긴급세미나

테러방지법과 사이버테러방지법, 무엇이 문제인가

일시 | 2015년 12월 7일(월) 오전 10시

장소 | 국회 의원회관 제1세미나실

주최 | 새정치민주연합 국회 정보위원회(신경민, 김광진, 문병호, 문희상, 박지원, 이종걸)

주관 | 민주주의법학연구회, 민주화를위한전국교수협의회, 정보인권연구소

프로그램

사회	정연순 변호사, 민주사회를위한변호사모임 부회장
인사말	신경민 의원, 새정치민주연합 국회 정보위원회 간사
발제1	**테러방지법, 현재 무엇이 문제인가?**
	오동석 교수, 아주대학교 법학전문대학원, 민주주의법학연구회
발제2	**사이버테러방지법, 현재 무엇이 문제인가?**
	이은우 변호사, 법무법인 지향, 정보인권연구소 이사
토론	정재원 교수, 국민대 국제학부(사회학), 민교협 정책위원
	장유식 변호사, 민주사회를위한변호사모임
	이태호 사무처장, 참여연대
	장여경 정책활동가, 진보네트워크센터
종합토론	
폐회	

목차

테러방지법, 현재 무엇이 문제인가

오동석 / 아주대학교 법학전문대학원 교수, 민주주의법학연구회

1. 테러를 방지할 수 있는 법은 없다

박근혜 대통령이 국가정보원의 숙원을 해결하기 위해 테러방지법 제정에 나섰다. 비록 다른 나라 사람들일지언정 대규모 범죄희생자들을 애도하는 것은 당연한 일이다. 그런데 자신을 대표로 뽑아준 사람들이 죽어가고 있는 것은 외면한 게 문제다. 그런데 국가적인 범죄로 억울하게 죽은 세월호 참사의 희생자들에 대한 애도와 그에 상응하는 진상조사와 대책 및 관련법을 요청하는 울부짖음을 깔아뭉개고 있는 건 용서할 수 없는 일이다. 이것은 그 애도의 진정성에 대한 의심이 아니라 분노다.

박근혜 대통령은 지난 11월 24일 예정에 없던 국무회의를 긴급히 소집하여 주재하면서 “각국은 테러를 방지하기 위한 선제적인 대책들을 세우고 있는 반면에 현재 우리나라는 테러 관련 입법이 14년간이나 지연이 되고 있다”고 발언했다. 그러나 왜 14년 동안 시민사회에서 테러방지법을 반대했는지, 다른 나라 테러방지법의 내용과 우리에게 부족한 것은 무엇인지에 대한 성찰은 없었다. 그게 있었다면 절대 그렇게 말하지 못한다.

지금 테러 방지 및 대응 체계는 어떠한지, 그렇다면 지금 대한민국은 테러라고 부르는 범죄행위들에 대해 속수무책 상태라는 것인지, 그래서 자신의 정부가 무능하다는 것에 대한 고백인지 어느 하나 제대로 설명하지 않았다. 오로지 “현재 테러방지법, 통신비밀보호법, 사이버테러방지법 등 국회에 계류된 테러 관련 법안들의 처리에 국회에 나서지 않고 잠재우고 있는데 정작 사고가 터지면 정부에 대한 비난과 성토가 극심하

다"는 변명만 있었다.[1)]

그렇다면 세월호 참사가 일어난 원인도 해난사고방지법을 제정하지 않아서였는지, 정부는 세월호특별조사위원회 관련해서 왜 그렇게 일을 할 수 없게 방해하고 있는지, 그래서 세월호 참사에 대한 진상 조사와 관련 입법 등 대응 조치가 필요하다고 긴급 국무회의를 소집해가면서 자책하고 관련자들을 문책하며 또한 국회에 읍소하지 않았는지 환장할 노릇이다.

한편 새누리당이 테러방지법안으로 내세운 법안은 12개에 이른다. 〈국가대테러활동과 피해보전 기본법〉(새누리당 송영근 의원 2013.3.27 발의), 〈국민보호와 공공안전을 위한 테러방지법안〉(새누리당 이병석 의원 2015.2.16 발의), 〈테러예방 및 대응에 관한 법률안〉(새누리당 이노근 의원 2015.3.12 발의), 〈국가 사이버안전 관리에 관한 법률안〉(새누리당 하태경 의원 2013.3.26 발의), 〈국가 사이버테러 방지에 관한 법률안〉(새누리당 서상기 의원 2013.4.9 발의), 〈사이버테러 방지 및 대응에 관한 법률안〉(새누리당 이노근 의원 2015.6.24 발의), 〈사이버위협정보 공유에 관한 법률안〉(새누리당 이철우 의원 2015.5.19 발의), 〈출입국관리법안〉(정부 2015.10.26 발의), 〈항공보안법 개정안〉(새누리당 하태경 의원 2015.7.3 발의), 〈항공보안법 개정안〉(새누리당 이노근 의원 2015.5.4 발의), 〈특정금융거래정보의보고 및 이용 등에 관한 법률〉(새누리당 박민식 의원 2015.3.6 발의), 〈통신비밀보호법 개정안〉(새누리당 박민식 의원 2015.6.1 발의)이다.

그런데 국가정보원이 테러방지법을 만들어야 한다고 주장한지 14년이 지나도록 도대체 어떤 일이 있었는가. 법 없이 테러를 방지할 수 없다면, 벌써 테러가 난무해야 했었을 것이다. 박근혜 정부가 걱정해야 할 거리는 정작 따로 있다. 2003. 3. 20.부터 2011. 12. 15.까지 이라크 '전쟁'에서 이라크 군과 경찰의 사망자 수는 2만 명, 반군은 1만 9천 명이다.[2)] 미군의 전투 중 사망자 수는 3518명이다. 2003-2011년 한국의 자살자 수는 116,971명이다.[3)] 박근혜 정부는 전쟁보다 더 참혹한 한국의 현실에 대해

---

* 2015. 11. 30. <테러방지법에 대한 시민사회단체 의견서>에 의존하여 작성했음.

1) 뉴스핌 2015. 11. 24.
<http://www.newspim.com/view.jsp?newsId=20151124000324&fromurl=na> 최근검색일: 2015. 11. 24. 아래 인용 같음.

2) 미국 보스턴 대학 네타 크로포드 교수의 통계이다. 이라크 민간인의 사망자 수는 12만 6000명이다. "이라크전 공식 종료, 9년 전쟁", 뉴스1 2011. 12. 18.

3) 위키백과. "대한민국의 자살".
<https://ko.wikipedia.org/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD%EC%9D%98_%EC%9E%90%EC%82%B4> 최근검색일: 2015. 12. 6.

먼저 책임을 져야 한다. 이전 정부의 일이라고 잡아뗄 일이 아니다. 〈자살예방 및 생명존중문화 조성을 위한 법률〉(법률 제10516호, 공포일 2011.3.30 시행일 2012.3.31)이 있다고 우길 일이 아니다. 법만 만든다고 될 일이 아니며, 원인과 해법은 따로 있음을 인정해야 한다.

2015년 등장한 테러방지법안들은 제목만 다를 뿐 과거 법안들과 거의 다를 바 없다. 다만 한 고등학생의 IS 가입 추정 사건과 주한미국대사의 피습 사건을 빌미 삼았을 뿐이다. 흔히 테러라고 부르는 사건과 직접적인 연관성이 없음에도 불구하고 언제나 결론은 테러방지법이었다. 기존의 테러 예방 및 대응 체계에 대한 진단과 평가는 14년 동안 한 번도 없었다. 결국 국가정보원을 강화하는 결과만을 초래할 뿐이라는 지적에 대해서도 묵묵부답이었다.

테러방지법을 한번 들여다보기만 하면 누구나 한 눈에 알 수 있다. 테러방지법을 제정한다고 테러를 예방할 수 있는 것도 아니고, 테러방지법 없이 테러에 신속하게 대응할 수 없는 것도 아니라는 것을. 온통 테러에 대응하기 위한 조직을 어떻게 만들자는 내용이 핵심이기 때문이다. 그것은 그 조직이 어떻게 작동할 것인가의 문제이다. 그렇다면 박근혜 정부는 먼저 새로운 법을 만들지 않으면 안 될 정도로 대한민국이 얼마나 '테러'에 대해 무능한지를 고백해야 한다. 국가정보원이 국가권력의 핵심에 똬리를 틀지 않으면 안 되는 이유가 무엇인지를 자백해야 한다. 남의 나라 테러로부터 배우기보다 '우리' 나라 세월호 참사부터 찬찬히 깊숙이 들여다보기를 간절히 권한다. 또 다른 세월호 참사를 방지하기 위해 무엇부터 해야 할지 깊은 반성 먼저 하기 바란다.

