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[9]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

9) 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.



주요정보통신기반 보호위원회 위원장(국무총리실장)에게 권한을 부여하고, 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.[10] 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[11]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.

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

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

이처럼 정보통신기반보호법은 국무조정실장에게 주요정보통신기반시설에 관한 보호계획의 종합, 조정, 제도 개선 등에 관하여 권한을 부여하고 있는데, 훈령은 편법적으로 국정원장에게 그 권한을 옮겨버린 것이다. 이는 법률과 모순된다.

(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)[12]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 전산망

12) 정보보호학회논문지(2009. 2)



이 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.

## 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 이행확인할 수 있는 권한을 가지고 있다. 이 과정에서 자료제출 요청, 실지 현장조사 포함하여 보호조치의 세부적인 내용을 확인 · 점검할 수 있고, 문제점이 발견되는 경우 보호대책의 개선권고를 할 수 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 등

을 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, 국가보안법에 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 위법행위보다 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 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 절취·훼손·왜곡전파하는 등 모든 공격행위 | 정보통신망법 제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.<br>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.<br>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<br>②컴퓨터등 정보처리장치 또는 전자기록 등 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.<br>1. 침해사고에 관한 정보의 수집·전파<br>2. 침해사고의 예보·경보<br>3. 침해사고에 대한 긴급조치<br>4. 그 밖에 대통령령으로 정하는 침해사고 대응조치 |

## 다. 사이버테러방지법안과 사이버위협정보공유법안이 창설하는 국가정보원의 새로운 직무

| 구분 | 사이버테러 방지 및 대응에 관한 법률안의 사이버안전 | 사이버위협정보공유법안 |
|---|---|---|
| 내용 | - 국가정보원장은 사이버위기를 효율적으로 관리하고 사이버공격 관련정보를 상호 공유하기 위하여 민 관 협의체를 구성 운영할 수 있음(안 제6조). | - 국정원장은 국가안보실장, 미래창조과학부 장관 등과 협의하여 범정부 차원에서 사이버위협정보를 공유하기 위한 방법과 절차를 마련함(안 제4조). |



| | | |
|---|---|---|
| 내용 | - 국가정보원장은 사이버테러 방지 및 대응관련 기본계획을 수립하고, 이에 따라 중앙행정기관의 장은 사이버테러 방지 및 대응관련 시행계획을 작성하여 책임기관의 장에게 배포하여야 함(안 제8조).<br>- 사이버테러에 대한 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 사이버안전센터를 둠(안 제10조).<br>- 책임기관의 장은 사이버공격 정보를 탐지 분석하여 즉시 대응할 수 있는 보안관제센터를 구축 운영하거나 다른 기관이 구축 운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제14조).<br>- 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 피해가 중대할 경우 관계 중앙행정기관의 장 및 국가정보원장에게 그 결과를 통보하여야 함(안 제15조).<br>- 국가정보원장은 사이버테러에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취해야 함(안 제17조) | - 국가의 주요 정보와 정보통신망을 관리하는 기관(이하 "사이버위협정보공유기관")은 사이버위협정보를 수집하고 상호 공유하여야 함(안 제4조).<br>- 사이버위협정보 공유를 효율적으로 수행하기 위하여 국정원장 소속으로 사이버위협정보 공유센터(이하 "공유센터")를 설치 · 운영함(제5조).<br>- 공유센터의 장은 공유된 사이버위협정보를 종합 분석하고 결과를 사이버위협정보 공유기관 및 관련 업체에게 제공하여야 함(안 제6조).<br>- 국정원장은 법무부 장관 등 국가기관 및 전문가가 참여하는 협의회를 구성하여 사이버위협 정보의 남용방지 대책을 수립하여야 함(안 제7조).<br>- 사이버위협정보를 보유한 사람은 공유센터의 장에게 신고하거나, 공유센터의 장이 사이버위협정보의 제공을 요청할 수 있음(안 제8조).<br>- 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(사이버위협정보공유센터)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 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.

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

반면, 미래창조과학부장관은 침해사고의 원인 분석 등의 업무도 아래와 같이 제한적으로 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 광범위한 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.
> 국가정보원장은 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 관

> 한 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. ❑

# 토론문

정재원[1]

○ 지난 정권에 이어 최근 몇 년 동안의 추세로 볼 때, '민주 대 반민주(혹은 독재)' 구도에서 '진보 대 보수' 구도로의 전환이라는 지식인 사회의 주장에 대해 의구심을 가져야 될 정도로 심각한 민주주의의 후퇴가 일어나고 있는데, 이 법안은 그러한 후퇴의 결정판이라고 할 수 있음. 국정원의 권력 강화를 기도하는 이 법안은 대선 개입 등 그 어떤 위법 행위에 대해서도 책임을 지지 않고 있는 현 상황 속에서 절대로 통과시켜서는 안 되는 반민주 악법임.

○ 성매매방지법처럼 해당 법으로도 충분히 단속할 수 있고, 실제로 그래야 하는 영역에 대해서는 막상 법의 집행에 대해 방조하거나 방치하고 있는데 반해서 정반대로 철저하고도 집요하게 법 제정 및 법 적용, 집행에 대해 욕심을 내는 것으로 미루어 볼 때, 이 법안 제정의 목적은 분명 테러 방지가 아닌 국정원 권력 강화를 통한 민중에 대한 통제 강화 등에 있음.

○ 법리 문제나 법이 가져올 문제에 대해서는 다른 토론자들이 더 자세히 논의할 것이므로 본 토론자는 사실상 국정원의 무소불위의 권력을 확대하고 인권

1) 국민대 국제학부(사회학), 민교협 정책위원

과 민주주의 탄압의 도구로 쓰일 수 있는 이 법을 제정하고자 하는 세력에 대해 다소 추상적이지만 거시적인 관점에서 지적하고자 함.

○ 우선 테러위험인물에 대한 정의와 이들에 대한 정보수집, 외국인테러전투원에 대한 정의, 대테러조사의 내용, 테러취약요인 사전 제거의 개념, 사이버 테러의 정의 등 무수한 부분에 있어서 그 범위의 모호함으로 인해 심각한 인권 침해가 예상된다고 할 수 있음.

○ 특히 지상파 방송과 신문 등 주요 언론들이 장악되어 있는 상태에서 유일하게 시민들의 저항의 공간이자 소통의 공간이 되고 있는 인터넷 언론이나 SNS 마저 통제함으로써 민주적인 공론장을 분쇄시키려는 시도에서 제안된 사이버 테러 방지법안은 사실상 사이버 탄압법이며 매우 위협적인 법이라고 할 수 있음

○ 구체적으로는 과거 용산 참사 직전 용산 철거민들에 대해 '도심 속의 테러리스트'라고 칭했던 한 여당 의원의 표현처럼 향후 야당과 노동단체, 시민사회단체는 물론 일반 서민들에게까지도 정부와 기업의 횡포에 맞선 정당한 항의 행동에 대해 테러리스트라는 혐의를 씌울 수 있다고 판단됨. 대추리 미군 기지 이전 반대 운동이나 제주 강정 해군기지 반대 운동, 밀양 송전탑 반대 운동과 같은 경우에도 유사한 혐의를 씌울 수도 있으며, 향후 있을 수 있는 저항 운동에 대해서 이러한 법의 악용은 충분히 예상됨.

○ 또한 이 법안을 악용하여 이주노동자 운동이나 북한 이탈 주민, 심지어는 중국 조선족 동포들에 대한 통제와 관리, 탄압 등을 자행할 수 있으며, 필요에 따라서는 조작을 통해 간첩은 물론 테러리스트 조직 적발 등의 방법으로 기존의 종북론으로 모든 것을 희석화시키고 젊은 극우보수층을 획득함으로써 재미를 보았던 지배 방식과 똑같은 효과를 노리며 권력 연장을 위해 사용될 수 있는 위험성이 있음.

○ 지난 민중총궐기 당시 왜 10만이 넘는 사람들이 시위에 참가했는지에 대한 본질은 사라지고 폭력/비폭력 여부가 중요한 것으로 여겨지게 만드는 등의



사례에서 보듯, 언론이 장악되어 있는 상황에서 프레임 전쟁에서 완전히 밀려 있는 상태에서 조작에 의한 혹은 실제 테러가 발생할 시 합리적인 반박이 불가능해지면서 테러방지법에 반대하는 진영의 정당한 논리가 순식간에 무력화될 수 있다는 점을 간과해서는 안 됨.

○ IS의 잔혹한 행위들이 수년간 이어져 왔고 그에 이어 파리 테러가 일어났을 때보다도 한국 내 인도네시아인이 이슬람 근본주의 조직(알 누스라)에 충성한 일로 추방되었다거나 시리아 현지에서 사망한 IS 조직원의 유품에서 한국어로 된 카드 등이 발견된 사건 하나로 한국 사회에서 훨씬 강한 테러에 대한 우려가 일어난 바 있는데, 이에서 보듯 프레임 전쟁에서 테러방지법을 반대하는 진영이 마치 안이한 생각을 가진 집단으로 비추어지지 않게 하기 위한 치밀한 대응이 필요함.

