테러방지법과 사이버테러방지법의 문제점 진단 토론회

국정원의 국민사찰 고삐 풀리다

일시 | 2016년 3월 22일(화) 오후 2시

장소 | 국회 의원회관 제2소회의실

주최 | 민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동공간 '활', 인권운동사랑방, 진보네트워크센터, 참여연대, 김광진 의원

프로그램

14:00 사회　　오동석 민주주의법학연구회 회장, 아주대 교수

14:10발표1　　국민보호와 공공안전을 위한 테러방지법의 문제점
– 위헌성을 중심으로
이광철 변호사, 민주사회를 위한 변호사 모임

14:30 지정토론　　오영중 변호사, 서울지방변호사회 인권위원장
이태호 참여연대 정책위원장

15:00 발표2　　사이버테러방지법, 무엇을 노리는가?
– 국가권력에 의한 사이버보안관제의 위험성
이은우 변호사, 정보인권연구소 이사

15:20 지정토론　　심우민 국회입법조사처 입법조사관
이동산 페이게이트 이사

15:40 휴식

15:50 종합토론

16:40 폐회

목차

발제 1

국민보호와 공공안전을 위한 테러방지법의 문제점 – 위헌성을 중심으로

이광철 / 변호사, 민주사회를 위한 변호사 모임

Ⅰ. 서

가. 경위

2016. 3. 3. 국민보호와 공공안전을 위한 테러방지법, 일명 테러방지법이 국회에서 통과되었음.

이 법은 테러방지에는 무용하고 오히려 테러방지를 빙자하여 국정원의 권한을 강화시켜, 국민과 야당, 정적을 사찰하고 국정원이 선거에 개입하는 것이 아닌가 하는 비판이 유력하였음에도 불구하고 청와대, 여당이 똘똘 뭉쳐 이 법을 통과시킨 것임

이제 법이 시행되고 있는 이상 그 위헌성에 관한 논거들을 집적하여 국회를 통한 정치적 폐기 추진과 아울러 헌법재판소 내지 법원에서 사법적인 해석투쟁을 병행하여야 할 것임

나. 위헌성 요약

테러방지법의 위헌성은 다음과 같은 점에서 찾아볼 수 있음

1) 첫째, 테러의 개념(제2조 제1호), 테러위험인물의 개념(제2조 제3호), 테러위험임물에 대한 “관련 정보 수집”, “추적” 등의 개념이 추상, 포괄적이어서 불명확·모호한 문제가 있음. 이는 결국 법집행자(국정원)의 자의에 따라 테러방지라고 하는 법 본래의 목적이 아닌 국내의 정치, 사회적 현안에 국정원이 광범위하게 개입할 수 있는 여지를 남기게 됨

2) 둘째, 헌법상의 영장주의 원리, 적법절차 원리 등 통제의 원리를 비켜나 있음. 특히 테러위험인물에 대한 조치를 담은 제9조, 그 가운데에서도 제9조 제4항의 “대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러조사 및 테러위험인물에 대한 추적“의 경우가 두드러짐

3) 셋째, 테러방지라는 목적과 그 수단으로서의 국민에 대한 규제조치 간의 형량관계에 있어서 헌법상의 과잉금지 원칙에 위반되고 있음

2. 추상, 포괄적·불명확·모호한 문제점 – 악용가능성

가. 명확성의 원칙의 의의와 적용범위

헌재 1999. 9. 16. 97헌바73 결정에 의하면 “법치국가원리의 한 표현인 명확성의 원칙은 기본적으로 모든 기본권제한입법에 대하여 요구된다. 규범의 의미내용으로부터 무엇이 금지되는 행위이고 무엇이 허용되는 행위인지를 수범자가 알 수 없다면 법적 안정성과 예측가능성은 확보될 수 없게 될 것이고, 또한 법집행 당국에 의한 자의적 집행을 가능하게 할 것이기 때문이다(헌재 1990. 4. 2. 89헌가113, 판례집 2, 49; 1996. 8. 29. 94헌바15, 판례집 8-2, 74; 1996. 11. 28. 96헌가15, 판례집 8-2, 526; 1998. 4. 30. 95헌가16 판례집 10-1, 341). 다만, 기본권제한입법이라 하더라도 규율대상이 지극히 다양하거나 수시로 변화하는 성

질의 것이어서 입법기술상 일의적으로 규정할 수 없는 경우에는 명확성의 요건이 완화되어야 할 것이다. 또 당해 규정이 명확한지 여부는 그 규정의 문언만으로 판단할 것이 아니라 관련 조항을 유기적·체계적으로 종합하여 판단하여야 할 것이다."라고 판시함

이법에 의한 테러의 개념, 테러위험인물의 개념, 대테러활동, 대테러 조사의 개념이 지나치게 포괄적이고 모호, 추상적이어서 법집행 당국에 의한 자의적 집행을 가능하게 할 우려가 현저함

나. 이 법의 경우

1) 테러개념의 문제

이 법 제1조는 "테러의 예방 및 대응 활동 등에 관하여 필요한 사항과 테러로 인한 피해보전 등을 규정함으로써 테러로부터 국민의 생명과 재산을 보호하고 국가 및 공공의 안전을 확보하는 것을 목적으로 한다."고 하고 있음

그러나, 테러의 정의 규정 자체에서 테러방지와 무관하게 국내의 정치적 사회적 현안을 "테러"라고 규정지을 수 있는 여지를 남기고 있음. 이를 제거하지 아니한 것은 불명확 · 모호의 문제로 헌법상의 명확성 원칙에 어긋난다고 할 것임

구체적으로 이 법 제2조 제1호 가목과 라목이 그것임

1. "테러"란 국가·지방자치단체 또는 외국 정부(외국 지방자치단체와 조약 또는 그 밖의 국제적인 협약에 따라 설립된 국제기구를 포함한다)의 권한행사를 방해하거나 의무 없는 일을 하게 할 목적 또는 공중을 협박할 목적으로 하는 다음 각 목의 행위를 말한다. 가. 사람을 살해하거나 사람의 신체를 상해하여 생명에 대한 위험을 발생하게 하는 행위 또는 사람을 체포·감금·약취·유인하거나 인질로 삼는 행위 라. 사망·중상해 또는 중대한 물적 손상을 유발하도록 제작되거나 그러한 위력을 가진 생화학·폭발성·소이성(소이성) 무기나 장치를 다음 각각의 어느 하나에 해당하는 차량 또는 시설에 배치하거나 폭발시키거나 그 밖의 방법으로 이를 사용하는 행위 1) 기차·전차·자동차 등 사람 또는 물건의 운송에 이용되는 차량으로서 공중이 이용하는 차량 2) 1)에 해당하는 차량의 운행을 위하여 이용되는 시설 또는 도로, 공원, 역, 그 밖에 공중이 이용하는 시설 3) 전기나 가스를 공급하기 위한 시설, 공중의 음용수를 공급하는 수도, 전기통신을 이용하기 위한 시설 및 그 밖의 시설로서 공용으로 제공되거나 공중이 이용하는 시설 4)

석유, 가연성 가스, 석탄, 그 밖의 연료 등의 원료가 되는 물질을 제조 또는 정제하거나 연료로 만들기 위하여 처리·수송 또는 저장하는 시설 5) 공중이 출입할 수 있는 건조물·항공기·선박으로서 1)부터 4)까지에 해당하는 것을 제외한 시설

지난해 11월의 민중총궐기의 경우 위 가목에 따라, 2009년의 용산참사의 경우 위 라목에 따라 이 법의 테러로 규정될 수 있음[1].

명확성의 원칙을 관철하는 방법에는 **개념을 구체적으로 한정하여 다의적 해석의 여지를 제거 내지 최소화하는 방안** 외에도 **다의적 해석의 여지로 인하여 법집행자의 자의에 따라 오남용을 할 수 있는 우려를 배제규정의 명문화로 제거하는 방안**을 고려해 볼 수 있을 것임

이에 따라 이 법이 국회에 직권상정되었을시 더불어민주당 이종걸 의원 외 106인의 의원들은 이 법안에 대한 수정발의를 통하여 제4조 단서에 “다만, 「집회 및 시위에 관한 법률」 제2조 제1호 및 제2호에 해당하는 행위에 대해서는 이 법을 적용하지 아니한다.”는 조항을 신설하였는바, 새누리당은 이 수정안을 받아들이지 않았음

결국 테러의 개념 안에 지난해 11월의 민중총궐기나 2009년의 용산참사 같은 사태를 이 법의 테러로 볼 수 있는 여지를 남겼고, 이는 결국 이 법의 테러 개념이 가진 추상, 포괄적 · 불명확 · 모호한 문제점의 문제에서 비롯되는 것임

2) ‘테러위험인물’ 개념의 문제

이런 테러 개념을 거의 무한대로 확장하는 것이 ‘테러위험인물’ 개념임(제2조 3호).

3. "테러위험인물"이란 테러단체의 조직원이거나 테러단체 선전, 테러자금 모금·기부, 그

1) 실제 새누리당 정갑윤 의원은 지난해 민중총궐기대회를 두고 “폭동을 넘어 대한민국 국민을 향한 명백한 테러범죄”라고 규정한 바 있고, 용산참사 직후인 2009. 1. 21. 국회 행정안전위원회에서 신지호 한나라당 의원은 이 참사를 도심테러라고 규정한 바 있음. 이번 총선에 출마하는 김석기 당시 서울경찰청장도 준도심테러 운운하며 자신의 과잉진압을 합리화했음

밖에 테러 예비·음모·선전·선동을 하였거나 하였다고 의심할 상당한 이유가 있는 사람을 말한다.

이 규정을 보면, 테러위험인물은 세가지 유형이 있다고 할 것인데, 첫째, 테러단체의 조직원, 둘째, 테러단체 선전, 테러자금 모금·기부자, 셋째 그 밖에 테러 예비·음모·선전·선동을 하였거나 하였다고 의심할 상당한 이유가 있는 사람

이 개념에서 문제가 되는 것은 “그 밖에 테러예비·음모·선전·선동을 하였거나 하였다고 의심할 상당한 이유가 있는 자”라는 대목임

예비란 범행 도구 구입 등과 같은 범죄의 실현을 위한 일체의 준비행위를 말하고, 음모란 범죄행위를 모의하는 것을 말하며, 선전이란 불특정 다수에게 어떤 주의·주장을 알려 이해를 구하거나 공명을 구하는 일체의 행위를 말하고, 선동이란 타인으로 하여금 일정한 행위를 실행할 결의를 생기게 하거나, 이미 생긴 결의에 자극을 주는 것을 의미함

테러 개념과 테러위험인물의 개념 정의를 합쳐서 보면, 용산참사나 민중총궐기 같은 사태에 관련된 사람들의 범위는 예비·음모·선전·선동 개념을 통해 더욱 확장되는데 여기에 ‘하였다고 의심할 상당한 이유’까지 해당하여 사실상 테러위험인물의 범위는 무제한이 됨[2)]

3) 대테러활동, 대테러조사의 개념

테러위험인물의 개념의 무제한성이 대테러활동 및 대테러조사의 개념을 통하여 더욱 증폭되고 확장됨

6. "대테러활동"이란 제1호의 테러 관련 정보의 수집, 테러위험인물의 관리, 테러에 이용될 수 있는 위험물질 등 테러수단의 안전관리, 인원·시설·장비의 보호, 국제행사의 안전확보, 테러위협에의 대응 및 무력진압 등 테러 예방과 대응에 관한 제반 활동을 말한다.
8. "대테러조사"란 대테러활동에 필요한 정보나 자료를 수집하기 위하여 현장조사·문서열람·시료채취 등을 하거나 조사대상자에게 자료제출 및 진술을 요구하는 활동을 말한다.

2) 더구나 테러위험인물의 지정절차가 법에 아무 것도 정해진 것이 없고, 오직 국정원장이 지정하면 테러위험인물이 됨. 후술함

대테러활동의 개념을 “테러 관련 정보의 수집, 테러위험인물의 관리, 테러에 이용될 수 있는 위험물질 등 테러수단의 안전관리, 인원·시설·장비의 보호, 국제행사의 안전확보, 테러위협에의 대응 및 무력진압 등 테러 예방과 대응에 관한 제반 활동”이라고 정의하는 결과 심지어 국제행사가 개최되는 경우에도 이 법 제9조 제4항에 따라 대테러조사나 테러위험인물에 대한 추적조사가 가능하게 됨

또한 "대테러조사"를 ‘대테러활동’에 필요한 정보나 자료를 수집하기 위한 현장조사·문서열람·시료채취 등을 하거나 조사대상자에게 자료제출 및 진술을 요구하는 활동이라고 개념정의하였는바, 이상의 테러, 테러위험인물, 대테러활동, 대테러조사 등의 개념을 통하여 국정원은 대한민국 국민 전체에 대하여 어떤 정보수집이나 자료수집, 조사도 무한대로 가능하게 된 것임

3. 영장주의 등 통제의 원리의 적용을 받지 않고 있는 문제

가. 테러위험인물에 대한 테러방지법의 취급

1) 대테러활동의 대상

테러위험인물로 지정되는 경우 대테러활동에 있어서 관리의 대상이 되어 대테러조사의 대상자가 됨(제2조 제6, 8호)

> 6. "대테러활동"이란 제1호의 테러 관련 정보의 수집, **테러위험인물의 관리**, 테러에 이용될 수 있는 위험물질 등 테러수단의 안전관리, 인원·시설·장비의 보호, 국제행사의 안전확보, 테러위협에의 대응 및 무력진압 등 테러 예방과 대응에 관한 제반 활동을 말한다.
> 8. "대테러조사"란 **대테러활동에 필요한 정보나 자료를 수집**하기 위하여 현장조사·문서열람·시료채취 등을 하거나 조사대상자에게 자료제출 및 진술을 요구하는 활동을 말한다.

2) 제9조의 취급

테러위험인물로 지정되면 제9조에 따라 ①출입국·금융거래 및 통신이용 등 관련 정보 수집과 금융거래 지급정지 등의 조치, ②위치정보, 개인정보 수집 ③추적 등을 당하게 됨

여기의 개인정보는 개인정보보호법의 민감정보를 포함하는 것[3]으로써, 심지어 성생활 등의 정보까지 수집이 될 수 있음

제9조(테러위험인물에 대한 정보 수집 등)
① 국가정보원장은 테러위험인물에 대하여 **출입국·금융거래 및 통신이용 등 관련 정보**를 수집할 수 있다. 이 경우 출입국·금융거래 및 통신이용 등 관련 정보의 수집에 있어서는 「출입국관리법」, 「관세법」, 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」, 「통신비밀보호법」의 절차에 따른다.
② 국가정보원장은 제1항에 따른 정보 수집 및 분석의 결과 테러에 이용되었거나 이용될 가능성이 있는 **금융거래에 대하여 지급정지 등의 조치**를 취하도록 금융위원회 위원장에게 요청할 수 있다.
③ 국가정보원장은 테러위험인물에 대한 **개인정보(「개인정보 보호법」 상 민감정보를 포함한다)와 위치정보**를 「개인정보 보호법」 제2조의 개인정보처리자와 「위치정보의 보호 및 이용 등에 관한 법률」 제5조의 위치정보사업자에게 요구할 수 있다.
④ 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 **대테러조사 및 테러위험인물에 대한 추적**을 할 수 있다. 이 경우 사전 또는 사후에 대책위원회 위원장에게 보고하여야 한다.

3) 부칙의 취급

대테러활동에 필요한 경우 통비법상 통신제한조치가 가능하게 되었고, 이에 따라 테러위험인물에 대한 관리를 위하여 통비법 제7조에 따라 통신제한조치가 가능하게 되었음[4]

---

3) 개인정보 보호법 제23조(민감정보의 처리 제한)

개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

4) 통신비밀보호법 제7조(국가안보를 위한 통신제한조치)

① 대통령령이 정하는 정보수사기관의 장(이하 "정보수사기관의 장"이라 한다)은 국가안전보장에 상당한 위험이 예상되는 경우 또는 「국민보호와 공공안전을 위한 테러방지법」 제2조제6호의 대테러활동에 필요한 경우에 한하여 그 위해를 방지하기 위하여 이에 관한 정보수집이 특히 필요한 때에는 다음 각호의 구분에 따라 통신제한조치를 할 수 있다. <개정 2001.12.29, 2016.3.3>

1. 통신의 일방 또는 쌍방당사자가 내국인인 때에는 고등법원 수석부장판사의 허가를 받아야 한다. 다만, 군용전기통신법 제2조의 규정에 의한 군용전기통신(작전수행을 위한 전기통신에 한한다)에 대하여는 그러하지 아니하다.

2. 대한민국에 적대하는 국가, 반국가활동의 혐의가 있는 외국의 기관·단체와 외국인, 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단이나 외국에 소재하는 그 산하단체의 구성원의 통신인 때 및 제1항제1호 단서의 경우에는 서면으로 대통령의 승인을 얻어야 한다.

또한 테러위험인물에 대한 조사에 필요한 경우 금융정보분석원장이 국정원장에게 특정금융거래정보를 제공할 수 있음[5)]

제2조(다른 법률의 개정) ① **통신비밀보호법 일부를 다음과 같이 개정**한다.
제7조제1항 각 호 외의 부분 중 "국가안전보장에 대한 상당한 위험이 예상되는 경우"를 "국가안전보장에 상당한 위험이 예상되는 경우 또는 「국민보호와 공공안전을 위한 테러방지법」 제2조제6호의 대테러활동에 필요한 경우"로 한다.
② **특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부를 다음과 같이 개정**한다.
제7조제1항 각 호 외의 부분 중 "조사 또는 금융감독 업무"를 "조사, 금융감독업무 또는 **테러위험인물에 대한 조사업무**"로, "중앙선거관리위원회 또는 금융위원회"를 "중앙선거관리위원회, 금융위원회 또는 **국가정보원장**"으로 한다.
제7조제4항 중 "금융위원회(이하 "검찰총장등"이라 한다)는"을 "금융위원회, 국가정보원장(이하 "검찰총장등"이라 한다)은"으로 한다.
③ **특정범죄신고자 등 보호법 일부를 다음과 같이 개정**한다.
제2조제1호에 바목을 다음과 같이 신설한다.
바. 「국민보호와 공공안전을 위한 테러방지법」 제17조의 죄

4) 제12조의 취급

제12조에 따라 테러선동·선전물은 긴급 삭제 등 요청의 대상이 됨

테러위험인물을 직접 대상으로 하는 규정은 아니나, 앞서 본대로 테러위험인물 유형 가운데 “테러 예비·음모·선전·선동을 하였거나 하였다고 의심할 상당한 이유가 있는 사람”이 있고, 여기에 ‘테러 선전·선동’이 들어 있기 때문에 이 법 제12조의 테러를 선동·선전하는 글 또는 그림 등을 인터넷 등에 게시한 사람은 결국

5) 특정 금융거래정보의 보고 및 이용 등에 관한 법률 제7조(수사기관 등에 대한 정보 제공)

① 금융정보분석원장은 불법재산·자금세탁행위 또는 공중협박자금조달행위와 관련된 형사사건의 수사, 조세탈루혐의 확인을 위한 조사업무, 조세체납자에 대한 징수업무, 관세 범칙사건 조사, 관세탈루혐의 확인을 위한 조사업무, 관세체납자에 대한 징수업무 및 「정치자금법」 위반사건의 조사, 금융감독업무 또는 **테러위험인물에 대한 조사업무**(이하 "특정형사사건의 수사등"이라 한다)에 필요하다고 인정되는 경우에는 다음 각 호의 정보(이하 "특정금융거래정보"라 한다)를 검찰총장, 국세청장, 관세청장, 중앙선거관리위원회, 금융위원회 또는 **국가정보원장**에 제공한다. <개정 2011.5.19, 2012.3.21, 2012.12.11, 2013.8.13, 2016.3.3>

1. 제4조제1항 또는 제4조의2에 따라 금융회사등이 보고한 정보 중 특정형사사건의 수사등과의 관련성을 고려하여 대통령령으로 정하는 정보
2. 제8조제1항에 따라 외국금융정보분석기구로부터 제공받은 정보 중 특정형사사건의 수사등과의 관련성을 고려하여 대통령령으로 정하는 정보
3. 제1호 및 제2호의 정보 또는 제4조의2 및 제6조에 따라 보고·통보받은 정보를 정리하거나 분석한 정보

테러위험인물로 지정될 가능성이 매우 높다고 할 것임

> 제12조(테러선동·선전물 긴급 삭제 등 요청)
> ① 관계기관의 장은 테러를 선동·선전하는 글 또는 그림, 상징적 표현물, 테러에 이용될 수 있는 폭발물 등 위험물 제조법 등이 인터넷이나 방송·신문, 게시판 등을 통해 유포될 경우 해당 기관의 장에게 긴급 삭제 또는 중단, 감독 등의 협조를 요청할 수 있다.
> ② 제1항의 협조를 요청받은 해당 기관의 장은 필요한 조치를 취하고 그 결과를 관계기관의 장에게 통보하여야 한다.

나. 통제 장치의 결여

1) 테러 개념 해당여부, 테러위험인물 해당 여부에 대한 어떤 통제장치도 없음

국정원장의 일방적 판단과 지정권이 무한대로 보장되어 있음

국회나 법원의 통제권능이 보장되어 있지 아니함

국가테러대책위가 이에 관여할 수조차 없음(제5조)

대테러센터 또한 이에 관여할 수 없고, 더욱이 대테러센터는 국정원에 의하여 장악당할 가능성이 대단히 높다고 봄. 국정원은 현재 테러정보통합센터를 운영중인바, 이 센터가 대테러센터로 전환될 가능성이 높다고 할 것임

2) 제9조, 제12조의 경우

여기서 가장 문제가 되는 것은 추적조사권임

추적은 감시, 미행, 사찰을 포괄하는 말인바, 테러위험인물에 대하여 이러한 추적조사를 함에 있어서 이 법에 정해진 유일한 통제장치는 사전 또는 사후에 대책위원회 위원장에게 보고하는 것이 유일함(제9조 제4항 후문).