2. 테러에 대한 대처가 오히려 인권에 더 위험할 수 있다

미국에서 9·11 테러는 여러 가지 면에서 많은 변화를 초래하였다. 그 중 부정적 영향은 인권 침해의 위험성이다. 자타가 선진국으로 인정하는 미국에서조차 '테러와의 전쟁'을 수행하는 과정에서 CIA가 2003년 3월 중순부터 포로들에게 멱살잡이, 손바닥으로 때리기, 복부가격, 오래 세워놓기, 냉방 고문, 물고문 등의 방법을 활용했음이 밝혀졌기 때문이다.[4)]

4) 경향신문 2005. 11. 22.
<http://news.khan.co.kr/kh_news/khan_art_view.html?artid=200511220724521&code=970201>, 최근검색일: 2015. 12. 6.

유엔 고등 판무관실(United Nations High Commissioner for Human Rights)의 '테러리즘대처와 인권과 자유의 관계에 대한 특별 보고'[5]는 2005년 발표한 「국제적인 대테러 행동 속에서 나타나는 다섯 가지 경향」을 다음과 같이 소개했다(이계수 외, 2006: 462 재인용).

첫째, 각국 정부는 마음에 들지 않는 정치·인종·지역 세력들에 테러리스트 혐의를 씌워 탄압하고 있다. 국제사회는 이런 경향에 무관심할 뿐 아니라 사실상 이러한 반인권적 정부들을 지원하고 있다. 둘째, 테러 혐의자들을 조사하는 과정에서 고문과 잔혹 행위 등이 빈번이 사용되면서 이러한 반인권적 행위를 금지하는 국제협약들의 근간이 무너지고 있다. 이는 가장 위험한 경향이다. 셋째, 테러리즘을 옹호하거나 찬양하는 내용 뿐 아니라 테러 행위에 사용될 가능성이 있는 모든 정보의 배포도 금지되고 있다. 이렇게 테러리즘에 대한 해석이 확대되면서 무고한 사람들의 희생이 늘어나고 있다. 넷째, 각국이 출입국 통제를 강화하고 있으며 그 결과 인종 차별이 심화되고 있다. 개별 국가들이 양자협정을 맺어 테러리스트 혐의자들의 신상정보를 비밀리에 주고받고 있으며 테러리스트 혐의자 수용소를 비공개적으로 운영하고 있다. 이는 분명한 국제법 위반이다. 다섯째, 테러 행위의 조사와 예방이 경찰권 확대 내지 남용의 근거가 되고 있다."[6]

과거 많은 테러 관련 법안이 제출되었지만, 국회를 통과하지 못했다. 테러 개념의 불명확성은 물론이고 과연 법률 제정으로 테러의 예방과 테러에 대한 신속한 대응이 가능할까 하는 의구심 때문이었다. 오히려 정보기관의 권한만 확장함으로써 국민의 인권이 위험에 빠질 것이라는 시민사회의 비판이 있었기 때문이었다.

과거 시민사회에서 테러방지법에 반대하는 목소리를 높였던 것은 테러를 용인하거나 테러방지 자체의 의미를 전적으로 부정하기 때문은 아니다. 테러방지라는 미명 아래 국가의 경찰권력, 정보권력을 강화하고 국민의 인권을 침해하거나 제한하는 일이 일어날 수 있다고 우려했기 때문이었다. 그렇다면 테러방지법을 제정해야 한다고 밀어붙이기보다는 현행 제도에 대한 보다 철저한 분석 및 평가가 선행되어야 하고, 그에 따라 어떻게 테러대응기구를 개혁할 것인가를 논의해야 한다(이계수 외, 2006: 457).

더욱이 반테러활동은 전통적으로 경찰 및 형사소추기관의 고유한 임무였다. 국정원이 이 임무와 관련하여 정보수집을 하기 시작한 것은 1990년대 중반 이후부터이다(1994년 1월의 안기부법 개정). 경찰 및 형사소추기관의 고유한 임무영역에 정보기관

---

5) The Special Rapporteur on the Protection and Promotion of Human Rights and Fundamental Freedoms while Countering Terrorism.

6) "대테러 전쟁 속에 인권은 사치품으로 전락," 프레시안 2005. 12. 7. 재인용.

이 개입하게 되면, 보안기관 사이에 마찰 및 커뮤니케이션에서 문제가 생길 수 있으며, 사후에는 책임소재가 불분명해질 수 있다(이계수 외, 2006: 566).

따라서 대테러역량의 강화는 새로운 법률 제정 또는 국가정보원의 직무를 확대하고 그 권한을 확장하는 데 있지 않다. 과거 테러 관련 법안은 국정원을 중심으로 인적·물적으로 상호중첩된 다수의 조직 및 인력이 결합하는 조직구성방식을 취하고 있으나, 지나치게 비대한 조직 외연으로 인하여 '테러'방지 업무(테러의 사전방지)에 대한 효율성이 현재보다 오히려 더 떨어질 수 있다. 또한 일단 테러가 발생한 이후에 필요한 조치들(테러의 사후진압)은 테러방지법이 예정하고 있는 복잡하고 혼란스러운 조직과 기구가 아닌 일상적인 경찰 및 행정기구들로도 충분히 그리고 보다 효율적으로 대응이 가능하다.

3. 테러방지법안은 위헌 주장에 대해 합헌을 입증해야 한다

테러방지법은 테러와 관련한 국가기구의 설치와 권한의 배분 및 조정 등 조직법적 수준에서 중대한 변경을 담고 있다. 특히 그 변화의 핵심에 국가정보원을 두는 한편 이를 통하여 국가권력의 실질적 통합가능성을 안고 있는 등 국가조직의 일반원칙과 권력분립을 지향하는 헌법질서의 기본구도를 벗어나는 양상을 보이고 있다. 그러나 그 어떤 테러방지법안도 이러한 구조변화의 필연성을 담보할 수 있는 국가적 위기에 대한 근거를 제시하고 있지 않다. 어제 오늘의 일이 아니지만 주먹구구식 입법이다.

엉터리입법을 방지하기 위해서는 다음과 같은 질문에 답해야 한다. 첫째, 형법이나 특별형법으로 방지하거나 대응할 수 없는 범죄행위로서 '테러'는 무엇인가? 둘째, 과거와 다른 '테러'가 발생한 한국 사회의 환경요인은 무엇인가? 셋째, 혹시 분단 상황이나 북한의 존재가 문제라면, 어떤 변화가 있었으며, 국가보안법은 어떤 문제가 있었는가? 넷째, 한국 사회에 어느 정도의 '테러' 위협이 존재하는가? 다섯째, '테러'가 사회질서 혹은 국가안보에 어느 정도로 위협이 될 수 있는 것인가? 여섯째, 테러가 일회적이지 않고 계속 반복될 것으로 예상하는가? 그렇다면 그 예상의 근거는 무엇인가? 일곱째, 기존의 국가조직 혹은 치안기구만으로 이러한 테러를 감당하는 것이 어느 정도로 무엇 때문에 불가능하거나 비효율적인가? 여덟째, 이상의 일곱 가지 질문에 답할 정도로 한국 사회에서 테러의 위험성을 상당한 개연성으로써 예측한 보고서가 있는가? 마지막으로 아홉째, 테러방지법 제정을 전제로 하여 각계 전문가의 의견을 들어 정부가 마련한 테러 방지 및 대응의 구체적 매뉴얼은 무엇인가?

이제까지의 수많은 테러방지법안은 이러한 질문에 대하여 아무런 답을 내놓지 못했다. 새로운 테러에 응하기 위해 새로운 법과 새로운 조직이 필요하다면, 그에 합당한 설명을 해야 한다. 자칫 낡은 조직과 대응체계에 새로운 상표만 덧붙인 것이 될 수 있기 때문이다.

테러방지법안의 테러 개념은 기존 국내법상의 범죄와 대비되는 개념으로서의 '테러'를 특정하지 못한 채 단순히 국제법상에서 특별히 규제하고 있다는 이유만으로 이들을 하나의 개념으로 통합하고 있다. 항공기납치, 민간항공에 대한 불법적 행위, 국제적 보호인물에 대한 범죄, 인질, 핵물질, 항해 및 해상플랫폼의 안전, 폭탄테러행위 등은 모두 국내법으로 처벌할 수 있는 범죄이다. 외국인이나 국제범죄조직이 그러한 범죄를 저지른다면, 경찰이나 검찰 등이 대응할 수 있다.

