프로그램의 실행, 확산을 통해 피해액이 계속 증가할 가능성이 높다.

이렇듯 사이버위기는 그동안 우리 인류에 커다란 위협이 되어왔던 일반적인 위기와는 그 본질을 달리하는 것으로, 특히 광역성 및 다양성을 지닌다. 즉, 일반적으로 사이버공격은 공격자가 목표로 정한 공격지점에 직접 접속하여 공격하는 것이 아니라 네트워크가 연결된 곳이라면 세계 어느 곳이든 공격을 감행할 수 있다. 특히 네트워크망에 대한 보안시스템이 잘 완비되고 국민들의 보안의식이 높은 선진국보다는 보안시스템이 취약한 국가에서 출발하여 여러 단계를 거친 다음 목표 전산망에 접근하여 필요한 정보를 빼내가는 우회적인 방법을 선택하는 것이 일반적이다. 따라서 사이버공간에 대한 공격이 발생했을 경우 피해를 당한 전산망에 대한 권한만 가지고 대응하는 것은 한계가 있으며, 더욱이 국제적 테러조직에 의한 범죄일 경우 국제적인 협력이

14) 《보안뉴스》, (2008. 10. 13), 참조.

없다면 사실상 조사자체가 불가능하다. 또한 사이버위기에 대한 대응은 과거와 같이 경찰이나 군(軍) 등이 물리적 책임지역을 가지고 독자적으로 업무를 수행할 수 있는 것이 아니라 네트워크에 연계된 각 기관들이 공동으로 상호 유기적인 협조체제를 구축하는 것이 필수적이므로 유관기관간의 유기적인 협조체계를 구축하고, 특히 이를 총괄조정하는 전문기관을 설립하는 것이 최대 현안으로 떠오르고 있다. 또한 사이버위기는 현실세계의 물리적 질서혼란과 달리 특정개인에 대한 것일지라도 사회 및 국가전체의 위기로 발전할 수 있고, 개인에 대한 사이버공격이라고 할지라도 그 개인이 대통령 등 국가기관을 구성할 경우에는 국가기관에 대한 공격으로 볼 수밖에 없는 특징 보유한다는 점에 주목하여야 한다.

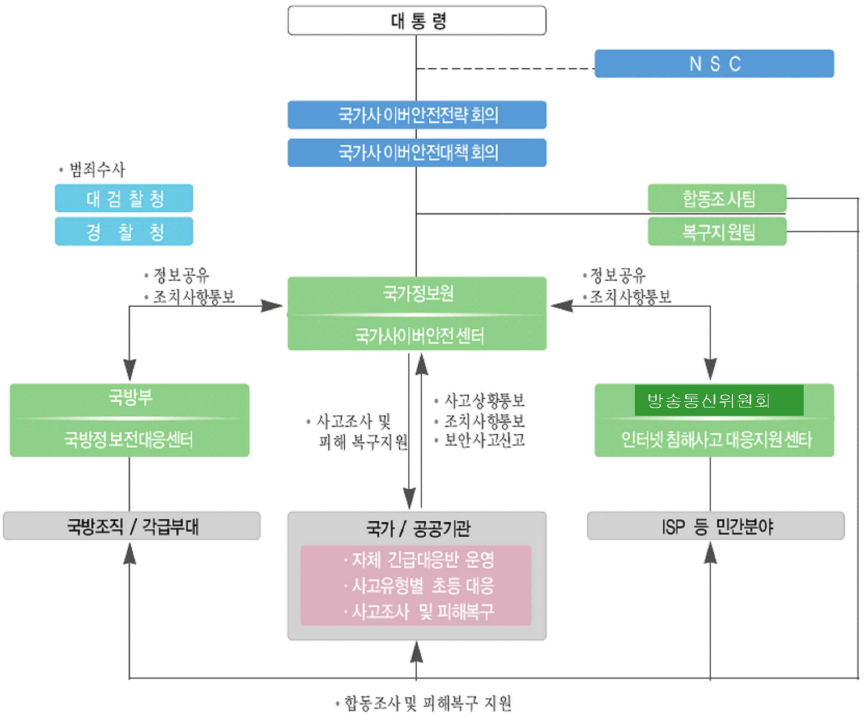
아래에서는 사이버위기를 효과적으로 대응하기 위한 법적 과제를 살펴보기 위한 논의로 먼저 우리나라의 사이버위기 대응체계에 대해 개관하고, 이어 미국의 사이버위기 대응체계에 관해 조직적 측면과 제도적 측면으로 나누어 살펴본다.

Ⅱ. 한국의 사이버위기 대응체계 현황 및 문제점

1. 관련 조직 현황

과거 한국은 경찰청, 국가정보원, (구)정보통신부 등을 통해 사이버공격에 대응하였으나, 2003년 '1·25 인터넷 대란' 이후 큰 허점을 보이게 되면서 사이버안보에 대한 국가적으로 관심을 가지게 되었다. 이에 국가안전보장회의(NSC)와 대통령안보보좌관 그리고 국가정보원에 국가사이버안전센터가 설립되기에 이르렀다. 현행 국가사이버위기 대응 조직을 개관하면 다음과 같다.

〔그림 1〕 국가사이버위기 대응체계



자료: 국가정보백서(2008)

(1) 국가정보원(국가사이버안전센터, 국가사이버안전전략회의 · 대책회의)

국가정보원은 1999년 1월 소속 컴퓨터 전문가로 국가전산망보안관리반을 편성하고 국가 공공기관 전산망에 대한 보안진단 및 보안시스템 운용기법 등 실무차원의 보안기술 지원활동을 하였다. 국가 차원의 사이버테러리즘 대응 업무를 원활하게 수행하기 위해 공공 및 민간부문의 협력체계를 국가기관협의체, 공기업협의체, 산·학·연 협의체 3개 부문으로 2002년 9월 구성한 '국가정보보안협의회'를 운영하고 있다. 특히, 2004년 2월 국가정보원은 기존의 '정보보안 119'[15]를 확대하여 「국가사이버안전

15) 1999년 8월 국가정보원 홈페이지에 정보보안 119사이트를 개설하여 국가·공공기관 정보통신의 해킹 바이러스에 대한 예방과 경보를 하고 사고 발생시 대응방법 및 복구에 필요한 기술적 지원을 제공하였다(현재는 국가사이버안전센터에 흡수되었음).

센터(NCSC: National Cyber Security Center)」를 설립하였다. 국가사이버안전센터는 2005년 1월 제정된 국가사이버안전관리규정에 의거하여 국가차원의 종합적이고 체계적인 사이버공격 대응을 위해 각종 사이버위협 정보를 수집·분석하여 관련 대응기구들과 정보공유 및 사이버위협 상황을 전파하고 예·경보를 발령하며, 평시에는 안전진단 등의 기능을 수행하고 있다.[16] 즉, ① 국가사이버안전정책 총괄 활동으로 국가사이버안전정책 기획·조정, 국가 사이버안전 관련 제도·지침수립, 국가 사이버안전 전략회의 및 대책회의 운영, 민·관·군 사이버안전 정보공유 체계를 구축·운영하고, ② 국가사이버안전 예방활동으로 국가 정보통신망의 안전성확인, 정보보안수준평가, 사이버전 모의훈련 실시, 정보통신망 보안성검토 및 안전측정업무를 수행하며, ③ 국가사이버위협정보의 수집·분석·전파 활동으로 24시간 365일 주요기관 대상 보안관제, "정상-관심-주의-경계-심각" 등 위협수준별 경보 발령, 보안분석정보 배포, 사이버안전 관련기술 개발 업무를 수행하며,[17] ④ 침해사고 대응 및 복구 활동으로 사이버공격 침해사고 접수, 사고조사 및 대책강구, 피해확산 방지 및 복구지원, 범정부 합동조사·복구지원팀을 구성·운영한다.[18]

「국가사이버안전전략회의」는 국가정보원장 소속으로 국가사이버안전에 관한 중요사항을 심의한다. 즉, 전략회의는 ① 국가사이버안전체계의 수립 및 개선에 관한 사항, ② 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, ③ 국가사이버안

16) 그런데 국가사이버안전센터의 기능을 고려할 때 당해 기관의 근거가 대통령 훈령에 불과하다는 점은 헌법 제96조의 행정조직법정주의 및 이를 구체화한 정부조직법 제4조(행정기관에는 그 소관사무의 범위에서 필요한 때에는 대통령령으로 정하는 바에 따라 시험연구기관·교육훈련기관·문화기관·의료기관·제조기관 및 자문기관 등을 둘 수 있다)에 반하는 것으로서 법적 논란을 피하기 어려운 문제점을 안고 있다.

17) 정보고속망 등 152개 기관의 27개 전산망을 연동한 종합·분석처리 시스템 등 14개 시스템을 통하여 사이버위협과 공격에 대하여 보안관제하고 있으며, 위협징후 탐지시 긴급 초동조치를 취함으로써 피해가 확산되는 것을 사전에 예방하고 방지하는 활동을 수행한다. 그런데 경보의 발령과 관련하여 위험에 따라 정해지는 수준별 경보에 대해서는 그에 합당한 행위제한이 따를 때 경보의 실효성이 담보될 수 있다 할 것이므로 이에 대한 사항은 훈령이 아닌 법률적 지위를 부여하여야 할 사항이며, 아울러 당해 법률에는 사이버위기 대응을 위한 여타 작용법적 근거를 보완하여야 한다.

18) 국가사이버안전관리규정 제8조.