제9조 제1항의 경우 테러위험인물에 대하여 출입국, 금융, 통신 등의 정보나 자료 수집권을 보장하면서 관련법의 절차를 따른다고 하였으나, 이 또한 제대로 된 통제장치라고 보기 어려움. 특히 통비법의 경우 제8조의 긴급통신제한조치를 허가 없이 통신제한조치를 취할 수 있음

제9조 제3항의 위치정보와 개인정보의 경우 그 정보를 위치정보사업자와 개인정보처리자에게 요구할 수 있도록 하고 있고, 제12조의 테러 선전, 선동표현물 등의 경우 긴급삭제 등 조치를 해당기관의 장에게 요구할 수 있다고 하여 마치 임의적이고 재량이 허용되는 것처럼 규정하고 있으나, 테러라는 전 사회적인 호들갑 아래 국정원장 내지 관계기관의 장의 요구를 임의적이고 재량 아래 거부할 수 있을지 극히 의문임

3) 영장주의를 통한 법원의 통제와 국회의 정치적 통제가 실효적으로 뒷받침되어야 할 것임

○ 영장주의

영장주의의 존재이유가 국민의 자유와 권리의 부당한 침해를 막자는데 있음. 즉 영장주의는 통제의 원리인 것임

이러한 취지를 관철시키자면 두 가지 요구가 충족되어야 함. 먼저 통제의 주체. 침해의 주체가 통제의 주체가 된다는 것은 논리모순임. 따라서 영장주의에 있어서 신분이 보장된 법관으로 하여금 그러한 강제처분의 필요성을 심사하게 하는 것은 영장주의의 당연한 요청이 됨[6].

다음으로 통제의 내용. 영장에 의하여 허가(내지 명령)되는 대상과 시기가 구체적으로 특정되어야 하고, 나아가 비례적으로 합치되는지 엄격히 심사되어야 함.

---

6) 헌재 1997. 3. 27. 96헌바28

형사절차에 있어서의 영장주의란 체포·구속·압수 등의 강제처분을 함에 있어서는 사법권 독립에 의하여 그 신분이 보장되는 법관이 발부한 영장에 의하지 않으면 아니 된다는 원칙이고, 따라서 영장주의의 본질은 신체의 자유를 침해하는 강제처분을 함에 있어서는 중립적인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여야만 한다는 데에 있다.

즉 영장에 의하여 허가(내지 명령)되는 대상과 시기가 수사의 필요성과 비례적 관점에서 용인되어야만 테러방지를 위한 이 조치들이 비로소 헌법적으로 정당화 되게 됨.

여기서 영장주의란, 국민에 대한 수사 등 사법절차에 적용되는 헌법원리인데, 과연 테러방지를 위한 위 조치들이 영장주의의 적용을 받는 사법절차인가 하는 의문이 있을 수 있음.

소위 테러방지법이 국가테러대책위원회 등 조직을 위한 행정조직법의 성격을 갖고 있음에 의문이 없음. 제5조 국가테러대책위원회, 제6조 대테러센터, 제7조 대테러 인권보호관, 제8조 전담조직의 설치 등이 이에 해당함

문제는 이 법에 의하여 테러위험인물로 지정되어 대테러활동 또는 대테러조사의 대상이 되어 제9조 내지 제12조의 조치를 당하게 되는 것을 어떻게 볼 것인가? (경찰)행정작용의 영역으로 볼 것인가, 아니면 수사작용 내지 수사에 준하는 작용으로 볼 것인가? 하는 점임

이 법 제1조(테러의 예방 및 대응 활동 등에 관하여 필요한 사항과 테러로 인한 피해보전 등을 규정함으로써 테러로부터 국민의 생명과 재산을 보호하고 국가 및 공공의 안전을 확보하는 것을 목적으로 한다.)의 규정에 비추어 테러위험인물 지정, 대테러활동, 대테러조사 등의 일련의 작용이 경찰행정의 작용영역에 해당할 여지는 분명히 있음. 특히 이 법 제2조 제8호("대테러조사"란 대테러활동에 필요한 정보나 자료를 수집하기 위하여 현장조사·문서열람·시료채취 등을 하거나 조사대상자에게 자료제출 및 진술을 요구하는 활동을 말한다.) 규정은 행정조사기본법 제2조 제1호("행정조사"란 행정기관이 정책을 결정하거나 직무를 수행하는 데 필요한 정보나 자료를 수집하기 위하여 현장조사 · 문서열람 · 시료채취 등을 하거나 조사대상자에게 보고요구 · 자료제출요구 및 출석 · 진술요구를 행하는 활동을 말한다.)는 규정을 차용한 것으로 보이는바, 이로써 대테러조사의 성격을 행정조사로 볼 수 있는 규범적 근거라고 볼 여지가 있음.

그러나 이 법상 테러의 개념은 그 개별구성인자들이 모두 범죄의 성격을 갖고,

테러를 예방한다는 것의 의미는 테러예비, 음모, 선전, 선동 등의 범죄예비단계에서 용의자를 적발하여 이를 사전에 무력화시키는 것으로 결국 범죄수사의 의미를 동시에 갖는다고 할 것임. 그렇다면 테러위험인물 지정행위는 결국 피의자에 대한 입건의 성격을 동시에 갖는다고 할 것임

이러한 테러위험인물에 대한 이 법 제9조, 제12조, 부칙조항에 의한 통신제한조치, 특정금융거래 정보의 지득 등의 절차를 수사절차로 이해함에 무리가 없다고 할 것이고, 따라서 수사절차의 통제 원리로서 영장주의가 적용된다는 점에 의문이 없음

○ 국회의 정치적 통제

이법에 의한 테러의 규정, 테러위험인물 지정, 대테러활동 등에 대하여 국회의 견제 감시가 필요하나, 이 법에 의한 국회에 의한 통제장치는 전무함

현재 국회의 상임위 중 국정원을 견제, 감시하는 것은 정보위인바, 전임위도 아니고, 위원 수도 불과 12인으로 실질적인 국정원 견제, 감시에 대단히 부족함

4) 대테러 인권보호관의 문제

이 법에 의한 유일무이한 통제장치로 대테러 인권보호관을 두고 있으나(법 제7조), 단 한명의 인권보호관이 방대한 규모와 밀행주의를 강조하는 국정원의 대테러활동을 통제한다는 것은 어불성설임

또한 자격, 임기 등을 대통령령으로 정하도록 하고 있어 이러한 인권보호관의 취지를 무색하게 하는 시행령이 예상되어 제2의 세월호 특별법 시행령 사태가 벌어질 것으로 봄. 이 점에서 포괄위임금지의 헌법 규정을 위배하였다고 볼 소지가 있음

다. 적법절차 원칙의 위배

1) 헌재의 결정

헌재 1992. 12. 24. 92헌가8 결정은 “우리 현행 헌법에서는 제12조 제1항의 처벌, 보안처분, 강제노역 등 및 제12조 제3항의 영장주의와 관련하여 각각 적법절차의 원칙을 규정하고 있지만 이는 그 대상을 한정적으로 열거하고 있는 것이 아니라 그 적용대상을 예시한 것에 불과하다고 해석하는 것이 우리의 통설적 견해이다. 다만 현행 헌법상 규정된 적법절차의 원칙을 어떻게 해석할 것인가에 대하여 표현의 차이는 있지만 대체적으로 적법절차의 원칙이 독자적인 헌법원리의 하나로 수용되고 있으며 이는 형식적인 절차 뿐만 아니라 실체적 법률내용이 합리성과 정당성을 갖춘 것이어야 한다는 실질적 의미로 확대 해석하고 있으며, 우리 헌법재판소의 판례에서도 이 적법절차의 원칙은 법률의 위헌여부에 관한 심사기준으로서 그 적용대상을 형사소송절차에 국한하지 않고 모든 국가작용 특히 입법작용 전반에 대하여 문제된 법률의 실체적 내용이 합리성과 정당성을 갖추고 있는지 여부를 판단하는 기준으로 적용되고 있음을 보여주고 있다(헌법재판소 1989.9.8. 선고, 88헌가6 결정; 1990.11.19. 선고, 90헌가48 결정 등 참조)고 판시한바 있음

2) 이 사안의 경우

○ 이러한 헌재의 설시에 의하면 헌법상 적법절차의 원리는 모든 국가작용에 적용되며, 그 내용은 국가작용이 형식적인 절차 뿐만 아니라 실체적 (법률)내용이 합리성과 정당성을 갖춘 것이어야 한다는 것으로 해석됨

○ 이 사안에서 테러방지를 위한 이 법의 입법은 형식적인 절차에 있어서 합리성과 정당성을 갖추지 못하였음

국회의장의 직권상정은 국회법이 정한 직권상정요건에 반하는 것이었음

정의화 국회의장은 지난 2. 23. 오후 이 법안을 본회의에 직권상정(심사기일 지정)해 처리한다는 방침을 정했고, 그 이유로 최근 북한 등으로부터의 구체적인 테러 위협 정보가 있음에도 테러방지법의 국회 처리가 지연되는 것에 대해 ‘비상사태’라고 판단한바 있음

국회법 제85조 제1항은 직권상정의 요건으로 1. 천재지변, 2. 전시·사변 또는 이에 준하는 국가비상사태, 3. 의장이 각 교섭단체대표의원과 합의하는 경우를 들

고 있는바, 정의화 의장은 테러방지법의 직권상정이 가능한 경우를 2. 전시·사변 또는 이에 준하는 국가비상사태로 보았음. 그러나 이러한 법률해석은 명문의 규정에 반할 뿐만 아니라 국회선진화법이라고 불리는 위 규정의 입법취지 나아가 그간 정의화 의장이 했던 직권상정 관련 언급과도 정면으로 배치되는 것임

우선, 직권상정이 가능한 “전시·사변 또는 이에 준하는 국가비상사태”란 그런 사태가 목전에 발생하였거나 발생이 곧 임박하여 국회 원내교섭단체의 의사협의가 불가능 또는 이를 기다릴 여유가 없을 정도의 급박한 상황을 의미하는 것이지, 법안의 내용에서 상정하고 있는 어떤 사태가 예정된다는 것을 의미하는 것이 아님은 너무나도 당연함 즉 정의화 의장이 이병호 국정원장으로부터 청취한 것으로 보이는 “북한 등으로부터의 구체적인 테러 위협 정보”가 있다는 사정은 테러방지법 제정의 필요성의 논거는 될 수 있을지언정 직권상정이 가능한 “전시·사변 또는 이에 준하는 국가비상사태”에 해당할 수는 없는 것. 더구나 정의화 의장이 들었다는 것은 국정원의 일방적인 첩보에 불과한 것으로 확인되지도 않은 사실을 “전시·사변 또는 이에 준하는 국가비상사태“라고 하는 것은 억지에 불과함

또한 직권상정이 가능하다고 해석하는 것은, 국회가 독단과 독선에 의한 몸싸움 등 극단적 대결과 반목이 아닌, 대화와 타협에 의하여 운영되도록 하기 위하여 도입한 국회선진화법의 취지에도 역행하는 것임. 정의화 의장은 그간 청와대와 새누리당의 이른바 쟁점법안에 관한 직권상정 요구에 대하여 ”입법부 수장이 불법임을 잘 알면서도 위법한 행동을 할 수는 없습니다.“라면서 단호하게 거부해 왔는바, 당시 이 법안의 직권상정 방침은 본인의 이러한 입장과도 정면으로 배치되었던 것임

○ 또한 이 법은 실체적 (법률)내용이 합리성과 정당성을 갖춘 것으로 보기 어려움

이 법이 없더라도 그간 대한민국 정부는 테러방지에 만전을 기해 왔고, 테러방지를 위하여는 이 법이 별 실효성이 없다는 점은 누차 지적된바 있음

앞서 본바와 같이 국내의 과격 양상을 띠는 시위나 용산참사 같은 사태를 테러로 규정하고 온 국민을 테러위험인물로 지목하여 심지어 성생활 정보를 포함하는 광

범위한 정보수집과 사찰, 감청 등의 조치를 취한 것이 과연 실체적 (법률)내용이 합리성과 정당성을 갖추었다고 할 수 있을지 의문임

4. 헌법상의 과잉금지 원칙에 위반

가. 서

기본권제한입법의 한계조항으로 평가받는 헌법 제37조 제2항은 기본권제한입법의 위헌성 심사와 관련하여 우선 목적상의 한계(국가안전보장·질서유지 또는 공공복리), 형식상 한계(법률), 방법상 한계(필요에 따라, 과잉금지원칙), 내용상 한계(제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다)를 규정하고 있음

이 가운데 과잉금지 원칙은 목적의 정당성, 수단의 적절성, 침해의 최소성, 법익의 균형성 등의 판단기준으로 세분화됨

이 법에 의하여 테러위험인물로 지정되어 제9조 또는 제12조의 조치를 당하는 것이 어떤 점에서 헌법상의 과잉금지 원칙을 위배하는지 검토함

나. 침해받는 기본권

통신의 비밀의 불가침(헌법 제18조), 사생활의 비밀과 자유(헌법 제17조), 일반적 행동의 자유(헌법 제10조에서 파생), 거주이전의 자유(헌법 제14조)

다. 이 법의 과잉금지원칙 위배 여부

1) 목적의 정당성

이 법에 의하여 테러를 예방할 수 있을 것인지 의문스러워 목적의 정당성에 의문이 있음

9.11 테러, 파리테러 등 테러의 일반적 양상이 매우 은밀하고 조직적으로 그리고 해외를 기점으로 하여 이뤄지고 있는데, 과연 그러한 해외의 기점 테러를 사전에 발각한다는 것이 얼마나 가능할지 의문임

국내의 테러발생의 진원지로 지목되고 있는 북한에 의한 테러의 경우 이 법에 의하면 북한은 테러단체가 아니어서 이 법이 실효적인 대비책이 된다고 보기 어려움

2) 수단의 적절성 및 침해의 최소성

이 법이 아니라도 테러위험인물의 지정 및 테러정보의 수집은 충분히 가능함

즉 국정원법 제3조의 직무범위에 대테러정보의 수집이 국내외적으로 가능하게 규정되어 있고, 테러를 구성하는 개별적인 범죄들에 대하여도 국정원이 보유한 수사권으로 충분히 정보수집이 가능함

그러한 법제에 의할 경우 국내정치적 현안을 테러로 규정짓는 일이 발생되기 어려울 것이라는 점에서 이 법의 수단의 적절성 및 침해의 최소성을 인정하기 어렵다고 할 것임

3) 법익의 균형성

법익의 균형성 차원에서 이 법의 문제 심각

테러방지라는 목적달성의 가능성은 추상적인데 반하여 이 법의 시행으로 인한 폐해는 국정원의 광범위한 민간인 사찰과 정치개입의 현실화로 인하여 구체적이고 현실적임

특히 ‘국제행사의 안전확보’가 이 법 제2조 제6호의 "대테러활동"의 하나로 예시되어 있는바, 앞으로 국제행사가 열리기만 하면 ‘국제행사의 안전확보’를 빙자하

여 마치 테러가 발생한 것처럼 민간인사찰과 광범위한 정보 수집의 행태가 발현될 것으로 보임

과거 국정원의 정치개입 및 선거개입, 간첩조작의 사례에서 이 법으로 인한 폐해는 더욱 증폭되고 심화될 것으로 보임

4) 본질내용 침해금지의 원칙 위배 여부

○ 법리

기본권의 본질적인 내용은 당해 기본권의 핵이 되는 실체를 말하고, 본질적인 내용의 침해라 함은 그 침해로 말미암아 당해 자유나 권리가 유명무실한 것이 되어 버리는 정도의 침해를 말함

같은 견지에서 헌재 1990. 9. 3. 89헌가95 결정은 "재산권의 본질적인 내용이라는 것은 재산권의 핵이 되는 실질적 요소 내지 근본적 요소를 뜻하며, 재산권의 본질적인 내용을 침해하는 경우라고 하는 것은 그 침해로 인하여 사유재산권이 유명무실해지거나 형해화(形骸化) 되어 헌법이 재산권을 보장하는 궁극적인 목적을 달성할 수 없게 되는 지경에 이르는 경우라고 할 것이다."라고 판시한바 있음

○ 이 사안의 경우

이 법에 의한 특히 제9조에 의하여 테러위험인물로 찍히는 경우 테러위험인물의 통신의 비밀의 불가침(헌법 제18조), 사생활의 비밀과 자유(헌법 제17조), 일반적 행동의 자유(헌법 제10조에서 파생), 거주이전의 자유(헌법 제14조)가 형해화될 것으로 보임

과거 패킷감청의 피해자인 고(故) 김형근 선생은 패킷감청의 사실을 알고나서는 극심한 스트레스를 받아 암에 걸릴 것 같다고 토로하였고, 실제 김형근 선생은 간암으로 사망한바 있음

5. 결어

발제 2

사이버테러방지법, 무엇을 노리는가?
– 국가권력에 의한 사이버보안관제의 위험성

이은우 변호사, 정보인권연구소 이사

1. 사이버공격과 그에 대한 대응

가. 사이버공격

- 사이버공격의[1] 위험 이상존한다.

- 시스코의 분석에 의하면 2014년에 시스코가 탐지한 것만으로도 매일 450억건의 이메일이 차단되고, 8천만건의 웹접속 차단, 6,450건의 파일 탐지, 3,186건의 네트워크 탐지, 5만건의 네트워크 침입이 탐지되었다고 한다.

나. 사이버공격의 예방활동

- 사이버공격을 예방하는 과정에서 개인정보가 수집되는 경우라면 개인정보보호법 또는 정보통신망이용촉진 및 정보보호에 관한 법률에 의해 요건을 갖추어야 한다.

1) 미래창조과학부 사이버안전센터 운영규정은 "사이버공격"이란 해킹·컴퓨터바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신망을 침 입·교란·마비·파괴하거나, 정보통신망을 통해 보관 유통되는 전자문서·전자기록물을 위조·변조·유출 ·훼손하는 일체의 공격행위를 말한다고 정의한다.

해당 법률에서는 동의를 받도록 하고 있다.

다. 사이버공격 예방활동의 기술 발전과 수집되는 정보의 양과 질

- 정보통신망의 위협을 차단하는 활동을 사이버안전대책[2] 또는 보안관제[3]라고 부르는데, 대체로 사이버공격의 탐지, 분석, 대응을 그 내용으로 한다. 보안관제 서비스는 정보를 수집하고, 모니터링 및 분석과 대응조치 및 보고의 과정을 거친다.

<출처 : 이글루시큐리티 보안관제 프로세스>

- 보안관제서비스는 24시간, 365일 정보를 수집하고, 보안이벤트 모니터링을 하

2) 미래창조과학부 사이버안전센터 운영규정 "사이버안전"이란 사이버공격으로부터 정보통신망을 보호하여 정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.

3) 미래창조과학부 사이버안전센터 운영규정 "보안관제"라 함은 전자문서·전자기록물 또는 정보통신망을 대상으로 하는 사이버공격 정보를 실시간 수집 ·분석·전파하는 일련의 활동을 말한다.

고, 취약점을 관리해야 한다. 최근에는 보안관제 기술이 비약적으로 발전하여, 트래픽을 모두 저장하고, 거의 실시간으로 이용자의 다운로드 파일을 추출하거나, 패킷 데이터를 분석하기도 한다.

- 아래는 국내 주요 공공기관의 사이버보안관제센터에 보안관제시스템을 공급하고, 위탁운영을 맡고 있는 주식회사 윈스의 보안솔루션에 대한 소개인데, 해당 솔루션은 실시간 사용자 다운로드 파일 추출(URL, Mail, FTP 등), 개인정보 유출 및 감염자 역접속 탐지, 사용자 세션 전수 수집 및 분석 기능을 가지고 있다고 한다.

