민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회

수 신 각 언론사 사회부

발 신 **민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회**

(담당 : 진보네트워크센터 오병일 02-774-4551, 참여연대 이은미 02-723-5302)

제 목 [보도자료] 6개 시민단체, 국정원의 '사이버 보안' 권한 강화한 「국가사이버안보법」 국회발의(안) 반대 의견서 제출

날 짜 2017. 2. 14. (의견서 포함 총 17 쪽)

보 도 자 료

6개 시민단체, 국가정보원의 '사이버 보안' 권한 강화한 「국가사이버안보법」 국회발의안 반대 의견서 제출

1. 민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회는 오늘(2017.2.14) 지난 1월 3일 정부가 국회에 발의한 「국가사이버안보법」에 대한 반대 의견서를 국회 정보위원회 사무처와 국회의원실에 제출했다고 밝혔다.

2. 이 법안은 지난 2016년 9월 1일 국가정보원이 입법예고한 「국가 사이버 안보 기본법」을 수정한 것이다. 이들 단체들은 기존의 입법예고(안)에 대해서도 반대 의견서를 제출한 바 있으나, 국회에 발의된 법안 역시 입법예고(안)과 마찬가지로 국정원의 사이버 보안 관련 권한을 강화하여 국정원에 의한 사찰과 감시를 확대할 우려가 있다고 지적했다.

3. 이들 단체는 이 법안의 근본적인 목적은 현재 대통령 훈령인 '국가사이버안전관리규정'에서 규정하고 있는 국정원의 사이버 보안 권한을 법적으로 보장하고자 하는데 있다고 지적하며, 이미 현재 국정원이 수행하고 있는 사이버 보안 관련 업무도 국정원법에서 규정하고 있는 국정원 본연의 직무를 벗어난 것이기 때문에 오히려 기존 국정원의 권한에 대한 재검토와 국정원 개혁이 필요한 시점이라고 비판했다.

4. 나아가 이들 단체는 이 법안이 국정원의 권한을 민간의 정보통신망으로 확대하여 민간에 대한 국가 감시가 강화될 것을 우려한다고 지적했다. 법안은 심의기구로서 ‘사이버안보위원회’를 두고 있지만, 국정원이 사이버 안보 기본계획을 수립·시행하는 등 실질적인 컨트롤타워 역할을 국정원에 부여하고 있다. 또한, 국정원이 책임기관에 대한 실태평가를 하고, 사이버위협정보공유센터를 운영하며, 사이버 안보 연구기관을 설립할 수 있도록 하는 등의 권한을 국정원에 부여하고 있다. 이들 단체는 국정원의 강화된 권한을 통해 다른 행정부처, 공공기관, 보안 업계 및 학계 등에 자신의 통제력을 강화하여, 자신과 권력자의 이익에 위해 이들 기관에 부당한 영향력을 행사할 수 있다고 지적했다. 특히, ‘국가안보위협 사이버 공격’의 개념이 지나치게 폭이 넓어 이들 기관 정보통신망의 민감한 정보들에 영장이 없이도 접근할 수 있고, ‘사이버 안보’를 명분으로 ‘개인정보보호법’ 적용의 예외를 받아 특정 이용자를 감시, 사찰할 수 있는 위험성이 크다고 지적했다.

5. 이들 단체는 주요 선진국들은 사이버 보안을 위한 원칙으로 인터넷의 개방성과 혁신, 프라이버시권을 비롯한 인권 존중, 공공과 민간의 협력, 투명하고 민주적인 거버넌스, 국제협력과 신뢰 등의 원칙을 강조하고 있으며, 밀행성과 은밀성이라는 정보기관의 특성은 이해관계자와의 협력이나 이러한 핵심적인 가치와 충돌할 수밖에 없다고 지적했다. 또한, 어떤 나라도 비밀정보기관에 사이버 보안의 컨트롤타워를 맡기는 나라는 없으며, 사이버보안 관련 국정원의 기존 권한도 다른 행정기관으로 이양해야 한다고 주장했다. 끝.

▣ 별첨1. 의견서

국가사이버안보법 국회발의안에 대한 의견서

정부는 지난 1월 3일, 국가사이버안보법(안)(이하 법안)을 국회에 발의하였습니다. 이 법안은 지난 2016년 9월 1일 국가정보원이 입법예고한 국가사이버안보기본법(안)(이하 입법예고안)을 수정한 것입니다. 우리 시민사회단체들은 입법예고안에 대해서 반대 의견서를 제출한 바 있습니다. 이번에 국회에 발의된 법안 역시 기존 입법예고안과 마찬가지로 심각한 문제를 안고 있으며, 이에 아래와 같이 입법에 반대하는 의견을 제출합니다.