전 관련 대통령 지시사항에 대한 조치방안, ④ 그 밖에 전략회의 의장이 부의하는 사항 등을 심의한다.[19] 전략회의의 위원은 교육과학기술부차관·외교통상부차관·법무부차관·국방부차관·행정안전부차관·지식경제부차관·보건복지가족부차관·국토해양부차관·대통령실외교안보수석비서관·방송통신위원회 상임위원·금융위원회 부위원장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 구성하며, 전략회의의 의장은 국가정보원장이 된다. 또한 이러한 전략회의를 지원하기 위해 「국가사이버안전대책회의」를 두며, 대책회의의 의장은 국가정보원의 사이버 안전업무를 담당하는 차장이 되며, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 한다.

⑵ 경찰청(사이버테러대응센터)

1995년 10월 외사관리관 산하에 분석팀과 수사팀으로 이루어진 해커수사대의 발족으로 컴퓨터 관련 범죄수사를 시작하다가 1997년 8월 원자력연구소 해킹사건 등 컴퓨터범죄가 주요 사회문제로 확대되자 사이버공간에서 이루어지는 해킹, 금융기관 전산망조작 등 각종 컴퓨터관련 범죄예방과 수사를 전담할 수사국 지능과 소속 컴퓨터범죄수사대로 개편했다.

2000년에 들어 국내·외적으로 사이버공격의 양상이 더욱 심각해짐에 따라 국가사회 정보통신기반을 체계적으로 보호하고 미래의 사이버공격에 대비하기 위해 사이버테러리즘과 정보전에 대한 예방과 분석, 추적수사 그리고 대응기법개발 등 종합적인 대응체계를 갖춘 전문기구로서 2000년 7월 사이버테러대응센터(CTRC: Cyber Terror Response Center)를 창설하였다.[20]

현행법상 일반 사회질서유지의 기본적인 과제를 수행하는 기관으로는 검찰청과 경찰청이 있는바, 사이버공간에 있어서 “공공의 안녕과 질서에 대한 위험 방지”는 현재 경찰법에 근거를 두고 있는 「경찰청과 그 소속기관 직제 시행규칙」[21] 제9조 제9항에

19) 국가사이버안전관리규정 제6조.
20) http://www.netan.go.kr/(2009. 5. 20 방문)
21) 행정안전부령 제38호(2008. 10. 15. 일부 개정).

의거하여 「사이버테러대응센터」가 "① 사이버테러의 탐지·추적수사 및 경보 등 조치, ② 사이버테러관련 수사기법의 연구·개발 및 국제경찰기구 등과의 협력, ③ 사이버범죄의 수사 및 지도 및 ④ 디지털매체 등 증거분석 업무 등" 수행하고, 검찰은 이러한 사이버범죄와 관련한 기소권과 수사지휘권을 행사한다(검찰청법 제4조). 「사이버테러대응센터」는 센터장을 중심으로 협력운영팀, 수사팀, 기획수사팀, 기술지원팀 등 4개 팀으로 구성되어 있으며, 사이버테러대응센터의 창설과 함께 전국의 14개 지방경찰청에 사이버범죄수사대를 설치하고 일선 경찰서에도 사이버수사전담반을 두어 상호유기적인 협력 활동을 전개하고 있다.

⑶ 국방부(국군기무사령부 국방정보전대응센터)

1999년 12월 국방부와 산하 각 군은 이러한 사이버공격에의 예방과 대응을 위한 컴퓨터사고대응팀(CERT: Computer Emergency Response Team)을 구축·운영하고 있으며 2000년에 국방통합보안관제실을 국방부 CERT상황실에 설치하여 운영중이다. 2001년 4월부터 합동참모본부에서 정보작전 차원의 사이버전 대응 활동을 위해 합참 정보작전방호태세(INFOCON: Information operation condition)를 제정·시행하고 있다.[22] 2002년 국방정보보호 기본계획을 수립하고 정보통신기반보호법을 근거로 하여 국방정보통신기반보호훈령을 제정하였으며, 2003년에는 국방부와 육·해·공군 본부 CERT상황실과 연동된 통합보안관리체계를 구축하였고, 2005년에는 합동참모본부와 각 군 등을 하나의 네트워크로 연결하여 실시간으로 보고, 지휘를 가능케 하는 지휘소자동화체계(C4I)가 구축되었다. 특히, '군 주요정보통신시설'에 대한 보안사고 예방 및 복구 등의 기술지원 업무를 맡고 있는 국군기무사령부는 2003년 11월 「국방정보전대응센터」를 출범시키고 날로 그 위협성이 커지고 있는 사이버전 대응을 위한 기능을 수행하도록 하였다.

22) 이는 컴퓨터 시스템을 비롯한 각종 유무선 네트워크와 C4I 체계 등 정보체계와 시설물들에 대한 내외부의 공격징후를 예상하거나 공격으로 인한 방어태세를 강화하여 그 피해를 최소화하기 위한 조치로 이를 기반으로 압록강훈련 및 을지훈련시 사이버전 모의훈련 등을 실시하고 있다.

2. 관련 법제 현황

현행법상 사이버공격 대응과 관련한 법률로는 「정보통신기반보호법」,[23] 「전자정부법」,[24] 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,[25] 「국가정보화기본법」[26]

23) 동법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하고자 하는 법으로서 사이버위기 대응 체계와 관련한 주요내용을 살펴보면 다음과 같다. 즉, 중앙행정기관의 장으로 하여금 소관분야의 정보통신기반시설중 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성 등을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하도록 하고(제8조), 지정된 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 두고 있다(제3조). 정보통신기반보호위원회는 주요 정보통신기반시설의 보호에 관한 사항을 심의한다. 위원장은 국무총리실장이며, 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원 및 위원장이 위촉하는 자로 한다. 중앙행정기관은 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하여 정보통신기반보호위원회의 심의를 거쳐 고시한다. 주요정보통신기반시설은 현재 공공부문과 민간부문에 걸쳐 다양하게 지정되어 있다. 행정안전부, 국가정보원 등은 필요하다고 판단되는 시설에 대하여 중앙행정기관에 주요정보통신기반시설의 지정을 권고할 수 있다. 주요 정보통신기반시설에 대하여 관계중앙행정기관장은 소관분야 주요 정보통신기반시설 보호지침을 제정하고 주요 정보통신기반시설 관리기관의 장에게 그 준수를 권고할 수 있으며, 보호에 필요한 조치를 명령 또는 권고할 수 있다. 주요 정보통신기반시설에 대한 침해행위는 누구에게나 금지된다. 이 외에도 주요 정보통신기반시설 침해에 대한 대응조치 및 관련 민간부문과의 협력 등이 규정되어 있다.

24) 전자정부법은 "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 목적"으로 하며, 법 제27조에서는 국회·법원·헌법재판소·중앙선거관리위원회 및 행정부에 대해 "전자정부의 구현에 요구되는 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련할 의무"를 부여하고 있다.

25) 정보통신망법에 따르면 정부는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보보호 등을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 하고(동법 제4조), 이를 위해 방송통신위원회가 전기통신사업자, 정보통신서비스 제공자, 나아가 정보통신망을 이용하는 모든 사람에게 일정한 조치의무를 부과하고 이행명령을 발하는 등 경찰권을 발할 수 있는 법적 근거를 두고 있다(제46조의3, 제48조, 제48조의2, 제48조의4, 제76조 등)

26) 이 법률 제4조에서는 정부에 대해 암호기술의 개발과 이용을 촉진할 의무를 부여함과 아울러 정보보안과 관련하여 행정안전부장관에 대해 "관계기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 이를 고시하고, 정보보호시스템을 제조하거나 수입하는 자에 대하여 이 기준의 준수를 권고"할 권한을 부여하고 있다(제37조 및 제38조).

등이 있다.[27] 특히, 국가사이버위기 대응체계와 관련하여서는 "국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적"으로 발하여진 대통령 훈령인 「국가사이버안전관리규정」[28]이 있다.[29]

3. 문제점

(1) 사이버위기 총괄전담기관의 부재

사이버공격은 초기단계에서부터 관련 정보의 유기적인 공유를 통한 평가가 없다면 그 파급효과를 효과적으로 대처하기 어렵고, 사후대처보다는 사전예방이 무엇보다도

27) 그 외에도 국가위기대응 법제로 계엄법의 적용도 검토해 볼 수 있다. 현실세계의 물리력에 의한 질서위기는 국가정보원장의 국내외 보안정보에 대한 수집·평가에 근거하여 국가안정보장회의의 심의(임의)와 국무회의의 심의(필수)를 거쳐 대통령이 계엄선포를 선포하고 군병력에 의한 질서유지를 하게 된다(계엄법 제1조 및 제2조). 계엄법은 계엄을 비상계엄과 경비계엄으로 나누고 비상계엄은 "대통령이 전시·사변 또는 이에 준하는 국가비상사태에 있어서 적과 교전상태에 있거나 사회질서가 극도로 교란되어 행정 및 사법기능의 수행이 현저히 곤란한 경우에 군사상의 필요에 응하거나 공공의 안녕질서를 유지하기 위하여 선포"하며, 경비계엄은 "대통령이 전시·사변 또는 이에 준하는 국가비상사태에 있어서 사회질서가 교란되어 일반행정기관만으로는 치안을 확보할 수 없는 경우에 공공의 안녕질서를 유지하기 위하여 선포"한다고 규정하고 있다. 현행 계엄법은 사이버위기와 관련한 사항을 따로 규정하고 있지 않으나, 인간의 신경망과 같은 국가정보통신망의 장애 그 자체가 국가질서에 대한 현저한 위협이 됨을 인식하여 물리적 국가위기에 상응하는 사이버 국가위기에 대응할 사이버계엄법의 가능성을 검토해볼 필요가 있다. 계엄법을 사이버위기에 직접 적용하기 위해서는 일부 개정이 수반되어야 하겠지만 현행 법규정을 두고 이를 상정해보면, 사이버공격의 정도가 심각하여 국가 안전보장 또는 국가이익에 중대한 위해가 발생하였거나 발생할 현저한 우려가 있는 사이버위기에 있어서는 동일한 절차를 통해 사이버계엄을 선포하고 사이버공간의 특성에 합당하게 현행 조직법상 정보보안에 있어 국가안전보장사무를 총괄하는 국가정보원이 이를 관장하도록 하여야 할 것으로 보인다.