- 이 회사의 솔루션은 이 뿐만 아니라 종합상황판 제공, 침입탐지 이벤트 분석, Raw Packet Data 분석, 수집된 이벤트 및 트래픽 로그의 정보가공, 실시간 이벤트 및 트래픽 데이터 모니터링, 이벤트 및 트래픽의 데이터에 대한 분석 및 조회 등의 기능을 가지고 있다고 한다.[4)]

4) http://www.wins21.com/product/product_030101.html?num=20

제품개요/소개 | 주요기능 | 특장점 | 구성도 | 라인업

주요기능

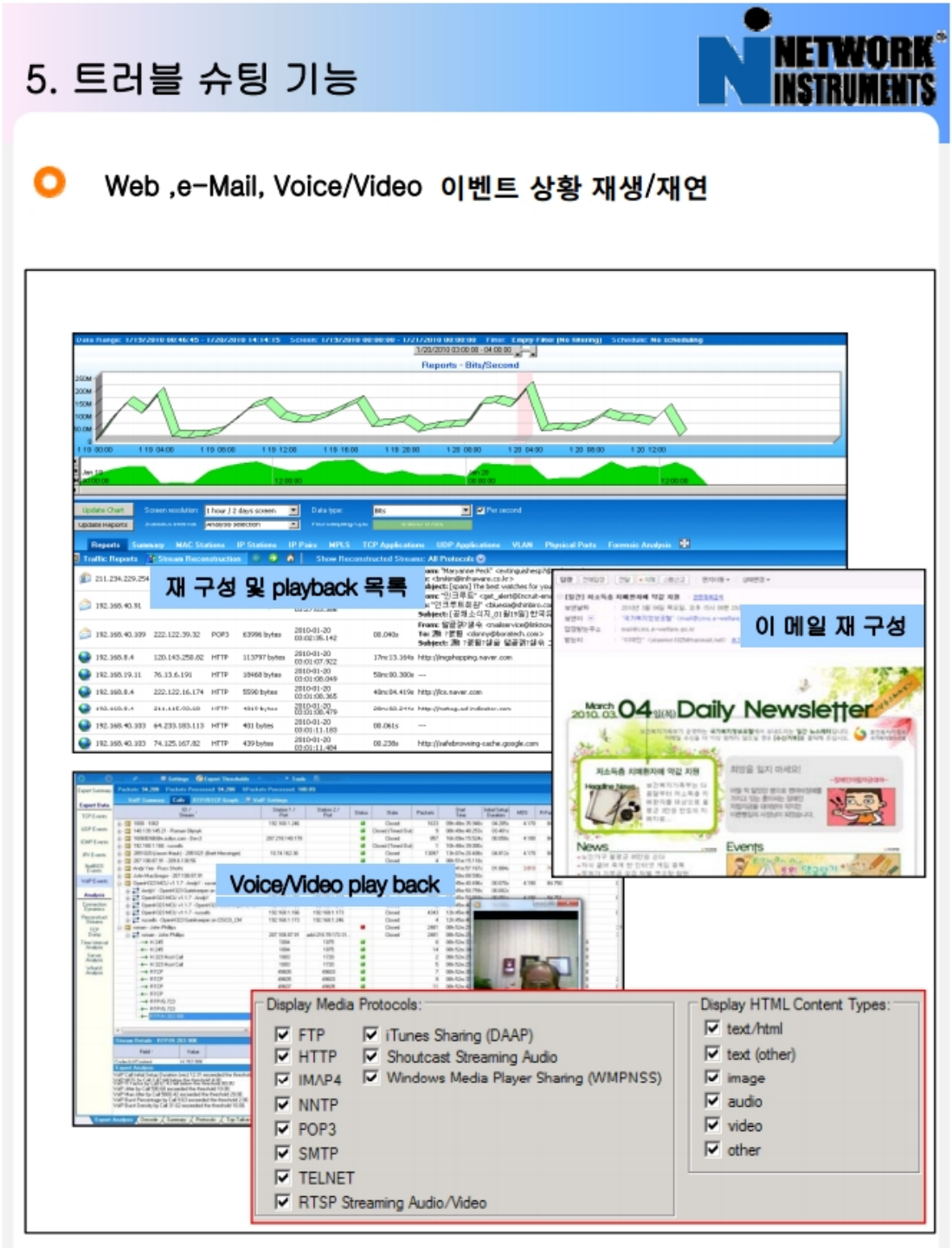
APTX (탐지)	실시간 사용자 다운로드 파일 추출(URL, Mail, FTP 등) 개인정보 유출 및 감염자 역접속 탐지 사용자 세션 전수 수집 및 분석 SNIPER IPS와 연동 차단 사이트 신뢰도 분석 학습을 통한 사이트 위험도 분석 IPS와 연계한 악성코드 유포지 및 C&C 서버 차단
Manager(관리/치료, Optional)	다양한 통계 및 검색 통합모니터링 및 정책 설정 치료 모듈 배포 및 모니터링 사용자 PC 악성코드 치료 및 복원 악성코드 상세 통계 분석 보고서
CVM(분석)	방악성코드 행위기반(Sandbox) 분석p> MS Office, 한글, 압축파일 등 분석 악성코드 배포지 및 C&C 서버 추출 국내/외 악성코드 패턴 통합 분석
암호화 통신	원격지 접속 통합관리자에 의한 안전한 중앙통제기능 수행을 위한 SSL 암호화 인터페이스 제공 SNIPER IPS Client에서의 안전한 제어기능 수행을 위한 SSL 암호화 통신채널 제공
Agent(감염 PC 탐지/치료, Optional)	감염 PC 탐지/치료 주기적 탐지 정책 업데이트 자동/수동으로 악성코드 치료 모든 Windows 계열(32/64bit) 지원

<스나이퍼 APTX 제품 소개>

- 모든 트래픽을 수집, 저장하여 이를 사후적으로 분석, 재생할 수 있게 해주는 솔루션중 유명한 것은 Viavi Solutions Inc.의 GigaStor라는 것이 있는데, 실시간으로 모든 트래픽을 수집, 저장하여 문제가 발생했던 그 시점으로 정확히 되돌아가 문제가 발생하기 전, 발생하는 동안, 그리고 발생 후의 상세한 내용을 패킷 레벨에서 직접 확인해 볼 수 있다고 한다.

- 특히 실시간으로 모든 트래픽의 대용량 데이터를 수집, 저장과 동시에 분석을 할 수 있다고 한다.

- 아래 그림은 이 솔루션으로 이메일을 재구성하고, 영상통화 비디오를 재생한 예시이다.



[GigaStor 제품 소개 : 네트웍 비정상 행위탐지 및 네트웍 사전관리를 위한 트래픽 포렌직 시스템]

- 이를 통하면 보안관제 서비스로 타임머신과 같이 원하는 시점으로 돌아가서 모든 행위를 감시할 수 있게 된다.

라. 우리나라의 일반적인 공공기관 보안관제서비스 요구사항

- 예를 들어 법무부에서 2010년에 발주한 보안관제센터 구축 관련 서비스의 경우 다음을 요구사항으로 제시하고 있다. 이를 보면 우리나라의 공공기관의 정보통신망에서 어떤 방식으로 보안관제를 수행하고 있는지를 엿볼 수 있다.

보안관제 현황 (2010년 법무분야 보안관제센터 구축 제안서 중)

구분	현황	향후
보안 관제	-유관기관(국가사이버안전센터(NCSC), 정부통합전산센터)에서 탐지·통보된 건을 처리하고 있음 - 본부에서 운영하는 바이러스월, IPS, 내부정보유출방지시스템 등을 통하여 비정상적인 트래픽 탐지·차단 - 유관기관 통보건 및 자체 탐지건을 확인·처리하고 있음 - 서울출입국관리사무소와 서울소년원에 DDoS 대응시스템이 구축되어 있음 ※ 확인 및 처리 작업은 백신 유지보수 인력 1명을 통하여 수행	- 자체 관제시스템 통하여 24시간 365일 보안 이벤트를 탐지하고, 처리 결과를 시스템으로 관리 - 소속기관 정보보안 담당자들과 처리 내용을 공유 - 유관기관과 유해트래픽 탐지 룰 및 사고처리 결과를 실시간으로 공유 ※ 보안관제 및 침해사고 대응 전문인력을 활용
관제 시스템	- 위협관리시스템(TMS) : 없음 - 통합보안관리시스템(ESM) : 없음	- TMS : 센서 12식 - ESM : Agent 50식을 활용

유해트래픽 탐지의 경우 - 유해트래픽 분석 및 위협관리시스템(기상청 2010년 제안서)

유해트래픽 분석 및 위협관리시스템(기상청 2010년 제안서)
o '06년 구축된 유해 트래픽 수집센서(7대) 및 분석 S/W, 등을 활용할 수 있어야 하며, 기존 장비와 호환이 가능하여야 함(만일, 활용이 불가능할 경우는 이에 대한 대책 제시) o '10년 추가되는 센서는 인터넷 등 중요 구간에 설치하고, 기 구축된 센서는 유관기관이 제공하는 탐지 룰 자동 적용 불가능에 따른 재활용 및 위치 이전 - 기 구축된 센서 7대에 대한 설치 위치 변경에 따른 지원 필요 또는 대안 제시 o 대상기관별 트래픽 수집·분류, 유해 패킷 탐지, 실시간 침입 탐지현황 조회 o 전송되는 데이터는 암호화하여 전송하여야 함 o 탐지장비는 관리서버로부터 수신한 탐지룰 실시간 적용 o 네트워크 인입구간의 모든 트래픽에 대한 시그니쳐 기반 탐지룰에 의해 유해 패킷 탐지 기능(탐지누수현상 없어야 함) - 탐지누수현상을 감시할 수 있는 누수율 현황관리 기능 포함 - 센서당 유입트래픽 900Mbps 기준, 사용자 정의 탐지룰 1,000개 적용상태에서 탐지누수 및 탐지성능 저하 없어야 함(오탐, 미탐 포함) o 연계시스템을 통해 배포되는 유관기관 PCRE기반 탐지 룰을 사용자의 변경 및 2차 작업없이 자동으로 실시간 적용 가능 - PCRE 문법 기반의 사용자 정의 탐지룰 입력·수정·삭제 기능(Snort 기반 문법) ·payload option : content, nocase, rawbyte, depth, offset, distance, within, uricontent, isdataat, pcre, byte test, byte jump 필수 ·Non-payload option : dsize, flags, flow, flowbits, itype, icode, icmp_id, icmp_seq 필수 - 탐지 룰을 적용(1,000개 이상)하고 네트워크 성능·운영에 영향이 없어야 함 - 장비의 트래픽 허용 용량 안에서 패킷 누수현상이 발생하지 않아야 하며 실시간 처리현황·모니터링이 가능해야 함 - 사용자의 개입 없이 자동화 처리가 가능해야 함 - 유관기관 탐지룰 배포 시스템과 연계 가능 - 유해트래픽 탐지시스템에서 전송받은 탐지룰명, 현황, 통계정보 및 패킷 Payload를 포함한 모든 탐지결과는 DB(RDBMS)에 실시간 저장 - 탐지결과(Payload 포함)에 대해서 유관기관이 정의한 데이터 형식(xml 포맷)에 따라 연계시스템에 전송 및 제공할 수 있어야 함

법무부에서 2010년에 발주한 보안관제센터 구축 관련 주요 요구사항

유해트래픽분석 및 위협관리시스템(TMS) 구축

- 해킹·웜·바이러스 등 외부의 사이버 위협에 대응하기 위하여 비정상 트래픽에 대한 실시간 탐지·분석 등을 통해 외부의 공격을 효과적으로 통제·대응하기 위한 시스템

통합보안관리시스템(ESM) 구축

- 다양한 종류의 정보보호시스템을 중앙통제·관리하고, 각종 보안이벤트를 수집하여 실시간 상관분석을 통해 위험도 및 침해사고를 조기에 탐지 및 대응하기 위한 시스템
- 분석된 정보는 통합분석시스템 등과 효율적 연동이 가능하여야 함
- ESM Agent 설치 대상 시스템 : 총 00개

통합분석시스템 구축

- ESM, TMS 등으로부터 다양한 보안정보를 전송받아 사이버 위협에 대한 위험도 측정 등 종합적인 관제기능과 침해경보를 발령하는 시스템
- 관제시스템에서 생성, 수집된 각종 정보를 공유할 수 있는 정보공유 포털 기능 제공
- 사이버 침해 사고 신고, 접수, 사고 처리, 결과 관리 등 사이버 침해 사고에 대응하기 위한 종합적인 업무처리 기능 제공

홈페이지 위·변조 탐지시스템 구축

- 관제 대상기관의 웹사이트(홈페이지) URL을 등록하여 홈페이지 위변조가 발생하는 경우 이를 즉시 탐지 경보하기 위한 시스템 구축
- 홈페이지 서비스 상태를 상시 모니터링, 홈페이지 운영 중단 등의 이상 상황 발생에 신속한 대응 지원

통합 저장시스템 구축

- 관제시스템에서 필요한 저장장치(스토리지)를 개별 시스템별로 별도 구축하지 않고 공동으로 사용할 수 있도록 구성

보안관제센터 네트워크 기반 구축

- 사이버 안전센터 내부 네트워크 및 보안체계 구성을 위한 네트워크 장비 및 보안장비 구성
- 예산절감과 운영 효율성을 위해 각 관제시스템에서 공동으로 사용할 수 있는 스토리지 구축

보안관제센터 기반시설 구축

- 관제실, 전산기계실, 사무실, 참관실 시설 설치 및 전기, 냉난방, 네트워크 등 시설 운영에 필요한 부대 시설 및 장비 도입

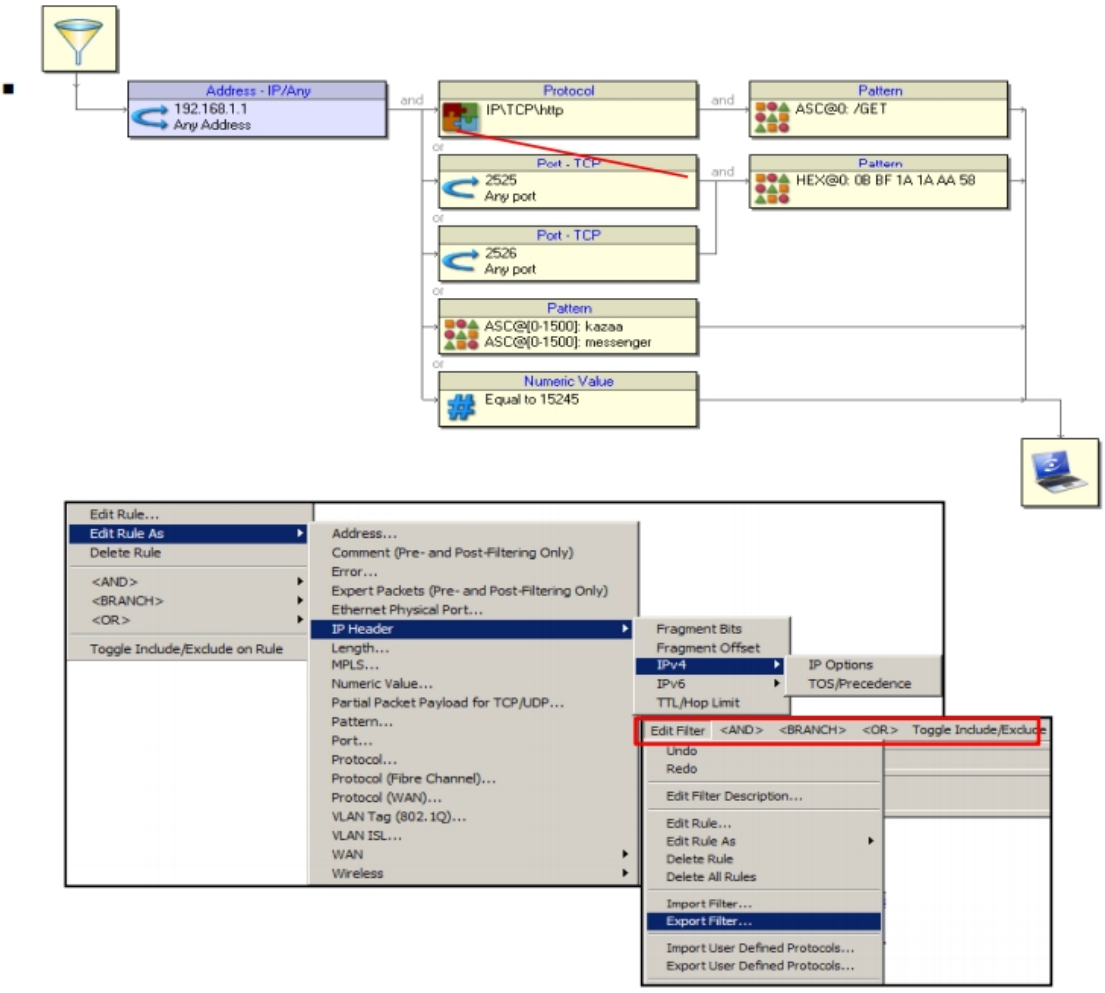
보안취약점 점검 및 분석

- 관제대상 기관의 네트워크 및 관련 시스템 취약점 점검 및 분석 수행
- 보안관제센터 운영을 위한 관제운영 및 침해사고 대응 등 관련 지침 수립 등

마. 보안관제의 악용 가능성

- 보안관제가 악용될 수도 있다. 예를 들어 인터넷서비스제공업체가 보안관제 솔루션을 이용하여 P2P 서비스 이용자의 트래픽을 차단하거나 속도를 제한하는 등 트래픽 관리를 하는 것이 대표적이다.

- 인터넷서비스제공업체가 보안관제 솔루션을 이용하여 자신이 원하는 대로 포트, 프로토콜, 패턴/IP 등을 만들어 탐지를 할 수 있기 때문에, 이를 이용하여 예를 들어 특정한 IP나 특정한 패턴(예를 들어 특정한 P2P 서비스 등), 특정한 값 등을 규칙으로 만들어 트래픽 관리를 할 수 있는 것이다.



[GigaStor 제품 소개 : 네트웍 비정상 행위탐지 및 네트웍 사전관리를 위한 트래픽 포렌직 시스템]

2. 보안관제 서비스의 위험

가. 보안관제 과정에서 과다한 개인정보 수집의 위험

- 기술의 발전 : 보안관제 기술의 발전으로 수집할 수 있는 이벤트나 개인정보의 범위가 비약적으로 늘어나게 되었다.

- 사실상 이용자가 발생시키는 모든 데이터를 수집하는 것이 가능할 뿐만 아니라, 수집한 정보를 실시간으로 분석할 수 있어서, 보안관제의 치밀함과 정확도는 상상을 뛰어 넘는 수준이 되었다.

- 치밀한 관리 : 그리고 보안관제 솔루션의 수집정책만 변경하면 얼마든지 다양한 분석을 할 수 있다. 이런 점에서 보안관제는 프라이버시 침해의 위험을 증대시키고 있다.

- 특히 현재의 공공기관의 보안관제 서비스의 요구조건이 프라이버시 보호와 조화를 이룰 수 있는 것인지도 의문이 아닐 수 없다.

- 원칙적으로 보안관제 서비스에 있어서도 수집하는 개인정보는 보안관제를 위해 필요한 최소한으로 하는 등 개인정보보호법과 정보통신망이용촉진 및 정보보호에 관한 법률의 규정을 엄격하게 준수해야 하는데, 이런 원칙이 준수되고 있다고 볼 수 있을지 의문이다.

- 보안관제를 목적으로 개인정보를 수집하게 되는 경우에도 수집하는 개인정보의 항목과 수집목적, 보유기간, 해당 개인정보가 제3자에게 제공되는 경우에는 제공되는 제3자 등을 명확하게 알리고 사전에 동의를 얻어야 하며, 이용목적을 달성한 경우는 지체 없이 삭제해야 하는데, 공공기관의 보안관제 서비스의 경우 현재 이런 원칙이 준수되고 있다고 보기 어렵다.

- 공공기관 외에도 민간분야의 보안관제 서비스에서도 이런 점은 문제이다.

나. 수집된 개인정보를 오남용할 위험

- 보안관제 서비스를 수행하는 과정에서 수집한 개인정보를 오남용할 위험은 더 크다.

- 공공기관이나 민간기업은 보안관제 서비스를 수행하는데 반드시 필요한 정보만을 수집해야 하고, 수집된 개인정보도 엄격하게 보안관제 서비스 목적으로만 이용해야 하는데, 이를 준수하기를 기대하기는 어려운 실정이다.

- 보통 공공기관이나 민간기업은 보안관제의 명목으로 이용자로부터 과다한 개인정보를 수집한 후 이를 보안관제 서비스 목적 외의 다른 목적으로 활용할 가능성이 아주 크다.

- 특히 보안관제 서비스를 통해서 간단하게 수집정책을 변경하기만 하면 아주 쉽게 개인정보 수집범위를 거의 무한대로 확장할 수 있고, 수집한 정보 분석도 고성능 솔루션으로 아주 쉽게 실시간으로 이루어지기 때문에 보안관제 서비스는 아주 손쉽게, 별다른 어려움 없이 보안관제 외의 목적으로 활용될 수 있다.

- 예를 들어 보안관제 서비스를 특정인에 대한 추적, 감시 서비스로 활용하려고만 하면, 얼마든지 특정인의 IP나 특정한 키워드를 대입하여 손쉽게 특정인의 활동에 대한 실시간 도청(서비스 접속, 일체의 활동, 이메일, 메신저, 통화 내역, 화상전화 도청 등)도 가능하고, 특정인과 연결되는 IP들이나, 그 IP와 또 다시 연결되는 IP 추적, 추적된 IP들의 활동내용에 대한 도청이 가능하다. 이렇게 확보된 정보를 바탕으로 다른 보안관제 서비스와 결합하면, 추가 추적, 분석을 통해서 정밀하게 실시간 감시가 이루어질 수 있기 때문이다. 이런 과정을 통해서 감시는 무한히 확장되고, 심화될 수 있다.

- 특히 보안관제 서비스를 통해 개인정보를 수집하거나, 대규모의 동시 도청을 해도 보안관제 서비스의 비밀성, 보안관제 서비스가 고도의 기술로 이루어진다는 점, 짧은 시간에 막대한 정보를 수집하여도 정보수집에 비용이 들지 않

고, 손쉽게 중앙집중적으로 정보수집이 가능하기 때문에 당사자는 이를 전혀 눈치챌 수 없는 경우가 대부분일 것이다.

다. 적법절차 보장이 이루어지기 어려움

- 보통 보안관제 서비스는 긴급하게 비밀리에 이루어지기 때문에 담당자가 그 요건을 확인하는 것이 곤란하다.