테러방지법안은 테러행위에 대해 내국인 범죄 또는 외국인 범죄의 구분은 물론 개인적·개별적 수준의 범죄 또는 조직적·집단적 범죄의 구분조차도 하지 않았다. 예컨대 인질 억류는 제3자 즉 국가, 정부 간 국제기구, 자연인, 법인 또는 집단에 대해 인질석방을 위한 명시적 또는 묵시적 조건으로서 어떠한 작위 또는 부작위를 강요할 목적으로 타인을 억류 또는 감금하여 살해, 상해 또는 계속 감금하겠다고 협박하는 행위이다. 이때 개인적 차원에서 발생하는 경우와 조직적·집단적 차원에서 발생하는 경우는 분명 사회질서와 국가안보의 측면에서 상당한 차이가 있다. 민간항공의 안전에 대한 불법적 행위, 예컨대 국제민간항공이 사용하는 공항에 근무하는 자에 대해 중대한 상해나 사망을 야기하거나 야기할 가능성이 있는 폭력행위를 행한 경우도 마찬가지다.

이병석법안은 대테러활동의 개념을 테러의 예방 및 대응을 위하여 필요한 제반 활동으로 정의하고 테러의 개념을 국내 관련법에서 범죄로 규정한 행위를 중심으로 국가안보 또는 국민의 안전을 위태롭게 하는 행위로 적시하고 있을 뿐이다(법안 제2조). 이노근법안은 미 대사의 피습 사건을 고려한 듯 외국인을 테러대상에 포함했다. 동시에 형법상 범죄행위를 되풀이하고 있다. 즉 제2조제1호의 개념 정의에서 "국가안보 및 공공의 안전을 위태롭게 하거나 공중(외국인을 포함한다)을 협박할 목적"으로 행하는 행위를 전제한 다음, 가목에서 "사람을 살해하거나 사람의 신체를 상해하여 생명에 대한 위험을 발생하게 하는 행위 또는 사람을 체포·감금·약취·유인하거나 인질로 삼는 행위", 나목에서 "「외교관 등 국제적 보호인물에 대한 범죄의 예방 및 처벌에 관한 협약」에서 정의한 국제적 보호인물을 살해·납치 또는 신체나 자유를 위태롭게 하거나 그러한 행위에 가담·지원·기도하는 행위(공관·사저·교통수단에 대한 가해행위를 포함한다)"를 테러 개념에 포함하고 있다. 테러 개념이 귀에 걸면 귀걸이 코에 걸면 코걸이 식으로 국가권력의 입맛에 따라 무한 확장할 수 있는 위험한 개념임을 쉽게 확인할 수 있다.

유럽의 일명 ‘베니스 위원회’는 〈안보기관의 민주적 감독에 대한 보고서〉를 발간하였다. 몇 가지 개략적 원칙을 참고할 수 있다(Venice Commission, 2007: 4). 첫째, 국가의 대내적 및 대외적 안보의 유지는 다른 가치 및 국익의 보호를 위하여 매우 중요하고 본질적이다. 국가는 효과적 정보와 안보기관을 필요로 한다. 둘째, 정보기관의 활동에 대한 외부적 제한뿐 아니라 내부적 제한이 있어야 하는 것이 중요하다. 셋째, 9/11 이후 테러리스트의 위협은 새로운 안보 위협을 가져왔다. 무엇보다도 업무와 권한의 집중이 아니라 기관 간 협력이 강화되어야 한다. 더 강력한 민주적 통제와 다른 유형의 통제가 오늘날 필요하다. 넷째, 안보기관은 국가권력의 잠재적 남용가능성을 안고 있다. “국가안보” 개념의 주관성 및 유연성은 국가에 대한 그것의 핵심적 중요성과 결합하여 정부가 이 분야에서 광범위한 활동 여지를 가지고 있다. 따라서 당국의 효과적 통치권한을 주면서도 정치적 남용을 막기 위한 기제를 수립할 필요가 있다. 다섯째, 안보 업무는 “답책성”이 있어야 한다. 답책성의 실무적 개념정의는 “활동에 대하여 해명 또는 설명을 하도록 책임을 지우고, 만약에 실수가 있었다는 것이 드러나면, 적절한 곳에서, 그 결과를 수용하도록 하고, 비판을 받거나 사태를 수습하도록 하게 함”을 의미한다. 여섯째, 답책성에는 네 가지 다른 형태가 있는데, 의회에 대한 책임, 사법적 책임, 전문적 책임, 진정을 통한 구제 제도 등이다. 뒤의 두 가지 형태는 처음 두 가지 책임 형태에 대한 보완수단 또는 대체수단이다.

4. 테러방지법안보다 국가정보원의 권력남용방지법안의 먼저다

테러 개념의 추상성·모호성은 곧장 대테러대책기구의 기능 범위에 대한 규정 부재에서도 나타난다. 국가대테러대책회의, 대테러센터 등을 가동하는 테러의 범주를 확정하지 않았을 뿐 아니라 그것을 결정하는 과정과 절차에 대한 규정 또한 존재하지 않는다. ‘테러’의 강도와 밀도가 어느 정도에 이를 때 대테러기구의 권한을 발동하는지, 그 권한발동의 절차는 무엇인지 그리고 그에 대한 국민적 감시·감독의 가능성은 어떻게 확보할 수 있는지에 대한 규정이 전혀 없다.

이러저런 테러 관련 조약들을 뭉뚱그려 그러모은 행위에 대해 ‘테러’의 이름표를 붙이고, 법만 만들어주면 알아서 잘 할테니 권력을 모아달라는 말밖에 되지 않는다. 그때그때 자의적 판단에 따라 ‘대테러대책’이라는 명분하에 국가권력을 한 곳에 집중시키는 위험만을 담고 있다. 그러니 테러방지법안은 헌법적 관점을 끌어들이지 않아도 국민을 허수아비로 만들어버린 꼴이다.

테러방지법안에서 예정하고 있는 대테러기구의 전체적인 구조는, ① 실질적, 포괄적인 대테러대책기관이 되는 대테러센터를 국가정보원장 소속하에 설치하며, ② 대테러센터가 주요 행정각부의 장 및 국무조정실장으로 구성되는 국가대테러대책회의를 실질적으로 관할, 행정각부의 권한·업무·기능을 조정, 통할하는 방식을 취하고 있다.

이병석법안의 경우 테러통합대응센터의 장은 테러단체 구성원 또는 테러기도 · 지원자로 의심할 만한 상당한 이유가 있는 자에 대하여 정보수집 · 조사 및 테러우려인물에 대한 출입국 규제 · 외국환거래 정지 요청 및 통신이용 관련 정보를 수집할 수 있도록 하고 있다(법안 제16조). 심지어 상임위원회 위원장은 테러를 선전 · 선동하는 글 또는 그림, 상징적 표현이나 테러에 이용될 수 있는 폭발물 등 위험물 제조법이 인터넷 등을 통해 유포될 경우 관계기관의 장에 긴급 삭제 등 협조를 요청할 수 있도록 하고 있다(법안 제23조). 또한 테러통합대응센터의 장은 외국인테러전투원으로 출국하려한다고 의심할만한 상당한 이유가 있는 내·외국인에 대하여 일시 출국금지를 법무부장관에게 요청할 수 있다(법안 제26조).

테러방지법안은 국가정보원에 구성되는 대테러센터를 중심으로 위로는 행정각부의 장에 대한 조정·통할기능과 아래로는 대테러대책기구에 대한 조정·통할의 기능이라는 이중적인 수준에서 대테러센터가 관여할 수 있는 여지를 확보한다. 테러방지법안에는 테러 방지를 빌미로 하여 국가정보원이 국가권력의 중심부에 똬리를 틀고자 하는 목적만이 존재한다는 비판이 있는 이유이다. 이런 의혹을 불식하고자 한다면 테러에 대응하기 위하여 설립하겠다는 '국가대테러대책회의', '대테러센터', '대테러대책본부' 등의 기구에 대해서 다음과 같은 질문에 답할 수 있어야 한다.

첫째, 과연 기존의 국가기구, 즉 행정자치부, 경찰청, 법무부, 검찰, 국가정보원 등은 테러방지법안이 예정하고 있는 테러에 대응할 능력이 없는가? 대테러 대응역량에 대한 조직 진단을 해보았는가? 가끔씩 언론을 통해 공개했던 대테러훈련은 무용지물인가?

둘째, 현재의 대테러 대응기구들이 대테러 대응능력이 없다면, 그 막강한 권력을 가진 기구들의 무능력은 도대체 어디에서 기인하는가? 당해 기구의 권한과 조직을 변화시킴으로써 감당할 수 없을 정도로 무능한 것인가?