28) 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로, 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망(「정보통신기반보호법」 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대하여는 적용 제외)을 대상으로 하는 대통령 훈령이다.

29) 사이버위기 대응을 위한 경찰법제의 보다 상세한 내용은 졸고(2009) 참조.

중요하다는 점은 주지의 사실이다. 이에 대해 우리나라는 지난 2003년 '1·25 인터넷 대란'과 2004년 '중국 해커에 의한 한국 주요기관 해킹 사건', 최근 '7.7 DDoS 대란'을 통해 수차례 뼈아픈 경험을 한 바 있다. 특히, 위 사태에 대한 대응 과정에서 국가정보의 취약점과 국가 사이버위기에 대한 대응체계상의 문제가 노출되어 이에 대한 개선책이 필요하다는 점이 지적되었을 뿐만 아니라, 목적과 장기적인 계획을 가지고 시도하는 특정세력의 조직적·전면적 사이버공격에 보다 강력한 보안조치가 필요하다는 점을 보여주었다.

이렇듯 사이버공격에 대한 사전예방의 중요성을 고려하여 후술하는 바와 같이 미국은 국토안보부가 '국가 대응 프레임워크', '국가 기반 보호 계획', '국가 사이버 공간 대응 시스템', '사이버 위험 관리 프로그램' 등의 전략과 프로그램의 진행으로 사이버공격을 예방하고 대응하기 위한 실질적인 조치들을 수행하고 있다. 특히 최근의 경우 '국가 사이버보안 종합전략'과 '사이버공간 정책 리뷰'에 의해 국토안보부가 정부 전산망을 적극적으로 감시하는 임무를 맡아 사이버침해 사고에 대한 사후 대응측면보다는 사전대응체계를 수립하는데 큰 역할을 맡고 있음은 시사하는 바가 크다.

현재 우리나라의 사이버 위기 대응기관으로는 앞서 살펴본 바와 같이 국가정보원의 국가사이버안전센터, 국방부의 국방정보전대응센터, 방송통신위원회의 인터넷침해사고대응지원센터를 주축으로 대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 국가보안기술연구소, 정보공유분석센터(ISAC) 등으로 다양하게 존재하고 있다. 문제는 이러한 다양한 기관이 존재하고 있음에도 실재 사이버위기가 발생하였을 경우 각 기관의 책임과 역할이 불분명하고, 무엇보다 강력한 리더쉽을 가진 총괄점담기관이 사실상 없다는 점이다.[30] 이는 사이버 위기대응에 대해 명확히 규정하는 법률 부재

30) 그에 반해 미국의 국토안보부는 '국토안보법'에 근거하여 공공과 민간부문 전체에 걸쳐, 그리고 물리적 위협이든 사이버공격이든 그 형태를 막론하고 보호조치를 총괄적으로 집행한다. 국토안보부는 연방정부의 정보보호 정책을 실시할 책임을 지고 있으며, 이것에 대한 실례로, 2002년에 발표된 "국토안보 국가전략"에서 국토안보부의 주요기반시설 보호를 총괄하는 역할을 명시, 2003년에 제시된 "사이버공간 보호를 위한 국가전략"에서는 연방정부의 각 기관이 완수해야 할 정보보호의 포괄적인 틀을 제시, 2004년부터 "국가 사고 관리 시스템"을 통한 사고대응 단일 체계 수립 및 표준화된 관리 계획 제시 등을 언급할 수 있다. 또한 미국, 독일, 프랑스 등은 사이버

와 각 부처간 역할과 책임소재가 불분명하며 2개 이상의 기관 및 부문이 연루되어 사이버위기 발생 시 효과적인 대응에 어려움이 존재하기 때문이다.

⑵ 통합법제의 부재

사이버위기는 그 특성상 공공부문과 민간부문을 구분하지 않으며, 개인적 법익의 침해에서 시작된 사이버공격이 국가적 안전을 위협하는 사이버위기로 발전될 가능성이 얼마든지 있음에도 불구하고 우리나라의 사이버위기 법제 현황을 분석해 보면, 공공분야와 민간분야에 따라 적용법령이 다르고, 또한 주요 정보통신 기반시설여부에 따라 다시 적용 법령이 달라지는 형태이다. 즉, 현재 공공부문과 민간부문을 막론하고 주요정보통신기반시설에 대하여는 「정보통신기반보호법」이 적용되지만, 그 외에는 공공부문은 「국가사이버안전관리규정」이 적용되고, 민간부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 적용된다. 이와 같이 내용이 상이한 법률이 적용됨에 따라 각 부문마다 사이버위기 대응체계가 별도로 이루어지게 되는 문제를 내포하고 있다. 사이버공격에 의해 '7.7 DDoS 대란'과 같은 위기가 초래될 경우 「정보통신기반보호위원회」의 보호대책과 「중앙안전관리위원회」의 국가안전관리기본계획안 및 「국가사이버안전전략회의」의 국가사이버안전 관련 정책간 모순 내지 충돌이 발생하거나 후속조치를 위한 기민한 대응이 어려울 가능성도 배제할 수 없는 것이다.

더구나 공공부문 중 주요 정보통신기반시설이 아닌 경우는 법률이 아니라 행정의 수반인 대통령에 속한 정부기관에 대해서만 구속력을 가지는 대통령 훈령(국가사이버안전관리규정)을 그 근거로 하는 바, 분야간 불균형 문제와 실재 사이버위기 발생시 당해 대통령 훈령을 근거로 현행법상 분산된 여타 사이버위기 대응조직의 협력과 지원을 효과적으로 이끌어 낼 수 있을지 의문이다. 물론 국가안전보장업무의 효율적인 수행을 위한 조직과 권한을 정한 법으로 국가정보원법이 있지만 동법에 의하면 국가

위기에 대한 총괄 전담조직이 존재하고 있고, 일본과 영국의 경우에는 우리나라와 같이 부문별로 기관이 존재하고는 있으나 이를 조정하기 위한 센터 내지 위원회가 존재하고 있어 각 대응 기관간 협력체계가 강화되어 있다는 점도 주목해야 한다. 이처럼, 미국, 독일, 프랑스 및 영국, 일본 등의 경우 이미 국가 사이버 위기대응 체계에 대한 정립을 끝낸 수준으로 인력 및 기술개발 보완 등의 활용 및 안정화 단계에 진입했다고 볼 수 있다.

정보원은 “국외정보 및 국내보안정보(대공·대정부전복·방첩·대테러 및 국제범죄조직)의 수집·작성 및 배포”, “국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무(각급기관에 대한 보안감사는 제외)”, “형법중 내란의 죄, 외환의 죄, 군형법중 반란의 죄, 암호불정사용죄, 군사기밀보호법에 규정된 죄, 국가보안법에 규정된 죄에 대한 수사”, “정보 및 보안업무의 기획·조정” 등의 권한(동법 제3조)을 보유하고 있는 반면, 이들 권한행사를 위한 작용법적 근거는 전무한 실정이다. 따라서 통합법제에는 총괄기관이 사이버위기 대응을 위해 관련 부처 내지 공공기관은 물론 민간에 적정 권한을 행사할 수 있는 여타 작용법적 근거를 마련하는 것이 중요한 쟁점이 된다.

Ⅲ. 미국의 사이버위기 대응체계 현황 및 시사점

1. 개 관

미국은 1970년대부터 이미 사이버공격의 심각성을 인식하고 대책을 세우고 법적 장치를 마련하기 시작하였으나, 사이버테러리즘에 대한 구체적인 대응책이 나타나게 된 것은 1991년 걸프전 당시 미 국방부의 사이트가 사이버테러리스트에 의해 해킹당한 사실이 상원 청문회를 통해 밝혀진 이후로 알려진다. 또한 사이버위기 대응과 관련된 국가정책은 사이버위협에 대한 위기감의 확산에 따른 국가주요기반보호의 필요성이 제기되어 1995년 주요기반보호위원회(PCCIP: President’s Commission on Critical Infrastructure Protection) 보고서에 근거한 「대통령 지시(PDD) 63」이 1997년 발표되면서 시작되었다. 1997년 6월 국가안보국(NSA: National Security Agency)이 미국의 주요 기관의 컴퓨터 보안상태 점검을 위해 태평양사령부 지휘통제소를 메일 폭탄(Mail Bomb) 등으로 가상공격하였는데, 중앙컴퓨터시스템이 파괴되어 위성과 군사시설 등에 대한 통제불능 상태에 빠지고 저장된 국방기밀들이 해킹당하는 결과가 초래되어 큰 우려를 낳았다. 이에 국가 주요기반시설에 대한 사이버위협에 대응하기 위한 계획이 각계의 의견수렴을 거쳐 2000년 1월 「정보시스템 보호를 위한 국가계획(National Plan for Information System Protection)」[31]으로 발표되어 국가 주요기반

보호를 위한 체계적인 전략개발이 주로 연방정부를 중심으로 이루어지기 시작했다. 특히, 이러한 미국의 사이버위기 대응 체계는 2001년 9. 11 테러를 계기로 급속한 진전을 이루게 되는 바, 2003년 3월 기존의 22개 다른 연방기관과 프로그램 및 기관들을 연방재난관리청(FEMA)과 함께 통합하여 국토안보부(DHS: Department of Homeland Security)를 신설하고 국가의 재난관리 및 국토안보 업무를 총괄하는 등 9.11 테러는 미국의 안보체계를 전면 재편하는 일대 전기가 되었다. 미국은 9.11 이후에 물리적인 공격과 더불어 사이버공격을 포함한 테러리스트의 위협과 공격으로부터 미국의 안전을 보장하기 위한 조치를 추진하였고, 이를 위해 총괄부서로서 국토안보부를 신설하고, 사이버안보 담당 대통령 특별 보좌관, 국가기반자문회의, 주요기반보호대통령협의회 등을 조직하였다. 이처럼 책임과 권한이 여러 부처에 분산됨으로 인해 발생하는 정책의 혼선을 방지하고 모든 역량을 한 곳에 집중하기 위해 국토안보부(DHS)의 창설로 대표되는 효율적인 대응체계를 마련한 것은 미국의 사이버안보전략이 갖는 가장 큰 의의로 평가된다.