- 반면 이를 통해 얻어지는 정보는 대규모적이고, 수집하는 정보의 범위도 모호하고, 특히 적법절차를 준수하도록 주장할 주체가 보안관제 서비스 수행자가 아니기 때문에 보안관제 서비스 과정에서 개인정보의 오남용(부당한 개인정보의 수집, 수집한 개인정보의 목적 외의 이용 등)이 이루어져도 정보통신 서비스 제공자나 보안관제 서비스 제공자가 적법절차를 보장하도록 요구할 것을 기대하기는 사실상 어려운 일이다.

- 공공기관의 경우는 정보통신망 운영주체와 보안관제를 지시하는 주체가 보통 상하의 지시관계에 있기 때문에 적법절차 보장을 요구한다는 것은 기대하기 어렵고, 민간기업의 경우도 운영주체와 보안관제를 지시하는 주체는 감독, 피감독의 관계이기 때문에 민간기업의 정보보호담당자가 그런 지시를 적법절차를 내세워 거부하는 것은 기대하기 어렵다.

라. 보안관제, 침해사고 원인분석과 영장주의 잠탈의 위험성

- 보안관제는 수사인가?
  - ■ 영장주의 잠탈 가능성이 매우 높다

- 현재의 정보통신망법의 침해사고 원인분석 등(**제48조의4 침해사고의 원인 분석 등**)

- 미래창조과학부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사

고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다. 〈개정 2013.3.23.〉

- 미래창조과학부장관은 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다. 〈개정 2013.3.23〉

- 미래창조과학부장관이나 민·관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다. 〈개정 2013.3.23〉

- **시행령 제60조(조사단의 사업장 출입)** ① 조사단이 법 제48조의4제4항에 따라 관계인의 사업장에 출입하는 때에는 그 권한을 나타내는 증표를 관계인에게 내보여야 한다.

마. 보안관제 서비스에 대한 부당한 침해

- 보안관제 서비스는 고도의 기술성 때문에, 고도의 기술을 가진 조직에 의해 부당하게 이용될 가능성도 아주 크다.

- 보안관제 서비스를 고도의 기술을 가진 조직이 몰래 감시 시스템으로 활용해도, 해당 정보통신서비스 제공자는 그 사실을 모를 수도 있다.

- 실제로 국가정보원은 우리나라 보안관제 서비스에 대한 인증을 담당하기 때문에 그 내부구조를 상세하고 파악하고 있다.

- 따라서 국가정보원이 보안관제 서비스 시스템을 몰래 부당하게 침해하여 감시 프로그램으로 이용하더라도 이를 막거나, 확인하기가 쉽지는 않은 것이다.

3. 사이버위협에 대해 국가는 어떻게 관여하는가?

가. 국가의 사이버 위협에 대한 대응 전략의 원칙[5)]

(1) 사이버위협 대응 원칙

- 국가가 사이버위협에 대응하는 전략을 수립하는 데 있어서 여러 가지 원칙들이 제시되고 있다. 각국은 각국의 상황에 맞는 원칙을 제시하고 있는데, 대체로 유사한 내용을 담고 있다.

- 예를 들어 유럽연합의 경우는 2013년의 제안[6)]에서 다음과 같은 5가지 원칙을 들고 있다. 1) 유럽연합의 핵심 가치는 현실 세계와 같이 디지털 세계에서도 적용된다. 2) 기본권, 표현의 자유, 개인정보와 프라이버시의 보호, 3) 모든 이를 위한 접근권, 4) 민주적이고 효율적인 다양한 이해관계자에 의한 거버넌스 옹호, 5) 보안을 보장하기 위한 책임의 공유.

- 이런 원칙 중 중요한 것은 대체로 공공과 민간의 협력에 관한 원칙, 신뢰와 참여의 원칙, 프라이버시와 인권 존중 및 열린 인터넷에 관한 원칙, 기술발전의 촉진과 기술중립성의 원칙 등을 들 수 있다.

(2) 공공과 민간의 협력

- 대부분의 네트워크가 민간 부문에서 운영하고 있으며, 기술의 발전에 발맞추기 위해서는 민간의 자원을 활용하는 것, 민간의 노력과 주도성을 활용하는

5) The IT Industry's Cybersecurity Principles for Industry and Government (Information Technology Industry Council (ITI) 2011)

6) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

것이 반드시 필요하다. 이 과정에서 민간 부문의 참여와 협력, 민간 부문의 리더십을 활용하는 것이 반드시 필요하다.

- “기존에 기여가 이루어진 노력과 자원을 바탕으로 공공과 민간의 파트너쉽이라는 균형을 맞추면서 이를 증진시키는 방향으로 이루어져야 한다는 원칙이다. 과거 10여년 이상 민간 부문에서 공공부문과 발 맞추어 사이버 보안과 관련하여 공공부문에 기여한 리더십과 자원, 기술혁신과 책임의식이 있으므로, 이러한 노력과, 투자, 파트너십을 최대한 활용해야만 효과적인 사이버 보안을 달성할 수 있다.” 사이버보안을 위한 기술과 전문성은 기본적으로 민간부문에서 창출되기 때문에 공공과 민간의 협력을 이끌어 낼 수 있는 사이버보안이 되어야 한다.[7)]

- 공공과 민간 사이의 정보의 공유와 협력이 필요하다는 것이다.

(3) 프라이버시와 인권 존중

- 각국은 사이버위협에 대응하는 것과 관련하여 한결같이 ‘프라이버시와 인권 존중은 사이버보안의 정책과 법률을 발전시켜 나가는 과정에서 우선적으로 고려되어야 한다’고 한다.[8)]

- 특히 사이버공간은 열려 있으며, 정보와 사상이 유통되고 공유되는 공간이기 때문에 이를 존중하는 것이 무엇보다도 중요한 원칙인 것이다.

- 이와 관련하여 ‘국가가 법을 준수하면서 적절하게 대응해야 하고, 개인의 사이버공간 접근권을 강화하는 방향으로 이루어져야 하고, 다양성을 보장하고 관용적이도록 해야 하고, 사이버공간이 혁신과 사상, 정보, 표현의 자유로운 유통의 장으로 유지되어야 하고, 프라이버시와 개인의 자유를 보장하고, 공정한 경쟁이 보장되는 공간이어야 한다’는 것이다.[9)]

---

7) The UK Cyber Security Strategy Protecting and promoting the UK in a digital world (2011)

8) 예를 들면 미국변호사협회(ABA)는 2012년에 채택한 Cybersecurity 5 principles 중 이를 천명하고, 영국 정부는 3대 원칙에서 이를 천명하고 있으며, 그 외 사이버 보안에 관한 원칙에서는 빠짐 없이 프라이버시와 인권 존중을 들고 있다

(4) 기술중립성

- 사이버위협에 대응하기 위해서는 기술의 발전이 무엇보다도 중요하다. 이를 위해서는 국가의 관여와 관련해서 '기술중립성'이 필요하다.

- 이는 민간의 주도성 보장, 민간과의 협력이 필요한 이유이기도 하다.

- 국가가 주도하거나, 국가가 강요하는 것은 기술중립성을 해치고, 기술발전을 가로막는다.

(5) 각 주체의 참여와 거버넌스 보장, 신뢰와 참여

- 사이버위협에 대한 대응의 주체는 이용자, 서비스제공자, 비정부 단체, 공공부문 등이다.

- 사이버위협에 대응하는 데 있어서 이들 주체의 참여를 보장하고, 주체들이 거버넌스를 가질 수 있도록 하는 것이 무엇보다도 중요하다.

- 이를 통해서 이들 주체가 신뢰할 수 있어야 한다.

(6) 기타

- 그 밖에도 주체들의 인식제고와 교육의 필요성, 사이버위협의 근절보다는 사이버위협의 관리, 현실가능성과 적정성, 지속적인 발전(법, 제도, 기술 등), 국제적인 협력 등 여러 가지 원칙들이 제시되고 있다.

나. 국가가 사이버위협에 관여할 수 있는 수단

(1) 사이버 범죄, 불법행위의 억제

- 사이버침입 행위를 범죄로 규정하고, 이를 억제하기 위한 노력

9) London Conference on Cyberspace

■ 범죄로 규정하는 경우 범죄 수사를 위해서 수사 등 국가가 관여할 수 있다.

■ 사이버침해행위가 발생하였을 경우 수사기관에 의한 수사

- 민사적 책임 규정

■ 민사 책임을 규정하는 경우 손해배상 청구 가능

(2) 서비스 주체에게 서비스의 안정성, 사이버 보안을 유지할 책임을 부여할 것인가?

- 서비스 주체에게 서비스의 안정성과 사이버 보안을 유지할 책임을 부여함. 그 방식은 다양함.

■ 보안요구사항을 법제화하기도 하고, 법제화하지 않고 일반적인 고객보호의무로 해석하기도 함.

■ 보안요구사항을 법제화하는 것이 오히려 자발적, 혁신적 대응을 억제하는 효과가 있다는 견해도 있음.

- 이를 위반할 경우 민사책임, 형사책임, 행정벌이나 시정조치 등

(3) 정보의 공유, 즉시대응팀(CERT)과의 협력

- 국가 또는 공공부문에서 민간과 사이버 위협 정보를 공유하고, 즉시대응을 할 수 있도록 촉진.

- 위협정보의 공유를 법제화할 것인가?

■ 유럽연합은 2016년부터 NIS Directive로 필수적인 서비스 분야에서 위협이 발생한 경우 보고의무를 부과하려고 함.

■ 미국의 경우는 위협정보 공유에 대한 법률이 프라이버시 침해 등의 이유로 계속 거부되다가, 최근 법률이 제정됨.

다. 국가별 상황

(1) 미국

- 행정명령 (오바마 대통령, 2013) “주요 인프라 사이버 보안 개선”[10]

  - 효과적인 사이버 보안정책은 공공, 민간 파트너십을 활용해야 하고, 새로운 위협, 기술. 비즈니스 모델에 대해 적용 가능해야 하고, 위험관리에 기반해야 한다.
  - 미국 연방 부서, 기관에 대해서
  - 사이버 위협정보 공유(정부는 민간에게 더 많은 실행가능한 사이버 위협정보를 공유한다.,
  - 사이버 보안 프레임워크 제정 - 사이버 위험 관리를 돕는 최선의 방법에 대한 기술,
  - 자발적 프로그램,
  - 혜택 제공,
  - 가장 위험한 주요 인프라를 식별할 것을 지시.

- 미국표준기술연구소(NIST) 주요 기반시설 사이버보안 강화를 위한 프레임워크[11]

  - 정책과 사업을 조정하는 표준, 방법론, 절차, 프로세스 및 사이버 위험에 대응할 수 있는 기술적 접근 방식 포함
  - 자발적 합의 표준 및 업계의 모범 사례 통합
  - 우선순위별, 유연하고 반복 가능하며 성능기반의 비용 효과적인 접근 방법
  - 기술적 중립, 처방이 아닌 프레임워크, 지속적 참여와 개선, 자발적 사용.
  - 위험 관리 접근법 : 공격을 중지하는 것이 아니라, 위험 관리에 초점을 둠.

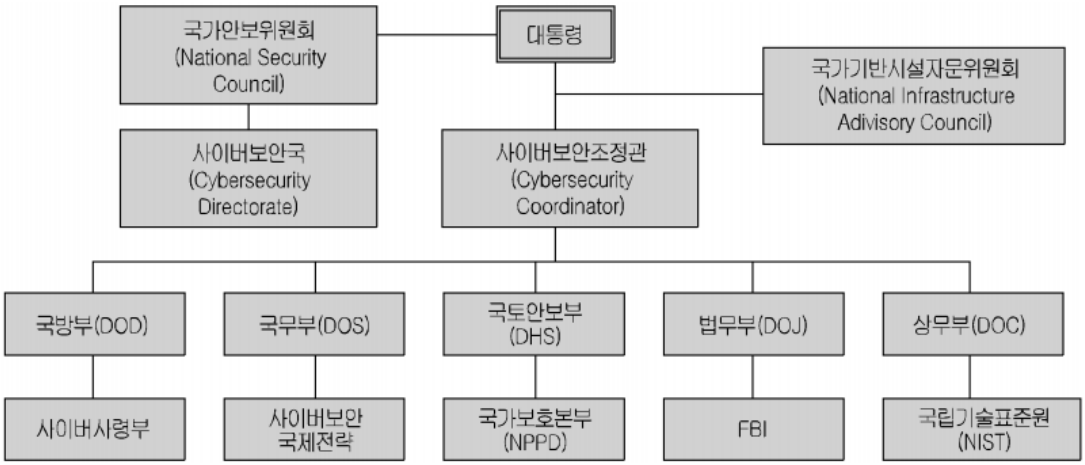
---

10) Improving Critical Infrastructure Cybersecurity Executive Order 13636

11) 사이버보안 프레임워크는 ▲‘프레임워크 코어(Framework Core)’ ▲‘프레임워크 구현(Framework Implemetation Tiers)’, ▲‘프레임워크 프로파일 (Framework Profile)’로 구성. ‘프레임워크 코어’는 주요 기반시설에 대한 사이버보안 대응 프로세스를 ▲인지 (Identify), ▲보호(Protect), ▲탐지(Detect), ▲대응(Respond), ▲복구(recover)로 구분하고 각 활동을 정의, ‘프레임워크 구현’은 조직이 처한 위기관리 상황, 위협 환경, 법률 및 규제 요건, 사업 목적 등에 따라 적용 가능한 단계별 사이버보안 위험 관리 방식을 제시, l ‘프레임워크 프로파일’은 조직이 수행하고 있는 사이버보안 활동의 현재 상태 (profile)와 목표 상태 간 격차를 파악하고, 이를 최소화할 수 있는 해결 과제 도출 방안을 제시(NIST, 사이버보안 프레임워크 최종본 (버전 1.0) 발표, KISA, internet ans security weekly, 2014. 2.)

- 미국 행정부 : 백악관, 국가안전보장회의(사이버조정관), 국토안보국, 국방부, 상무부(국립표준기술연구소), 법무부, 기타. 역할분담,

미국의 사이버위협에 대한 대응 조직



(2) 유럽연합

- 유럽연합의 사이버 보안 전략 : 개방, 안전, 보안이 되는 사이버공간(2013. 7. 2.)[12)]
  - ■ 사이버 복원력 달성Achieving cyber resilience
  - ■ 사이버 범죄의 획기적 감소
  - ■ 공통 안보 방위 정책(Common Security and Defence Policy, CSDP)과 관련한 사이버 방위 정책의 발전
  - ■ 사이버 보안과 관련한 산업과 기술적 자원 발전
  - ■ 유럽연합과 유럽연합의 핵심 가치를 위한 일관된 국제적 사이버공간 정책의 수립

- NIS directive (2016)

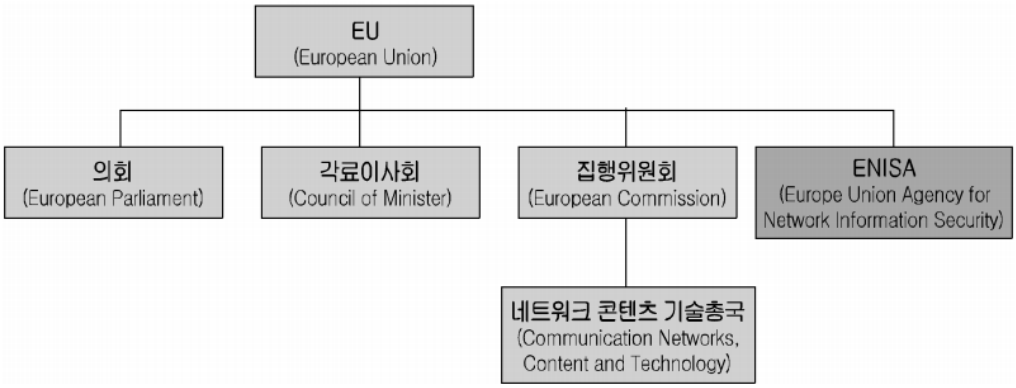
12) Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace

■ 2015년 12월 합의가 이루어짐. 2016년 최종 제정될 것임. 2년 시한 각국 이행법률 제정.

■ 필수 서비스와 디지털 서비스 제공자[13]는네트워크와정보보안요구사항을부과함. 해당 기관과 컴퓨터 보안 사고 대응팀에 보안 사고 보고 의무 부과.

■ 각국은 그에 대한 팀을 설립할 의무.

■ 디지털 서비스 제공자와 필수 서비스 운영자는 각각 다른 수준으로 규율을 받음.



4. 우리나라의 현재의 법제도 국가는 지나치게 관여하고 있다 보안관제 서비스의 주체와 그에 대한 감독권을 중심으로

가. 우리나라의 정보통신망의 안정성과 신뢰성 보호를 위한 법제와 침해사고 방지

- 우리나라 현행법상 사이버안전대책과 보안관제는 정통망법, 정보통신기반보호법 등이 적용된다.

---

13) 핵심 사회 경제적 활동의 유지에 필요한 서비스를 제공하는 법인.

○ 전기, 가스 공급자와 운송 시스템 운영자, 운송부문. 항공, 철도. 도로. 해상 운송, 금융 부문은 은행과 신용기관. 증권거래 기관, 건강과 식수, 디지털 인프라 부문. 도메인 이름 등록 기관과 도메인 이름 시스템 서비스 제공자. 인터넷 교환 지점 는 필수 서비스 운영자

○ 디지털 서비스 제공자는 다른 취급을 받음.

- 정통망법도 법적 안정성을 훼손할 수 있는 가능성이 있다

- 원칙은 자율 : 해당 정보통신서비스제공자 등에게 사이버안전대책을 수립, 수행할 책임과 권한을 주고 있다. 다만, 국가에게는 사이버안전대책의 기준을 고시로 제정하여 권고할 수 있는 권한을 주고 있으며, 정보통신서비스 제공자에게 매년 인증을 받을 의무를 부과하고 있다.

- 침해사고 발생시 원인분석의 경우 법적 안정성에 문제가 있을 수 있음 : 정보통신서비스 제공자에게 침해사고가 발생한 경우에는 신고의무를 부과하고, 침해정보 등의 공유를 유도하고 있다. 정통망법은 침해사고가 발생한 경우 일정한 절차를 통해서 침해사고를 조사할 수 있도록 하고 있는데, 이는 일종의 수사절차에 준하는 상황으로 볼 수 있다. 그런데 현재 정통망법은 침해조사의 요건과 방법, 절차, 적법절차의 보장, 영장주의의 적용 등에 대해서 명료하고 투명한 기준을 제시하지 않고 모호한 조항만을 두고 있어서 법적 안정성을 심각하게 훼손하고 있다.

- 반면 정보통신기반보호법에 의하여 공공기관이 운영하는 정보통신기반시설에 대해서는 국가가 통일적으로 정보통신보호지침을 수립하고 있으며, 심지어는 관제서비스도 통합형으로 운영하고 있다. 그런데 정보통신기반보호법은 정통망법보다도 더 모호한 규정으로 이루어져 있어서 공공기관에서 운영하는 정보통신망이나 주요정보통신기반시설의 경우 적법절차의 보장이 형해화되어 있다. 특히 법적 근거가 될 수 없는 대통령 훈령에 불과한 국가사이버안전보장에 관한 훈령에 의하여 국가정보원이 국가사이버안전에 관한 막대한 권한을 부여받고, 이를 행사하고 있어서 심각한 문제를 드러내고 있다.

나. 정통망법과 침해사고 대응

(1) 정보통신서비스 제공자에게 부과된 보호조치를 할 의무, 매년 안전진단을 받을 의무

- 정통망법은 정보통신서비스 제공자에게 정보통신망의 안정성 및 정보의 신뢰

성을 확보하기 위한 보호조치를 해야 할 의무를 부과하고(정통망법 제45조 제1항), 아울러 사전점검 의무도 부과하고 있다(제45조의 2). 그리고 정보보호 최고책임자를 지정할 의무(제45조의 3)와 매년 정보보호안전진단을 받을 의무를 부과하고 있다(제46조의 3). 안전진단 결과는 미래창조과학부장관에게 제출해야 하고, 미래창조과학부장관은 안전진단 결과에 따른 개선 권고를 할 수 있고, 해당 업체는 개선 결과를 제출할 의무가 있다.

- 한편, 정보통신망의 안정성 및 신뢰성을 확보하기 위하여 기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자는 정보보호 관리체계가 미래창조과학부장관이 고시한 기준에 적합한지에 관하여 정보보호 관리체계 인증기관으로부터 인증을 받을 수도 있다. 그리고 집적정보통신시설 사업자는 긴급한 경우에 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있게 하여 집적정보통신시설 사업자의 긴급대응 의무를 부과하고 있다(제46조의 2).

(2) 국가의 감독권은 고시와 권고

- 한편 정통망법은 국가의 감독권을 정보보호조치에 대한 고시를 제정하여 이를 지킬것을 권고하는 방식으로 제한하고 있다. 이에 대한 고시의 제정은 주무부서인 미래창조과학부장관이 한다(제2항). 미창부장관이 제정하는 고시에는 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치, 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치, 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치의 기준을 포함하고 있다.

(3) 침해사고 발생시에 국가가 갖는 확대된 권한 – 침해 신고의무와 사고의 조사

- 반면 침해사고가 발생하면 국가가 정보통신망 운영자에 대하여 감독하고 개입하는 권한이 커진다. 침해사고가 발생하는 경우 정보통신망은 정보통신서비스 제공자에게 신고의무를 부과한다. 이때 신고의 상대방은 미래창조과학부장관이나 한국인터넷진흥원이된다(제48조의 3). 이들 행정기관은 정보통신망의 안정성을 주무업무로 하고 있는 기관들이다. 기본적으로 정통망법은 침해사고의

원인을 분석하고 피해의 확산을 방지하여야 하는 책임을 정보통신서비스 제공자 등 정보통신망을 운영하는 자에게 부과하고 있는데, 미래창조과학부장관이나 한국인터넷진흥원도 침해사고의 신고를 받거나 침해사고를 알게 되면 침해사고에 관한 정보의 수집·전파, 침해사고의 예보·경보, 침해사고에 대한 긴급조치를 하여야 할 책임과 권한을 갖게 된다. 그런데 그 권한은 침해사고에 대한 정보의 수집, 전파, 침해사고의 예보, 경보, 침해사고에 대한 긴급조치를 넘어서지는 않는다.