○ 따라서 효과적인 대응을 위해서는 미국판 테러방지법이라고 할 수 있는 '애국법'으로 인한 민주주의와 인권에 대한 탄압의 사례는 물론, 세계 곳곳에서의 소위 테러방지법과 유사한 법 제정 이후 테러는 방지하지 못 하고, 예외 없이 독재 정권 유지를 위한 민주주의와 인권 탄압을 위한 도구로 쓰였다는 사실 등을 구체적으로 제시할 필요가 있음. 이를 위해서는 기존의 독재 국가나 이슬람 지역 국가들 외에도 소위 민주적인 국가들에서도 유사한 법안이 테러는 방지하지 못 하고 인권 탄압의 도구로 쓰였다는 사례들이 풍부하게 밝혀질 필요가 있음

○ 또한 정당 정치, 선거 정치, 의회 정치의 뒤에서 숨어 그 이면에서 작동하는 관료 지배, 그리고 이들과 학맥, 지연 등으로 얽혀 있으면서 이들을 통해 자신들의 이익을 관철시키고 있는 특권과 탐욕을 위한 우리 사회의 실질적 지배 구조에 대한 인식을 새롭게 할 필요가 있음.

○ 과거 정권은 교체되었으나 전혀 개혁되지 않았던 각종 관료 기구들을 상기해 볼 때, 현재의 갑작스러운 테러에 대한 호들갑스러운 정부의 목적은 무엇보다 정권 재창출을 위한 물리력 기구에 대한 장악과 그를 위한 이들 기구들의

권한 확대에 있겠지만, 그 외에도 정권의 교체와 상관없는 자신들의 독자적 이익구조를 확보함으로써 향후 정권이 상대적으로 민주적인 정부로 교체되더라도 우리 사회의 기득권 지배 구조를 공고화하려는 데에 그 궁극적 목적이 있음.

○ 이러한 구조가 고착될 경우 향후 정권이 교체되더라도 개혁되지 않은 이들 물리력 기구들로부터의 압박은 강고할 것이고, 그 결과 민주정부에서조차 탄압의 강도는 줄지 않았다는 관념 속에서 실망감이 확대되어 많은 이들을 혼란스럽게 할 것이며, 결국 일베와 같이 민주정부에 대한 공격을 더 선호하고, 사회불평등으로 인한 저항의 방향을 보수 정권으로 향하지 않고 사회적 약자나 소수자 등으로 향하는 집단들을 양산하게 될 것임.

○ 기득권의 이해를 반영하는 여당과 정부에 의한 '포퓰리즘'이나 '종북몰이'의 효과가 약해질 수 있는 상황에서 젊은 층들을 포함한 '반보수/친야당'적 성향을 가진 집단들을 쉽게 사로잡을 수 있는 가장 손쉬운 방법이 바로 테러방지를 가장한 공포 조장을 통한 지배임. 일베 등 이미 확보된 극우보수적 일부 젊은 층 외에도 진보적인 집단에서도 외국인혐오증이나 이슬라모포비아가 만연해 있는 사회적 분위기는 상당히 오래 이어질 것이 예측되는 가운데, 테러방지법은 보수기득권 지배집단의 권력 유지와 연장에 매우 효과적인 통제 수단이 될 수 있음. □

# 토론문

장유식[1]

## 1. 때만 되면 등장하는 테러방지법

2001년 9월 미국에서 발생한 9·11테러 이후 한국에서 테러방지법을 제정하고자 하는 시도는 14년째 계속되고 있다.

그러나, 그 14년동안 테러방지법을 둘러싼 입법환경은 전혀 바뀌지 않았다. 즉, 여전히 테러방지법은 만들어서는 안되는 악법이다. 테러방지법은 테러의 예방이나 대응과는 본질적으로 무관하며, 국가정보원에 무소불위의 날개를 달아줄 뿐이기 때문이다.

## 2. 테러방지법은 테러의 예방이나 대응과는 본질적으로 무관하다

○ 흔히 테러방지법이 테러의 예방이나 대응을 위한 것이라고 생각할 수 있지만, 테러의 개념을 어떻게 규정하는지에 따라 수많은 논의가 있을 수 있다. 항공기납치, 폭탄테러, 인질, 핵물질, 국제범죄조직 등은 현행 국내법으로도 모

1) 변호사, 민주사회를위한변호사모임

두 처벌할 수 있다. 그런데, 테러방지법에는 새로운 유형의 테러의 개념은 전혀 없다.

○ 한국에 테러의 위험이 갑작스럽게 높아졌다는 근거도 전혀 없다. 파리에서 발생한 총격사건은 과거 미국이 벌인 이라크전쟁이나 이스라엘-팔레스타인간의 분쟁과 궤를 같이 하는 것이며, 그와 같은 위협은 수십 년 전부터 계속되어 왔다.

○ 분단국가인 대한민국은 강력한 군대와 경찰, 국정원, 기무사, 검찰 등 국가기관이 존재한다. 통합방위법 등 30여개의 법령이 테러에 대한 대응을 명시하고 있다. 즉, 기존의 조직, 기존의 법령으로도 테러에 대한 대비는 충분하다. 만약 그렇지 않다면 이는 국가기관의 직무유기에서 비롯된 결과일 따름이다.

○ 시민사회단체는 국가기관이 아니기 때문에 기존의 조직과 법령으로 테러에 대한 대비가 충분하다는 것을 실증적으로 증명하기는 어렵다. 그러나, 이는 시민사회의 몫이 아니다. 정부가 테러방지법을 만들고자 한다면, 기존의 조직과 법령으로 테러에 대비가 불충분해서 반드시 테러방지법을 만들어야 한다는 점에 대한 입증책임과 설명책임을 이행해야 할 것이다.

○ 본질적으로 테러를 100% 방지한다는 것은 불가능하다. 예컨대, 자살테러는 제아무리 테러방지법을 촘촘하게 만들어놓더라도 막을 수 없다는 것이 전문가들의 진단이다. 테러의 발생원인을 성찰하여 이를 제거하는 것이 더 중요하다.

## 3. 테러방지법은 국정원에 날개를 달아줄 뿐이다.

○ 무엇보다도 그 14년동안 국가정보원은 아무것도 바뀌지 않았다. 막강한 수사권을 그대로 보유하고 있고, 국내보안정보에 대한 수집권도 갖고 있다. 국회 등을 통한 통제는 이루어지지 않고 있다. 국정원은 여전히 정치에 개입(국정원 댓글사건)하거나, 간첩을 조작(유우성 사건)하고 있다. 결국 국정원은 비밀정보기관으로서의 역할을 방기하고 있다.



○ 국정원이 정보기관으로서의 본연의 역할을 하지 못함에 따라 국민의 안전과 생명이 위협당하고 있는 것이다. 국정원이 제 역할을 못하기 때문에 테러의 위험도 높아지는 것이다. 국정원이 제대로된 정보기관으로 개혁되어야만 진정한 의미에서의 테러방지가 가능하다. 테러방지법에 대한 가장 효과적인 대안이 '국정원 개혁'이 되는 근거이다.

○ 국가정보원은 이미 2003년 12월부터 국정원 내에 '대테러상황실'을 설치·운용하고 있다. 상황실에는 국가정보원 직원 외에, 경찰청, 행정자치부, 국방부에서 파견된 인력들이 합동으로 근무하고 있다. 사이버테러 대응 단위도 운용하고 있다. 여기에서 더 나아가 법률에 의거 대테러센터를 만들어서 국정원에 무소불위의 권력을 쥐어줄 이유가 없다.

○ 국정원 개혁이 이루어지지 않음으로써, 국정원은 현재로서도 매우 위험한 존재이다. 진정으로 테러를 방지하고 싶다면, 테러방지법을 만들고 싶다면 국정원부터 개혁해야 한다.

○ 테러방지법이 제정되면 국정원이 '테러'라는 명분으로 민간단체를 테러단체로 규정하고, 휴대폰을 도감청하고, 금융정보를 마음대로 들여다볼 수 있는 세상이 될 것이다. 국정원은 법을 지키겠다고 하겠지만, 누가 이를 믿을 수 있겠는가.

○ 테러방지법은 결코 한국적 상황에서 테러방지의 효과적인 대안이 될 수 없다. 설사 백보를 양보하여 필요성을 인정한다고 하더라도 '국정원이 중심이 되는 테러방지법'은 그 필요성에 비해 인권과 민주주의의 후퇴에 대한 우려가 크고도 명백하다. ■

# 토론문

장여경[1]

지난해 이맘때 쯤 국회 미래창조과학방송통신위원회 공청회장에 있었다. 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」 제정을 논의하는 자리였다. 이 신기술에 대한 법안을 둘러싼 주요 쟁점 중 하나는 뜻밖에도 국가정보원 문제였다. 정부가 발의한 법안에서 국정원이 민간 클라우드 컴퓨팅 서비스에 대한 '기준'을 정하도록 한 것이다. 당연한 반발이 일었다. 국민들은 디지털 플랫폼에 대한 정보·수사기관의 개입에 민감해져 있었다. 국정원 전 원장을 비롯한 간부들이 국내정치와 선거에 개입했다는 사실이 드러났고, 국회 국정원 개혁특위는 무력하게 끝난 상황이었다. 카카오톡 압수수색 논란이 일자 외국산 메신저로 이동한 사이버망명객이 2백만 명에 달했다.