무엇보다 미국은 연방정부만으로는 더 이상 사이버위협에 대응키 어렵다는 인식하에 관련 업계의 협조를 비롯한 모든 국민의 적극적 참여와 국제적인 협조가 절실하게 요구된다는 점을 주목하였다. 이에 2002년 9월 18일 「사이버안보국가전략(National Strategy to Secure Cyberspace)」[32]의 초안을 발표하고 사이버공간에의 의존성 심화와 새로운 취약성의 발견 및 네트워크의 글로벌화 등에 따라 증대되는 사이버위협에의 지속적인 대응과 국가 차원의 위험관리의 중요성을 강조하였다. 이후 사이버안보 국가전략은 수차례의 의견수렵과정을 거쳐 2003년 2월 14일 최종적으로 확정되었는 바, 사이버안보를 국가의 주요기반시설의 보호에 한정하지 않고 기존의 개념을 확장

31) 이 국가계획은 크게 사이버위협에 대한 대비와 예방, 탐지와 대응, 안전한 기반구축 등으로 이루어져 있으며 이에 기초하여 연방침입탐지네트워크(FIDNET: Federal Intrusion Detection NETwork)가 운영되고 있다. 이 FIDNET의 목적은 주요 기반구조자산과 공유된 상호의존성을 확인하고 취약성을 제안하며, 침입행위의 실시간 탐지와 이에 대한 신속한 대응으로 주요 정보시스템 보안을 위한 견고한 기초(Strong Foundation)를 구축하는 것이다.

32) Whitehouse(2003. 2), 『The National Strategy to Secure Cyberspace』.

한 국가안보차원에서의 사이버안보의 중요성을 재확인하고 주요기반시설 및 핵심자산에 대한 물리적 보호전략과 양축을 이루게 되었다.[33] 사이버안보국가전략에서 미국은 사이버안보는 국민의 참여 없이 연방정부만으로 수행할 수 없는 매우 어려운 과제이므로 사이버안보에 대한 인식제고와 교육훈련, 기술개발과 취약성 해결 등으로 시장의 활성화, 정보의 공유와 운영계획의 수립 등 민간부문과 공공부문 간의 긴밀한 체계구축을 최우선 원칙으로 제시하고 있다. 또한 사이버위협의 동적 특성을 고려하여 사이버위협에 유연하게 대응하고 책임과 의무를 명확히 하며 지속적인 정책의 필요성을 제시하고, 국가간의 정보공유, 취약성 감소노력, 사이버테러리즘 대응을 위한 국제적인 협력체계 구축의 필요성을 강조하고 있다. 2008년 1월에는 부시 대통령이 "NSPD-54/ HSPD-23"을 승인함으로서 이를 바탕으로 한 「국가사이버보안종합전략(CNCI : Comprehensive National Cyber Security Initiative)」이 수립되었다. 이는 신 사이버보안을 위해 결정한 비밀정책으로, 지금까지는 각각의 침입사고에 대한 사후 대응에 비중이 높았다면, 이제 사전대응 체계 구축으로 사이버안보를 달성하겠다는 의지를 나타내고 있다.[34]

이후 오바마 행정부가 수립된 이후에도 역시 사이버보안은 중대한 정책이슈로 주목받게 되었으며, 이는 오바마 대통령이 취임후 60일 이내에 기존 연방 사이버보안 정책에 대한 검토와 향후 전략 수립을 위한 보고서 제출을 국가안보이사회(NSC) 등 관련기관에 요청한데서도 이 같은 의지를 짐작할 수 있다. 이에 따라 최근 2009년 5월말에는 ① 백악관, 연방차원 등 최상위 리더쉽에 따른 정책 추진, ② 보안교육, 전문인력 양성 등 디지털 국가를 위한 역량 제고, ③ 민·관 협력을 위한 파트너쉽 구축 등 사이버보안 책임 분배, ④ 효율적인 정보 공유 및 대응 능력 강화, ⑤ 보안 강화를 위한 혁신 촉진 등을 내용으로 하는 「사이버공간 정책 리뷰」(Cyberspace Policy Review:

33) Whitehouse(2003. 2), 『The National Strategy for The Physical Protection of Critical Infrastructure and Key Asset』.

34) "The Murky Waters of the White House's Cybersecurity Plan", July 23, 200: http://www.cdi.org/program/document.cfm?DocumentID=4345&from_page=../index.cfm (2009. 6. 2 방문)

Assuring a Trusted and Resilient Information and Communications Infrastructure)[35] 를 발표하였다. 동보고서에서는 단기실행계획(10개) 및 중기실행계획(13개)을 제시하고 있으며, 특히 단기실행계획 첫 번째로 국가사이버보안 정책 추진을 총괄할 사이버보안책임관을 임명할 것을 제안하고 있다. 이에 따라 백악관은 사이버보안의 총괄책임자로서 이른바 사이버 차르(Cyber Czar)를 임명한 바 있다.[36]

2. 관련 조직 현황

(1) 국토안보부(DHS)

미국은 911테러 이후, 2002년 6월 부시 미국 대통령이 상원에 제출한 '국토안보법(안)'을 계기로 2003년 3월 정식 출범한 국토안보부(DHS)를 중심으로 테러방지 및 자연재해, 재해 등을 총집결시킨 총체적 재해·재난 관리체계를 구축하고 있다. 국토안보부는 기존의 대통령 자문기구 성격의 '국토안보국'을 격상시킨 것으로, 국토안보부의 편입되는 기구들에는 세관, 이민국, 해양수비대, 교통보안국, 연방재난관리청(FEMA) 등 22개 기관에 이른다.[37]

국토안보부는 미국에 대한 공격을 막고, 국토의 위협과 테러에 대한 취약점을 축소시키며, 테러리스트에 의한 공격으로 발생된 피해복구 지원 및 위험 최소화를 위한 임무를 수행한다. 즉, 국토안보부의 임무에는 ① 미국의 핵심 자원과 주요기반시설을 보호하기 위한 종합적인 국가전략 개발, ② 주요기반시설에 대한 공격에 대응하여 위기관리 기능 수행, ③ 주요정보시스템 마비에 대비한 긴급복구와 관련 민간 및 정부기

35) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf(2009. 8. 5 방문)

36) 한편 지난 5월 초대 사이버 차르로 국가안보이사회(NSC) 사이버보안책임자인 멜리사 해더웨이(Melissa Hathaway)를 임명하였으나, 최근 8월 사퇴함에 따라 후임을 물색중인 것으로 알려졌다.

37) 국토안보부는 직원 18만명 이상, 연간 예산 400억 달러의 막대한 인적·물적 기반을 토대로 국경경비, 재난 및 화생방 공격대비 활동, 과학기술 확보, 정보분석, 이민관리, 사이버 보안 등의 활동을 수행한다. 사이버테러리즘을 포함한 모든 대테러 활동 임무는 민·관·군의 모든 기반산업과 관련되어 상호 영향을 미치기 때문에 기존 행정부처나 정보기관 중 특정 1개 부서가 맡기에는 너무 방대한 범위라고 판단하였기 때문에 모든 관련 조직, 법령 및 예산을 통합·정비하여 국토안보부를 신설한 것이다.

관 기술지원, ④ 다른 연방기관들과 협력하여 주정부, 민간부문, 학계, 공공, 일반국민 등을 대상으로 하는 경부 발령과 정보보안 대책 및 자문 제공, ⑤ 다른 기관과 연계하여 국가안보에 관한 새로운 과학적 지식과 기술 연구개발 수행 및 재정지원 등이 있다. 국토안보부는 연방정부의 정보보호 정책을 실시할 책임을 지고 있으며, 이를 규정한 것이 2003년 2월에 제시된 「사이버공간 보안 국가전략(National Strategy to Security Cyberspace)」이다. 이는 연방정부의 각 기관이 완수해야 할 정보보호의 포괄적인 틀을 제시하고 있다.[38)]

국토안보부의 장은 대통령이 임명하고 상원이 인준하는데, 국토안보부 장관은 국방장관이나 법무장관과 같은 지위로, 미국 내 재난안보와 관련한 모든 정보에 접근할 수 있는 권한을 가지고 있으며, 여기에는 사법당국과 정보기관, 기타 정부기관의 자료는 물론 미국의 인프라 및 기타 취약대상과 관련한 정보도 포함된다.