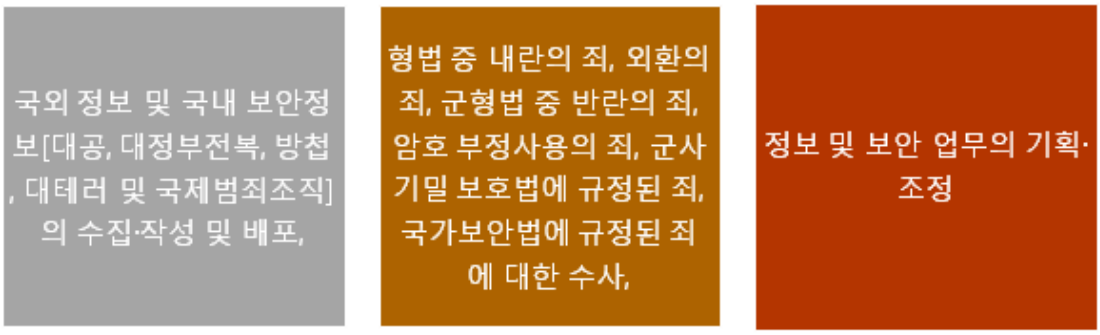
- 한편 정보통신망 침해사고가 중대한 침해사고인 경우는 미래창조과학부장관에게 침해사고 원인분석 등 조사권한이 있다. 이러한 조사는 침해사고의 원인분석 및 대책을 마련하기 위한 것이기 때문에 과징금 부과나 기타 필요한 행정처분을 내리기 위해 거치는 조사절차로 볼 수는 없다. 정통망법은 이 조사와 관련해서 몇 가지 강제력을 갖는 수단들을 규정하고 있다. 즉, 미래창조과학부장관은 해당 정보통신서비스 제공자 등에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있고, 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 관련자료의 제출을 요구할 수 있고, 민·관합동조사단이 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 이때 통신비밀보호법의 통신사실확인자료에 해당하는 자료의 제출은 통신비밀보호법에 의하도록 하고 있다. 미래창조과학부장관이나 민·관합동조사단은 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하도록 하고 있다.

- 한편 형사소추를 위한 수사도 이루어질 수 있는데, 이 때는 형사소송법이 적용될 것이고, 행정처분을 위한 조사인 경우에는 행정절차법 등이 적용될 것이다.

5. 그렇다면 현재 국정원은 어떻게 사이버에 관여하며, 이는 적법한가?

가. 국정원법에 규정된 국정원의 직무

<국정원법의 국정원의 직무>



- 국정원이 만약 사이버안전에 대한 업무를 수행한다면, 대공, 대정부전복, 방첩과 대테러의 보안정보에 국한. 그 업무의 기획, 조정에 국한

- 사이버 범죄의 수사는 내란죄나 국가보안법에 대한 것으로 제한.

- 공공부문의 보안관제 담당, 침해사고 조사 등은 국정원법 위반

- 민간부문의 정보통신망에 대한 보안관제, 침해사고 조사 등은 엄격하게 금지되어야 한다.

나. 현실에서 정보통신기반보호법을 통한 관여는 국정원법에 위반됨

(1) '정보통신기반보호법' 제정 당시 제시한 '제정 이유'

- 정보통신기반보호법은 주요정보통신기반시설의 보호와 침해사고의 대응을 위해서 2001년에 제정된 법이다.[14]2001년에 정보통신기반보호법이 제정될 때

14) 정보통신기반보호법이 제정될 때 제시된 제정이유를 보면 정보통신기반보호법 외에 사이버테러방지법을 별도로 제정할 필요가 무엇인지를 새삼 생각하게 만든다. 그 제정이유가 현재의 사이버테러방지법의 제정이유와 너무나도 흡사하기 때문이다. 제정이유는 "정보화의 진전에 따라 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹·컴퓨터바이러스 등을 이용한 전자적 침해 행위가 21세기 지식기반국가의 건설을 저해하고 국가안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설을 보호하기 위한 체계적이고 종합적인 대응체계를 구축하기 위해 정보통신기반보호법 제정됨."이라고 되어 있다. 이런 이유로 정보통신기반보호법을 제정했음에도 법령의 미비로 사이버 침해를 막기가 어렵다는 것은 이해하기 힘들다. 사이버테러방지법이 필요하다면, 정보통신기반보호법이 있음에도 불구하고 사이버 침해를 막기 어려운 점이 무엇인지를 구체적으로 제시해야 한다.

제시된 제정이유를 보면 2015년에 사이버테러방지법을 제정해야 한다고 주장하는 논거와 정확하게 일치한다.

- 정보통신기반보호법의 제정이유를 보면 “정보화의 진전에 따라 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹·컴퓨터바이러스 등을 이용한 전자적 침해 행위가 21세기 지식기반국가의 건설을 저해하고 국가안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설을 보호하기 위한 체계적이고 종합적인 대응체계를 구축하기 위해 정보통신기반보호법 제정됨.”이라고 되어 있다. 이런 이유로 정보통신기반보호법을 제정했고, 그 법이 현재 시행되고 있다면, 그 법이 있음에도 불구하고 법령의 미비로 사이버 침해를 막기가 어려운 것이 무엇인지를 구체적으로 제시할 수 있어야 한다. 만약 현재의 정보통신기반보호법으로도 충분하다면 별도로 사이버테러법을 제정할 이유는 없는 것이다.

(2) 주요정보통신기반시설 – 지정 권고

- 국정원장은 지정권고권을 갖는다

- 정보통신기반보호법의 적용대상이 되는 주요정보통신기반시설[15]에는공공기관에서운영하는정보통신망과주요민간의정보통신시설이포함되어있다.[16]

- 주요정보통신기반시설로는 2014년 12월 현재 정보통신 및 미디어, 금융기관, 교통수송, 에너지, 원자력, 식·용수, 식품의약품관리, 보건복지, 정부기관, 사회안전시설, 건설·환경, 지리정보, 기타 등의 분야에서 17개 관계중앙행정기관, 188개 관리기관, 292개 주요정보통신기반시설이 지정·관리되고 있다고 한다.

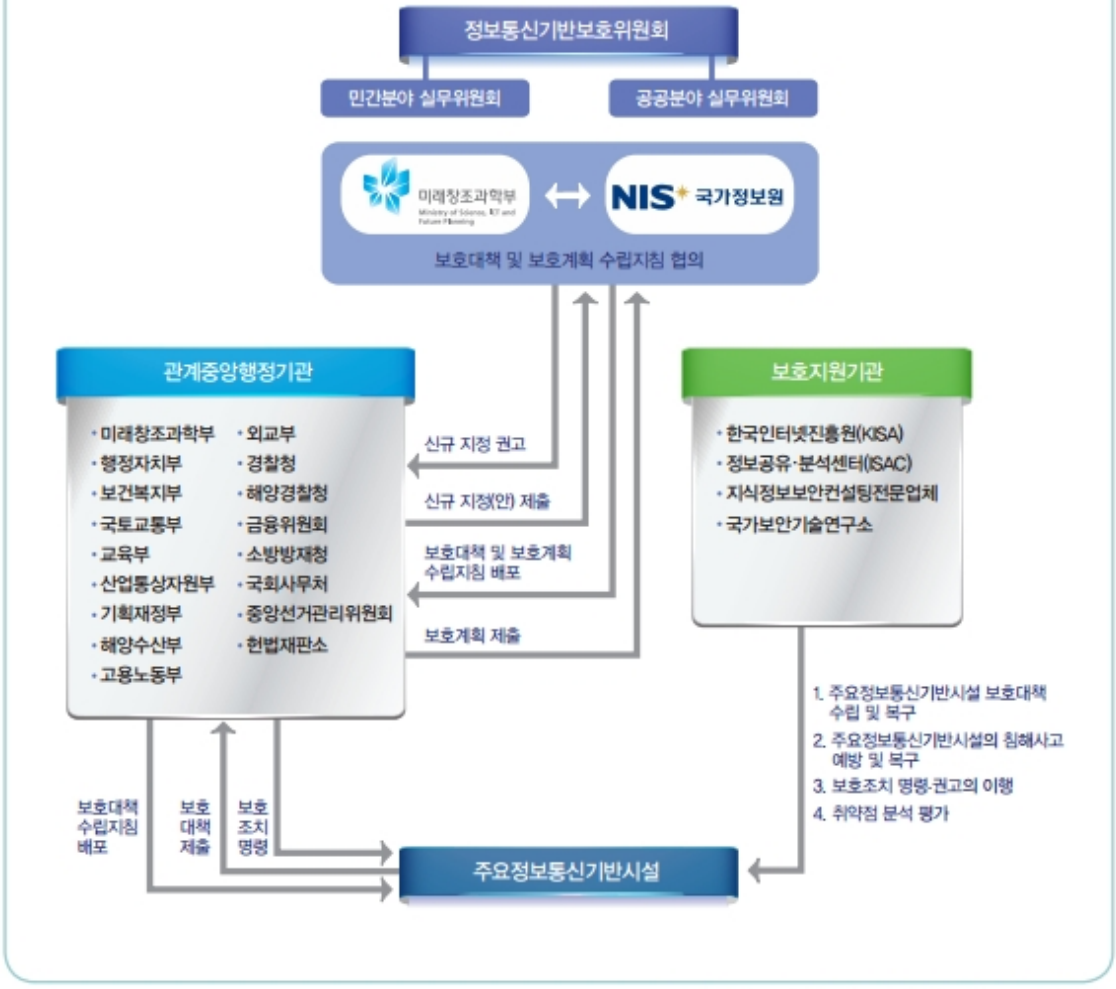
- 한편 시행령은 미래창조과학부장관과 국가정보원장에게 주요정보통신기반시설 지정 대상의 선정을 위하여 주요정보통신기반시설지정조사반을 두고, 각 조사

15) 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망

16) 중앙행정기관의 장은 정보통신기반보호위원회의 심의를 거쳐 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하도록 함

반으로 하여금 자료를 제출받는 등 주요정보통신기반시설 지정 필요성을 검토하게 할 수 있다고 규정하고 있다. 이런 과정을 거쳐서 미래창조과학부장관과 국정원장은 주요정보통신기반시설로 지정 권고를 할 수 있다.

[그림 3-2-1-1] 주요정보통신기반시설 보호 추진체계



[출처 : 한국인터넷진흥원, 정보통신기반보호 가이드(2014)]

<출처 : 국가정보보호백서 2015>

(3) 주요정보통신기반시설보호위원회(위원장 : 국무총리실장)

- 주요정보통신기반보호법은 주요정보통신기반시설 보호정책의 조정에 관한 사항, 보호계획의 종합·조정에 관한 사항과 보호계획의 추진 실적에 관한 사항, 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항 등을 심의하기 위하여 국무총리 소속하에 국무조정실장을 위원장으로 하는 정보통신기반보호위원회를 두도록 하고 있다.

(4) 보호대책 및 보호계획 수립지침 à 해당 관리기관장의 보호대책과 중앙행정기관의 보호계획 à 이행여부 확인(자료요구), 보호지침, 보호처분의 강력한 권한

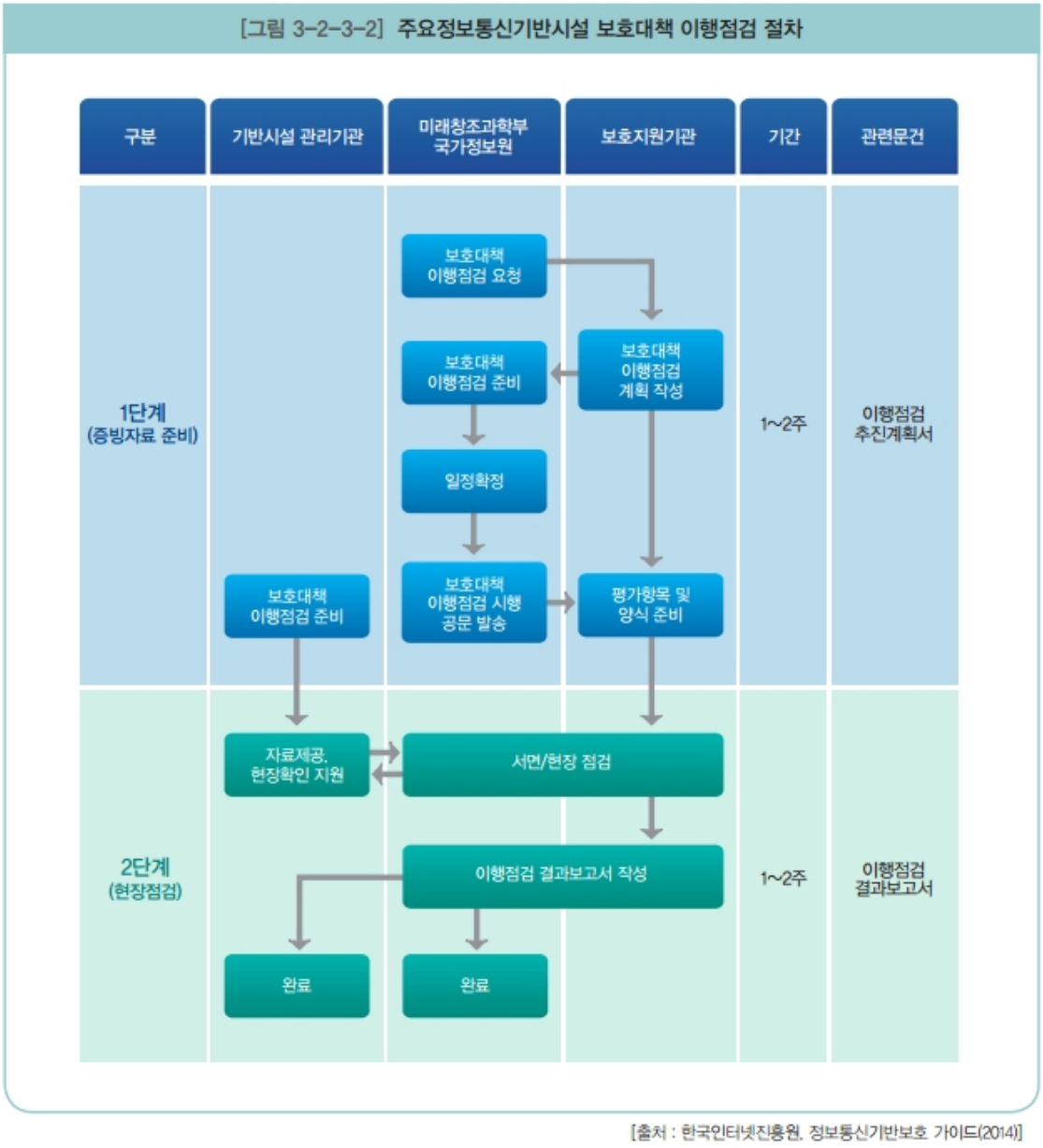
- 정보통신기반보호법은 미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다고 규정하고 있다.

- 주요정보통신기반시설을 관리하는 기관의 장으로 하여금 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책("주요정보통신기반시설보호대책")을 수립·시행할 의무를 부과하고 있다.

- 관리기관장은 보호대책을 주요정보통신기반시설을 관할하는 관계중앙행정기관의 장에게 제출해야 한다.

- 미래창조과학부장관, 국가정보원장, 국방부장관은 관리기관의 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있는 권한을 부여받고 있다. 이때 미래창조과학부장관, 국가정보원장, 국방부장관은 이행여부를 확인하기 위하여 필요한 경우 관계중앙행정기관의 장에게 제출받은 주요정보통신기반시설보호대책 등의 자료 제출을 요청할 수 있다고 규정하고 있다.

- 주요정보통신기반보호법은 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있도록 하고, 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치(주요정보통신기반시설의 보호에 필요한 조치)를 명령 또는 권고할 수 있도록 하고 있다.



<출처 : 국가정보보호백서 2015>

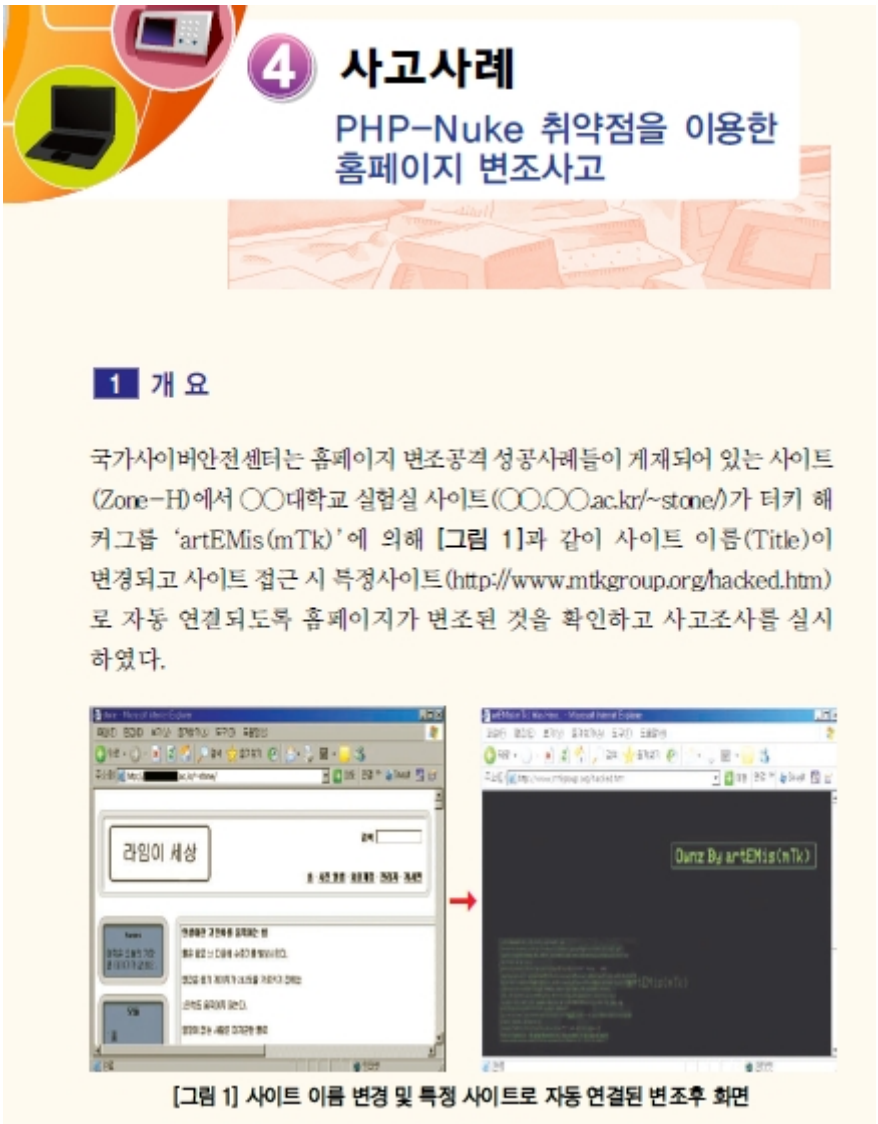
(5) 침해사고의 통지 - 침해사고 조사 : 영장주의의 잠탈

- 관리기관의 장이 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원에 그 사실을 통지하여야 한다. 그리고 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다. 이 경우 관계기관도 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다.

- 한편 침해사고를 통지할 관계 행정기관은 국가기관 또는 지방자치단체의 장이 관리기관의 장인 주요정보통신기반시설 및 도로·철도·지하철·공항·항만 등 주요 교통시설, 전력, 가스, 석유 등 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설에 해당하는 주요정보통신기반시설의 경우는 국가보안업무를 수행하는 기관 또는 관계중앙행정기관이 된다.[17]

(6) 보안관제 대행은 매우 심각한 문제 - 사실상 모든 보안관제를 국정원이

17) 사이버 시큐리티(국가사이버안전센터 발간 월간지) 2007년 3월호 기사의 사고사례를 보면 국정원이 KAIST의 홈페이지 해킹 사고를 조사한 것이 실려 있다.