공청회장에서는 국정원이 클라우드 서비스에 관여하면 국내 서비스에 대한 국민 불신으로 이어질 수 있다는 지적이 이어졌다. 전문가, 야당 의원은 물론 여당 일부 의원들까지 지적에 나섰다. 결국 주무부처인 미래창조과학부는 국정원 관련 조항을 제외하는 수정안을 마련하여 법안을 통과시켰다. 그로부터 일년이 지났다. 국정원 해킹사찰 의혹이 일었지만 국정원이 국회의 자료제출 요구에 버티기로 일관하며 아무것도 제대로 밝혀지지 않았다. 그 와중에 난데없이 사이버테러방지법 논란이 불거졌다.

1) 정책활동가, 진보네트워크센터



현재 국회에서 논의중인 테러방지법 12개 법안 가운데 4개 법안이 사이버테러방지법안이다. 파리테러 이후 급물살을 타고 있는 이 법안들을 살펴보면 국정원이 비극적인 사건을 자기 기관 욕심에 이용하는 것은 아닌지 우려가 생긴다. 왜냐하면 사이버테러방지법안들에서 국정원이 민간 인터넷 서비스에 대한 지휘·감독권을 요구하고 있기 때문이다. 클라우드컴퓨팅법에서보다 더 큰 권한이다.

국정원은 이미 국가사이버안전규정에 따라 국가망을 관리해오고 있었다. 이런 마당에 사이버테러방지법이 필요한 이유는 민간 인터넷까지 관리하기 위해서이다. 이 법안에 따르면 국정원장 산하에 설치되는 '국가사이버안전센터'는 민·관·군을 아울러 지휘·감독한다. 이렇게 국정원의 지휘·감독을 받게 될 민간에는 집적정보통신시설사업자, 즉 IDC와 주요정보통신서비스 제공자, 즉 통신사, 포털, 쇼핑몰이 포함된다. 언제? '사이버테러'를 예방하고 대응하기 위해 상시적으로. 그런데 '사이버테러'란 무엇인가? 법안에 따르면 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신망을 공격하는 행위를 말한다. 그런데 인터넷에서 해킹 사고나 바이러스 유포란 것은 늘 일어나는 일이다. 결국 국정원이 상시적으로 민간 인터넷 서비스에 개입할 수 있는 것이다.

어떻게? 먼저 사이버테러 사고가 일어났을 때이다. 사고에 대한 조사결과를 보고받은 국정원은 해당 인터넷 서비스에 특정한 조치를 요구할 수 있고, 서비스 제공자는 특별한 사유가 없는 한 이에 따라야 한다. 또 국정원은 사고 발생 때 뿐 아니라 이를 '예방'하기 위하여 많은 일을 할 수 있다. 국정원은 인터넷 서비스 기관들로부터 인터넷망, 소프트웨어의 취약점을 보고받는데, 보고하지 않는 기관들은 형사처벌 받는다. 카카오톡 취약점을 몰라 카카오톡 해킹을 못했다면 앞으로는 보고된 취약점을 활용할 수 있을 것이다. 인터넷망에 대해 상시적으로 엿보는 것도 가능하다. 국정원은 지금도 국가보안법 수사를 위해 패킷감청기법으로 인터넷회선에 대해 감청하고 있는데 이 법이 제정되면 일일이 영장을 받을 필요도 없어질지 모르겠다. 이 법에 따라 국정원이 만들 시행령에서 더 많은 것들을 요구할 수도 있다.

다른 나라에는 사이버테러법이 있다고? 한국도 이미 충분히 사이버테러에 대응해 왔다. 그간 우리도 수많은 개인정보 유출 사고, 해킹 사고, 디도스 공격

을 경험했다. 그리고 그때마다 정부 각 부처는 대응 노하우 뿐 아니라 자기 감독권한도 하나씩 늘려 왔다. 그렇게 민간 인터넷을 관리해 온 것이 미래창조과학부, 한국인터넷진흥원 등이다. 미래창조과학부 사이버안전센터 운영규정에서는, "사이버공격이란 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 말한다"고 정의하고 있다. 사이버테러방지법안에서 규율하려는 행위와 다를 바 없는 대상들을 이미 미래부가 규율해 온 것이다. 왜 갑자기 비밀정보기관인 국정원이 이를 관리해야 하는지에 대해서는 아무런 설명이 없다.

지난해 반테러 보고관이 유엔 총회에서 경고했듯이 디지털 환경에서 정보기관의 정보수집을 통제하지 못한다면 국민들의 "프라이버시는 말살"될 것이다. 인터넷 회선 전체에 오가는 패킷을 들춰보는 기술은 이미 비밀이 아니며 위험한 수준까지 남용되고 있다. 인터넷회선 사업자가 웹하드 서비스를 차단하기 위해서나 이동통신사가 보이스톡과 같은 엠보입(mVoIP) 서비스를 차별하는 데도 사용되고 있다. 하물며 디지털 시대 국가 감시는 과거보다 더욱 은밀하게, 대규모로, 손쉽고도 저렴하게 엿볼 수 있는 수준이다. 인터넷에 올라온 정보를 수집해서 분석하면 어떤 사람의 행동거지는 물론 머릿속 생각까지 실시간으로 알 수 있다.

한국이 다른 나라보다 상황이 더 나쁜 이유는 국가정보기관이 매우 비대하다는 데 있다. 한국의 유일한 국가정보기관은 국내파트, 해외파트, 수사, 정보, 기획조정 직무를 한 몸에 다 가지고 있다. 때로는 영장을 가지고 감청하고 때로는 대통령 승인만으로 감청할 수 있다. 국내파트, 해외파트, 신호파트, 수사, 정보 등 정보기관'들'의 권한과 기관이 명확하게 분리되어 상호견제와 정보공유를 하도록 한 다른 나라와 너무 다르다. 그러니 한국에서 국정원의 권한 오남용을 둘러싼 논란이 그치지 않는다. 국제사회 기준으로도 문제가 있다. 올해 유엔 자유권 위원회는 국정원의 통신수사를 감독할 수 있는 기제를 도입해야 한다고 한국 정부에 권고했다.

그러나 한두 명의 감독관제를 도입한다고 해서 국정원에 대한 감독이 가능할 것 같지는 않다. 이 공룡 비밀정보기관의 직무에 대한 근본적인 개편 없이는 이 기관이 진짜 하고 있는 일에 대해서 통제하는 것이 불가능할 것이기 때문이다.



국회가 해야 할 일은 국정원에 대한 국민들의 실망과 불신에 대해서 답하는 것이다. 아무 것도 변하지 않았는데 국정원의 새로운 직무를 넓혀주는 것은 국민에 대한 배신이다. 이것은 국민의 정보인권에 관한 문제이고 정치공학적으로 교환할 대상이 아니다. 사이버테러에 더 이상의 대안은 필요 없다. 여전히 언제든지 국내정치에 개입하고 선거에 개입할 수 있는 국가정보기관에 대한 개혁, 그것이 사이버테러보다 선결해야 할 문제이다. ❑

# 국민의 안전을 지키려면
# 테러방지법 대신 국정원 개혁부터[1]

이태호[2]

대통령이 험악한 말로 테러방지법 제정을 압박하고 있다. "우리나라가 테러를 방지하기 위해서 기본적인 법체계조차 갖추지 못하고 있다는 것을 IS(이슬람국가)도 알아버렸다. 이런데도 천하태평으로 테러방지법을 통과시키지 않을 수 있겠나?", "테러방지법이 통과되지 못하면 테러에 대비한 국제공조도 제대로 할 수가 없고 (다른 나라와) 정보 교환도 할 수 없다"며 겁을 주고는 '긴급명령을 발동'해서라도 법을 제정하겠다고 협박한다.

## 테러 발생하면 니가 책임질래?

원유철 새누리당 원내대표 역시 지난 화요일(12.7) 원내대책회의에서 '테러가 일어나면 야당 책임'이라고 윽박질렀다. "G20 국가 중에 테러방지법이 제정되지 않은 곳은 우리나라를 포함해 단 3곳뿐"이란다. 이 법의 제정에 의문을 제기하는 것은 무책임하고 불순한 것으로 간주한다. "테러나면 니가 책임질래?"라고 눈을 부라리는 앞에서 누가 감히 "그게 과연 필요하냐"고 따져 물을 수 있겠는가?

1) 「허핑턴포스트」 기고 '테러방지법이 없다고? 이미 지나칠 정도로 많다!' 2015년 12월 15일
2) 참여연대 사무처장



그러나 그들이 말하지 않는 것이 있다. '테러 방지'에 관한 한 우리나라는 G20에 속한 어느 나라보다도 강력한 기구와 제도를 운영하고 있다는 사실이다. 우리나라는 식민지와 냉전 시대를 거치면서 시민통제에 관한 한 G20 나라 중 최고의 안보국가로 정평이 나 있다. 이미 통제가 지나쳐 과도하게 시민의 인권을 침해하고 있다. 조금만 생각해보라.