셋째, 테러에 대응하기 위해 국가정보원을 중심으로 전혀 새로운 대테러 조직을 짜야 한다면, 미국처럼 별도의 행정각부로서 국토안보부를 설치하여 국무총리의 통할 아래 모든 정보기관을 통합 또는 재배치하는 근본적인 정부조직 변화를 꾀해야 하는 것은 아닌가?

마지막으로 국민들이 국가정보원을 신뢰하고 있지 않음을 고려하여 국가정보원을

해외정보기관, 사이버정보기관, 대북정보기관으로 분리하고, 대테러 정보 업무를 공유하도록 하는 방안을 꾀할 수는 없는 것인가? 사람들은 유신독재 회귀를 말하고 있는데, 대통령에 대해서만 책임을 지며 다른 어떤 기관에 의한 통제도 불가능한 국가정보원장에게 국가대테러대책회의와 대테러센터를 실질적으로 혹은 법적으로 관할하게 하는 것이 과연 바람직한가? 국가정보원장이 대테러 기능을 매개로 하여 여타의 국가행정각부를 사실상 통할하는, 권력분립의 예외적 현상을 야기할 수 있다는 의문에 대해 어떻게 답할 것인가? 그럼에도 불구하고 아무런 응답도 없이 테러방지법만 만들면 된다는 식의 독재 국가적 태도는 무엇 때문인가?

사실 테러방지법안은 과거 독재 정권 못지않게 '제왕적 대통령'의 권력을 강화하는 내용을 담고 있다. 국가정보원은 대통령 직속기관이기 때문이다. 더욱이 테러방지법안은 경우에 따라서 대책회의의 장이 대통령을 경유하여 군 병력을 동원할 수 있도록 하고 있다. 하지만 이러한 군 병력의 동원 체제는 헌법 위반의 혐의가 있을 뿐 아니라 조직법상으로도 이중적 낭비이다. 헌법은 전시·사변 또는 이에 준하는 국가비상사태에 한하여 병력으로 군사상의 필요에 응하거나 공공의 안녕질서를 유지할 수 있기 때문이다(헌법 제77조). 즉 헌법은 계엄을 선포한 경우에 한해서만 군 병력을 동원할 수 있도록 허용하고 있다. 군복을 입지 않은 민간인에 의한 군사독재의 부활 또는 평시 군사독재 아니냐는 의심을 벗기 어렵다.

5. 국가안보보다 인간안보로 접근해야 한다

각국에서 다투어 제정한 반테러법이 비밀정보기관을 비밀경찰로 바꾸는 데 일조하는 법이라는 평가도 있다. 국가정보원은 수사권을 가지고 있기 때문에 이미 비밀경찰체제이라는 주장도 있다. 그렇기 때문에 테러방지법 제정이 결국은 무수히 많은 인권침해사건을 일으킨 국가정보원이 권력의 중심에 서고자 하는 프로젝트라는 의견이 지배적이다.

많은 사람들의 인명피해를 초래할 수 있는 범죄행위를 막고자 한다면, 기존의 범죄대응 체계를 점검하는 일부터 시작해야 한다. 경찰과 검찰 등 관련 기관들의 책임을 묻는 국정조사를 진행해야 한다. 대통령은 테러 관련 법 제정을 요청하기 이전에 정부의 수반으로서 현재의 대테러 체계가 부실한 까닭에 대해 책임을 져야 한다. 대응능력 부재의 원인을 제대로 진단해야 올바른 해법을 낼 수 있다. 기존 대응체계의 무능력이 명백하게 드러나는 경우에 한하여 테러방지법을 제정하는 일이 설득력을 가질

것이다.

그러나 그렇다고 대테러 담당의 중심 역할을 국가정보원이 맡는 것은 헌법적으로 인정하기 어렵다. 무엇보다도 국가정보원의 수사권한을 제거해야 한다. 국가정보원을 순수 정보수집기관으로 바꾸고 해외정보수집기관과 국내정보수집기관을 분리하는 것을 전제로 해야 한다. 그 이후에 '테러'를 방지하고 대응하는 체계를 다시 만드는 일을 할 수 있다.

1994년에 유엔은 '인간안보'(human security)라는 새로운 개념을 통해 세계화와 공공재의 민영화로 인해 점증하는 사회적, 개인적 삶에서의 불안정에 대응하는 방법을 제시했다. 테러가 왜 발생하는지에 대해 한번이라도 진지하게 생각해 본 사람이라면 따라서 이제는 국가안보(national security)에서 인간안보로 정책의 초점을 옮겨야한다는 주장에 공감할 것이다.

오늘날 우리는 조그마한 사건으로도 큰 재앙에 직면할 수 있는 고도기술사회에서 살고 있다. 대도시들은 '테러'와 그에 준하는 사태가 발생하면 걷잡을 수 없는 혼란에 빠지게 될 것이다. 테러방지법에 반대한다고 해서 세월호 참사와 같은 재난에 대해 무관심한 것은 절대 아니다. 테러방지법과 같은 방식의 대처에 반대한다는 뜻이지 만약의 위험을 예방하고 대처하는 자세는 절대적으로 필요하다.

전문가들은 그 어떠한 테러방지법을 동원하더라도 '자살테러'는 막을 수 없을 것으로 본다. 9·11 테러는 현대와 같은 고도의 발전된 위험사회가 얼마나 위험한가 하는 것을 분명하게 보여주었다. 어떤 사회도 위험과 폭력으로부터 100% 안전할 수는 없다. 절대적 안전을 내세우면서 그것을 달성하기 위한 국가의 권한확대를 시도한다면 이는 국민을 우롱하는 일이자 국민과 인권에 대한 위협이 될 것이다.

그러므로 다른 방식으로 접근해야 한다. 한국 사회의 실정을 고려한다면 광범위한 재난예방 및 재난구조체계를 구축하는 것이 무엇보다도 필요하다. 고도기술사회가 갖고 있는 그 자체의 위험에 대처하기 위해 국가의 예산을 어디에 쓸 것인가 하는 부분은 매우 중요한 정책적인 판단이다. 시간과 돈과 인력을 적절하고 필요한 부분에 균형 있게 투입할 수 있는 지혜를 모아야 한다. 〈4·16세월호참사 특별조사위원회〉가 세월호 참사의 진상과 원인을 규명하고 세월호 참사에 대처하지 못한 국가 무능력을 진단·평가하며, 국회와 함께 대형재난에 대한 예방 및 대응 체계를 마련한 입법 활동을 하는 과정에서 우리는 테러에 대한 해법도 어느 정도는 찾을 수 있을 것이라고 믿는다.

〈참고문헌〉

민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동공간 '활', 인권운동사랑방, 진보네트워크센터, 참여연대(2015). 테러방지법에 대한 시민사회단체 의견서. 2015. 11. 30.

이계수·오동석·오병두(2006). 테러대응법령과 기구에 대한 비교연구. 치안논총 22, 454－599.

뉴스1 2011. 12. 18. "이라크전 공식 종료, 9년 전쟁". 〈http://news1.kr/articles/?498883〉 최근검색일: 2015. 12. 6.

오마이뉴스 2007. 6. 27. "당신의 생체 정보가 미-일을 오간다면?". 〈http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0000418991〉 최근검색일: 2015. 4. 30.

오마이뉴스 2011. 12. 18. "마지막 미군, 이라크 철수 완료, 9년 전쟁 '종결'". 〈http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001672350〉 최근검색일: 2015. 12. 6.

위키백과. "대한민국의 자살". 〈https://ko.wikipedia.org/wiki/%EB%8C%80%ED%95%9C%EB%AF%BC%EA%B5%AD%EC%9D%98_%EC%9E%90%EC%82%B4〉 최근검색일: 2015. 12. 6.

사이버테러방지법[7]은 전면적 국가사이버감시법이다

이은우 / 변호사, 정보인권연구소 이사, 진보네트워크센터 운영위원

1. 정보통신서비스의 질, 안정성, 신뢰성을 보장하기 위한 보안관제

가. 사이버공격과 보안관제

정보통신망에는 사이버공격[8]의 위험이 상존한다. 사이버공격은 경제적, 정치적, 사회적 동기 등 다양한 동기에 의해 시도된다. 시스코의 분석에 의하면 2014년에 시스코가 탐지한 것만으로도 매일 450억 건의 이메일이 차단되고, 8천만건의 웹 접속 차단, 6,450건의 파일 탐지, 3,186건의 네트워크 탐지, 5만 건의 네트워크 침입이 탐지되었다고 한다.

사이버공격으로부터 정보통신망을 안전하게 보호하고, 서비스의 질을 유지하고, 신뢰성을 보장하기 위해서는 사이버위협에 적절하게 대응하는 일은 당연히 필요하다.