[그림 1] 사이트 이름 변경 및 특정 사이트로 자동 연결된 변조후 화면

대신하는 의미의 '지원'

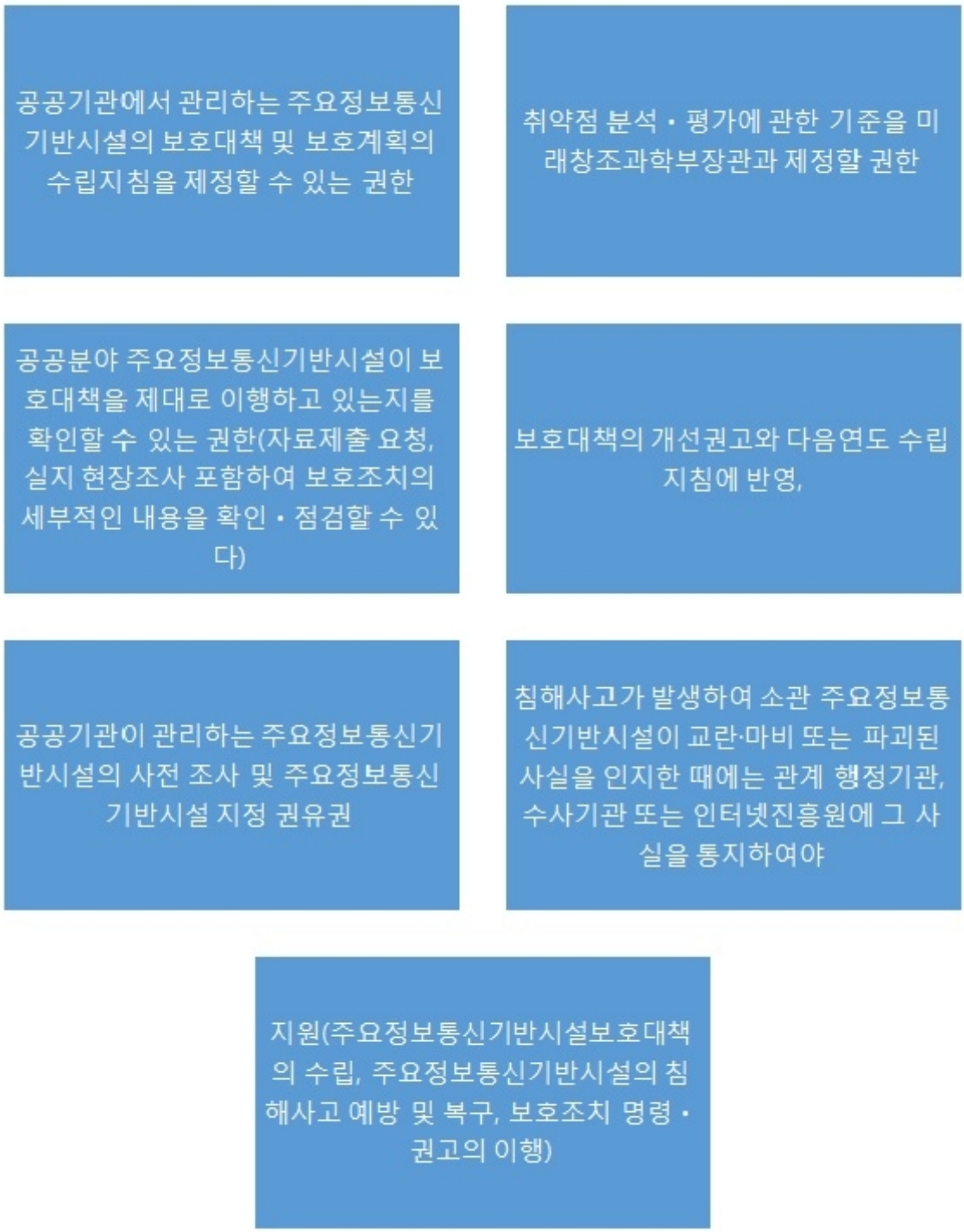
- 관리기관의 장이 필요하다고 인정하거나 주요정보통신기반시설보호위원회 위원장이 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관, 국가정보원장, 국방부장관 기타 전문기관의 장에게 주요정보통신기반시설보호대책의 수립, 주요정보통신기반시설의 침해사고 예방 및 복구, 보호조치 명령·권고의 이행 지원을 요청할 수 있다.

- 특히 도로·철도·지하철·공항·항만 등 주요 교통시설, 전력, 가스, 석유 등 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설의 경우에는 국가정보원장에게 우선적으로 지원을 요청하게 하였다.

- 지원의 내용이 '주요정보통신기반시설보호대책의 수립, 주요정보통신기반시설의 침해사고 예방 및 복구, 보호조치 명령·권고의 이행'이어서 사실상 모든 보안관제를 대신 수행하는 수준이다.

- 반면 국정원은 금융정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 안된다고 규정하고 있다.

<주요정보통신기반보호법에 의한 국정원의 역할>



다. 대통령훈령인 국가사이버안전관리규정을 통한 국정원의 사이버 관여는 상위법과 국정원법에 위반됨

(1) 훈령의 적용범위와 효력

- 대통령훈령으로 국가사이버안전관리규정이 제정되었는데, “국가사이버안전[18]에관한조직체계및운영에대한사항을규정하고사이버안전업무를수행하는기관간의협력을강화함으로써국가안보를위협하는사이버공격으로부터국가정보통신망을보호함을목적으로한다.”고 그 제정 목적을 밝히고 있다.

- 이는 법적 근거 없이 국정원에게 권한을 부여하는 것이어서 그 효력이 의문시된다.

- 이 훈령은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대하여 적용하되, 정보통신기반보호법에 의하여 지정된 주요정보통신기반시설에 대하여는 적용하지 않는다고 규정하고 있는데, 논리적으로도 모순이다.

- 훈령은 국정원장이 국가사이버안전과 관련된 정책 및 관리에 대하여는 관계중앙행정기관의 장과 협의하여 이를 총괄·조정한다고 규정하여 국가사이버안전과 관련된 정책 및 관리에 대한 최고 권한을 부여하고 있는데,

- 반면, 정보통신기반보호법은 국무총리실장에게 그 권한을 부여하고 있어서, 법률에 위반되는 권한 부여이다.

- 그리고 주요정보통신기반시설이 아닌 공공기관의 정보통신망에 대해서만 국정원장이 그와 같은 권한을 갖는다는 것은 논리적으로 모순적인 논리이기 때문이다.

---

18) 이 훈령은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 사이버공격이라고 정의하고, 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 "사이버안전"이라고 정의하고 있다.

어쨌든 주요정보통신기반시설에 대해서는 주요정보통신기반시설법에 의하여 주요정보통신기반보호위원회 위원장(국무총리실장)에게 권한을 부여하고, 그 외의 공공기관이 운영하는 정보통신망에 대해서는 훈령이 적용된다는 것이다.

(2) 훈령에 의한 국정원장의 권한

- 국가사이버안전전략회의 의장 : 훈령은 국가정보원장에게 국가사이버안전과 관련된 정책과 관리의 총괄 조정 권한을 부여하고 있다. 훈령은 국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의를 두고, 의장을 국가정보원장이 맡도록 하고 있다.[19]

- 전략회의의 권한 : 정책 결정권

  ■ 전략회의는 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 사항을 심의한다.

- 법령에 근거를 두고 설치, 권한 부여된 정보통신기반보호위원회와 배치됨

  ■ 반면, 정보통신기반보호법은 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 둔다고 규정하고 있다. 25인 이내의 위원[20]으로구성되는기반보호위원회는국무총리실장이 위원장이되고, 국정원 차장은 위원이 된다. 그 외 대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다. 위원회에는 실무위원회를 두는데, 공공분야와 민간분야로 나뉘어 있다. 위원회는 주요정보통신기반시설 보호정책의 조정에 관한 사항, 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항, 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항, 주요정보통신기반시설 보호와 관련된 제도의 개선에

19) 위원은 교육과학기술부차관, 외교통상부차관, 법무부차관, 국방부차관, 행정안전부차관, 지식경제부차관, 보건복지부차관, 국토해양부차관, 대통령실 외교안보수석비서관, 방송통신위원회 상임위원, 금융위원회 부위원장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 한다.

20) 위원은 기획재정부차관, 미래창조과학부차관, 외교부차관, 법무부차관, 국방부차관, 행정자치부차관, 산업통상자원부차관, 보건복지부차관, 고용노동부차관, 국토교통부차관, 해양수산부차관, 국가정보원 차장, 금융위원회 부위원장, 방송통신위원회 상임위원으로 구성된다.

관한 사항, 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항을 심의한다. 사실상 동일한 역할의 위원회가 병존하는 모순적인 구조를 가지고 있다.

- 상위법 위반

■ 정보통신기반보호법은 국무조정실장에게 주요정보통신기반시설에 관한 보호계획의 종합, 조정, 제도 개선 등에 관하여 권한을 부여하고 있는데, 훈령은 편법적으로 국가정보원장에게 그 권한을 옮겨버린 것이다. 이는 법률과 모순되는 것이다.

(3) 국정원의 사이버안전센터는 보안관제센터의 역할을 함

- 훈령은 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 목적으로 국정원에 국가사이버안전센터를 두도록 함.

- 사이버안전센터는 국가사이버안전정책의 수립, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가사이버안전매뉴얼의 작성·배표, 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원 등을 그 업무로 하고 있다.

- 특히 훈령에 의하여 국정원은 사이버위협 관련 정보의 수집, 분석, 전파, 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원 업무를 수행할 수 있는 권한을 부여받고 있는데, 이는 법적인 효력이 없는 것이다.

<국가사이버안전센터 업무 소개>

주요업무

국가사이버안전 정책 총괄

- 국가사이버안전 정책기획 • 조율
- 국가사이버안전 관련 제도 • 지침 수립
- 국가사이버안전 대책회의 운영
- 民 • 官 • 軍 정보공유체계 구축 • 운영

사이버위기 예방활동

- 각급기관 전산망 보안컨설팅 및 안전측정
- 보안적합성 • 암호모듈 검증
- 사이버위기 대응훈련
- 정보보안 관리실태 평가
- 정보보안 공공분야 주요정보통신 기반시설 보안관리

사이버공격 탐지활동

- 24시간 365일 각급기관 보안관제
- 단계별 사이버위기 경보발령
- 각급기관 보안관제센터 운영 및 교육 지원
- 신종 해킹 탐지기술 개발 • 지원

사고조사 및 위협정보 분석

- 해킹사고 발생 시 사고조사 및 원인규명
- 사이버위협정보 및 취약점 분석
- 국내외 유관기관과 협력체계 구축
- 유가치 사이버위협 신고 포상 및 보안권고문 배포

6. 국정원의 더 큰 힘 - 보안적합성 검증(정보보호시스템에 대한 안전성을 검증), 암호모듈 검증을 통한 정보보안분야 관장

가. 보안적합성 검증

- 전자정부법 제56조 및 '공공기록물 관리에 관한 법률 시행령' 제5조
  - ■ 국가·공공기관에 도입하는 정보보호시스템에 대한 안전성을 검증하는 제도

- 국가, 공공기관과 주요정보통신기반시설(네트워크 장비)이 보안기능이 포함된 IT제품, 정보보호시스템(2016년 1월 현재 24종), 네트워크 장비 도입 시
  - ■ 국가사이버안전센터에 보안적합성 검증을 신청해야 함.

- 특히 정보보호시스템 도입시는 CC인증 제품을 도입해야 함

나. CC인증

- 상용 IT제품의 보안기능을 국제 기준 및 절차에 따라 평가하고 그 결과를 보증하는 제도. 국가, 공공기관 도입 정보보호시스템 여부와 무관.

- 국가정보원 → IT보안인증사무국과 국가보안기술연구원

- 소스코드도 제공해야 함.

다. 암호모듈 검증

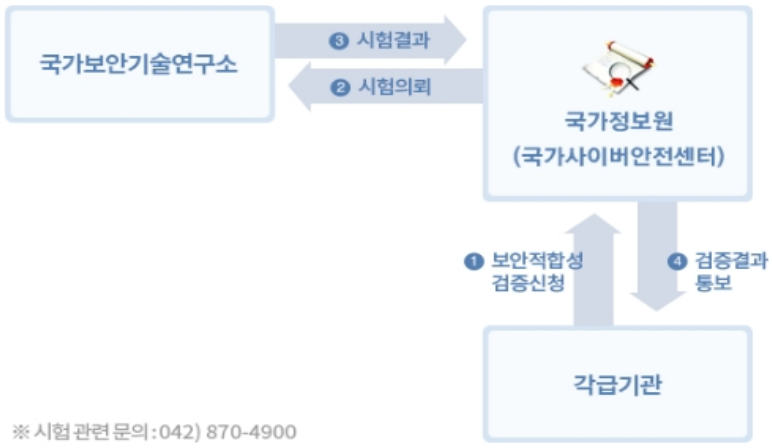
- 암호모듈 검증 : 거의 모든 암호모듈을 국정원이 검증함(메일 암호화, 구간 암호화, PKI, 통합인증(SSO), 디스크·파일 암호화, 문서 암호화(DRM 등), 키보드 암호화, 하드웨어 보안 토큰, DB 암호화, 기타 암호화).

- 전자정부법 시행령 제69조와 [암호모듈 시험 및 검증지침]

- 검증시 제출물 : 기본 및 상세 설계서, 형상관리문서, 개발과정 각 단계별 수행해야 하는 시험항목, 각 시험항목별 시험목적, 시험절차 및 결과서, 제품 및 소스코드

- 암호에 대한 통제 : 국가, 공공기관은 국가사이버안전센터가 안전성을 확인한 검증필 암호모듈을 탑재해야 함.

국가 • 공공기관 정보보호시스템 검증절차



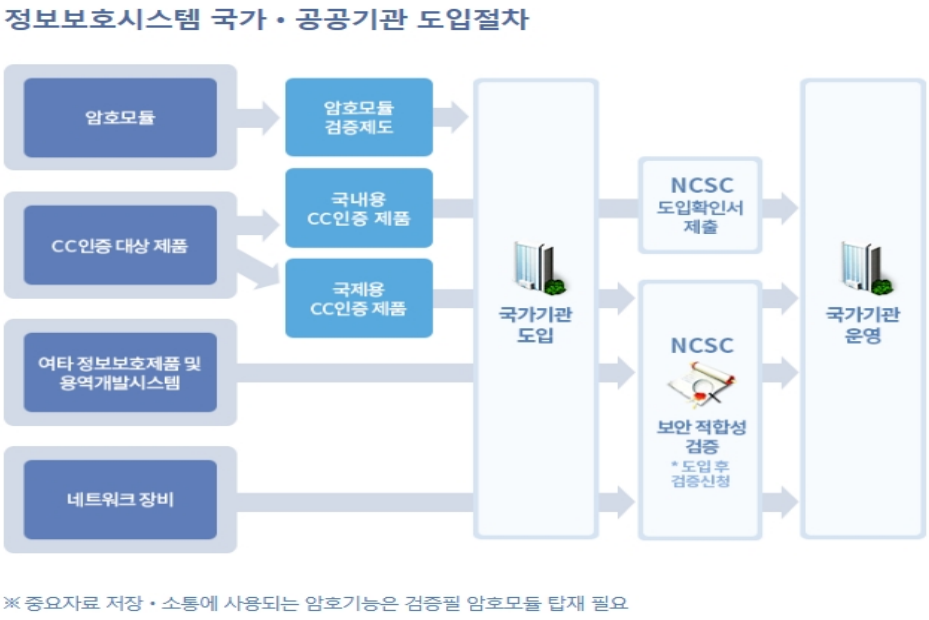
※ 시험 관련 문의 : 042) 870-4900

국가사이버안전센터의 역할

1) 정보보호시스템 보안적합성 시험기준 • 방법수립
2) 국가 • 공공기관의 보안적합성 검증신청서 접수
3) 시험기관에 시험의뢰 및 시험결과 검토
4) 검증결과 통보 및 보완조치 이행여부 확인

시험기관의 역할

1) 정보보호시스템 보안적합성 시험기준 • 방법 연구
2) 정보보호시스템에 대한 시험실시 및 시험결과 작성
3) 필요 시 보완사항에 대한 추가시험 실시



라. 공인인증서, 금융권

- 공인인증서의 암호 모듈도 국정원에서 암호모듈 인증을 받아야 함

- 금융기관은 2015년 3월까지 국정원 보안성 심사를 마친 제품만 사용할 수 있었음.

마. 영향

- 국내의 거의 모든 정보보안업체의 제품은 국가에 납품하는 제품이 아니더라도 국정원으로부터 CC인증, 암호모듈 인증을 받음.

- 결국, 민간부문에 대해서도 국정원이 CC인증, 암호모듈 인증을 통해서 정보 파악 가능함.

- 암호에 대한 국가의 통제가 이루어지고 있음.

- 국정원은 국내의 민간부문 보안관제를 수행하고 있는 보안관제업체에 대해 막강한 영향력 행사하고, 암호, 정보보안산업에 막강한 영향력을 행사하고 있음.[21]

7. 현재 행사하고 있는 국정원의 사이버 권한 요약

- 대통령 훈령에 의한 사이버안전전략회의

- 국가사이버안전센터

- 국가, 공공기관에 대한 보안관제, 공공 기반시설의 보안관제

- 주요정보통신기반보호법에 의한 참여

8. '사이버테러 방지법'은 국정원에게 어떤 권한을 부여하는가?

가. 침해사고 대응행위와 대비되는 제한이 없는 사이버안전

- 사이버테러방지법은 사이버테러[22]로부터정보통신시설과정보를보호하기위해수행하는관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동을 사이버안전이라고 규정하면서 대응의 범위를 광범위하게 하고 있다. 즉, 정보통신시설과 정보를 보호하기 위한 모든 활동이 사이버안전[23]이라는것이다.

---

21) 국가보안기술연구원은 패밀리 기업을 선정하고 있음

22) "사이버테러"란 외국이나 대한민국의 통치권이 사실상 미치지 아 니하는 한반도내의 집단, 해킹·범죄조직 및 이들과 연계되거나 후 원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목 적으로 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단 에 의하여 정보통신망을 공격하는 행위를 말한다.

23) "사이버안전"이란 사이버테러로부터 정보통신시설과 정보를 보호하기 위하여 수행하는 관리적·물리적·기술

- 이는 기존의 정보통신망법[24]이미래창조과학부장관의침해사고대응행위를침해사고정보수집, 긴급조치, 침해사고 관련정보 보고를 받는 것으로 한정한 것과 대조적이다.

나. 사이버안전센터를 통한 정책의 수립과 집행권한으로 국정원은 사이버 사찰 능력을 갖출 수 있다

- 사이버테러방지법에 의하면 국가정보원에 신설하는 사이버안전센터(사이버위협정보공유센터)는 사실상 모든 일을 할 수 있다.

> 제6조(사이버안전센터의 설치) ① 사이버테러에 대한 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 사이버안전센터(이하 “안전센터”라 한다)를 둔다.
> ② 안전센터는 다음 각 호의 업무를 수행한다.
> 1. 사이버테러 방지 및 대응 정책의 수립
> 2. 전략회의 및 대책회의 운영에 대한 지원
> 3. 사이버테러 관련 정보의 수집·분석·전파
> 4. 국가정보통신망의 안전성 확보
> 5. 사이버테러로 인하여 발생한 사고의 조사 및 복구 지원
> 6. 외국과의 사이버 공격 관련 정보의 협력
> ③ 국가정보원장은 제1항의 안전센터를 운영함에 있어 국가차원의 종합판단, 상황관제, 위협요인 분석, 사고 조사 등을 위해 민·관·군 합동대응팀(이하 “합동대응팀”이라 한다)을 설치·운영할 수 있다.
> ④ 국가정보원장은 합동대응팀을 설치·운영하기 위하여 필요한 경우에는 중앙행정기관 및 지원기관의 장에게 인력의 파견과 장비의 지원을 요청할 수 있다.

- 사이버안전센터는 사이버테러 방지 및 대응 정책을 수립하는 일을 담당하는데,

적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함.

24) 제48조의2(침해사고의 대응 등) ① 미래창조과학부장관은 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다.

1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 대통령령으로 정하는 침해사고 대응조치

이는사실상 시행령의 제정 권한을 갖는 것이다. 국가정보원의 사이버안전센터가 시행령을 제정할 경우, 이를 통해 국정원은 사이버위협정보의 수집과 종합과 분석, 사이버테러 예방을 위한 정보통신망에 대한 감시, 정보수집, 조사 등을 할 수 있는 권한을 가질 수 있을 것이다. 결국 국정원의 사이버안전센터는 사실상의 상시 감시, 정보수집기구가 될 것이다.

- 기존의 정보통신망법에 의하면 침해사고 대응 업무를 수행하는 미래창조과학부장관(한국인터넷진흥원)의 업무는 제한적[25]인데반해서국정원이사이버안전센터를통해서갖는권한은훨씬더포괄적.

- 미래창조과학부장관은 침해사고에 관한 정보 수집, 전파, 침해사고의 예보, 경보, 침해사고에 대한 긴급조치, 기타 대응조치를 할 수 있음에 반해

- 국가정보원의 사이버안전센터는 정책의 수립, 전략회의와 대책회의 운영, 사고의 조사 등 광범위한 권한을 부여받고 있다는 것을 알 수 있다.

---

25) 제48조의2(침해사고의 대응 등) ① 미래창조과학부장관은 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다.

1. 침해사고에 관한 정보의 수집·전파

2. 침해사고의 예보·경보

3. 침해사고에 대한 긴급조치

4. 그 밖에 대통령령으로 정하는 침해사고 대응조치

② 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 미래창조과학부장관이나 한국인터넷진흥원에 제공하여야 한다.

1. 주요정보통신서비스 제공자

2. 집적정보통신시설 사업자

3. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자

③ 한국인터넷진흥원은 제2항에 따른 정보를 분석하여 미래창조과학부장관에 보고하여야 한다.

④ 미래창조과학부장관은 제2항에 따라 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있다.

⑤ 미래창조과학부장관이나 한국인터넷진흥원은 제2항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다.

⑥ 미래창조과학부장관이나 한국인터넷진흥원은 침해사고의 대응을 위하여 필요하면 제2항 각 호의 어느 하나에 해당하는 자에게 인력지원을 요청할 수 있다.