G20 중 우리나라처럼 온·오프라인 모든 면에서 광범위하게 시민들의 사생활과 일거수일투족을 정부가 환히 들여다볼 수 있는 나라가 몇이나 되겠는가? G20 중 어느 나라 검찰이 기소권, 수사권을 독점한 채 강력한 권한을 행사하고 있는가? 우리나라 검찰은 세계 최고 수준의 막강한 권한을 가지고 있다. 과연 G20 중 출입국제도, 주민등록제도가 우리나라처럼 촘촘한 나라가 또 있는가? G20 중 우리나라 국정원처럼 국내외 정보수집기능, 비밀경찰기능(수사기능), 정책기획 기능, 나아가 작전 및 집행기능에 이르기까지 무소불위의 권한을 지닌 정보기구를 두고 있는 나라가 또 있는가? 과연 G20 나라 중 우리나라만큼 많은 수의 군대와 경찰을 두고 있는 나라가 몇이나 있는가? 심지어 '치안한류'라는 이름으로 이를 해외에 자랑하고 파견하고 있다.

이런 나라에서 정부와 정치권이 나서서 '테러나면 니가 책임질래?'라고 공포 분위기를 조성하는 것이야말로 무책임한 것 아닌가?

테러방지법이 없다는 주장도 사실이 아니다. '테러방지법'이라는 이름의 법이 없을 뿐이다. 식민지 시대와 분단을 거치면서 '테러'라는 용어가 정치적으로 악용되어 왔고 전 세계적으로 비슷한 현상이 일어나고 있어 이 용어를 쓰지 않고 있을 뿐, IS에 의해 파리에서 일어난 민간인에 대한 무차별 공격과 유사한 인질사태 또는 무장공격행위를 예방하고 대응하기 위한 법과 제도는 무수히 많다. 사실 많은 나라에서 '테러방지법'이란 하나의 법이 아니라 여러 가지 개별법들의 묶음을 말한다. 같은 맥락에서 우리나라는 이미 수많은 '테러방지법'을 가지고 있다고 볼 수 있다.

## 테러방지법이 없다고? 천만에! 지나칠 정도로 많다.

우선 '테러'에 직접 대응하는 대비태세를 갖추기 위한 각종 법령과 기구가 이미 마련되어 있다. '적의 침투 도발이나 그 위협에 대응'하기 위하여 각종 국가

방위요소를 통합하여 동원하는 통합방위법, 그리고 이를 뒷받침할 비상대비자원관리법을 제정하여 시행하고 있는 것이다. 통합방위사태가 선포되면 국무총리가 총괄하는 중앙통합방위협의회가 각 지역 행정조직과 경찰조직, 군과 예비군, 그리고 국정원 등 정보기구를 통합적으로 운용할 수 있다. 통합방위사태는 대통령이 국무회의의 심의를 거쳐 선포하고 통제구역을 설정한다. 기타 시민들의 대피, 구조  구난 활동을 체계적으로 수행하기 위해서 국민안전처도 2014년 세월호 참사 이후 신설됐다. 육해공군과 해병대, 그리고 경찰과 해경은 제각각 대테러특공대를 구성해 운영하고 있다. 쌍용차 노조 파업 진압에 경찰대테러특공대가 동원되어 구설수에 오른 바 있지 않은가? 게다가 한국이 지닌 대테러능력에는 한미연합사가 지닌 정보·작전 능력도 포함해야 한다. 한국과 미국 간에는 군사정보를 공유하는 군사비밀보호협정이 체결되어 있다. 한국 국방부는 주한미군을 비롯한 미군의 정보자산으로부터 도움을 받고 있고 매년 정기적으로 한미 대테러훈련도 실시하고 있다. 그 밖에 국가대테러활동지침에 따라 국무총리가 주관하는 국가테러대책회의도 오래전부터 운영해오고 있다.

'사이버 안전'을 위해서는 이미 정보통신기반보호법, 전기통신사업법, 통신비밀보호법 상 비밀보호예외조항 등 다양한 법 제도가 도입되어 시행되고 있는데, 시민들의 통신기록을 무단으로 대량수집하고 도  감청까지 하고 있어 갈등을 빚고 있다. 공안당국은 카카오톡을 비롯한 SNS를 임의로 감청하고, 테러단체도 아닌 평범한 시위대를 추적할 목적으로 통신사업자의 기지국 통신자료를 통째로 가져가는 것을 비롯해 영장 없이 가입자 정보, 통신사실 확인자료, 위치정보 등을 광범위하게 수집하고 있다. 국경없는기자회는 2009년 이래 우리나라를 '인터넷감시국'으로 분류하고 있다. 영국의 경제지 이코노미스트는 지난해 2월 게재된 '한국이 인터넷 공룡인 진짜 이유'라는 제목의 기사에서 "한국인들이 광속 인터넷 환경을 누리고 있지만 자유로운 인터넷 사용은 허용되지 않고 있다"고 분석하고 "한국은 암흑시대에 머물러 있다"고 비꼬았다[3].

테러 관련 자금 추적 장치 역시 촘촘하기 그지없다. 범죄에 사용되는 자금을 추적할 수 있는 자금세탁방지제도인 범죄수익은닉규제법과 금융거래정보보고법은 참여연대를 비롯한 시민단체들의 노력으로 제정되었는데 G20 최고수준

3) 백종민 기자, "'한국 인터넷, 속도만 빠른 암흑기' 「이코노미스트」" 아시아경제, 2014.02.12 http://view.asiae.co.kr/news/view.htm?idxno=2014021209154874154



이라는 평가를 듣고 있다. 그 밖에 공중등협박목적자금조달금지법(일명 테러자금조달금지법)도 2008년 제정하여 UN뿐만 아니라 미국, EU 등에서 요청한 개인과 단체의 자금을 세밀하게 추적하고 있다. 이 법에 따르면 '테러 관련 자금'이라고 의심되면 영장 없이 금융거래를 동결하고, 수사에 필요한 정보는 검찰총장, 경찰청장, 그리고 국민안전처장에게 제공된다. 외국환관리법도 해외금융거래에 대해 유사한 통제장치를 가지고 있다.

'테러위험 인물'들의 출입과 동선을 추적하기 위한 출입국 관리제도 역시 다른 어느 나라보다 통제가 심해 인권침해가 빈발하는 것으로 악명을 떨치고 있다. 예를 들어 2010년 G20 정상회담을 앞두고 경찰청은 중동, 아프리카, 동남아시아의 이슬람권 57개국에서 입국한 5만여 명의 국내 체류상황을 조사해 그 중 행적이 의심스러운 외국인 99명을 특별히 '관리'했다. 또한 경찰청은 "법무부와 국가정보원 등도 테러 용의자 명단을 확보해 입국금지 대상에 포함하고 있으며, 현재 입국이 금지된 테러 혐의 외국인은 5천여 명에 달한다"고 발표했다. 그런데 이 명단 때문에 시민사회단체의 G20 관련 학술회의에 참가할 예정이었던 파키스탄 여성단체 대표 칼리크 부슈라(Khaliq Bushra), 네팔노총 사무총장 우메쉬 우파댜에(Umesh Upadhyaya), 국제농민단체 비아 캄페시나 대표인 헨리 사라기(인도네시아) 등 6명의 비자가 거부되었고, 필리핀 소재 개발원조단체인 이본 인터내셔널(IBON International)의 폴 퀸토스 부장을 비롯한 8명의 필리핀 활동가는 비자를 받고도 공항에서 무더기로 입국불허 통지를 받아야 했다. 이들은 대부분 미국을 비롯한 전 세계의 국제행사에 자유롭게 참여해 오던 인사들이었다. 2010년 2월에는 경찰이 대구 이슬람 사원 주변에서 근무하는 이맘과 이주노동자 등 2명의 파키스탄인이 탈레반 구성원이라고 발표하였으나 재판 과정에서 검찰과 경찰은 관련 혐의를 입증하지 못했다.

## 법이 없어 국제공조와 정보교환이 어렵다?

박근혜 대통령은 테러방지법이 제정되지 않으면 국제공조도 정보교환도 제대로 할 수 없을 것처럼 강변하지만, 사실이 아니다. 국제 정보공조는 테러방지법 제정과는 거의 상관관계가 없고 지금 현재도 국제공조와 정보교환은 활발히 이루어지고 있다.

우선, 앞서 언급했듯이 한미 간 군사비밀보호협정이 체결되어 있고 연례적인 대테러 군사훈련, 대량살상무기 확산방지 훈련을 실시하고 있다. 미국 국가안보국(NSA)가 전 세계와 자국민을 무차별 사찰하고 감청해온 사실을 폭로한 에드워드 스노든이 한국 언론과의 화상대화에서 밝힌 바에 따르면, 한미 정보당국 간에는 최소한 "국방 측면의 정보 공유가 일어나고 있다[4]."

테러 관련 자금 추적을 위한 국제 정보교환과 공조 역시 활발하다. 한국은 지난 2015년 7월부터 1년간 국제자금세탁방지기구(FATF)의 의장국을 맡고 있다. 의장은 신제윤 전 금융위원장이다. 유엔 협약 및 유엔 안보리 결의 관련 금융조치를 이행하는 태스크포스(TF)인 FATF는 금융시스템을 이용한 자금세탁과 테러  대량살상무기 확산 관련 자금조달을 막는 역할을 한다. 이미 시행 중인 공중등협박목적자금조달금지법(일명, 테러자금조달금지법)은 UN의 요청뿐만 아니라 미국 등 우방국의 요청만 있으면 위험인물로 지목된 개인과 단체의 금융거래를 동결하고 해당 자금의 조성과 은닉에 관련된 이들을 처벌할 수 있게 하고 있다.