나. 보안관제 기술 발전과 수집되는 정보의 양과 질

7) 이하 '사이버테러 방지 및 대응에 관한 법률안' 및 '국가 사이버테러 방지에 관한 법률안', '사이버위협정보 공유에 관한 법률안'을 사이버테러방지법으로 총칭한다.

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

정보통신망의 위협을 차단하는 활동을 사이버안전대책[9] 또는 보안관제[10]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 하고, 취약점을 관리해야 한다. 최근에는 보안관제 기술이 비약적으로 발전하여, 트래픽을 모두 저장하고, 거의 실시간으로 이용자의 다운로드 파일을 추출하거나, 패킷 데이터를 분석하기도 한다.

---

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

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

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.[11]

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 솔루션 중 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 확

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

인해 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.

다. 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.

(1) 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

(2) 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 50개

(3) 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

(4) 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

(5) 통합 저장시스템 구축

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

(6) 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

(7) 보안관제센터 기반시설 구축

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

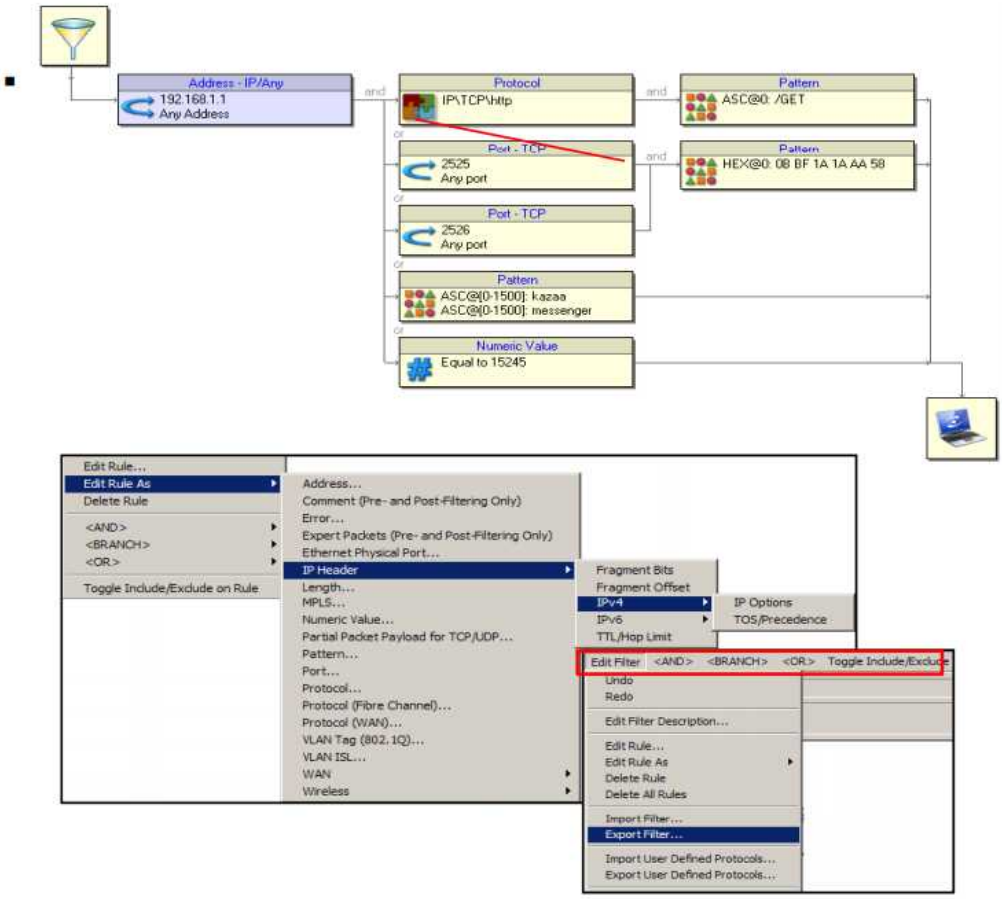
(8) 보안취약점 점검 및 분석

○ 관제대상 기관의 네트워크 및 관련 시스템 취약점 점검 및 분석 수행

○ 보안관제센터 운영을 위한 관제운영 및 침해사고 대응 등 관련 지침 수립 등

라. 보안관제의 악용사례

한편 보안관제가 악용되기도 하는데, 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

앞에서도 보았듯이 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. 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.

나. 보안관제 과정에서 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 솔

루션으로 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 또다시 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 않고, 손쉽게 중앙집중적으로 정보수집이 가능하기 때문에 당사자는 이를 전혀 눈치 챌 수 없는 경우가 대부분일 것이다.

다. 보안관제 서비스 과정에서 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 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 상세하게 파악하고 있다. 따라서 국가정보원이 보안관제 서비스 시스템을 몰래 부당하게 침해하여 감시 프로그램으로 이용하더라도 이를 막거나, 확인하기가 쉽지는 않은 것이다.

3. 우리나라의 정보통신망의 안정성, 신뢰성 보호를 위한 법제 - 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. 정통망법은 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. 반면 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 국가사이

버안전에 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 신뢰성을 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 지킬 것을 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 발생 시에 국가가 갖는 확대된 권한 - 침해 신고의무와 사고의 조사

반면 침해사고가 발생하면 국가가 정보통신망 운영자에 대하여 감독하고 개입하는 권한이 커진다. 침해사고가 발생하는 경우 정보통신망은 정보통신서비스제공자에게 신고의무를 부과한다. 이때 신고의 상대방은 미래창조과학부장관이나 한국인터넷진흥원이 된다(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 원인 분석 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 관련 자료의 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, 이때는 형사소송법이 적용될 것이고, 행정처분을 위한 조사인 경우에는 행정절차법 등이 적용될 것이다.

다. 정보통신기반보호법과 침해사고 대응

(1) 정보통신기반보호법을 제정한 이유

정보통신기반보호법은 주요정보통신기반시설의 보호와 침해사고의 대응을 위해서 2001년에 제정된 법이다. 2001년에 정보통신기반보호법이 제정될 때 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

정보통신기반보호법의 적용대상이 되는 주요정보통신기반시설[12]에는 공공기관에서 운영하는 정보통신망과 주요 민간의 정보통신시설이 포함되어 있다.[13]

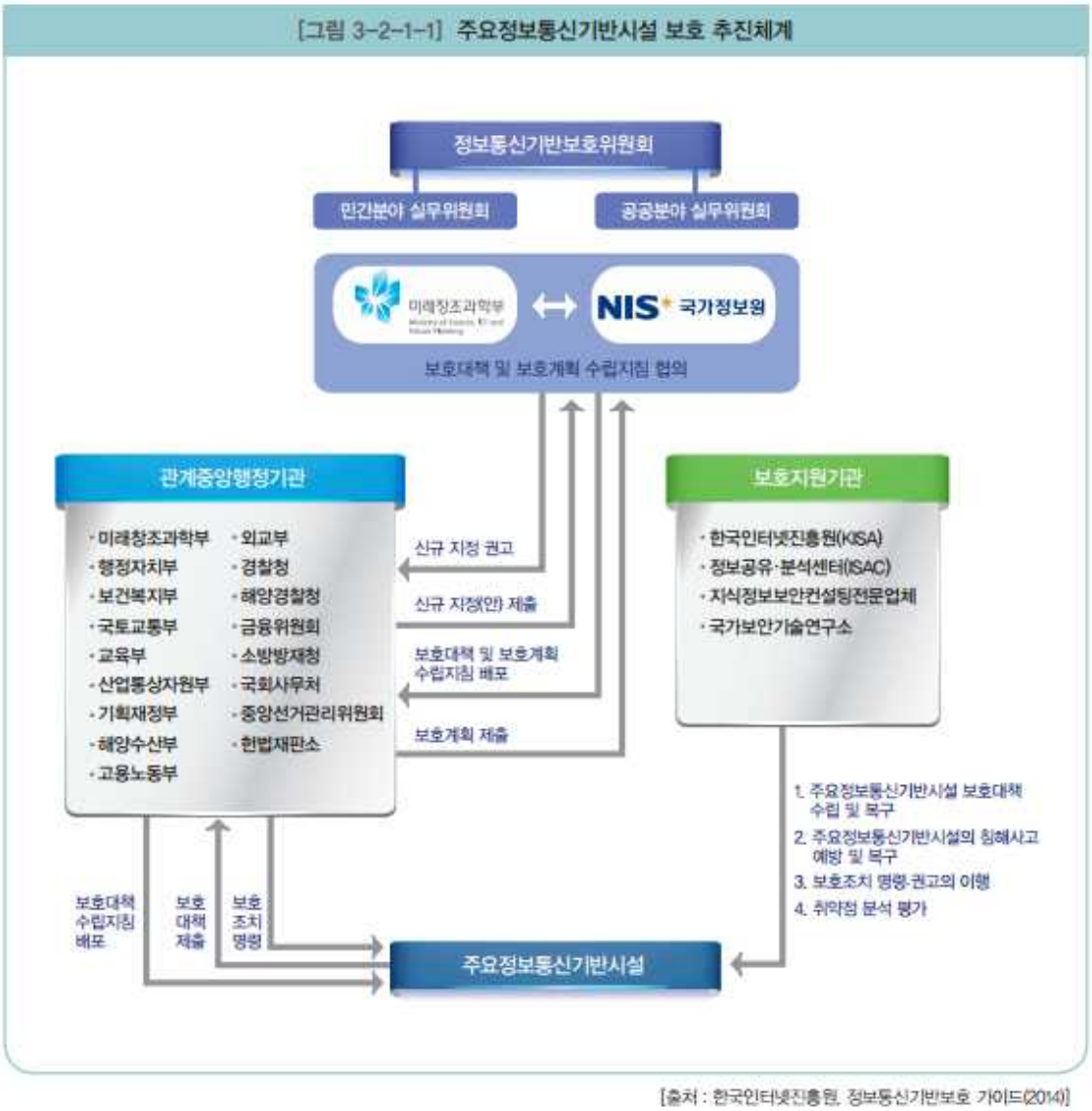
주요정보통신기반시설로는 2014년 12월 현재 정보통신 및 미디어, 금융기관, 교통수송, 에너지, 원자력, 식·용수, 식품의약품관리, 보건복지, 정부기관, 사회안전시설, 건설·환경, 지리정보, 기타 등의 분야에서 17개 관계중앙행정기관, 188개 관리기관, 292개 주요정보통신기반시설이 지정·관리되고 있다고 한다.