정보통신망법	사이버테러 방지법
▪ 침해사고에 관한 정보의 수집·전파 ▪ 침해사고의 예보·경보 ▪ 침해사고에 대한 긴급조치 ▪ 그 밖에 대통령령으로 정하는 침해사고 대응조치	▪ 사이버테러 방지 및 대응 정책의 수립 ▪ 전략회의 및 대책회의 운영에 대한 지원 ▪ 사이버테러 관련 정보의 수집·분석·전파 ▪ 국가정보통신망의 안전성 확보 ▪ 사이버테러로 인하여 발생한 사고의 조사 및 복구 지원 ▪ 외국과의 사이버 공격 관련 정보의 협력

– 반면, 미래창조과학부장관은 침해사고의 원인 분석 등의 업무도 제한적으로 규정하고 있다.[26)]

다. 민간부문까지 국정원의 직할 영역이 된다 – 사이버테러 방지 및 위기관리 책임기관의 범위

– 책임기관(제2조 제5호)은

■ 국가기관(그 소속·산하기관을 포함)과 지방자치단체(그 소속·산하기관을 포함)

■ 공공기관

■ 주요정보통신기반시설을 관리하는 기관

26) ► 미래창조과학부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민•관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다.

► 미래창조과학부장관은 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.

► 미래창조과학부장관은 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민•관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.

► 미래창조과학부장관이나 민•관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.

► 제2항에 따른 민•관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.

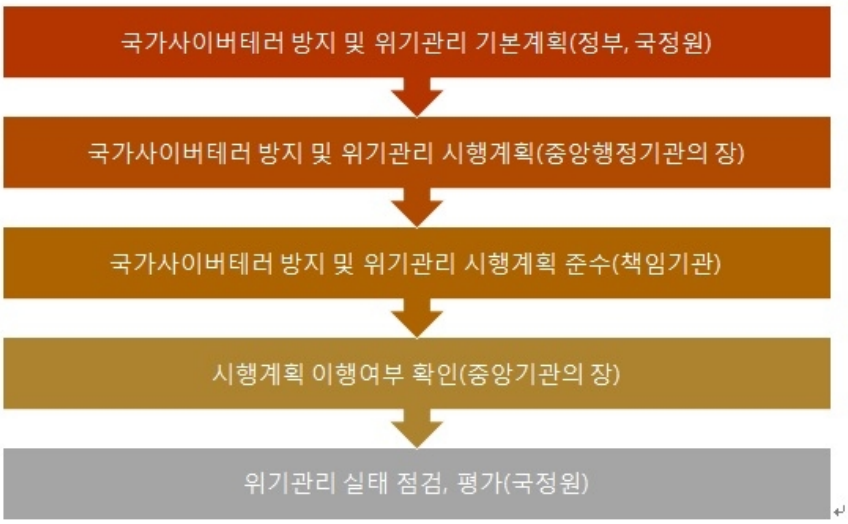
- 집적정보통신시설사업자
- 주요정보통신서비스 제공자
- 국가핵심기술을 보유한 기업체나 연구기관
- 방위산업체 및 전문연구기관

- 책임기관에 국가기관, 공공기관은 물론, 주요정보통신기반시설과 주요정보통신서비스제공자가 포함됨.

라. 국정원은 공공, 민간(책임기관)에 기본계획, 시행계획, 이행확인, 실태 점검과 평가(제4조, 제5조)를 통한 개입, 사이버테러방지대책(제7조)을 통해 밀착 개입할 수 있다

- 국가사이버테러 방지 및 위기관리 기본계획 수립, 시행(국정원)(제4조, 제5조)

- 이를 통한 책임기관에 대한 직접적인 관여 가능함.



-사이버테러방지대책을 통한 관여(제7조)

- 국정원이 각 정보통신서비스제공자 등이 자율적으로 시행할 사이버위협 대응 대책에 대해 지시와 관여

- 소관 정보통신망과 정보의 안전성과 신뢰성 확보를 위한 사이버테러방지대책 수립지침을 통해서 보안관제에 관여

마. 공공, 민간(책임기관)에 보안관제센터 구축 운영책임을 부여하여 직, 간접적으로 보안관제 통제 가능(제8조 제1항)

- 책임기관의 장은 사이버테러정보를 탐지, 분석하여 즉시대응조치를 할 수 있는 기구를 구축, 운영해야 함

- 또는 국가, 지자체 및 산하기관이 운영하거나, 행정기관(국정원)이 지정하는 보안관제전문업체가 운영하는 보안관제센터에 업무를 위탁해야 함.

- 보안관제센터에 대한 것은 대통령령으로 정한다고 포괄위임.

- **현재 공공부문의 경우 보안관제센터의 구체적인 활동내역, 수준, 정보공유 등을 규정하여 실제적인 통제를 하고 있음.**

- 이와 같이 국정원은 사이버테러방지법에 의하여 민간분야까지 아우르는 통합적인 보안관제센터를 직, 간접적으로 운영할 수 있게 되는데, 국정원은 이를

통해서 정보통신망에 대한 총체적이고, 상설적인 감시업무를 수행할 수 있는 집행기구로 기능할 것이다.

- 특히 국정원은 각종 보안솔루션에 대한 인증업무를 수행하고 있기 때문에 보안솔루션의 기능에 정통하다. 따라서 보안관제센터를 통해서 민간분야에 대한 상시 감시능력을 보유하게 될 것이다.

바. 공공, 민간(책임기관)과 사이버테러 정보와 취약점 정보의 공유를 통한 통제(제8조 제2항)

- 책임기관의 장은 사이버테러 정보와 정보통신망· 소프트웨어의 취약점 등의 정보를 국정원장과 공유해야 함.

- 구체적 내용은 대통령령으로 정한다고 포괄위임.

사. 사이버위협정보통합공유체계의 구축 운영(제8조 제3항)

- 이를 통한 국정원의 권한 행사

- 구체적인 것은 대통령령으로 정한다고 포괄위임.

아. 국정원은 민간기업에 대해서도 사이버 침해에 대한 수사권을 갖게 되고, 이를 통해서 부적절한 정보수집을 시도할 수도 있다

- 사이버테러방지법은 국정원에게 모든 정보통신망에 대한 사이버침해의 수사를 할 권한을 부여하고 있는 것과 마찬가지이다.

- 사이버테러방지법은 명목상으로는 중앙행정기관의 장에게 사고조사의 권한을 부여하고 있지만, 중앙행정기관의 장이 국정원장에게 기술적 지원 요청이라는 명목으로 사고조사를 요청할 수 있다. 이는 눈 가리고 아웅하는 것이나 다름 없다.

- 국정원은 포털, 언론사, 금융기관 등의 해킹사고 등에 대한 수사를 통해서 이들 민간기업에 대해 위법사실을 꼬투리 삼아서 부적절한 정보수집 등을 할 수 있을 것이다.

제9조(사고조사) ① 중앙행정기관의 장은 사이버테러로 인하여 소관분야에 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하여야 한다. 또한, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 한다
② 제1항의 경우 피해가 중대하거나 확산될 우려가 있는 경우 중앙 행정기관의 장은 즉시 미래창조과학부장관, 국가정보원장 및 금융위원장 등 대통령령으로 정하는 전문기관의 장에게 사고조사 등 기술 적 지원을 요청할 수 있다. 다만, 국회, 법원, 헌법재판소, 중앙선거 관리위원회는 해당기관의 장이 필요하다고 인정하는 경우에 한한다.
③ 국가정보원장은 제1항에 따라 사고조사 결과를 통보받거나 제2항에 따라 사고조사를 한 결과, 피해의 복구 및 확산방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.
④ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사이버테러와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

자. 사이버위기경보와 사이버위기대책본부

- 경계단계 이상의 사이버위기경보시 대책본부 구성

- 각 단계별 의무이행 수준은 적정한지

- 현재 주의 단계[27)]

27) 국정원 국가사이버안전센터의 주의 단계 대응 요령

o 각급기관은 위기대응 실무매뉴얼에 따라 사이버위기 '주의' 경보단계 대응활동 수행(국정원 홈페이지 → 사이버위기경보 → 경보단계 참고)

o 각급기관 및 보안관제센터 근무보강 등 비상근무태세 유지

o 전산망 장애, 사이버공격 등 특이징후 포착시 국가사이버안전센터 및 국가안보실(위기관리센터)로 즉시 통보

o 소속·산하기관에 '주의' 경보 전파 및 경보 상향조정에 따른 기술·관리적 보안대책 수행(위기대응 표준매뉴얼 및 실무매뉴얼 참고)

o 기관별 자체 '긴급대응반' 가동 준비 및 필요시 긴급 운영

국가 사이버안전에 심각한 영향을 초래할 수 있는 상황에 대해 미리 예측하여 경보 하는 표시 등급입니다. 국가사이버안전센터는 24시간 365일 국내외 온라인 네트워크와 각종 웜・바이러스 등을 감시하고 있습니다.

경보단계	
	경보단계 [심각] - 국가적 차원에서 네트워크 및 정보시스템 사용 불가능 - 침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고발생 - 국가적 차원에서 공동 대처 필요
	경보단계 [경계] - 복수 정보통신서비스 제공자(ISP)망 - 기간 망의 장애 또는 마비 - 침해사고가 다수기관에서 발생했거나 대규모 피해로 발전될 가능성 증가 - 다수 기관의 공조 대응 필요
	경보단계 [주의] - 일부 네트워크 및 정보시스템 장애 - 침해사고가 일부 기관에서 발생 했거나 다수기관으로 확산될 가능성 증가 - 국가 정보시스템 전반에 보안태세 강화 필요
	경보단계 [관심] - 웜・바이러스, 해킹기법 등에 의한 피해발생 가능성 증가 - 해외 사이버공격 피해가 확산되어 국내 유입우려 - 사이버위협 징후 탐지활동 강화 필요
정상단계	
	경보단계 [정상] - 전 분야 정상적인 활동 - 위험도 낮음 웜・바이러스 발생 - 위험도 낮은 해킹기법・보안취약점 발표

TOP

차. 이와 같이 국정원은 정보통신시설의 안전을 유지할 책임을 근거로 국정원은 민간기업에 대한 예비적인 보안관제를 통해서 정보수집과 사찰이 가능하다

- 사이버테러방지법은 국정원에게 소관정보통신시설의 안전을 유지할 책임을 부여하고 있는데, 이는 역으로 국정원의 권한을 의미한다.

- 게다가 소관정보통신시설의 범위가 모호하기 때문에 결국 정보통신시설의 안전을 유지할 권한을 갖는 것과 마찬가지이다. 정보통신시설의 안전을 유지할 책임과 권한을 행사하기 위해서 국정원은 실질적인 사이버침해가 발생하기 전에도 언제든지 예비적인 보안관제를 통해서 광범위한 정보수집과 사찰을 할 수 있게 된다.

9. 사이버테러방지법과 관련한 끔찍한 시나리오

가. 국정원이 사이버테러 방지라는 미명 아래 포털, 통신사, 은행, 언론사의 해킹 사고를 조사할 권한을 가지고 기업의 뒷조사를 한다

- 사이버테러방지법이 제정되면 국정원은 사이버테러방지라는 미명 아래 포털이나 통신사, 은행이나 언론사의 해킹 사고를 조사할 권한을 갖게 된다. 이 경우 국정원은 기업에 대한 뒷조사를 통해서 알게 된 해킹정보를 가지고 민간기업에 대해서 정보수집을 위한 압박수단으로 활용할 수 있게 된다.

나. 국정원은 정보통신망의 안전 보호라는 미명 아래 치밀한 보안관제 서비스를 이용해서 대량감시를 할 수 있다

- 국정원은 사이버테러방지법이 제정되면 정보통신망의 안전 보호 책임을 맡게 되며, 정보통신망의 안전 보호라는 미명 아래 치밀한 보안관제 서비스를 악용할 수 있다. 이 경우 국정원은 사실상 법원의 제어 없이 광범위한 민간 사찰을 수행할 수 있게 된다. 국정원에 집중된 취약점 분석 정보, 국정원이 파악한 보안관제 솔루션의 기능적 특성, 해당 민간기업의 적법절차 생략, 흔적이 남지 않는 감시 능력을 이용할 경우 국정원은 무소불위의 감시기관이 될 것이다.

다. 국정원이 시행령을 제정하여 보안관제 솔루션의 표준을 정하고, 은밀한 보안관제를 한다

- 국정원은 사이버테러방지법이 제정되면 시행령을 제정하여 정보통신망의 안전한 관리를 위해서 보안관제 솔루션의 표준을 정할 수 있다. 이런 표준을 통해서 국정원은 은밀한 보안관제를 수행할 수 있다.

라. 국정원이 지방자치단체의 뒷조사를 하여 꼬투리를 잡을 수 있다

- 사이버테러방지법이 제정된 후 국정원은 강화된 보안관제 능력을 바탕으로 지방자치단체에 대한 보안관제를 통해서 해킹 사실, 비위, 기타 사이버 침해 사실 등을 파악하고, 이를 바탕으로 뒷거래를 할 수도 있다. 이 모든 것들은 민주주의에 대한 중대한 위협이 될 수 있다.

10. 개선방안은 어떻게 되어야 하는가?

가. 그 동안 우리나라의 공공부문 사이버위협대응은 준수해야 할 기본원칙에서 벗어나 효율성, 민주성, 신뢰성 등을 모두 잃어 왔다

- 국정원이 공공부문을 관할하는 것의 문제점(기반보호법과 국가사이버안전규정)
  - ■ 공공부문의 자체적인 대응능력 제고 등 주체의 적극적 참여를 보장하지 못하고, 통제위주이고, 기술중립성도 보장되지 않는다.
  - ■ 효율성, 민주성, 신뢰성을 모두 잃음.

나. 공공부문의 자율성을 보장하고, 국정원이 아닌 미래창조과학부나 독립기관에서 담당해야 한다.

- 국가는 원칙으로 돌아가서 사이버위협에 대응해야 하고,

- 국정원은 대북관계 정보의 수집과 정보의 제공 등의 업무로 국한해서 담당해야 한다.

다. 국정원이 정보보호와 관련해서 갖고 있는 비대한 권한은 정보보호산업을 좀먹는다

- 국정원이 보안적합성 심사, CC 인증, 암호모듈 인증 등을 관장하여 투명성, 기술중립성, 신뢰성, 공정한 경쟁, 인권과 사생활 보호 등이 보장되지 못한다.

- 국정원의 권한을 미래창조과학부장관에게 넘기거나, 민간에 이양해야 한다.

라. 이런 와중에 제안된 사이버테러방지법은 기존의 문제를 심화시킨다

- 민간의 협력과 참여를 보장할 수 없다.

- 기술중립성도 보장되지 않는다.

- 인권과 프라이버시, 표현의 자유 등이 보장되지 않는다.

- 민간의 주도성이 전혀 보장되지 않는다.

- 이용자 등 주체의 참여도 보장되지 않는다.

마. 현재의 상황은 국가정보원법의 국정원 직무범위와도 모순됨

토론 1

서울지방변호사회 인권위원회 결의문

오영중 / 변호사, 서울지방변호사회 인권위원장

정의화 국회의장이 직권상정한 국민보호와 공공안전을 위한 테러방지법안(의안번호 18582, 이철우 의원대표발의)은 헌법상 기본권과 헌법과 법률이 정한 영장주의, 죄형법정주의, 적법절차를 심각하게 침해할 우려가 높다.

이 법안이 그대로 통과되면 국가정보원은 초헌법적 정보수집권한을 가지게 된다. 즉, 테러, 테러단체, 테러위험인물, 대테러활동 등 이 법안의 핵심적인 개념들이 지나치게 모호하고, 국가정보원의 자의적 판단으로 국민의 통신의 비밀, 사생활의 비밀, 표현의 자유, 집회시위의 자유가 침해될 것이다. 그럼에도 국가정보원을 통제할 법적 장치는 매우 미흡하고 실효성이 없다.

이러한 중대한 인권침해를 초래할 법률안에 대해서는 입법의 필요성 뿐만 아니라 법안의 내용을 국민들에게도 내실있게 설명한 후 국회에서의 충실한 토론과 숙의를 거쳐야 함에도 불구하고 국회의장이 국가비상사태라는 명목하에 직권상정하고, 정부여당이 이를 다수의 힘으로 표결처리하려는 것은 국가안보, 테러방지라는 목적으로도 정당화되지 않는다.

서울지방변호사회 인권위원회는 이 테러방지법안이 국민의 기본권을 심각하게 침해하고 법치주의의 근간을 훼손하는 것으로 판단하고 서울지방변호사회가 공식적

으로 이 법률안에 대한 반대의견을 국회에 제출해 줄 것을 건의하기로 결의한다.

2016. 2. 26.

서울지방변호사회 인권위원회

토론 2

국민보호와 공공안전을 위한 테러방지법의 문제점

이태호 / 참여연대 정책위원장

1. 한국에는 테러방지법이 없다?

새누리당 이철우 의원은 유엔안전보장이사회 결의 1373호가 테러방지법 제정을 각국에 요구했는데 우리나라는 지금까지 테러방지법을 제정하지 않고 있어 테러방지법을 제정해야 한다고 주장했다.

1) 유엔안전보장이사회 결의 1373호의 주된 내용[1)]

유엔 안전보장이사회는 2001년 9월 28일에 결의 제1373호56)를 통과시켰는데, 이 결의는 특히 테러자금조달억제를 위한 포괄적인 전략을 담고 있다. 이 결의의 본문 1항 전체가 테러자금조달에 대한 대책에 해당하는 것으로서, 모든 국가가 다음의 4개 항목을 실시할 것을 요구하고 있다.

① 테러자금의 제공을 방지하고 억제할 것

② 자국민에 의한 행위 또는 자국의 영역내에서의 행위로서 테러행위를 실행하기

1) 도중진, 이진국, 이천현, 손동권, "테러자금조달의 억제를 위한 법제도설계방안에 관한 연구", 한국형사정책연구원,

위해 사용될 것을 의도하였거나 알면서, 수단 여하를 불문하고, 직접 또는 간접적으로, 자금을 고의적으로 제공하거나 모금하는 행위를 범죄화할 것

③ 테러행위 실행자, 실행기도자 또는 테러행위에의 참가자 및 편의제공자의 자금 및 기타 금융자산 또는 경제적 자원, 그러한 자에 의해 직접 또는 간접적으로 소유되거나 지배되고 있는 단체의 자금 및 기타 금융자산 또는 경제적 자원 및 그와 같은 단체를 대신하거나, 그러한 자와 단체의 지시에 따라 행동하는 자와 단체의 자금 및 기타 금융자산 또는 경제적 자원을 지체 없이 동결할 것

④ 자국민 또는 자국의 영역 내에 있는 개인 및 단체에 대해서도, 테러행위를 실행하거나 실행을 기도하거나 테러행위의 실행에 편의를 제공하거나, 테러행위에 참가하는 자의 이익을 위해서, 그러한 자에 의해 직접 또는 간접적으로 소유되거나 지배되고 있는 단체의 이익을 위해서, 그리고 그러한 자를 대신하거나 그러한 자의 지시에 따라 행동하는 개인 및 단체의 이익을 위하여, 모든 자금 및 금융자산, 경제적 자원 또는 금융 및 기타 서비스를 직접 또는 간접적으로 이용가능하게 하는 것을 금지할 것

2) 테러자금조달금지법 2007

대한민국 국회는 이미 2007년 12월 “공중 등 협박목적을 위한 자금조달행위의 금지에 관한 법(일명, 테러자금조달금지법)”을 제정해 2008년 2월부터 시행하고 있다.

3) 미국의 테러방지법(애국자법)과 한국에 이미 존재하는 테러방지법제들

테러방지법의 대표격이라 할 수 있는 미국의 애국자법(The USA PARIOT Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)은 제정되자마자 그 비효율성과 부작용에 대한 비판에 직면해 2006년 개정으로 독소조항이 대폭 삭제되었고, 2015년 6월 2일 통과된 미국자유법(The USA FREEDOM Act, Uniting and

Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act)에 의해 논란이 되어 왔던 215조도 폐지되었다.

애국자법은 여러 개의 개별법의 개정안--전자통신프러이버시법(Electronic Communications Privacy Act), 컴퓨터사기및오용에관한법(Computer Fraud and Abuse Act), 해외정보사찰법(Foreign Intelligence Surveillance Act), 가족교육권및프라이버시법(Family Educational Rights and Privacy Act), 자금세탁통제법(Money Laundering Control Act), 은행비밀법(Bank Secrecy Act), 금융프라이버시권리법(Right to Financial Privacy Act), 공정금융거래보고법(Fair Credit Reporting Act), 이민및국적법(Immigration and Nationality Act), 1984년형사범죄피해자법(Victims of Crime Act of 1984), 텔레마케팅및소비자사기및오용예방법(Telemarketing and Consumer Fraud and Abuse Prevention Act)--을 포함하는 패키지 입법이다.

우리나라도 이미 「범죄수익은닉규제법」, 「특정금융거래정보의보고및이용등에관한법률」, 「공중협박목적등자금금지법」, 「외환관리법」, 「금융실명거래및비밀보장에관한법률」, 「전자금융거래법」 등 자금거래 규제에 관한 법을 촘촘히 제정, 시행하고 있다. 게다가 통신기반 보호와 사이버 범죄 예방을 명분으로 정부는 「정보통신기반보호법」, 「전기통신사업법」, 「통신비밀보호법」과 「개인정보호법」의 예외조항등을 법제화하여 시행하고 있다. 또한 「국가보안법」, 「국가정보원법」, 「주민등록법」, 「출입국관리법」, 「범죄인인도법」 도 모두 테러방지를 예방할 수 있는 조항을 두고 있다. 「형법」, 「특정범죄가중처벌법」, 「폭력행위 등 처벌에 관한 법률」, 「항공보안법」, 「선박위해처벌법」, 「철도안전법」, 「원자력안전법」, 「방사능방재법」, 「화학물질관리법」, 「총검단속법」, 「범죄인인도법」 역시 테러방지를 위한 법이다. 테러대비테세를 규정한 법으로는 「통합방위법」, 「비상대비자원관리법」 등이 있다.