국토안보부는 2005년 조직개편을 통해 정보보호와 관련되어 국토안보부 장관에게 국토안보와 관련된 현안에 대해 자문하는 국토안전보장자문위원회(HSAC: Homeland Security Advisory Council)와 국토안보부 장관과 대통령에게 공공 및 민간영역의 주요 기반시설의 보안과 관련된 사항을 자문하는 국가기반시설자문위원회(NIAC: National Infrastructure Advisory Council)가 설립되었다.[39)] 이후 국토안보부는 2006년 4월 부시 대통령이 서명하고 2007년 3월 1일부터 효력이 발생된 포스트-카트리나위기관리개혁법(the Post-Katrina Emergency Management Reform Act)[40)]에 의하여 일부 조

38) http://www.dhs.gov/xprevprot/programs/gc_1158611596104.shtm(2009. 6. 20 방문)

39) Congressional Research Service(2005).

40) 포스트-카트리나위기관리개혁법(the Post-Katrina EmergencyManagement Reform Act)은 국토안보부 내의 새로운 리더십 정립과 기능 조정, 재난관리청(FEMA)의 기능 추가, 그리고 기존 국토안보법의 수정을 가져왔다. 즉, 동법은 재난관리청(FEMA)에 준비국(Preparedness Directorate)의 기능을 이관시켰고, 기존의 준비국은 국가보호프로그램국(NPPD: National Protection and Programs Directorate)으로 개명되었다. 국가보호프로그램국(NPPD)은 기반보호실(OIP:Office of Infrastructure Protection), 사이버보안통신실(OCS&C: Office of Cyber Security and Communications), 위험관리분석실(ORM&A: Office of Risk Management and Analysis), 정부간프로그램실(OIP: Office of Intergovernmental Programs), 그리고 미국방문실(US-VIST)로 구성되어 있다. http://www.dhs.gov/xabout/structure/gc_1169243598416.shtm(2009. 6. 20 방문)

직적 변경이 있었고, 연방재난관리청(FEMA: Federal Emergency Management Agency) 또한 재조직되었다.[41]

국토안보부는 유비쿼터스 시대를 대비하기 위해 핵심 정보보호전략으로서 국토안보 대통령령 7호(HSPD-7)를 근거로 국가기반구조와 주요자원(CI/KR: Critical Infrastructure/ Key Resource)보호를 개선하기 위해 2006년 6월 「국가기반보호계획(NIPP: National Infrastructure Protection Plan)」을 발표하였다. 이 계획에는 국가기반구조와 주요자원 보호 프로그램을 구현하기 위한 보안 협력모델 수립, 장기적 위험 감소 프로그램 실행, 국가기반구조와 주요자원 보호를 위한 자원의 효율적 사용 극대화 등을 담고 있다. 이를 위해 에너지, 물, 식량, 의료, 교통 및 정보통신과 같은 국가의 핵심자산 및 자원을 보호하기 위한 민간부문과의 협력관계를 규명하는 프레임워크를 포함하고 있다. 동계획에서 국토안보부는 기반구조부문조정위원회(SCC: Sector Coordinating Council) 및 정부부처조정위원회(GCC: Government Coordinating Council)를 운영하고, 핵심 기반구조의 소유자와 운영자에게 정보를 제공할 수 있는 프로토콜을 구현할 것을 밝히고 있다.

⑵ 대통령직속 주요기반보호위원회

대통령직속 주요기반보호위원회(PCIPB)는 미국의 비상통신망을 포함한 주요기반의 정보시스템을 지원하는 물리적 자산의 안전을 확보하여 미국의 국민, 경제, 정부업무 및 국가안보를 보호하기 위해 설립한 최고정책기관으로서 주요기반보호정책을 효과적으로 집행하고 강화할 수 있는 조직이다. 특히, 동위원회는 2003년 2월 미국의 정보통신기반을 보호하기 위한 「사이버공간 보안 국가전략(National Strategy to Security Cyberspace)」을 수립하여 사이버안보를 위한 전략적 목적[42]과 국가전략 수

41) 즉, 미국 역사상 가장 참혹한 자연재난이었던 2005년 허리케인 카트리나 대응에서 나타난 문제점들을 치유하기 위하여 좀 더 강한 사전준비 임무를 포함하여 실질적인 재난관리 권한을 FEMA에 부여하였다. http://www.fema.gov/about/history.shtm(2009. 6. 20 방문)

42) 미국의 주요기반시설에 대한 사이버공격 예방, 사이버공격에 대한 국가적 취약성 감소, 사이버공격 발생시 피해와 복구시간의 최소화 등이다.

립의 원칙[43] 및 국가적 우선순위[44]를 기초로 전략을 구체화하고 있다.

3. 관련 법제 현황

(1) 애국법(USA PATRIOT ACT of 2001)

동법은 법집행기관과 정보기관간의 정보 수집 및 공유체계에 구조적·법적인 제약을 해소시킴으로써 대테러 기관간 협력을 강화시킨 것이다. 이를 위해 테러 혐의자에 대한 감청 허용요건과 영장주의를 완화하고 테러조직과 관련된 은행계좌나 자산의 동결 등을 규정하였다.[45] 또한, 테러범죄자들이 미국으로 입국하는 것을 막고 미국내 테러용의자들의 추방을 쉽게하기 위하여 구금 및 추방의 요건을 대폭 완화하는 한편, 테러행위에 대한 처벌도 크게 강화하였다. 이후 2006년 개정된 애국법은 애국법의 개선 및 권한 재부여 법(USA PATRIOT Improvement and Reauthorization Act of 2005)과 애국법의 부가적 권한 재부여에 관한 수정안(USA PATRIOT Act Additional Reauthorizing Amendment Act of 2006)의 두 개의 법률로 구성되어 있다. 개정 법률은 9·11 테러 이후 연방당국에 주어진 광범위한 감시와 수사권한을 대부분 유지하고 있으며 2005년 말 효력이 완료되어 있던 16개 조항 중에서 14개 조항을 영구 법제화하고 2개 조항은 2009년 12월 30일 까지 4년 연장돼 효력을 가지게 되었다.[46]

(2) 관리예산처 지침(Circular A-130)

미국 연방정부의 컴퓨터보안을 포함한 정보자원관리의 중심기관은 관리예산처(OMB)이다. OMB는 연방정보보안 정책에 필요한 최소한의 통제장치들을 수립하여

43) 국가적 노력(모든 국민의 참여), 프라이버시와 국민의 자유보호, 규제와 시장지배력, 책임소재(국토안보부의 역할), 유연성 확보, 중장기 계획 수립 등이다.

44) 사이버안보를 위한 우선순위(Critical Priorities)는 국가사이버안보대응 시스템, 국가사이버안보 위협 및 취약성 축소 프로그램, 국가 사이버안보 인식 및 프로그램, 정보의 사이버공간 보호, 국가안보 및 국제 사이버안보 협력 등이다.

45) 미국 연방법전 제18권 제1030조.

46) http://www.usdoj.gov/olp/pdf/usa_patriot_improvement_and_reauthorization_act.pdf(2009. 6. 20 방문)

각 정부기관들이 정보보안에 관한 책임을 지도록 요구하고 각 기관들의 정보보안 프로그램과 기관관리통제시스템을 상호연계시키고 있었다. 관리예산처(OMB: Office of Management and Budget)는 정보자원의 관리와 정보보안에 있어 요구되는 임무수행에 필요한 사항들을 기술한 지침(Circular A-130)을 발표하였다. OMB Circular A-130의 〈부록Ⅲ〉연방정보자원보안(Security of Federal Automated Information Resources)은 연방정보보안정책에 필요한 최소한의 통제장치들을 수립하고, 각 기관들이 정보보안에 대한 책임을 지도록 하면서 각 기관 정보보안프로그램과 관리통제시스템을 상호연계시키도록 규정하고 있다. 세부내용에 따르면 관리예산처는 연방정보자원보안정책을 총괄 및 감독하며 상무부, 특히 국립표준기술연구소(NIST: National Institute of Standards and Technology)는 보안관련 표준 및 지침을 개발하고 인사관리처(OPM: Office of Personal Management)는 정보보안교육 및 훈련을 지원하고 각 기관의 침해사고 대응 및 취약성 정보공유 및 조정 등을 포함한 기타 기관들의 역할을 규정하고 있다.[47)]

그러나 OMB의 지침 성격을 가진 Circular A-130으로는 급증하고 있는 새로운 보안침해 및 기술에 대하여 충분한 대응을 할 수 없다는 인식하에 보완의 필요성이 제기됨에 따라 2000년 10월 정보보안 프로그램 관리와 평가측면을 강조하는 '정부정보보안개혁법(Government Information Security Reform Act)'이 제정된 것이다. 연방정부의 정보보안관리 강화의 필요성은 계속되었는데 정부정보보안개혁법이 2002년 10월까지 유효한 한시법적 형태를 가지고 있음에 따라 정부정보보안개혁법을 영구화할 수 있는 방안으로 2001년 11월 국토안보법의 일부로서 연방정보보안관리법(FISMA)이 제정되었다.[48)]

(3) 국토안보법(Homeland security Act of 2002)

2002년 6월 6일 부시 대통령은 미국내 테러대책을 총괄하는 국토안보부의 창설을

47) http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html(2009. 5. 20 방문)
48) http://csrc.nist.gov/drivers/documents/FISMA-final.pdf(2009. 6. 22 방문)

제안하였고, 2002년 11월 국토안보법[49]을 제정하여 이에 대한 법적 근거를 확보하였다.[50] 국토안보법은 포괄적인 테러리즘으로부터 미국의 전체 국가기반을 보호하기 위해서 제정된 법으로서 특히 사이버안보와 관련된 규정으로는 제2장의 정보분석 및 기반시설 보호(IAIP: Information Analysis and Infrastructure Protection)에 관한 규정과 제10장의 정보보안(Information Security)에 관한 규정이 대표적이다. 제2장에서 FBI의 국가기반보호센터(NIPC), 국방부의 국가통신시스템(NCS), 상무부의 주요기반보장국(CIAO) 및 에너지부의 국가기반시뮬레이션 및 분석센터와 에너지안보 및 보장 프로그램, 총무성(GSA)의 연방컴퓨터 사고대응센터(FedCIRC) 등의 기관에 속한 직무와 인적자일 및 권한과 책임이 국토안보부로 이관하도록 규정함으로써, 국토안보부가 각종 테러리즘과 관련된 모든 정보를 수사기관과 법집행기관으로부터 제공받을 수 있게 하고 있다.