외국환관리법 역시 유엔과 우방국과의 긴밀한 정보교류와 공조 속에 시행되고 있다. 외국환관리법의 하위지침인 '국제평화 및 안전유지 등의 의무이행을 위한 지급 및 영수 허가지침'에 따르면 유엔 결의로 제재를 결정한 개인이나 단체 외에도 미국 대통령령(Executive Order), 유럽연합이사회(The Council of the European Union)가 지명한 개인 및 단체에 대해서 기획재정부가 금융제재를 할 수 있도록 되어 있다. 지난 3월, 기획재정부는 IS 대원 27명을 포함해 669명을 금융제재 대상자에 포함시키고 수시로 업데이트하고 있다.

4) '에드워드 스노든과의 화상 대담 "빅브러더가 통제하는 사회 되지 않으려면?"', 홍지민 기자, 서울신문, 2015.10.30, http://www.seoul.co.kr/news/newsView.php?id=20151030500245 "정보 공유는 한국과도 일어나고 있다. 어떤 맥락이냐에 따라 옳고 그른지 정해진다. 북한이란 요소가 있어서 국방 측면으로 정보 공유가 일어나고 있습니다. 북한의 군사 징후가 일어나는 지 등에 대해서 정보 공유가 일어나고 있는데 그것은 타당하고 적절하다고 생각합니다. 걱정되는 것은 영미 동맹권과 일어나는 정보 공유다. 파이브 아이즈에 속한 미국, 영국, 호주, 뉴질랜드, 캐나다는 군사적 필요성이나 테러 차단 차원을 넘어 광범위하게 정보를 공유한다. 그런데 그러한 정보 공유로 테러 차단이나 사건 해결에 대한 구체적인 성과를 내지 못했다. 광범위한 감청이 일어나지만 테러 방지에 도움이 되지 않았다는 것이다. 권력, 경제, 외교, 사회적 통제를 위해 감찰이 일어난다는 게 더 맞다고 본다"



그런데, 오히려 우방국과의 과도하고 근시안적인 협력이 문제가 되는 경우도 적지 않다. 이란제재가 그 대표적인 사례다. 2010년 9월 이명박 정부는 이란의 핵 프로그램에 대한 미국의 제재요청을 받아들여 102개 단체와 24명의 개인을 금융제재 대상자로 지정하였다. 여기에는 이란과 교역하는 우리 기업들의 결재은행인 이란 국영 멜라트 은행도 포함되어 있다. 유엔 안보리 결의안 1929호는 이란의 40개 단체와 1명의 개인만을 제재대상으로 지정하였고, "이 결의안의 어떠한 조항도 국가들이 이 결의안 범주를 넘어선 조치나 행동을 취할 것을 강요하지 않는다는 점을 강조한다"고 밝히고 있다. 한국의 이란제재는 미국 국내법에 따른 것으로서 유엔 안보리 결의에는 위배되는 것이라는 해석이 가능하다. 한국 정부는 유엔 안보리 결의를 위배하면서까지 미국의 요청에 따름으로써 결과적으로 이란과의 교역단절에 따른 막대한 손실을 초래한 셈이다.

우방국과의 잘못된 국제공조 중 최악의 사례는 이라크 전쟁과 파병이다. 한국 정부는 이라크 후세인이 핵을 개발하고 있고, 테러세력과 연관되어 있다는 미국의 일방적인 주장을 받아들여 UN도 승인하지 않은 전쟁에 한국군을 파견했다. 한국은 당시 영국 다음으로 많은 세계 3위 규모, 3600여 명의 군대를 파견했다. 그러나 점령 직후 이라크에 핵 프로그램이 없었고, 후세인 정권과 테러집단과는 관련이 없었다는 사실이 재확인되었고 미국 정부조차 이를 인정하지 않을 수 없었다. 9·11 사건을 예측하지 못한 데 이어 두 번째의 치명적인 '정보실패'였던 셈이다. 그런데 미국과 그 동맹국들의 이라크 불법점령 이후 이라크는 이슬람 극단주의자들을 불러 모으는 지하드의 성지가 되어버렸다. 이라크 내부 저항세력의 끈질긴 게릴라전을 소탕하는 과정에서 무고한 민간인이 다수 희생 당했다.[5] 특히 관타나모 수용소(미국령 쿠바), 바그람 기지 수용소(아프간),

5) 이라크에서의 민간인 사망에 대해서는 여러 가지 통계가 있다. 인터넷 사이트인 '이라크 보디카운트 Iraq Body Count'에 따르면 2003년 이라크 침공 이후 이라크에서 무장폭력에 의해 희생된 민간인 수는 149,061명에서 169,310명에 이른다. 이라크보디카운트는 문서로 보고되거나 보도된 사건에 한해서만 집계하는 방식을 취하고 있어 실제 사망자수를 모두 반영하지 못할 수 있음을 인정하고 있다(https://www.iraqbodycount.org). 2010년 10월, Wikileaks가 'Iraq War Logs' 라는 닉네임으로 미 육군 이라크 현장 리포트 수십만 건을 원본 그대로 공개했는데, 이들 보고서를 통해 2004년부터 2009년까지 보고된 109,000명의 사망자 중 66,081명이 민간인이었다. 한편, 존스홉킨스 대학의 공중보건 전문가들이 2006년 10월 발표한 랜싯보고서(The Lancet Study)는 이라크 침공 이후인 2003년 3월부터 2006년 6월 사이에 601,027(426,369-793,663)명이 전쟁과 관련된 이유로 사망했다고 주장하여 큰 논란이 일었다.

아부그라이브 교도소(이라크) 등 해외 수용시설에서 미군이 '적 전투원(enemy combatant)'으로 의심된다는 이유로 증거도 없이 수감된 민간인들을 고문, 학대했다는 사실이 전 세계에 알려지면서 미국이 주도한 '테러와의 전쟁'은 전 세계에 테러리즘을 확산하는 자양분이 되고 말았다. '파리 테러'를 주도한 IS도 이즈음 이라크를 기반으로 형성되었다.

## 부족한 것은 테러방지법이 아니라 국정원의 해외정보수집능력

그렇다면 '테러를 방지'하는데 부족한 것이 아무것도 없다는 건가? 그렇지는 않다. 취약한 구석이 있다. 지금 우리나라에서 가장 취약한 구석은 뭘까? 단언컨대 국가정보원의 해외정보수집능력이다. 박근혜 대통령이 강조해 마지않는 '국제 정보 교류 및 공조의 강화'를 위해서도 국정원을 개혁하여 해외정보수집과 분석에 집중하게 해야 한다.

유감스럽게도 우리나라 국가정보원은 그 덩치나 무제한의 권한에 비해 독자적인 해외정보수집능력이 지극히 부족하다. 대북, 해외, 국내 정보 수집을 독점하고, 기획조정이라는 이름으로 각급 정부부처와 기관들을 쥐락펴락하며, '대내 심리전'을 빙자해 민간인들을 사찰하거나 정치에 개입하는 등 불필요한 일에 시간과 인력을 낭비하고 있기 때문이다. 최근 수년간 일어난 국정원의 민간인사찰사건, 대선개입사건, 불법해킹사건, 중국 동포 간첩조작사건 등은 국정원 일탈행위의 일각을 보여주고 있다[6].

국정원의 일탈을 보여주는 증거뿐만 아니라 국정원의 무능을 보여주는 사례도 끝없이 열거할 수 있다. 특히 다음에 열거하는 것은 국정원이 IS에 대해 독

6) "5·16 이후 정권 안보에 주안점을 두고 출범한 게 국정원입니다. 해외 활동, 대북공작 활동조차 정권의 안보와 연계해 수행한 경우가 많습니다. 군사독재 시절의 악명은 말할 것도 없고, 민주화 이후에도 국정원은 이런 한계를 극복하지 못했습니다. 권영해 전 안기부장이 일으킨 북풍 사건, 국정원 미림팀의 전방위 불법 감청 사건, 댓글사건 등 국내 정치 개입이 끊이지 않았습니다. 박근혜 정부에서는 휴대전화 불법감청 및 해킹 의혹이 불거졌고요. 여전히 정권안보기구로 작동한다는 의심의 근거가 되는 일이 계속 드러난 겁니다." ""대북 해외활동도 '정권 안보' 연계 국내 파트-경찰 수사기능 통합해야"-국정원 고위간부의 '국정원 정치공작' 비판", 신동아 2015년 9월호. http://shindonga.donga.com/3/all/13/114166/1



자적인 정보수집능력을 갖추고 있을 가능성이 거의 없음을 보여주는 정보 실패 사례다.

2003년 이라크 파병 당시 국정원은 석유자원 확보와 안전 등을 고려할 때 이라크 북부가 파병지로 바람직하다는 의견을 내놨다. 첫 파병지로 거론된 곳은 이라크 북부의 모술이었다. 군과 국정원은 모술이 안전하다고 주장했고, 군이 주도한 현지조사단의 정부 측 참가자들은 현지 군부대 등을 건성으로 시찰한 후 모술이 안전하다고 보고했다. 민간연구자로서 현지조사단에 참여했던 박건영 교수만 유일하게 조사단 일정이 실제 조사를 포함하지 않았으므로 '모술이 안전한 파병지'라는 결론에 찬동할 수 없다고 밝혔다. 하지만, 유엔 이라크지원단이 타전하는 일일보고서에는 모술이 이라크에서 (종족 간) 무장갈등이 가장 심한 곳 중의 하나로 보고되고 있었다. 모술이 위험한 지역이라는 정보를 국내에 제공한 것은 국정원이 아니라 유엔을 모니터하던 시민단체, 참여연대였다. 한편, 우여곡절 끝에 이라크 북부의 아르빌에 자이툰 부대를 파견하기로 한 한국정부는 아랍어 통역병을 모집해서 현지로 파견했는데, 현지에 도착해서야 아르빌 지역에서는 아랍어가 아닌 쿠르드어를 사용한다는 사실을 확인했다. 이것이 당시 우리나라 해외정보력의 수준이었다.