2. 테러방지법이 없어서 알 누스라 추종 외국인 처벌 못했다?

새누리당 이철우 의원은 인도네시아인이 테러단체에 자금을 송금했는데도 이를 처벌하지 못하고 추방 조치에 그쳤다고 강변하고 있다.

알 누스라를 추종했다는 인도네시아인의 사례는 더 꼼꼼히 따져봐야 한다.

지난해 적발된 알 누스라를 추종했던 인도네시아인 A(가명)는 추방된 것이 아니라 현재 검찰에 붙잡혀 조사를 받고 있다. 그는 지금 위조사문서행사와 총포도검화약류등단속법·출입국관리법·전자금융거래법 위반 등의 혐의로 구속되 검찰의 수사를 받고 있다. "'테러방지법'이 없어서 테러예비범을 '추방'조치밖에 못하고 있다"는 새누리당의 주장과는 달리 그는 여러 형사범죄 위반죄로 구속되어 있는 것이다. A씨 검거 후 경찰청 외사정보과장은 A씨의 테러 위험성에 대해 "단순 추종, 지지는 일반적으로 적용할 법이 없다", "향후 자생적 테러리스트(일명 외로운 늑대)가 될 수도 있다고 보고 실체를 찾아내는 것이 가장 중요하다"고 말했다. 테러방지법이 없어서 처벌할 수 없다고 한 것이 아니라 단순 추종 지지는 법적으로 처벌할 수 없다고 말한 것이다 검찰은 3월11일 그에게 '사문서위조죄'를 적용 1년6개월을 구형했다.

인도네시아 A씨가 알 누스라를 찬양하는 사진을 찍는 것을 도운 친구 2명도 검거되었는데 죄명은 출입국관리법 위반 등이었다. 불법체류자였기 때문이었다. 경찰은 국내법상 테러단체를 추종했다고 처벌하기는 어렵지만 테러 연루 가능성을 수사할 필요가 있다고 보고 A씨는 물론 B씨 등 2명에 대해서도 추가 조사를 벌이고 있다. 경찰은 '별다른 혐의점이 발견되지 않을 경우'에는 이들은 강제추방 수순을 밟을 예정이다. 이 말은 테러단체를 추종한 것을 처벌할 수 없지만 테러에 연루되었다면 처벌할 수 있다는 뜻으로 해석해야 옳다. 추방은 테러에 연루된 증거가 없을 때 행해지는 것이지 '테러예비범'인데도 추방 외에 방법이 없는 것은 아니다. 테러단체 추종자와 테러예비범은 엄격히 다르다. 마치 공산당 (당원도아닌) 지지자와 내란예비자와 다른 것처럼.

한편, 검찰은 검거된 A에게서 안 누스라를 추종한 사실은 확인했고 그가 '시리아 내전 지하드 전사'에게 200만원을 보낸 사실도 확인했다. 하지만 그가 새누리당 이철우 의원이 주장하듯이 알 누스라에게 돈을 보냈는지는 아직 확인되지 않았

다. 그는 보낸 자금 200만원이 알 누스라에게 보내진 것이라고 확인한 바 없다. 단지 “A씨가 11차례에 걸쳐 인도네시아 사업가를 거쳐 시리아 내전에 참여 중인 지하드 전사에게 돈을 보냈다”는 사실만 확인했을 뿐이다. 검찰은 지금 “이 자금이 테러와 관련된 것인지 확인”하는 중이다. 이철우 의원은 과연 누구로부터 이 인도네시아인이 알 누스라에게 송금했다는 사실을 확인했는가? 상대가 외국인이라는 이유로 확인도 안 된 허위사실을 유포하면 곤란하다.

그런데, 이 사건은 경찰과 검찰이 발견하고 수사한 사건이다. 찾아내기 어렵다는 Lone Wolf(개인 자생 테러리스트)를 적발한 것이다. 새누리당 이철우 의원은 무슨 근거로 국정원이 없으면 안 된다고 주장하는가? 국정원이라면 과연 11번을 쪼개서 인도네시아 사업가를 거쳐 총액 200만원에 불과한 돈을 쪼개 보내 지하드 전사를 도운 이를 (경찰과 달리) ‘예방’단계에서 찾아낼 수 있다고 장담할 수 있는가? 이런 걸 미리 예방할 수 있으려면 국정원은 얼마나 촘촘하게 모든 종류의 거래정보를 뒤질 수 있어야 하는가? 그것은 오직 50여명의 흉악무도한 ‘테러위험인물’들만 겨냥할 것인가?

더불어 ‘테러단체추종자’ 혹은 ‘테러위험인물, 테러혐의자라 해서 우리 헌법과 국내법이 보장하는 권리를 함부로 침해해도 된다는 발상은 매우 위험하다는 점만 추가해두고자 한다. 이주자에 대한 추방은 이주자에게 삶의 터전을 박탈하는 것인 만큼 중대한 처벌행위이다. 또한 국내법의 보호를 박탈하겠다는 의미이다. 만약 테러위험인물로 규정된 추방될 경우, 그 사람은 앞으로 영영 제3국으로 가기 힘들어질 것이고 자국에서도 매우 심각한 수사나 처벌에 노출될 것이다.

3. 저인망식 사찰의 문제점과 비효율성

저인망식 무더기 사찰은 미국에서도 많은 문제점을 야기했고 테러방지에 그다지 효과가 없다는 사실도 확인되었다.

NSA와 FBI의 무더기 개인정보 수집 남용사례와 비효율성

2004년 조지 W. 부시 대통령이 구성했던 '대통령 직속 사생활보호 및 시민자유 검토 위원회(The President's Privacy and Civil Liberties Oversight Board)'는 "NSA의 통화기록 프로그램이 대테러 조사활동에 가시적인 성과를 냄으로써 미국에 가해지는 위협을 개선했다는 어떤 증거도 없다"고 비판했다.

미국 인권단체 미국시민자유연맹(ACLU)에 따르면 "2003년부터 2006년까지, FBI는 약 200,000건의 '국가안보레터'를 발행하여 인터넷 서비스 제공업체들로부터 사용자정보를 수집하였는데, 오직 단 한 건만 테러용의자 유죄입증에 사용되었던 것으로 밝혀졌다"고 한다.

미국 애국자법의 sneak and peek (잠입영장) 남용사례

미국은 9.11이후 애국자법(테러방지패키지법)을 제정하면서 수사기관의 정탐 및 잠입(sneak and peek)을 허용했다. 사후고지수색영장(Delayed-notification search warrant) 제도를 도입함으로써 용의자의 거주지나 시설 등에 고지 없이 몰래 잠입하고 나중에 고지하는 제도를 도입한 것이다. 몰래 잠입하고 수색하고도 당사자에게 알리지 않는다는 점에서 이것은 긴급체포나 급습과는 전혀 다른 조사방법이다. 그러나 현실에서 이 제도는 테러용의자에게는 거의 적용되지 않고 주로 마약사범이나 일반형사범죄 수사에 편의적인 수단으로 악용되었다. 2013년 미국에서 청구된 사후고지 영장 11,129건 중 오로지 51건만이 테러리즘 수사를 위한 것이었음을 보여준다. 0.5%다. 마약사건에는 전체의 84%인 9,401건이다.

한국에서 이런 제도가 도입된다면 마약사범 수사만큼이나 시국사건 수사에 악용될 소지가 크다. 국정원은 인도네시아 외교관들이 머무는 숙소에 몰래 잠입했다가 발각된 사례가 있다. 물론 사전이건 사후건 간에 수색영장을 발급받지 않은 상태였다. 테러방지법 제9조 4항의 '테러위험인물에 대한 추적'은 정체가 모호한 개념이다. 미행을 의미하는지 잠입도 포함되는지 알 수 없다. 미국은 그나마 수사당국이 영장을 발부받되 당사자에게는 알리지 않는 방식이지만, '테러방지법' 제9조 4항 추적은 영장 없이도 '수사'목적이 아닌 경우에도 정보수집을 위해 '추적'할 수 있게 되어있다.

NSA의 프리즘 프로그램, IT서비스시장에 1800억달러 손실 초래[2)]

"사단법인 Forrester Research의 분석에 따르면, 미국 NSA의 사찰프로그램인 프리즘에 대한 공포로 인해 클라우드, 호스팅, 아웃소싱 업체들의 거래손실이 1800억달러에 이를 수 있다고 한다."

4. 사이버테러?

법률적으로 정의내리기 힘들고 국익에도 바람직하지 않다

사이버 테러리즘에 대해 미 의회에 제출된 보고서(2015)[3)]

"사이버전쟁과 마찬가지로, 사이버테러리즘이 무엇인지에 대해서는 합의된 정의는 없다. 가장 가까운 정의는 '애국자법'에 따라 개정된 미형법 2332b조의 "국경을 초월하는 테러행위" 규정, '컴퓨터사기및남용법'에 따라 개정된 미형법 1030a-c조에 정의된 몇가지 행위와 위해 사례들이다. 이 행위의 주목할만한 점은 가해자가 테러행위가 아니라 형사범죄를 저지르고 있는 것으로 간주되며, 범행에 대한 처벌로 벌금 또는 금고(투옥)을 검토되고 있다는 점이다. 국가행위자에 의해 이루어질 경우, 전쟁행위로 간주되어야 한다는 주장도 있다. '컴퓨터사기및남용법'은 이런 식으로 개인이나 조직에 적용되도록 작성되었다."

"As with cyberwarfare, there is no consensus definition of what constitutes cyberterrorism. The closest in law is found in the USA PATRIOT Act 18 U.S.C. 2332b's definition of "acts of terrorism transcending national boundaries" and reference to some activities and damage defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. A notable aspect

2) "NSA's Prism Could Cost IT Service Market $180 Billion", CLINT BOULTON, THE WALL STREET JOURNAL, 2013/08/16
http://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion/

3) CRS Report R43955, "Cyberwarfare and Cyberterrorism: In Brief", Catherine A. Theohary & John W. Rollins, March 27, 2015, http://fas.org/sgp/crs/natsec/R43955.pdf

of this act is its discussion of the "punishment for an offense" entails fines or imprisonment and suggests the offending party is undertaking a criminal act rather than an act of terrorism, which some argue is an act of war if undertaken by a state actor. The CFA is written in such a manner that it could be applied to an individual or groups."

"사이버테러리즘이라는 용어가 왜 법률적으로 규정되어오지 않았는지 설명할 수 있는 수많은 이유가 있다. 해당되는 행위들이 뭐라고 이해해야 할지, 그 한도를 특정하기 어렵다는 점도 포함된다. 확실한 레드라인을 분명히 표현할 경우 낮은 수준의 사건도 사이버테러로 대응해야 되는 것은 아닐지? 사이버공간에서 미래 미국의 행위를 제약하지 않도록 전략적인 기동성을 유지하는 것도 어려울 수 있다."

"There are a number of reasons that may explain why the term "cyberterrorism" has not been statutorily defined, including the difficulty in identifying the parameters of what should be construed applicable activities, whether articulating clear redlines would demand a response for lower-level incidents, and retaining strategic maneuverability so as not to bind future U.S. activities in cyberspace."

토론 3

사이버테러방지법안의 입법체계 검토[1)]

심우민[2)]/ 국회입법조사처 입법조사관

1. 사이버테러 대응의 법적 체계

□ 우리나라의 사이버테러 대응의 법적체계는 크게 두 개의 근거 법령에 의해 이루어지고 있는데, 그것은 「정보통신기반보호법」(법률) 및 「국가사이버안전관리규정」(대통령훈령)임

○ 사실 이 밖에도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)」 "제6장 정보통신망의 안정성 확보 등"의 제반 규정도, 일반적인 정보보호 및 보안업무라는 명목으로 사이버테러 방지와 연관성을 가짐

□ 결국 위와 같은 체계를 취하고 있는 것은, 국가조직 체계 내부에서의 사이버테러 대응은 기본적으로 「국가사이버안전관리규정」에 근거를 두고 수행하되, 민간영역 및 중요시설과 연계되어 사이버테러가 발생하는 경우에 대비하여 「정보통신기반보호법」을 제정한 것이라고 이해할 수 있을 것임

○ 따라서 「정보통신기반보호법」은 정부에 의해 지정된 "주요정보통신기반시설"을 기본 수범자로 하고 있는데, 이러한 주요정보통신기반시설에는 이미 민간

1) 이 토론문은 현재의 입법쟁점인 「사이버테러방지법」의 입법체계상 의문점들을 검토한 것으로, 특정 입장을 지지하거나 반대하기 위한 것이 아님을 밝혀둡니다. 또한 이는 필자가 속해 있는 기관(국회입법조사처)의 공식적인 입장 또는 견해가 아니라는 점도 양해 부탁올립니다.

2) 국회입법조사처 입법조사관; 법학박사(legislation21@gmail.com)

영역의 사업자들도 포함되어 있음

○ 즉 동법의 취지는 민간영역에 사이버테러를 명목으로 국가가 함부로 개입하게 되는 경우 사업자 및 이용자의 기본권 침해가 발생할 수 있어, 이를 예외적인 경우에만 인정하기 위한 것이라고 판단됨(헌법 제37조 제2항의 기본취지)

- 사실 「국가사이버안전관리규정」의 경우 그 수범자를 기본적으로 국가기관 및 공공기관을 대상으로 하는 것이기 때문에 대통령훈령으로 규율이 가능했던 것으로 보임

□ 이를 전제로, 이하에서는 현재 발의된 「국가 사이버테러 방지 등에 관한 법률안(이하, 사이버테러방지법안)」에 관한 의문점들을 제시해보고자 함

2. 위기관리책임기관의 범위

□ 「사이버테러방지법안」은 제2조 제5호에서 동법의 기본 수범자라고 할 수 있는 “사이버테러 방지 및 위기관리 책임기관”을 규정하고 있음

○ 이러한 책임기관에는 ‘국가기관 및 공공기관, 주요정보통신기반시설, 집적정보통신시설사업자, 주요정보통신서비스 제공자, 국가핵심기술 보유 기업 및 연구기관, 방위산업 관련 업체 및 전문연구기관’이 이에 해당함

□ 이 중 가장 첨예한 논쟁의 대상이 되고 있으며, 동법의 궁극적인 제정취지를 뒷받침 해주고 있는 “주요정보통신서비스 제공자”의 개념적 범주라고 할 수 있음

○ 「사이버테러방지법안」 국가정보원을 사이버테러 대응의 컨트롤타워로서 정립함과 동시에, 융합시대에 대비하기 위한 목적으로 민간영역 다수의 사업자들까지 규율대상으로 하여, 사이버테러 대응 업무의 효과성을 제고하겠다는 취지를 가지고 있음

○ “주요정보통신서비스 제공자”의 개념과 관련하여 「사이버테러방지법안」 제2조 제5호 다목에서 「정보통신망법」 제47조의4 제2항을 준용하고 있음

□ 그런데 「사이버테러방지법안」이 준용하고 있는 「정보통신망법」 어디에도 “주요정보통신서비스 제공자”의 개념정의가 존재하지 않는다는 점에서, 자의적 해석 및 집행이 이루어질 가능성이 있음(입법오류)

○ 실제 「정보통신망법」 전체 규정들 중 “주요정보통신서비스 제공자”라는 용어는 총 2차례 출현하는데, 그 중 하나가 동법 제47조의4(이용자의 정보보호) 제2항이고, 다른 하나가 제48조의2(침해사고의 대응 등) 제2항이지만, 그 어디에도 이에 관한 개념정의는 존재하지 않음

○ 다만 입법연혁을 살펴보면, “주요정보통신서비스 제공자”라는 용어가 「정보통신망법」에 처음 도입되었을 당시에는 개념정의 규정이 존재했는데, 이에 의하면 이는 “전기통신사업법 제2조제1항제1호의 규정에 의한 전기통신사업자로서 전국적으로 정보통신망접속서비스를 제공하는 자(이하 ”주요정보통신서비스제공자“라한다)”로 되어 있었고, 2012년 「정보통신망법」 개정시 삭제되었음

○ 여기서 학계의 전통적인 해석에 의하면 ‘정보통신망 접속서비스 제공자’는 통신망사업자(통신 3사)를 의미하는 것임

□ 이상과 같은 입법적 불비 또는 오류에도 불구하고, 「사이버테러방지법안」상의 “주요정보통신서비스 제공자” 규정을 유지한다고 한다면, 연혁적 해석을 통해 이를 ‘정보통신망 접속서비스 제공자’로 해석하는 방안이 있을 것인데, 만일 그렇다면 기존의 「정보통신기반보호법」과 별도로 새로이 사이버테러 대응법제를 구성해야하는 이유가 불분명함

○ 즉 기존의 「정보통신기반보호법」도 이미 국가 및 공공기관은 물론이고, 민간영역에서의 사이버 침해 또는 위협에 대응할 필요가 있는 다수의 시설들을 주요정보통신기반시설로 포함시키고 있음

○ 이에 의하면, 결국 국가정보원을 사이버테러 대응체계의 중심으로 정립하기 위한 목적만이 존재하면, 또한 그렇다면 기존의 「국가사이버안전관리규정」만으로도 충분히 그러한 목적을 달성할 수 있는 것은 아닌지 하는 의문이 있음

3. 기타 입법체계적 검토가 필요한 사항

□ 추진체계의 문제

○ 「사이버테러방지법」이 제정되는 경우 기존의 「정보통신기반보호법」과 사실상 그 규율영역이 상당부분 유사하기 때문에, 대응체계가 일원화되는 것이 아니라 오히려 혼선이 발생할 여지가 있는 것은 아닌지에 대한 검토가 필요함

○ 또한 동법은 민간영역 사업자와 관련한 「정보통신망법」 제47조의4 제1항(미래창조과학부 소관부분), 즉 “정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다”라는 규정의 모호성을 가중시킴으로써, 향후 바람직하지 않은 방향으로 활용될 수 있음

□ 민·관·군 합동대응팀 및 정보공유

○ 「사이버테러방지법안」 제6조 제3항에 근거한 ‘국가사이버안전센터’ 내 ‘민·관·군 합동대응팀’(제6조 제3항)의 운영과 관련하여, 민간영역의 인적·물적 자원을 활용한 (상시)대응(동 법안 제11조 제1항은 위기시에는 “민·관·군 전문가가 참여하는 사이버위기대책본부”를 구성 및 운영하도록 하고 있음)은 사업자 및 이용자의 기본권(영업수행의 자유 및 이용자 프라이버시 등) 침해를 발생시킬 여지가 높기 때문에, 그 구성 절차와 소관 업무에 대해 법률에 명확하게 규정해 둘 필요가 있음에도 불구하고, 대통령령에 조차 이를 위임하고 있지 않아, 결과적으로 국가정보원장에게 상당한 재량을 부여하고 있음

○ 이는 「사이버테러방지법안」 제8조 제2항에 근거한 정보공유 사안에 있어서도 마찬가지이며, 특히 이용자 프라이버시 보호에 관한 사항은 헌법상 기본권 제한에 해당하는 것이기 때문에 명확한 절차규정이 필요함에도 불구하고, 관련 절차 등 실무적인 규정을 대통령령에 위임하고 있음

4. 제언

□ 국가안전 등 공익적 목적을 위한 사이버테러대응 체계의 개선이 필요하다는 점을 인정한다고 할지라도, 이러한 입법적 개선작업은 기존의 법령체계에 대한 면밀한 분석을 토대로 이루어져야 할 것이라고 판단됨

○ 사이버테러 대응체계 구성과 관련하여, 우리나라의 경우에는 성문법을 중심으로 한 법치국가로서의 특수성을 가지고 있어, 사안별로 중보식 형태로 관련

행정규제를 추가하는 방식으로 입법을 개선해 나가는 국가들의 사례를 참조하는 것에는 한계가 있다는 점에 유의해야할 필요가 있음

○ 또한 이미 「정보통신망법」 등에는 소위 보안관제의 목적으로 활용되고 있는 규정들이 상당 수 있기 때문에, 체계 중복을 피하여 사이버테러 대응업무의 효율성을 기하기 위해서는, 관련 규정과의 관계를 반드시 고려해야 함

○ 우리나라의 경우에는 이미 주민등록번호는 물론이고, 공인인증서, 아이핀 및 휴대폰 등 획일적·범용적인 개인 식별정보의 활용이 제도적으로 만연해 있기 때문에, 국가안전 및 안보의 사안을 고민할 때에는 단순히 외국의 대응제도 참조가 중요한 것이 아니라, 우리나라의 특수한 환경도 고려한 가운데 국가행위에 의한 기본권 침해를 최소화할 수 있는 세심한 입법이 필요할 것이라고 판단됨

○ 이러한 견지에서, 오히려 기존에 사이버테러 대응체계의 근간이었던 「정보통신기반보호법」 및 「국가사이버안전관리규정」은 물론이고, 「정보통신망법」상 보안관련 규정들의 상당부분도 개선이 필요할 수 있음

토론 4

사이버테러방지법의 문제점 토론문

이동산 / 페이게이트 이사

주최: 민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동공간‘활’,
인권운동사랑방, 진보네트워크센터, 참여연대, 김광진 의원

문의: 참여연대 행정감시센터 02-723-5302, 진보네트워크센터 02-774-4551

테러방지법과 사이버테러방지법의 문제점 진단 토론회