연방정보보안관리법(FISMA: Federal Information Security Management Act of 2002)으로도 불리는 제10장은 연방을 지원하는 주요 정보자원에 대한 보호 및 통제를 위한 포괄적인 프로그램을 제공하고 고도로 네트워크화된 국가기반의 보안을 위하여 민간 부문의 국가기관 전체의 정보보안 노력을 조정하여 사이버위협에 대해 효과적으로 대응할 수 있도록 국토안보부가 정부 전체를 관리·감독하도록 하고 있다.[51] 연방정보보호관리법은 국립표준기술연구소(NIST)에 정보보안 정책, 절차, 그리고 실

49) http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm(2009. 6. 20 방문)

50) 국토안보법은 테러리즘에 관해 "인명에 위험하거나 주요기반시설 또는 핵심자원을 파괴할 잠재적인 행위와 미국의 모든 주 또는 기타 세부 행정구역의 형법에 대한 위반행위를 포함하고, 일반국민을 협박하거나 위압하려는 의도, 협박이나 위압을 통하여 정부정책에 영향을 미치고자 하는 의도, 대량파괴, 암살 또는 납치 등을 통하여 정부의 업무수행에 영향을 미치고자 하는 의도를 나타낸다"고 정의하고 있다. Homeland security Act of 2002, SEC. 2. DEFINITIONS(15).

51) 연방정보보안관리법은 2002년 11월에 만료 폐기된 정부정보보안개혁법(Government Information Security Reform Act of 2000)의 한시법 조항을 삭제하고, 전자정부법 2002(e-Government Act of 2002)의 제3장 정보보안에 삽입된 법이다. 연방정보보안관리법의 목적은 연방정부의 운영 및 자산에 대한 정보보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크 제공, 국가보안 및 법집행기관 전반에 걸친 관련 정보의 보안 위험에 대한 효율적인 관리 및 통제방안 제공 그리고 연방정부 정보 및 정보시스템 보호를 위한 최소한의 통제 및 유지 방안 개발 등에 있다.

무 뿐만 아니라 정보시스템을 보호하기 위한 표준과 가이드라인 대응에 관한 기관들에게 기술적인 지원을 제공하는 임무를 부여하고 있다.

미국의 정보보호 관련 각 정부기관의 개별적인 과제의 예산은 연방정보보안관리법(FISMA)에서의 정보보호의 정의를 사용하고 있는데, 동법에서의 정보보호에 대한 정의는 '정보 및 정보시스템의 가용성, 무결성, 기밀성을 제공하기 위해 불법적인 접근, 이용, 공개, 변형, 파괴로부터 보호하는 것'이라고 되어 있다.[52]

(4) 사이버보안연구개발법

2002년 11월 27일에 제정된 '사이버보안연구개발법(Cyber Security Research and Development Act of 2002)'의 주요 내용은 국립과학재단(NSF)과 국립표준기술원(NIST)에 새로운 연구 프로그램을 신설하는 것이다. 이에 따라 국립과학재단에 사이버안보 관련 연구개발의 혁신을 위한 연구센터(Institute for Security Technology Studies)와 장학금 제도를 신설하고 국립표준기술원에 정부·연구계·산업계의 연구보조금 프로그램을 신설하였다.[53]

(5) 기타 대통령령

대통령령 제3호 '국토안보경보시스템'(HSPD-3 : Homeland Security Advisory System)은 2002년 3월에 테러 위험과 관련된 정보를 공유하고 이를 사전에 경고할 수 있는 시스템 창출을 규정하고 있다.[54]

대통령령 제5호 '국내 사고관리'(HSPD-5 : Management of Domestic Incidents)는 2003년 2월에 미국내 사고 발생시 정부간 및 민간영역과의 효율적 협력을 통해 관리할 수 있도록 그 체계를 정하고 있다. 특히, 동명령에 따라 국토안보부는 연방 국내사고 관리의 총 책임자로 지명되었으며 테러 공격, 주요 재난 발생 등과 같은 비상

52) http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf(2009. 6. 15 방문)

53) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ305.107.pdf(2009. 6. 15 방문)

54) Homeland Security Presidential Directive-3: http://www.fas.org/irp/offdocs/nspd/hspd-3.htm(2009. 6. 20 방문)

사태의 예방, 준비, 대응 및 복구를 위한 연방자원 배분 및 업무조정의 책임을 부여받았다.[55]

대통령령 제7호 '주요기반 식별, 우선순위 설정 및 보호'(HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection)는 2003년 12월에 테러 행위로부터 보호해야할 주요 기반시설 및 자산을 식별하고 보호활동의 우선순위를 설정하며 보호활동을 수행할 수 있는 프레임워크 구성을 규정하여 국토안보부 및 연방과 지방정부 등 기반시설 보호를 위한 참여자들의 책임과 역할을 정하고 있다.[56]

대통령령 제8호 '국가준비'(HSPD-8: National Preparedness)는 2003년 12월에 미국의 테러활동에 대한 예방, 보호, 대응 및 복구를 강화할 수 있는 준비태세 강화 정책을 수립하도록 규정하고 있다.[57]

그 외 대통령령 제23호 및 제54호(HSPD-23/NSPD-54)는 2008년 1월에 연방정부 사이버보안에 대해 커다란 전략적 변화를 꾀하고자 미국 정부 전산망을 적극적으로 감시하는 정책을 수립하도록 규정하고 있다. 동 명령에 따라 국토안보부 내에 국가사이버안전센터(NCSC: National Cyber Security Center)가 설립되었으며 국가 사이버 안전 센터의 미션은 연방 기관들간의 협력을 통해 사이버 위협으로부터 미국 정부의 컴퓨터와 통신 시스템을 보호하는 것으로 알려지고 있다.

(6) 2009 사이버보안법안(Cybersecurity Act of 2009)

앞서 설명한 바와 같이 오바마 행정부는 2009년 「사이버공간 정책 리뷰」를 발표하고 국가사이버보안 정책 추진을 총괄할 사이버보안책임관(사이버 차르)을 임명하는 등 강력한 사이버보안 체계 확립을 위한 노력을 경주하고 있다. 이와 같은 오바마 행정부의 의지에 의회는 그에 상응하는 제도적 근거를 마련하기 위한 입법적 조치로 화

55) Homeland Security Presidential Directive-5:
http://www.fas.org/irp/offdocs/nspd/hspd-5.html(2009. 6. 20 방문)
56) Homeland Security Presidential Directive-7:
http://www.fas.org/irp/offdocs/nspd/hspd-7.html(2009. 6. 20 방문)
57) Homeland Security Presidential Directive-8:
http://www.fas.org/irp/offdocs/nspd/hspd-8.html(2009. 6. 20 방문)

답하고 있다. 즉, 존 록펠러 연방 상원의원은 사이버 보안에 관한 포괄적 입법조치로서 사이버보안법(안)(S.773)을 입안하였다.

이 법안은 국가사이버안보 정세를 안정화하기 위한 전례가 없는 대응책으로 백악관 자문기구로 외부 전문가로 구성된 사이버안보 고문 위원단의 창설, 상무부 아래 실시간 정보시스템 마련 등의 내용을 담고 있는 것으로 알려졌으며, 크게 ① 연방 정부 내 사이버안보 프로파일의 대폭적인 확장 및 사이버 관련 정부 기능 및 권한의 능률 강화, ② 국민 인식 촉진 및 인권 보호, ③ 사이버안보에 있어 정부와 민간 분야의 관계 재설정, ④ 장기적인 해결책 개발을 위해 사이버안보의 혁신과 창의력 촉진 등의 내용을 담고 있다.[58] 그런데 법안의 내용에는 인터넷 정보의 열람 내지 압수에 있어 영장주의가 제한되는 등 기본권 제한에 관한 사항도 포함되어 향후 논란이 예상된다. 동 법안이 제정될 경우에는 이는 사이버보안에 관한 기본법적 지위를 지닐 것으로 예상되는바, 귀추가 주목된다.