지금 모술 인근 지역은 IS가 점령한 상태로 쿠르드족, 투르크족 등 3파전의 무장갈등이 지속되고 있다. 하지만 국정원도 군도 외교부도 한국의 이라크 파병이 이라크, 특히 우리가 파병했던 이라크 북부지역의 평화와 재건에 과연 긍정적인 영향을 미쳤는지 어떤 모니터 보고서도 내놓지 않고 있다. 참여연대가 매년 국회를 통해 자료를 요청하지만 단 한 번도 국회에 공개된 바 없다. 이렇게 이라크 상황에 대한 평가나 정보가 부족한 상태에서 이명박 정부는 자원외교라는 이름으로 이라크 만수리야와 아카스 가스전 개발에 투자했다. 이 사업은 IS와 이라크 정부군 간의 내전이 격화됨에 따라 2014년 6월부터 현장작업이 중단된 상태다. 어디 이라크뿐인가? 20조 이상의 손실을 낳은 것으로 평가되는 자원외교의 실패에는 부정부패도 있지만 고질적인 해외정보부족이 큰 몫을 하고 있다. 이게 국정원과 정부의 해외정보력 수준이다. 이런 국정원에게 테러방지법을 던져준다고 한들 제대로 일을 할 수 있겠는가?

박근혜 정부의 국정원에서 북한 담당 기획관(1급)으로 일했던 구해우 미래전략연구원 원장은 신동아와의 인터뷰에서 "국정원은 정권안보기구로 출범했

다는 태생적·체질적 한계를 극복하지 못했다", "국가 안보보다 정권 안보를 중시하는 체질 때문에 정치권력에 줄 대는 행태가 나타났다"고 혹평했다. 그는 또 "정보기관 요원들이 댓글 공작이나 하고, 북한과 관련해 소설 같은 이야기를 흘리는 언론플레이 공작이나 하는 것은 부끄러운 일"이라며 "해외 및 북한 파트와 국내 파트를 분리하는 것을 포함한 구조 개혁을 단행해야 한다"고 주장했다[7]. 그는 "정권안보기구로서의 성격이 강한 국정원뿐 아니라 검찰 또한 과도한 권력집중 및 정치화의 병폐"를 갖고 있다면서 "국정원의 국내 분야는 경찰의 수사기능과 합쳐 미국 연방수사국(FBI)과 비슷한 형태의 중앙수사국(KFBI)으로 통합"하고 "검찰은 수사 기능을 KFBI에 넘기고 미국식 공소유지 전담기구로 재편"하며, "국정원은 해외 및 북한을 담당하는 독립 정보기구"로 개혁할 것을 제안한다.

이렇듯 국정원이 오남용 해온 과도한 권한과 기능-국내정보수집기능, 수사기능, 기획조정기능, 대내 심리전(작전) 기능-을 없애고 해외와 북한 관련 정보수집을 전담하게 해야 한다는 것은 일부 진보인사만의 주장이 아니다. 보수 진보를 넘어 정보개혁을 위한 필수조치로 받아들여지고 있는 것이다. '해외정보국'으로의 개편! 국정원이 국민의 안전에 지금보다 훨씬 더 기여할 수 있는 길은 바로 그것이다.

## 테러방지법은 국정원 밥그릇 지키기법

그런데, 지금 국정원이 밀어붙이고 있는 테러방지법, 사이버테러방지법은 불행하게도 역방향으로 가고 있다. 이들 법안은 무늬만 테러방지법일 뿐 사실상 국정원이 그 본령인 해외정보수집기능을 강화하기보다 국내 정보수집, 조사와 수사, 정책 조정, 작전 기능, 그 밖의 시민 사찰과 정치 개입을 더욱 강화하도록 고안된 법안이다. 국정원의 비효율과 무능을 더욱 극대화하고 인권침해만 가중시킬 우려가 크다.

7) '"대북 해외활동도 '정권 안보' 연계 국내 파트-경찰 수사기능 통합해야"-국정원 前 고위간부의 '국정원 정치공작' 비판', 신동아, 2015년 9월호 http://shindonga.donga.com/3/all/13/114166/1



무엇보다도, 여당 의원들에 의해 국회에 제출된 테러방지법안들은 법률적으로 모호한 '테러' 행위를 예방한다는 명분으로 국정원 등 국가기관에 과도하고 포괄적인 권한을 부여하고 있다. 4개의 테러방지법안은 국정원에게 테러 및 사이버 테러 정보를 수집 분석할 뿐만 아니라, 정부 부처의 행동계획을 수립하고 나아가 대응을 직접 지휘하면서 필요시 군을 동원하는 등 집행기능까지 수행하는 광범위한 권한을 부여하고 있다. 예를 들면 국정원 산하에 대테러센터를 두어 정보를 집중하고, 국무총리가 주관하고 정부 유관 부처가 참여하는 국가테러대책회의를 두되 그 산하 대테러상임위원회의 의장 역시 국정원장이 담당한다는 것이다. 지역과 부문의 테러대응협의체도 해당 지역과 부문의 국정원 담당자들이 주관한다. 국정원에 의한, 국정원을 위한, 국정원의 테러방지법인 것이다.

박근혜 정부와 국정원이 추구하는 테러방지법은 미국의 사례를 따르는 것처럼 보이지만 사실은 미국의 체계와 사뭇 다르다. 9·11 전후 미국은 3년간 논의 끝에 2004년 정보기구를 개편했는데, 그 핵심은 정보분석취합기능을 CIA에서 떼어내는 것이었다. CIA에 집중된 정보분석기능이 정보실패를 가져왔다는 판단 때문이었다. 대신 정보취합분석을 전담할 국가정보국장실(ODNI)을 신설하고, 해외 정보 수집은 CIA(중앙정보국)과 DIA(국방정보국), 국내 정보 수집과 수사는 FBI(연방수사국), 전자신호 정보 수집은 NSA(국가안보국), 영상정보 수집 및 분석은 NRO(국가정찰국), NGA(국가공간정보국)등으로 각 정보기구의 역할을 전문화하였다. 국가정보국장실은 이들 정보기구들을 포함한 총 17개 부서(보통 intelligence community)에서 올라오는 각종 정보를 취합하여 분석하고 데이터베이스를 축적하는 국가독립기구로서 대통령과 NSC(국가안전보장회의), 국토안보부를 보좌한다.

정보 수집·분석 기능과 조사·수사 기능도 각각 분리되어 있다. 해외에서 군사작전 중에 체포된 '적 전투원'에 대해서 일부 CIA와 DIA가 수사하지만, 대부분의 조사 및 수사 기능을 FBI가 담당한다. 특히, 잠재적인 테러 위협을 조사하고 대비하기 위해 FBI 산하에 테러리스트조사센터(The Terrorist Screening Center)를 별도로 운영하는데 이 센터는 FBI 산하 기구이지만 법무부, 국무부, 국방부, 국토안보부 등이 협력하여 운영한다.

요약건대, 9·11로부터 미국 정보당국이 얻은 교훈은 정보 독점은 정보 실패를 낳는다는 것이다. 따라서 9·11 이후 미국 정보 개혁의 핵심은 정보 수집과 분

석의 분리, 정보주체와 집행주체의 분리, 각급 기관 간 견제와 균형의 확대를 지향했다. 그런데 한국에서는 비대하고 무능하며 국내 정치 개입을 일삼는 국정원에게 더욱 많은 사찰 기능과 독점적 권한을 부여하는 방향으로 테러방지법을 제정하려 하고 있는 것이다.

## 인권침해 논란 속에 폐지된 미국판 테러방지법

한편, 최근 국회에 제출된 테러방지법안, 사이버테러방지법안들은 하나같이 국정원 등의 공안기구에 '테러단체' 혹은 '테러위험 인물'을 지정할 권한을 주고 '테러위험 인물로 의심할 만한 상당한 이유'가 있는 경우 출입국관리기록, 금융거래정보 및 통신사실 확인자료 등을 영장 없이 요구할 권한도 부여하고 있다. 평범한 해킹도 사이버테러의 범주에 포함하고, 모든 통신사마다 의무적으로 도감청 설비를 구비할 것을 의무화하는 독소조항도 있다. 반면, 국정원이 지닌 과도한 권력에 비해 그 인력 예산 활동 내역에 대해서는 정부 내부와 국회를 막론하고 어떤 견제와 감시도 미치지 못해 불투명한 반민주적 기구의 대명사로 국내외에 오명을 떨치고 있는 실정이다.