한편 시행령은 미래창조과학부장관과 국가정보원장에게 주요정보통신기반시설 지정대상의 선정을 위하여 주요정보통신기반시설 지정조사반을 두고, 각 조사반으로 하여금 자료를 제출받는 등 주요정보통신기반시설 지정 필요성을 검토하게 할 수 있다고

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

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

규정하고 있다. 이런 과정을 거쳐서 미래창조과학부장관과 국정원장은 주요정보통신기반시설로 지정 권고를 할 수 있다.



(출처 : 국가정보보호백서 2015)

(3) 주요정보통신기반시설 보호위원회

정보통신기반보호법은 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 소속하

에 국무조정실장을 위원장으로 하는 정보통신기반보호위원회를 두도록 하고 있다.

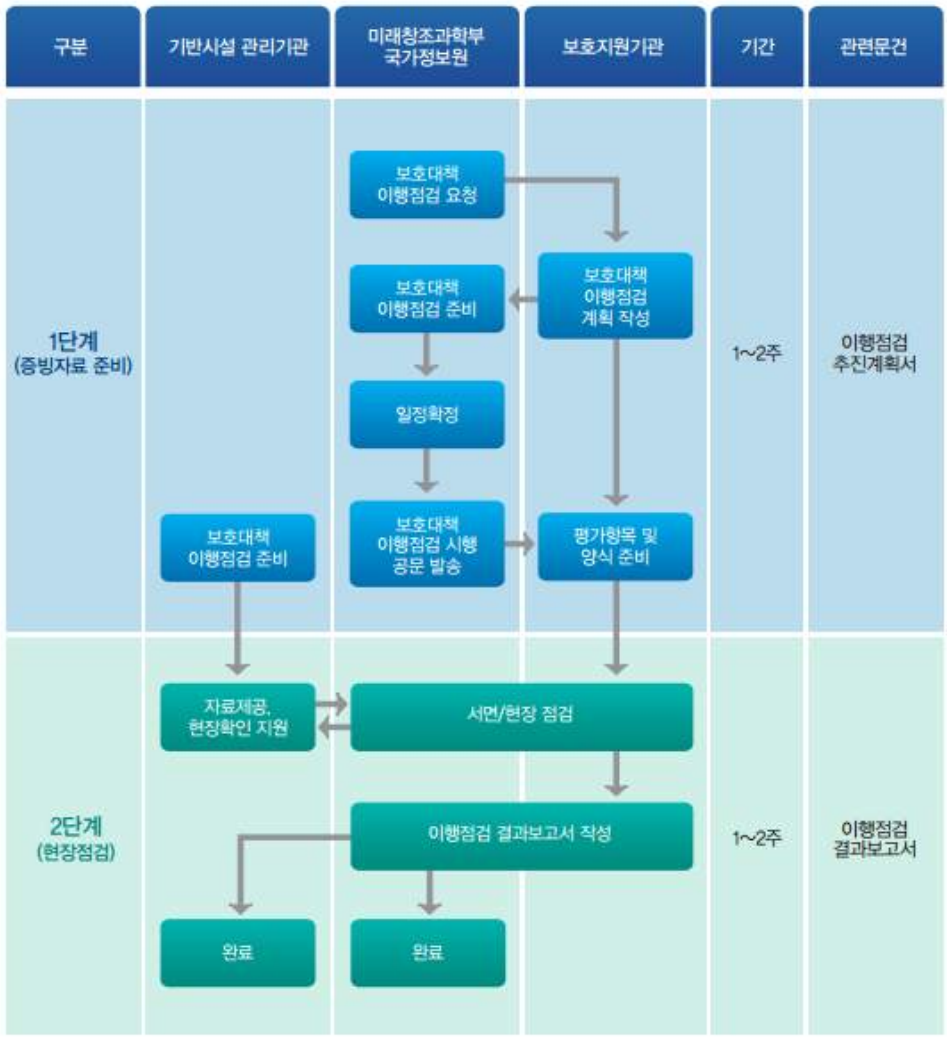
(4) 해당 관리기관장의 보호대책과 중앙행정기관의 보호계획

정보통신기반보호법은 미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설 보호대책 및 주요정보통신기반시설 보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다고 규정하고 있다. 그리고 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("주요정보통신기반시설 보호대책")을 수립·시행할 의무를 부과하고 있다. 관리기관장은 보호대책을 주요정보통신기반시설을 관할하는 관계중앙행정기관의 장에게 제출해야 한다.

(5) 보호대책의 이행여부 확인

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

[그림 3-2-3-2] 주요정보통신기반시설 보호대책 이행점검 절차



[출처 : 한국인터넷진흥원, 정보통신기반보호 가이드(2014)]

(출처 : 국가정보보호백서 2015)

(6) 보호지침, 보호처분

정보통신기반보호법은 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.

(7) 침해사고의 통지

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.

(8) 지원

관리기관의 장이 필요하다고 인정하거나 주요정보통신기반시설 보호위원회 위원장이 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관, 국가정보원장, 국방부장관 기타 전문기관의 장에게 주요정보통신기반시설 보호대책의 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.

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

(9) 정보통신기반보호법에 의한 국정원의 역할

정보통신기반보호법에 의하면 국정원은 (i) 공공기관에서 관리하는 주요정보통신기반시설의 보호대책 및 보호계획의 수립지침을 제정할 수 있는 권한, 취약점 분석·평가에 관한 기준을 미래창조과학부장관과 제정할 권한을 가지고, (ii) 공공분야 주요정보통신기반시설이 보호대책을 제대로 이행하고 있는지를 이행 확인할 수 있는 권한을 가지고(이 과정에서 자료제출 요청, 실지 현장조사 포함하여 보호조치의 세부적인 내용을 확인·점검할 수 있다), (iii) 보호대책의 개선권고와 다음연도 수립지침에 반영, (iv) 공공기관이 관리하는 주요정보통신기반시설의 사전 조사 및 주요정보통신기반시설 지정 권유권 등을 부여하고 있다.

라. 대통령훈령인 국가사이버안전관리규정에 의한 국정원의 권한

(1) 훈령의 적용범위와 효력

한편 대통령훈령으로 국가사이버안전관리규정이 제정되었는데, "국가사이버안전[14]에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다."고 그 제정 목적을 밝히고 있다. 그런데 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 모순이 된다. 왜냐하면 훈령은 국정원장이 국가사이버안전과 관련된 정책 및 관리에 대하여는 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다고 규정하고 있는데, 주요정보통신기반시설이 아닌 공공기관의 정보통신망에 대해서만 국정원장이 그와 같은 권한을 갖는다는 것은 논리적으로 있을 수 없는 논리이기 때문이다. 어쨌든 주요정보통신기반시설에 대해서는 주요정보통신기반시설법에 의하여 주요정보통신기반 보호위원회 위원장(국무총리실장)에게 권한을 부

14) 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.