4. 시사점

미국의 경우, '전자정부법'의 일부인 '연방정보보안관리법'에 따라 각 연방기관은 예산절차의 일환으로서 관리예산처에 정보보호 대책의 상황을 보고하도록 하여 정보보호 정책과 예산을 연계시킨 형태로 분석된다. 관리예산처는 직접 정보보호조치를 집행하지는 않지만 '연방정보보안관리법'에 근거하여 전자정부에서 각 연방기관의 정보보호조치를 감독하고 이를 예산집행 등에 반영함으로써 공공부문 정보보안 일반에 대한 실질적인 평가 역할을 수행함으로써 사이버보안 확립에 기여한다. 한편 국토안보부는 '국토안보법'에 근거하여 공공과 민간부문 전체에 걸쳐, 그리고 물리적 위협이든 사이버공격이든 그 형태를 막론하고 보호조치를 총괄적으로 집행한다. 국토안보부는 연방정부의 정보보호 정책을 실시할 책임을 지고 있으며, 이것에 대한 실례로, 2002년에 발표된 「국토안보 국가전략」에서 국토안보부의 주요기반시설 보호를 총괄

58) 법안의 자세한 내용은 http://thomas.loc.gov/cgi-bin/query/z?c111:S.773(2009. 8. 10 방문) 참조

하는 역할을 명시한 점, 2003년에 제시된 「사이버공간 보호를 위한 국가전략」에서는 연방정부의 각 기관이 완수해야 할 정보보호의 포괄적인 틀을 제시한 점, 2004년부터 '국가 사고 관리 시스템'을 통한 사고대응단일 체계 수립 및 표준화된 관리 계획을 제시한 점 등을 언급할 수 있다. 또한 국토안보부는 '국가 대응 프레임워크', '국가기반보호계획', '국가 사이버공간 대응 시스템', '사이버 위험 관리 프로그램' 등의 전략과 프로그램의 진행으로 사이버 공격을 예방하고 대응하기 위한 실질적인 조치들을 수행하고 있으며 최근의 경우 "국가 사이버보안 종합전략"에 의해 미국 정부 전산망을 적극적으로 감시하는 임무를 맡아 사이버침해 사고에 대한 사후 대응측면보다는 '사전' 대응체계를 수립하는데 중요한 역할을 담당하고 있음을 알 수 있다.

(1) 대응체계 · 전략 측면

미국의 사이버안보전략이 갖는 가장 큰 의의는 사이버위기를 대응하기 위한 모든 역량을 국토안보부를 중심으로 집중하여 보다 효율적인 대응체계를 마련한 것이다. 또한 정부기관과 민간에서 컴퓨터사고대응팀(CERT), 정보공유분석센터(ISAC: Information Sharing and Analysis Centre)를 운영하고, 국방부는 CERT를 운영하여 민·관·군이 상호 공조하는 CERT와 ISAC 위주로 정보보안 정책을 추진하고 있다. 다만, 최근 국토안보부의 리더십 부재, 민간부문의 참여를 유도할 수 있는 구체적인 유인책의 결여, 추진 프로그램의 운용을 위한 재원의 부족, 정부기관 간의 적절한 역할 분담 등 일부 문제점도 지적되고 있다.[59]

또한 사이버위기에 효과적으로 대응하기 위한 연구개발도 소홀할 수 없다. 미국은 사이버보안연구개발법(2002년)을 제정하고, 국가사이버공간방어전략(2003년), 사이버보안우선순위의 위기(2005), 연방 사이버보안 및 정보보증 연구개발 계획(2006년)을 발표하는 등 사이버보안을 연방정부 연구개발 분야에서 최우선 프로그램 중 하나로 선정하고 연구개발 정책을 강화하고 있음은 우리에게 시사하는 바가 크다.

59) 이하 하옥현(2004) 참조.

⑵ 법제도 측면

사이버위기를 대응하기 위한 법제와 관련하여 9·11 테러 이후 UN 안보리는 결의안 1368호와 1373호를 통해 회원국들에게 강력한 대테러법을 제정할 것을 촉구하였다. 그리고 이러한 UN의 요구에 부응하여 대부분의 국가가 테러에 대비하기 위한 각종 제도를 정비하고 있다. 즉, 미국은 애국법과 국토안보법을 제정·시행 중에 있고, 영국은 기존의 반테러법을 대폭 강화하였다. 독일 또한 기존의 보안관련 법률을 새로운 테러위협상황에 적응토록 개정하는 것을 목적으로 하는 테러대책법을 제정하였으며, 일본과 프랑스도 테러대응을 위한 특별법을 제정하였다.[60]

우리나라도 2002년 9월까지 대테러법을 제정하겠다는 보고서를 UN에 제출하였고 2001년 11월 정부안을 마련하여 국회에 제출하였으나 논란만 거듭하다 2004년 5월 국회회기 종료와 함께 법안이 폐기되고 말았다. 그리고 논란이 되었던 인권보호 조항 등이 수정 보완되어 17대 국회에서도 3건의 테러방지법안이 재발의 되었으나, 이 또한 정치적 논란만 남긴 채 결실을 보지 못하였다.[61] 그러나 국가의 안보를 위협하는 사이버공격 등을 대응하기 위한 대테러활동의 법적 시스템을 구축하고 대테러 활동의 투명성 보장은 물론 국제사회와의 협력체제의 강화가 필요한 시점에서 사이버위기 대응을 위한 법제의 필요성을 부인할 수 없으며, 다만 구체적인 경찰작용법제에 있어서 부당한 인권침해를 방지하기 위한 장치에 대한 논의가 병행되어야 할 것임은 물론이다.[62]

---

60) 보다 상세한 내용은 국가보안기술연구소(2008) 참조.

61) 테러대응체계의 확립과 대테러활동 등에 관한 법률안(공성진 의원 대표발의), 테러방지 및 피해보전 등에 관한법률안(조성태 의원 대표발의), 테러예방 및 대응에 관한 법률안(정형근 의원 대표발의) 등이다.

62) 마침 이와 관련해서는 2008년 10월 28일 의원입법으로 「국가 사이버위기관리법안(공성진 의원 대표발의)」이 발의되어 향후 이에 대한 활발한 논의가 진행될 것으로 기대된다. 특히, 현재 대통령 훈령에 근거한 국가사이버안전센터에 대한 법적 근거를 담은 동 법안의 주요내용은 다음과 같다. ㉠ 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제4조), ㉡ 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련정보를 상호 공유하기 위하여 민·관 협의체를 구성·운영할 수 있음(안 제5조). ㉢ 국가정보원장은 국가사이버위기관리종합계획을 수립하고 이에 따라 위기관리기본지침을 작성하여 책임기관의 장에게 배포하고, 책임기관의 장은 세부지침을 수립·시행하여야 함(안 제6조). ㉣ 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수

Ⅳ. 결 론

한국의 사이버 위기 대응을 위해서는 무엇보다 분산된 기능을 총괄·조정하고 사이버위기에 신속하고 효과적으로 대응할 수 있도록 단일화된 법률, 제도 및 정책을 중심으로 통합적으로 재구성하여야 할 것이다. 즉, 사이버 위기 대응을 조직적이고 전문적으로 대응할 수 있도록 법적 근거를 갖는 총괄전담기관이 컨트롤 타워가 되어 일원화된 대응 체계를 구축하여야 한다. 아울러 민간부문과 공공부문을 포괄하는 범국가적 차원의 사이버위기 대응을 위한 계획수립, 정보보호 인력양성, 정보보호 예산의 우선적·안정적 확보, 보안기술개발, 정보보호 산업의 육성, 국제공조체제 확립, 보안 인식 제고를 위한 교육 등을 위한 법제도적 기반이 절실하다.

아래에서는 우리나라 사이버위기 대응을 위한 핵심적 과제로 전문적이고 실효성있는 총괄전담기관, 통합법제 마련 방향에 관해 논하면서 결론에 갈음하고자 한다.

1. 총괄전담기관으로서 국가정보원의 권한과 책임 설정

사이버공격에 효과적으로 대응하기 위해서는 공공부문과 민간부문을 망라하는 국

있는 보안관제센터를 구축·운영하거나 다른 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조), ㉤ 책임기관의 장은 사이버공격을 탐지하여 사이버위기 발생 가능성을 조기에 차단·예방하는 등 피해를 최소화하기 위하여 신속한 대응조치를 취하여야 함(안 제9조), ㉥ 책임기관의 장은 사이버공격으로 인해 피해가 발생한 경우에는 자체 사고조사를 실시하고, 그 결과를 관계 중앙행정기관의 장 및 국가정보원장에게 통보하여야 하며, 국가정보원장은 필요한 경우에 직접 사고조사를 실시할 수 있음(안 제10조), ㉦ 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취해야 함(안 제12조), ㉧ 정부는 심각단계의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등을 위하여 관계 기관 및 전문인력이 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제13조), ㉨ 관계 중앙행정기관의 장 및 국가정보원장은 사이버위기관리에 필요한 기술개발·국제협력 등 필요한 시책을 추진할 수 있음(안 제14조 및 제16조), ㉩ 정부는 사이버공격 기도에 관한 정보를 제공하거나 사이버공격을 가한 자를 신고한 자에 대하여 포상금을 지급할 수 있음(안 제18조), ㉪ 직무상 비밀을 누설한 경우에는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 보안관제센터를 구축하지 아니한 경우에는 2천만원 이하의 과태료에 처할 수 있음(안 제19조 및 제20조).

가사이버위기 총괄전담기관을 창설하여 각 기관별 임무와 기능을 유기적으로 통합하고 일관성있는 정책수립과 민·관·군 협력체제를 내실화시켜야 한다. 이 전담기관은 미국의 국토안보부와 같이 물리적 차원의 국가안보 기능과 함께 새로운 정부부처로 창설할 수도 있을 것이나, 아직 국가사이버안보 관련 업무가 체계화되지 않은 상황에서 우선 그에 관한 전문성을 지닌 「국가정보원」을 국가사이버안보에 대한 총괄전담기관으로 지정하고 실질적인 권한과 책임을 부여하는 방안이 필요하다. 현행 정부조직법을 고려할 때 국가의 안전보장과 관련한 조직으로 물리적 위협에 대하여는 국방부[63]가, 국가안전을 위협하는 정보위협에 대하여는 국가정보원[64]이 각 일차적인 책임을 수행하는 것으로 해석되며, 현재 국가정보원이 국가사이버안전의 총괄지원기관인 국가사이버안전센터를 운영하고 있는 점 등을 고려할 때 사이버위기 대응을 위한 총괄기관으로서의 기능하는데 적합한 능력을 갖춘 조직으로 평가된다. 더욱이 국가정보원이 거의 40여년간 국가보안 업무를 수행하면서 쌓은 노하우를 적극 활용함은 물론, 국내외 정보 협력 및 분석이 중요한 사이버위기의 특성을 고려할 때 이른바 고등경찰[65]인 국가정보원의 차별화된 전문성을 활용하는 것이 필요하다.