이 문제에 대해서도 미국의 사례는 참고할 만하다. 미국은 9·11 사건 직후, 패키지 테러방지법인 애국자법(The USA Patriot Act of 2001)[8]을 제정했는데, 이 법은 제정되자마자 그 비효율성과 부작용에 대한 비판에 직면해 2006년 대폭 개정되었고, 그 후에도 독소조항에 대한 논란이 이어져 2015년 6월 2일 결국 폐기, 미국자유법(The USA Freedom Act[9])으로 대체되었다.

8) 애국자법(The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)은 여러 개별법의 개정안, 즉 전자통신비밀보호법(Electronic Communications Privacy Act), 컴퓨터사기및오용에관한법(Computer Fraud and Abuse Act), 해외정보사찰법(Foreign Intelligence Surveillance Act), 가족교육권및사생활보호법(Family Educational Rights and Privacy Act), 자금세탁규제법(Money Laundering Control Act), 은행비밀법(Bank Secrecy Act), 금융프라이버시권리법(Right to Financial Privacy Act), 공정신용거래보고법(Fair Credit Reporting Act), 이민및국적법(Immigration and Nationality Act), 1984년 형사범죄피해자법(Victims of Crime Act of 1984), 텔레마케팅및소비자사기및오용방지법(Telemarketing and Consumer Fraud and Abuse Prevention Act)을 포함하는 패키지 종합입법이다.

9) The Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act



그중 대표적인 독소조항의 하나가 애국자법 215조다. 215조는 NSA가 외국인과 자국민에 대해 무더기로 도 감청하고 통신기록을 수집할 수 있도록 허용하여 인권침해 논란을 빚었다. 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 비판했지만, 2006년 이 법을 대폭 개정한 후에도 이 독소조항은 사라지지 않았다. 2013년, 전 NSA 직원 에드워드 스노든이 미국 정부가 전 세계와 자국민을 상대로 무차별 도 감청을 자행해왔다는 사실을 폭로한 후에야 비로소 이 독소조항의 개폐가 정부와 의회에서 진지하게 논의되기 시작했다. 2015년 6월 애국자법이 폐지된 후 이를 대체한 미국자유법(The USA Freedom Act)은 그동안 논란이 되어왔던 NSA의 외국인과 자국민에 대한 무차별 도 감청과 무더기 통신기록 수집을 금지하고, 대신 자국민에 대해서는 '영장 받은 선별적 감청'만 가능토록 했다.

애국자법의 또 다른 독소조항 중 하나는 '국가안보레터(National Security Letters)'다. 애국자법 505조는 FBI가 일종의 행정명령인 '국가안보레터'를 발송하여 인터넷 서비스 제공자, 도서관, 은행, 신용카드업체 등에게 가입자의 통신기록 또는 거래기록을 통째로 요구10)할 수 있도록 했다. 국가안보레터 제도는 예전에도 있었던 제도지만 애국자법 제정과 더불어 그 발행요건을 대폭 완화한 것이다. 심지어 국가안보레터를 받은 사업자는 고객의 정보를 FBI에 제공했다는 사실조차 고객에게 알릴 수 없도록 했다(gag order). 2014년 오바마 대통령이 구성한 '대통령 직속 정보재검토 그룹(The President's Intelligence Review Group)'은 "다른 유사한 수단들이 법원의 허가를 필요로 하는데 반해 국가안보레터만 FBI에 의해 발행되어야 할 원칙적 이유를 찾을 수 없다"며 이 제도의 개선을 요구하기도 했다. 하지만 애국자법 대신 제정된 '미국자유법(The USA Freedom Act)에서도 법원의 허가 없이 레터를 발행할 수 있도록 한 조항은 폐지되지 않고 존속하게 되었다[11]. 다만, 미국자유법은 국가안보레터 발행

10) "bulk collection of communications or financial records"

11) 국가안보레터의 인권침해 여부와 더불어 실제 효과에 대해서도 논란이 이어져 왔다. 미국 인권단체 미국시민자유연맹(ACLU)에 따르면 "국가안보레터가 가장 빈번히 발행된

시 FBI를 비롯한 관계기관은 이용자 정보를 통째로 요구하지 못하고 필요한 정보를 특정하도록 제한했고,[12] 국가정보장(DNI, Director of National Intelligence)으로 하여금 매년 국가안보레터 발행 건수와 정보수집 건수를 웹사이트에 의무적으로 공개하도록 하였다. 또한 과거의 '함구령(gag order)'도 일부 개선하여 레터를 받은 사업자는 매년 총 몇 번의 레터를 통해 총 몇 명의 기록을 제공했는지 공개할 수 있게 하였다.

## 나오며 : 프랑스에 테러방지법이 없어서 '파리 테러'를 당한 게 아니다

한마디로, 지금 국회에 제출되어 있는 테러방지법안과 사이버테러방지법안들은 미국에서는 이미 폐기되거나 제한되고 있는 것을 국정원과 검 경에게 부여하는 독소조항을 가득 담고 있다. 이 법안이 통과되어서는 안 된다.

미국, 영국, 스페인, 러시아, 프랑스 등 이슬람 극단주의 단체로부터 무장공격을 당한 나라들이 '테러방지법'이 없어서 당한 것은 아니다. 이들 나라의 대외정책이 정의롭지 못해 해당 지역의 주민들에게 큰 불행을 안겨주었기 때문에 극단주의 세력의 표적이 된 것이다. IS는 우리나라가 미국을 도와 파병했던 이라크에서 사실상 시작되었다. 우리나라가 IS 테러의 표적이 되었다면, 테러방지법이 없어서가 아니라 미국을 도와 세계 3위 규모의 군대를 이라크에 파견하고, 그 후로도 이라크 등에 일어난 재앙에 대한 책임감을 느끼는 대신 석유자원 확보니 가스전 개발이니 하는 몰염치한 일에 아무런 현지 정보도 없이 엄벙덤벙 나섰기 때문일 수 있다. 우리나라 정부가 첫 파병지로 물색했던 모술은 지금 IS가 점령하고 있다.

변화가 절실하다. 대책도 시급하다. 가장 절실한 변화는 테러와의 전쟁에 협

2003년부터 2006년까지, FBI는 약 200,000건의 국가안보레터를 발행하여 인터넷 서비스 제공업체들로부터 사용자정보를 수집하였는데, 오직 단 한 건만 테러용의자 유죄입증에 사용되었던 것으로 밝혀졌다"고 한다. ACLU, "America's Surveillance Society", 2008. 11. 18

12) CRS report RS22406, "National Security Letters in Foreign Intelligence Investigations: A Glimpse at the Legal Background", Charles Doyle, Senior Specialist in American Public Law, July 31, 2015.



력해온 지난 14년간의 우리나라 대외정책을 돌아보는 일이다. 공포를 과장하고 적개심을 고취하는 것으로는 문제를 해결할 수 없다. 지금 가장 시급한 대책은 테러방지법이 아니다. 국정원을 개혁하여 해외정보수집에 집중하게 함으로써 국민이 준 세금이 아깝지 않게 하는 일이다. ◻

# 연구소 동향

# 연구소 동향

## ◈ 정보인권연구소 창립발기인 총회 개최 [7월 9일]

2015년 초 정기총회에서, 진보네트워크센터는 그 동안 함께 활동해 왔던 정보인권 전문가들과 함께, 새로운 연구소 설립을 추진하기로 결의하였습니다.

1998년 11월 설립 이후, 진보네트워크센터는 정보인권 옹호를 위한 다양한 활동을 해 왔습니다. 이슈 캠페인, 대체 법안의 개발, 기자회견과 토론회, 성명서 발표, 교육 및 강좌, 정보인권 연구, 국제 연대 등 활동의 방식도 다양합니다. 나름대로 열심히 했지만, 역량의 부족으로 많은 한계도 있었습니다. 종종 현안 이슈에 밀려, 대중 교육이나 연구 등에 많은 역량을 투여하지 못했습니다. 발빠른 대응이 필요한 경우도 있지만, 긴 호흡으로 차근차근 준비해야 하는 사업도 있습니다. 그래서 정보사회의 변화를 좀 더 심도있게 분석하고, 인권적 관점에서 정보통신 정책을 수립하며, 정보인권에 대한 대중적 인식의 확산을 위해서는 현안 대응 중심의 활동에 매몰되지 않도록 별도의 단체를 설립할 필요가 있다는 문제의식에 합의가 모아졌습니다. 이것이 연구와 교육 중심의 '정보인권연구소' 설립을 추진하게 된 배경입니다.

정보인권연구소는 인터넷 표현의 자유, 프라이버시 보호, 지식 공유지의 확대, 망중립성, 민주적인 거버넌스 등 그 지향에 있어서는 진보네트워크센터 다

르지 않습니다. 또한, 현실 이슈나 운동과 호흡을 함께 하면서 이를 뒷받침하기 위한 연구를 수행할 예정입니다.

2015년 상반기 동안 많은 분들과 정보인권연구소 설립의 문제의식을 공유하였고, 함께 할 것을 결의하였습니다. 그 결과 드디어 7월 9일, 사단법인 정보인권연구소(준)는 창립 발기인 총회를 진행하게 되었습니다. 이 자리에서 설립 취지문과 정관, 사업계획과 예산 등이 승인되었고, 표현의 자유 연대와 사이버 사찰금지법 제정에 많은 기여를 하셨던 이호중 교수(서강대 법학전문대학원)가 이사장으로 추대되었습니다. 또한, 그동안 표현의 자유와 개인정보 영역에서 많은 활동을 해 오셨던 김기중, 이은우 변호사, 국내외 인터넷 거버넌스 영역에서 많은 기여를 하고 계신 이영음 교수(한국방송통신대학교), 진보네트워크센터 오병일 활동가가 이사로 선임되었습니다. 또한, 공안 기구 감시를 위해 함께 활동을 해 오셨던 이광철 변호사가 감사를 맡아주셨습니다.