여하고, 그 외의 공공기관이 운영하는 정보통신망에 대해서는 훈령이 적용된다는 것이다.

(2) 훈령에 의한 국정원장의 권한

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.[15] 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.

반면, 정보통신기반보호법은 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 둔다고 규정하고 있다. 25인 이내의 위원[16]으로 구성되는 기반보호위원회는 국무총리실장이 위원장이 되고, 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 관한 사항, 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항을 심의한다. 사실상 동일한 역할의 위원회가 병존하는 모순적인 구조를 가지고 있다.

이처럼 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.

---

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

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

(3) 국정원의 사이버안전센터

훈령은 국정원에 국가사이버안전센터를 두도록 했는데, 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 목적으로 하다. 사이버안전센터는 국가사이버안전정책의 수립, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가사이버안전매뉴얼의 작성·배포, 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.

마. 국가보안관제업무의 효율적 수행방안의 제안 어디에서도 민간분야에 대한 국정원의 사이버 관할권을 부여하자는 주장은 없었다.

그동안 국가보안관제업무의 효율적 수행방안에 대한 여러 논문에서도 국정원에게 민간분야에 대한 사이버 관할권을 부여하자는 주장은 제시되지 않았었다.

예를 들어 '국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구'(김영진, 이수연, 권헌영, 임종인)[17]도 국가 보안관제업무의 효율적 수행방안으로 (i) 보안관제센터 구축 및 운영기준 표준화, (ii) 보안관제 의무화, (iii) 단계별 중첩 보안관제 실시, (iv) 보안관제정보 공유 제도화, (v) 보안관제역량 제고방안 마련 시행, (vi) 법·제도적 기반 조속마련 필요를 들고 있는데, 여기에서도 보안관제 의무화의 대상으로는 모든 국가·공공기관에 대해 보안관제를 의무화하도록 규정해야 한다고 하여, 국가와 공공기관만을 그 대상으로 하고 있다. 그 이유로 국가·공공기관의 전산망은 상호 연동되어 있으므로 어느 한 기관에서 보안관제를 철저히 하여 사이버 위협을 탐지, 차단한다고 하더라도 다른 기관의 전산망이 보안취약으로 사이버공격을 당하거나 악성코드에 감염될 경우 안전성을 보장하기는 어렵다는 점을 들고 있다. 그래서 국가 전체 전산망의 안전성을 높이기 위해서는 헌법, 사법, 입법기관을 포함한 모든 국가·공공기관 및 지방자치단체의 정보통신망에 대하여 보안관제를 의무적으로 실시하도록 하여 국가차원에서 체계적으로 사이버공격을 탐지, 차단하여야 한다고 주장하였다.

---

17) 정보보호학회논문지(2009. 2)

4. 현행법령상 국정원은 사이버침해 사고의 조사 및 복구 지원 업무를 수행할 수 있는가?

가. 정보통신기반보호법과 국가사이버안전규정에 의한 국정원의 권한

정보통신기반보호법에 의하면 국정원은 공공기관에서 관리하는 주요정보통신기반시설의 보호대책 및 보호계획의 수립지침을 제정할 수 있는 권한을 가지고, 공공분야 주요정보통신기반시설이 보호대책을 제대로 이행하고 있는지를 이행 확인할 수 있는 권한을 가지고 있다. 이 과정에서 자료제출 요청, 실지 현장조사 포함하여 보호조치의 세부적인 내용을 확인·점검할 수 있고, 문제점이 발견되는 경우에는 보호대책의 개선 권고를 할 수도 있고, 다음연도 수립지침에 반영할 수도 있다.

한편 관리기관의 장이 필요하다고 인정하거나 주요정보통신기반시설 보호위원회 위원장이 보완을 명하는 경우 주요정보통신기반시설 보호대책의 수립, 주요정보통신기반시설의 침해사고 예방 및 복구, 보호조치 명령·권고의 이행 지원을 할 수 있다.

공공부문의 주요정보통신기반시설에 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 국정원, 수사기관 또는 인터넷진흥원에 그 사실을 통지하여야 한다. 이때 국정원은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취할 수도 있다.

그런데 민간부문의 경우는 도로·철도·지하철·공항·항만 등 주요 교통시설, 전력, 가스, 석유 등 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설의 경우 외에는 침해사고의 통지, 침해사고의 조사, 보호대책의 이행여부의 확인 등을 할 수 없다. 그리고 국정원은 금융정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 안된다.

나. 국정원법

한편 국정원법은 국정원의 직무를 국외 정보 및 국내 보안정보[대공, 대정부전복, 방첩, 대테러 및 국제범죄조직]의 수집·작성 및 배포, 형법 중 내란의 죄, 외환의 죄, 군형법 중 반란의 죄, 암호 부정사용의 죄, 군사기밀 보호법에 규정된 죄, 국가보안법

에 규정된 죄에 대한 수사, 정보 및 보안 업무의 기획·조정으로 들고 있다.

이에 의하면 국정원이 사이버안전에 대한 업무를 수행하는 것은 엄격하게 국가안보와 관련되는 것으로 국한해야 하고, 특히 민간부문의 정보통신망에 대해서는 수사권 등을 갖는 것은 엄격하게 금지되어야 한다.

5. ‘사이버테러방지법’은 국정원에게 어떤 권한을 부여하는가?

가. ‘사이버테러’ 또는 ‘사이버위협정보’는 정보통신망법의 위법행위보다도 더 넓은 개념이다

현재 제안된 사이버테러방지법은 ‘사이버테러는 전자적 수단에 의해 정보통신시설을 침입 또는 교란 또는 마비 또는 파괴하는 행위나, 정보를 절취, 훼손, 왜곡 전파하는 등 모든 공격행위를 말한다’고 하여, ‘정보통신’에서의 모든 공격행위를 ‘사이버테러’로 규정하고 있다.

그런데 이와 같은 규정은 정통망법의 정보통신망 침해행위보다도 더 넓은 개념이다. 예를 들어 ‘교란’이라는 의미는 불명확하며, 정보통신망법은 정보의 훼손, 멸실, 변경, 위조와 관련해서도 이를 목적으로 한 악성프로그램(정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램)을 전달 또는 유포하는 것만을 금지하고 있는데, 사이버테러방지법은 정보의 절취, 훼손, 왜곡전파를 모두 사이버테러로 규정하고 있다. 그리고 정보의 ‘왜곡전파’도 ‘사이버테러’로 규정하고 있는데, 이는 긴급조치 제9호에서 ‘유언비어를 날조, 유포하거나 사실을 왜곡하여 전파하는 행위’를 금지행위로 하여 처벌하였던 것에 비견되는 것이다.

[사이버테러 방지 및 대응에 관한 법률안과 정보통신망법의 비교]

구분	사이버테러 방지 및 대응에 관한 법률안	정보통신망법
내용	해킹·컴퓨터 바이러스·서비스 방해·전자기파 등 **전자적 수단**에 의하여 **정보통신시설**을 **침입·교란·마비·파괴하거나**	정보통신망법 제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

	정보를 절취·훼손·왜곡전파하는 등 모든 공격행위	② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다. ③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

[사이버테러 방지 및 대응에 관한 법률안과 형법의 비교]

구분	사이버테러 방지 및 대응에 관한 법률안	형법
내용	해킹·컴퓨터 바이러스·서비스 방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 절취·훼손·왜곡전파하는 등 모든 공격행위	형법 제314조 ②컴퓨터등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여사람의 업무를 방해한 자도 제1항의 형과 같다.

나. 침해사고 대응행위와 대비되는 제한이 없는 사이버안전

사이버테러방지법은 사이버테러로부터 정보통신시설과 정보를 보호하기 위해 수행하는 관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동을 사이버안전이라고 규정하면서 대응의 범위를 광범위하게 하고 있다. 즉, 정보통신시설과 정보를 보호하기 위한 모든 활동이 사이버안전이라는 것이다. 이는 기존의 정보통신망법이 미래창조과학부장관의 침해사고 대응행위를 침해사고 정보 수집, 긴급조치, 침해사고 관련정보 보고를 받는 것으로 한정한 것과 대조적이다.