허나 국가정보원을 활용하는 방안은 우리나라의 현대사에서 정보기관이 보여준 부정적 모습에 대한 국민적 트라우마로 여러 가지 우려가 제기되고 있는 실정이다. 허나 최근의 사이버공격 유형이 단순히 개인의 법익에 위해를 가하는 것을 넘어 국가적인 혼란과 안전에 대한 위협으로 극대화되고 있는 사정을 감안할 때, 전문적이고 강력한 정보력을 지닌 국가정보원의 역할을 활용하는 것은 불가피한 측면이 있다. 더욱이 우리나라가 유일한 분단국가로서 북한과의 대치를 망각할 수 없는 멍에를 지고 있을 뿐만 아니라, 주변 여러 강대국을 복잡한 이해당사자로 둘 수 밖에 없는 지리적·역사적

63) 정부조직법 제28조 참조.

64) 정부조직법 제15조, 국가정보원법 제1조 및 제3조 참조.

65) 고등경찰이란 프랑스법에서 유래한 개념으로, 경찰에 의하여 보호되는 법익을 기준으로 한 구별이다. 원래 고등경찰(haute police)은 사회적으로 보다 우월한 가치를 지니는 법익을 보호하기 위한 경찰활동을 의미하였으나, 나중에는 사상·종교·집회·결사·언론의 자유에 대한 정보수집·단속과 같이 국가의 존립과 유지를 보장하기 위하여 국가적 기관 및 제도에 대한 위해를 방지하는 활동을 의미하게 되었다. 이광윤 외(2002).

특수성을 고려할 때 사이버위기를 대응하는데 정보기관의 역할을 배제하고는 효과적인 대응을 기대하기 어렵다.[66] 따라서 현재 전자정부, 주요정보통신기반시설 등 공공부문과 통신재난관리를 담당하는 행정안전부, 민간부문을 담당하는 방송통신위원회, 개인·사회의 질서유지를 담당하는 경찰청 등이 1차적으로 각 소관 분야의 사이버안전을 담당하되, 당해 위험요인이 국가안보를 위협하거나 그 가능성이 의심되는 경우에는 총괄전담기관인 국가정보원에 관련 정보를 신속히 통보하도록 하고, 총괄기관의 임무 수행을 위한 협조에 적극 응하여야 함은 물론 필요시 총괄기관의 지시에 따라 대응조치를 수행하도록 관련 법적 근거를 마련하여야 한다.

그런데 국가정보원의 총괄기능에 대해서는 전문성 등 많은 장점과 불가피성에도 불구하고, 역시 한국 현대사에서 정보기관의 이미지는 빅브라더(Big Brother)의 망령을 쉽게 지워버릴 수 없는 현실적인 난제가 있다. 때문에 국가정보원에 사이버위기 대응을 위한 총괄권한을 부여하는 것은 국민이 납득할 수 있는 역기능 방지장치를 마련하는 것이 무엇보다 중요하다. 이와 관련하여 미국의 국토안보부가 공식적으로 국가사이버 통제로 발생할 수 있는 개인의 자유권 침해에 대해 미리 안전장치를 두고 이를 적극 활용함으로써 불필요한 의심을 해소하는 것은 참고할 만하다. 즉, 국토안보부 조직에 프라이버시 담당관과 민권·자유 담당관을 둠으로써 국민이 국가 정보기관에 대해 갖는 근본적인 의구심을 해소시켜주고, 세련된 정책 실행을 위한 고도의 조직체계를 구성하고 있는 점을 벤치마킹할 필요가 있다.[67]

2. 사이버위기 대응을 위한 통합법 체계 마련

사이버공간은 정보통신기술의 비약적인 발전과 더불어 정보기기와 컴퓨터 그리고 인터넷 등의 네트워크로 연결된 가상의 공간으로 이미 국민 생활의 보편적인 영역으

66) 북한은 인터넷을 통해 한국과 미국 첩보를 수집하고 전산망을 교란하는 사이버전쟁 전담부대인 '기술정찰조'를 확대·편성해 운용하고 있는 것으로 알려졌다. 기술정찰조는 인민군 총참모부 정찰국 소속으로, 군 컴퓨터 전문요원을 양성하는 평양의 지휘자동화대학 졸업생 위주로 100여명이 활동 중인 것으로 알려져 있다. 상세 내용은《매일경제》, (2009. 5. 5).

67) 우형진(2007).

로 자리매김하였고, 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있음은 주지의 사실이다. 이러한 특수성으로 말미암아 복잡·고도화되며, 시공간의 제약을 벗어나 발생하는 모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있다. 따라서 정부와 민간이 참여한 국가차원의 종합적인 사이버위기 대응체계를 구축하도록 하고, 이를 통하여 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 총괄전담기관(국가정보원)을 통한 국가의 역량을 최대한 결집하여 신속히 대응할 수 있도록 법적 근거를 마련하여야 한다. 즉, 사이버공격을 대응하기 위한 정부기관 상호간의 업무분장을 통한 기관 상호간의 조정과 통제의 원리를 갖춘 기본법적 성질을 가지는 법률의 제정을 통해 사이버 공격으로부터 국가위기를 사전예방하기 위한 법체계를 정립할 필요가 있다. 현대 유비쿼터스사회는 개인과 사회 및 국가가 하나의 망으로 연결된다는 점에서 국가를 구성하는 개인이나 특정 사회영역에 대한 위협은 국가에 대한 위협으로 연결될 가능성이 내포되게 된다. 따라서 다양한 사이버공격에 대하여는 사회질서를 담당하는 경찰과 행정각부 및 국가질서를 담당하는 국가정보원이 징후를 초기단계부터 서로 공유하고 단계별로 주무기관을 구별하되 징후의 변화발전을 전체적으로 모니터링할 수 있는 전문기관을 둘 필요가 있다고 할 것이다.[68] 다시 말해 전체적인 총괄기관과 단계별 소관기관을 구분하여 역할을 설정하고, 사이버위기 발생시 총괄전담기관의 권한과 책임을 명확히 하는 것이 무엇보다 중요하다. 아울러 사이버위기에 있어 공공부문과 민간부문, 중앙과 지방자치단체 어느 한곳이라도 별개의 단절된 위험범위가 아닌 점을 고려할 때 모든 주체가 일관되고 통일된 사이버보안계획을 수립·집행할 수 있도록 국가단위의 사이버보안계획을 최상위에 두고, 그 아래에 중앙 행정각부의 사이버보안계획 및 시·도의 사이버보안실시계획을 수립하도록 추진체계를 확립하여야 할 것이다. 또한 국가사이버위기를 등급별로 구분하고 그에 따른 행위제한의 내용을 구체화하는 세심한 작업도 필요하다.

68) 특정기관의 정보독점을 통한 전제적 지배를 방지하기 위해서 모니터링센터는 각 기관 모두가 참여하는 공동관제의 형태로 구성하는 것이 바람직하다.

참고자료

국가정보원(2006/2007/2008), 『국가정보보호백서』.

국가안전보장회의(2006), 『국가위기관리에 관한 법제화 방안』.

국가보안기술연구소(2008), 『국가 사이버위기 관리 체계 강화방안에 관한 연구』.

국가사이버안전센터(2008), 『Monthly 사이버시큐리티(3월호)』.

김도승(2009), 『사이버공간에서의 경찰법이론에 관한 연구』, 성균관대학교 박사학위논문.

김민식 외(2009), "통합적 사이버 위기관리 체계의 필요성에 관한 연구: 미국과 한국의 제도 및 정책 비교를 중심으로", 정보·보안 논문지 제9권 제1호.

김열수(2005), 『21세기 국가위기관리체계론(한국 및 외국의 사례비교연구)』, 오름.

박동균(2004), "한국 경찰의 위기관리능력 제고방안: 미국과 일본 사례의 교훈을 중심으로", 한국공안행정학회보 제18호.

안철현(2005), "국가 위기관리 개념의 변화와 위기관리 체계의 구축방향", 비상기획보 제73호.

이재은 외(2006), 『재난관리론』, 대영문화사.

우형진(2007), 『넷 전쟁과 인터넷 보안군』, SERI 연구에세이, 삼성경제연구소.

이광윤·김민호·강현호(2002), 『행정작용법론』, 법문사.

정국환·유지연(2009), 『디지털재난 그 의미와 대응의 새로운 패러다임』, KISDI이슈리포트.

조호대(2006), "사이버테러 대응 방안에 관한 연구", 한국위기관리논집 제2권제1호.

하옥현(2004), 『국가 사이버안보체계 구축 전략』, 고려대학교 박사학위논문.

《매일경제》, (2009. 5. 5), "북한에 사이버전쟁 부대가 있다".

《보안뉴스》, (2008. 10. 13), "공공기관, 사이버침해사고 여전히 증가추세".

Congressional Research Service(2005), 『Department of Homeland Security Reorganization: The 2SR Initiative』.

Whitehouse(2003), 『The National Strategy to Secure Cyberspace』.

_____, 『The National Strategy for The Physical Protection of Critical Infrastructure and Key Asset』.