## ◈ 정보인권연구소 공식 창립행사 및 창립토론회 개최 [9월 23일]

정보인권연구소는 9월 23일 오후 4시, 시청역 부근의 스페이스노아 커넥트홀에서 공식 창립행사를 개최하였습니다.

먼저 정보인권연구소 이사장이신 이호중 교수님께서 정보화의 진전에 따라 정보인권 침해가 늘어남에도 이에 대한 인식이 부족한 현실에서 정보인권연구소가 운동의 폭과 깊이를 확대하는 역할을 할 것임을 다짐하는 힘찬 인사말씀을 해주셨구요. 네 분의 축사가 있었는데요. 특별히 선배(?) 연구소 설립자분들께 축사를 요청했습니다. 인권연구소 '창'의 류은숙 연구활동가는 인권연구소 설립 당시에 들었던 걱정과 우려에도 불구하고, 척박한 현실에서 민간 연구소가 갖는 가치가 작지 않다며 정보인권연구소의 건투를 빌어주셨습니다. 이어 한겨레 신문사 부설 '사람과디지털연구소' 구본권 소장님께서 연구소의 위상과 역할은 다르지만, 결국 사람을 위한 기술이라는 공통의 지향을 갖고 있는 두 연구소가 함께 해나가기를 바란다는 연대의 말씀을 해주셨습니다. 이어 '민주사회를위한변호사모임' 조영선 사무총장께서 축사를 해주셨는데요, 민변에서도 최근 정보인권과 관련된 위원회 설립을 고민하고 계신다고 합니다. 마지막으로



정보인권연구소의 산파 역할을 한 진보넷 이종회 대표님의 축사가 있었습니다.

2부에서는 창립토론회 〈디지털 압수수색과 정보인권〉이 개최되었습니다. 이사를 맡고 계신 김기중 변호사님께서 사회를, 그리고 이사장인 이호중 교수님이 발제를 맡아주셨는데요. 정보인권연구소 이사님들이 향후 실천적 연구에 앞장서시겠다는 의지를 보여주신 것이라고 생각합니다. ^.^ 연세대 법학전문대학원 한상훈 교수님, 민변의 이광철 변호사님, 전 노동당 부대표 정진우님, 진보넷 신훈민 변호사가 패널 토론을 진행했습니다.

이호중 교수님은 발제문에서 디지털 압수수색과 관련된 기존 대법원 판례 및 형사소송법 개정안의 의미와 한계를 지적하면서, 현행 법률과 판례에서 여전히 공백 상태로 남아있는 문제들을 제기하였습니다. 즉, 기존 대법원 판례는 하드디스크 등에 저장된 디지털 정보를 대상으로 한 것인데, 지난 2014년 카카오톡 압수수색 사례에서와 같이 서비스 업체에서 보관하고 있는 디지털정보의 압수수색이 어떤 원칙과 절차에 의해 이루어져야 하는지는 여전히 정립되지 않은 상태인 것이죠. 이러한 디지털 정보는 다수간의 '통신'과 관련된 내용이라는 점에서, 기존의 압수수색보다 조건과 절차가 더욱 엄격하게 규정될 필요가 있으며, '사이버사찰 긴급행동'은 이러한 내용을 담은 통신비밀보호법 개정안을 이미 국회에 발의한 바 있습니다. 나아가 최근 국가정보원의 RCS 해킹 프로그램을 통한 사찰 논란에서 볼 수 있듯, 기존의 감청과 압수수색으로 규정할 수 없는 새로운 방식의 수사기법을 어떻게 사회적으로 규제할 것인지도 과제로 남아 있습니다. 이 모든 의제들이 정보인권연구소가 안고 가야할 과제일 것입니다. 발제문은 정보인권연구소 홈페이지에서 다운받으실 수 있으니, 관심있으신 분들은 참고하시기 바랍니다.

## ◈ 토론회 〈유럽 사법재판소, 미국-EU 정보공유 협정 무효화의 의미〉 개최 [10월 22일]


지난 10월 6일, 유럽 사법재판소는 유럽연합(EU)와 미국 간 정보공유 협정(세이프하버)은 EU 시민의 프라이버시 권리를 충분히 보호하지 못하는 것으로 무효라고 판결했습니다. 지금까지 이 협정에 의해 구글, 페이스북 등 미국의 글로벌 기업들은 유럽 시민들의 개인정보를 미국의 본사와 공유할 수 있었습니다. 그런데, 유럽 사법재판소가 위 협정이 유럽 시민의 개인정보를 충분히 보호할 수 없다고 제동을 건 것입니다. 전자프론티어재단(EFF), 프라이버시인터내셔널(Privacy International) 등 전 세계 정보인권단체들은 이 결정을 환영하며, 스노든의 폭로로 드러난 미국 정부의 무차별 감시가 이러한 판결의 원인이 되었음을 지적하고 있습니다.

세계적인 개인정보보호 규범에 큰 영향을 끼칠 이번 판결의 의미를 분석해보기 위해 10월 22일, 프란체스코 교육회관에서 정보인권연구소가 토론회를 개최하였습니다. 이호중 교수님의 사회로, 정보인권연구소 이사를 맡고 계신 이은우 변호사님이 발제를 하셨고, 장여경 (진보네트워크센터 활동가), 양홍석(변호사, 법무법인 이공), 구본권(사람과디지털연구소 소장)님이 토론자로 참여해주셨습니다. 마침, 10월 16일에는 지난 2014년 국내 정보인권단체와 활동가들이 제기한, 구글에 대한 개인정보 공개 소송에 대한 선고가 있었는데요. 이 판결 역시 글로벌 기업인 구글이 국내 개인정보보호법을 준수할 의무가 있는지에 대한 것인만큼, 유럽 사법재판소의 판결과 연계하여 살펴볼 수 있는 계기가 되었습니다. 구글 판결에서는 국내 이용자들의 개인정보보호를 위해 구글 본사 역시 국내법을 준수할 필요가 있다는, 의미있는 결론을 내리기는 했지만, 구글이 미국법에 의해 비공개 의무가 있는 경우에는 공개하지 않아도 된다고 하여 아쉬움 역시 남겼습니다. 그러나 이제 1심이 끝났을 뿐이고, 이에 대해 항소를 할 예정입니다.



## ◈ 긴급세미나 〈테러방지법과 사이버테러방지법, 무엇이 문제인가〉 개최 [12월 7일]

파리에서 발생한 끔찍한 테러 이후, 전 세계적으로 테러 방지를 명분으로 한 통제 정책이 도입되고 있습니다. 한국 역시 예외가 아닙니다. 현재 국회에서는 12개에 이르는 테러방지법 및 사이버테러방지법이 계류되어 있습니다. 여당과 대통령은 테러방지법이 없어 한국이 테러에 무방비 상태라고 야단입니다. 사실일까요? 그렇지 않습니다. 이미 한국은 테러에 대응하기 위한 법제를 촘촘히 갖추고 있고, 오히려 너무 과도해서 인권침해 논란을 야기하고 있습니다. 이를 제대로 활용하지 못하여 테러에 제대로 대응하지 못한다면, 그것은 정부와 여당의 무능력에서 기인한 것일 뿐입니다. 현재 국회에 상정된 테러방지법안들은 단지 국정원의 권한 강화를 목적으로 하고 있습니다. 사람들의 고통과 슬픔을 이용해서 자신들의 권한 강화에 이용하는 것은 더욱 나쁜 일이지요.

이에 정보인권연구소는 새정치민주연합 국회정보위원회, 민주주의법학연구회, 민주화를위한전국교수협의회 등과 함께 테러방지법안과 사이버테러방지법안의 문제점 및 대안을 논의하기 위한 긴급 세미나를 개최하였습니다. 이번 이슈 리포트는 이 세미나의 발표문 및 관련 컬럼을 주로 싣고 있습니다. ❑

# 이슈리포트 <정보인권>을 발간하며 …

안녕하세요. 정보인권연구소(이사장 이호중)입니다.

정보인권연구소는 '인권'적 관점에서 정보화에 따른 사회변화를 분석하고 제도적 대안을 모색하기 위해 2015년 9월 23일 창립하였습니다.

정보인권연구소는 주요 정보인권 이슈에 대한 연구 성과와 관련 자료를 모아 이슈리포트 <정보인권>을 비정기적으로 발간할 예정이며, 정보인권에 관심 있는 연구자, 전문가, 활동가들께 발송하려고 합니다.

이슈리포트 <정보인권>을 계속 받아보고자 하시는 분들, 그리고 정보인권연구소의 활동에 함께 하고자 하시는 분들은 **정보인권연구소의 '회원'이 되어 주세요.**

* 아래 주소에서 온라인으로 가입하실 수 있습니다.
http://idr.jinbo.net/member

정보인권연구소에 많은 관심과 참여 바랍니다.

정보인권연구소 드림