구분	사이버테러 방지 및 대응에 관한 법률안의 사이버안전	정보통신망법의 침해사고 대응행위내용
내용	“사이버안전”이란 사이버테러로부터 정보통신시설과 정보를 보호하기 위하여 수행하는 관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함.	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

다. 사이버테러방지법안과 사이버위협정보공유법안이 창설하는 국가정보원의 새로운 직무

사이버테러방지법안	사이버위협정보공유법안
- 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련정보를 상호 공유하기 위하여 민·관 협의체를 구성·운영할 수 있음(안 제6조). - 국가정보원장은 사이버테러 방지 및 대응관련 기본계획을 수립하고, 이에 따라 중앙행정기관의 장은 사이버테러 방지 및 대응관련 시행계획을 작성하여 책임기관의 장에게 배포하여야 함(안 제8조). - 사이버테러에 대한 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 사이버안전	- 국정원장은 국가안보실장, 미래창조과학부 장관 등과 협의하여 범정부 차원에서 사이버위협정보를 공유하기 위한 방법과 절차를 마련함(안 제4조). - 국가의 주요 정보와 정보통신망을 관리하는 기관(이하 “사이버위협정보 공유기관”)은 사이버위협정보를 수집하고 상호 공유하여야 함(안 제4조). - 사이버위협정보 공유를 효율적으로 수행하기 위하여 국정원장 소속으로 사이버위협정보 공유센터(이하 “공유센터”)를 설치·운영함(제5조). - 공유센터의 장은 공유된 사이버위협

센터를 둠(안 제10조). - 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제14조). - 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 피해가 중대할 경우 관계 중앙행정기관의 장 및 국가정보원장에게 그 결과를 통보하여야 함(안 제15조). - 국가정보원장은 사이버테러에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취해야 함(안 제17조)	정보를 종합 분석하고 결과를 사이버위협정보 공유기관 및 관련 업체에게 제공하여야 함(안 제6조). - 국정원장은 법무부 장관 등 국가기관 및 전문가가 참여하는 협의회를 구성하여 사이버위협 정보의 남용방지 대책을 수립하여야 함(안 제7조). - 사이버위협정보를 보유한 사람은 공유센터의 장에게 신고하거나, 공유센터의 장이 사이버위협정보의 제공을 요청할 수 있음(안 제8조). - 공유센터의 장은 사이버위협정보 공유 활동에 대한 결과를 평가하고 그 결과를 국회에 보고하여야 함(안 제9조).

라. 국가정보원은 사이버안전센터를 통해서 우리나라 사이버범죄 예방과 대응의 사령탑을 넘어서서 사이버사찰의 권한을 갖는다.

(1) 사이버안전센터를 통한 정책의 수립과 집행권한을 갖는 경우 국정원은 사이버 사찰 능력을 갖출 수 있다

사이버테러방지법에 의하면 국가정보원에 신설하는 사이버안전센터(사이버위협정보 공유센터)는 사실상 모든 일을 할 수 있다.

제10조(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, 이는 사실상 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.

참고로 기존의 정보통신망법에 의하면 침해사고 대응 업무를 수행하는 미래창조과학부장관(한국인터넷진흥원)의 업무는 아래와 같이 제한적인데 반해서 국정원이 사이버안전센터를 통해서 갖는 권한은 훨씬 더 포괄적이라는 것을 알 수 있다.

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 침

해사고의 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.

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.

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

반면, 미래창조과학부장관은 침해사고의 원인 분석 등의 업무도 아래와 같이 제한적

으로 규정하고 있다.

> 제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다.
>
> ② 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.
>
> ③ 미래창조과학부장관은 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.
>
> ④ 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.
>
> ⑤ 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.
>
> ⑥ 제2항에 따른 민·관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.

(2) 정보통신시설의 안전을 유지할 책임을 근거로 국정원은 민간기업에 대한 예비적인 보안관제를 통해서 정보수집과 사찰이 가능하다

한편 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 광범위

한 정보수집과 사찰을 할 수 있게 된다.

(3) 국정원은 민간기업에 대해서도 사이버 침해에 대한 수사권을 갖게 되고, 이를 통해서 부적절한 정보수집을 시도할 수도 있다

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

> 제15조(사고조사) ① 중앙행정기관의 장은 사이버테러로 인하여 소관분야에 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하고, 피해가 중대하거나 확산될 우려가 있는 경우 즉시 관계 중앙행정기관의 장 및 국가정보원장에게 그 결과를 통보하여야 한다.
>
> ② 국가정보원장은 제1항에도 불구하고 국가안보 및 이익에 중대한 영향이 미친다고 판단되는 경우 관계 중앙행정기관의 장과 협의하여 직접 그 사고조사를 실시할 수 있다.
>
> 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.
>
> ④국가정보원장은 사이버테러를 저지른 자에게 범죄혐의가 있다고 판단되고, 그를 사이버테러단체의 구성원으로 의심할 만한 상당한 이유가 있는 경우에는 그에 대한 출입국관리기록·금융거래정보 및 통신사실 확인자료의 제공을 관계 기관 및 단체에 요청할 수 있다.
>
> ⑤ 제4항에 따른 출입국관리기록·금융거래정보 및 통신사실 확인자료의 제공에 관한 구체적인 절차 등에 관하여는 「출입국관리법」·「특정 금융거래정보의 보고 및 이용 등에 관한 법률」·「통신비밀보호법」에 따른다.
>
> ⑥ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사이버테러와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

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

마. 국정원의 보안관제센터는 민간분야에 대한 상시감시기구로 운영될 수 있다

국정원은 사이버테러방지법에 의하여 민간분야까지 아우르는 통합적인 보안관제센터를 운영할 수 있게 되는데, 이는 국정원이 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.

제14조(보안관제센터 등의 설치) ① 책임기관의 장은 사이버테러 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축·운영하거나 다음 각 호의 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 한다. 다만, 「정보통신기반 보호법」 제16조에 따른 정보공유·분석센터는 보안관제센터로 본다.

1. 관계 중앙행정기관

2. 국가정보원

3. 제2조제1항제8호바목의 보안관제전문업체

② 책임기관의 장은 제1항에 따른 사이버테러 정보와 정보통신망·소프트웨어의 취약점 등의 정보(이하 “사이버위협정보”라 한다)를 관계 중앙행정기관의 장 및 국가정보원장과 공유하여야 한다.

③ 국가정보원장은 제2항의 사이버위협정보의 효율적인 관리 및 활용을 위하여 관계기관의 장과 공동으로 사이버위협정보통합공유체계를 구축·운영할 수 있다.

④ 누구든지 제2항에 따라 공유하는 정보에 대하여는 사이버위기관리를 위하여 필요한 업무범위에 한하여 정당하게 사용 관리하여야 한다.

⑤ 제1항에 따른 보안관제센터와 제3항에 따른 사이버위협정보통합공유체계 구축·운영 및 정보 관리에 관한 사항과 제2항에 따른 사이버테러 정보의 공유에 관한 범위·절차·방법 등에 관한 사항은 대통령령으로 정한다.

바. 과연 사이버테러라는 규정은 적절한가? 사이버테러라는 규정으로 국가정보원의 직무를 넓히지 않으면 안될 필요가 있는가?

사이버테러라는 것은 국정원법의 대테러 업무의 범위로 포괄할 수 있는 '테러'로 보기 어려운 개념이다. 실제로 이는 대체로 사이버 안전(cyber security)이라는 규정으로 사용되고 있으며, 이를 국가정보기관에서 담당하는 것은 매우 위험하기 짝이 없다. 게다가 국가안보와 관련되는 사이버위협에 대해서는 현재의 정보통신기반보호법이나 국가정보원법으로도 충분하다. 사이버테러방지법이나 사이버위협정보공유법의 사이버테러나 사이버위협이라는 규정은 국가정보원의 직무범위를 정하는 것이기 때문에 엄격하게 규율해야 한다.

6. 세 가지 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.

7. 결론

이상으로 본 바와 같이 현재의 규율체계로도 우리나라의 법제상 사이버 안전을 보장하는 데는 아무런 지장이 없다. 오히려 국정원은 불확실한 법적 근거를 바탕으로 국가안보와 관련된 범위를 넘어서 사이버 위험과 관련된 부문에 그 업무영역을 소리 없이 넓혀 왔었다. 정보통신망의 특성에 비추어 현재 국정원의 사이버에 대한 관할권도 이를 민주적으로 통제하는 것이 아주 어려운 상태다.

이런 상황에서 사이버테러방지법은 국정원이 사이버 분야에서 민간 감시의 합법적 권한을 갖기 위한 시도이며, 가장 위험스러운 법안이라고 볼 수 있다. 사이버테러나 사이버위협이라는 명목으로 정보통신망에 대한 정부의 관여가 이루어지는 것도 사생활 침해, 국가감시의 우려가 제기되고 있는 실정인데, 이를 국정원이 수행한다는 것은 민주국가에서는 도저히 용납될 수 없는 것이다.