1. 국가정보원의 사이버 보안 권한은 시대착오적

이미 국가정보원은 2005년에 만들어진 국가사이버안전관리규정에 따라 국가사이버안전과 관련된 정책 및 관리를 총괄·조정하고 국가사이버안전전략회의와 국가사이버안전센터를 운영하는 등 정책적, 실무적 측면에서 국내 사이버 보안의 컨트롤타워로서 역할하고 있습니다. 그러나 국가사이버안전관리규정은 대통령 훈령에 불과하기 때문에, 이 법안의 근본적인 목적은 현재 국가사이버안전관리규정에서 규정하고 있는 국정원의 권한을 법적으로 보장해주는 것에 있습니다. 그러나 국정원이 사이버 보안의 컨트롤타워로서 역할하는 것은 국정원 본연의 직무를 벗어나는 것일 뿐만 아니라 인권을 침해할 우려가 있으며, 국내 사이버 보안에도 부정적인 영향을 미치게 됩니다. 따라서 기존 국정원의 권한에 대한 재검토가 필요한 시점에, 오히려 법적 근거를 마련해주는 것은 적절하지 못합니다.

현재 국정원은 국내 사이버 보안과 관련하여 다음과 같은 역할을 하고 있습니다.

- 국가사이버안전 관련 정책 및 관리 총괄·조정 (국가사이버안전관리규정)
  - 국가사이버안전기본계획 수립·시행
  - 국가사이버안전전략회의 및 대책회의 운영
  - 국가사이버안전센터 운영
- 공공분야 주요정보통신기반시설의 사이버 보안 (정보통신기반보호법)
- 공공기관 정보보안 관리실태 평가
- 국가·공공기관이 도입하는 정보보호시스템에 대한 보안적합성 검증
- 암호모듈 검증
- 보안관제 및 사이버 공격 정보 수집
- 정보보호제품 평가·인증에 관여

이와 같이 국내 사이버 보안 관련하여 국정원이 많은 역할과 권한을 갖고 있는 것은 여러 가지 문제점을 갖고 있습니다.

첫째, 이는 국정원법에서 규정한 국정원의 직무 범위를 크게 벗어난 것입니다.

국정원의 핵심 업무는 '국가안전보장'에 관련된 것이며, 비록 특정 사이버 공격이 국가안보에 영향을 미칠 수 있으나 사이버 보안 업무 전체를 국가안보적 시각에서 바라보는 것은 협소할 뿐만 아니라, 사이버 보안 정책에 부정적인 영향을 미칠 수 있습니다. '국가안보'의 특성상 사이버 보안 정책이 통제위주로 추진될 수 있으며 기본권과 자율성을 제약할 가능성이 크기 때문입니다. 예를 들어, 암호모듈 검증 업무를 보더라도, 과거에는 비밀정보요원만이 암호를 사용해 왔다면, 인터넷이 보편화된 현재에는 일반 기업 뿐만 아니라 개인 이용자의 통신 보안을 위해서도 암호 사용이 일반화되었습니다. 이런 상황에서 여전히 국정원이 과거의 관행대로 '암호자재'의 관리 업무를 담당하는 것은 적절하지 않습니다. 사이버 보안이 개인의 정보보안에서부터 인터넷 상의 사기나 해킹 등 민간 부문의 사이버 보안이 대부분을 차지하는 것을 고려할 때 국정원이 국내 사이버 보안의 총괄·조정 역할을 맡는 것은 과도한 직무범위 설정이라고 아니할 수 없습니다.

둘째, 국정원이 사이버 보안 관련 역할을 맡음으로써 사이버 보안 정책의 투명성과 사회적 감독 기능이 약화됩니다.

주지하다시피, 비밀정보기관으로서 국정원은 여타 정부부처에 비해 언론이나 국회에 의한 감독과 견제 기능이 약할 수밖에 없습니다. 조직, 인력, 예산, 사업 등 모든 측면에서 투명하게 공개되지 않기 때문입니다. 실제로 국내 사이버 보안 관련하여 국정원이 수행하고 있는 정책 자료, 사업 내용, 예산 등이 투명하게 공개되고 있지 않습니다. 이에 따라 사이버 보안 영역에서도 국정원의 권한 남용을 우려할 수 밖에 없고, 사이버 보안 정책에 대한 합리적인 토론이 가능하지 않기 때문에 오히려 국내 사이버 보안에 부정적인 영향을 초래하게 됩니다.

셋째, 사이버 보안을 위한 이해관계자와의 협력과 민간의 자율성을 저해합니다.

미국, 영국, 일본 등 세계 주요 선진국들은 사이버 보안 정책의 수립과 집행 과정에서 다양한 이해관계자의 참여와 민간의 자율성을 강조하고 있습니다. 네트워크의 운영이나 기술 개발이 주로 민간 영역에서 이루어지고 있기 때문입니다. 그러나 비밀정보기관인 국정원이 국가 사이버 보안의 총괄·조정 역할을 맡고 있는 상황에서는 이해관계자와의 협력이나 민간의 자율성을 기대할 수 있을지 의문입니다. 또한, 세계 주요 선진국들은 사이버 보안 전략을 수립하면서 기본권의 보장, 인터넷의 개방과 혁신, 민주적인 거버넌스를 핵심적인 가치로 내세우고 있습니다. 밀행성과 은밀성이라는 정보기관의 특성은 이해관계자와의 협력이나 이러한 핵심적인 가치와 충돌할 수밖에 없습니다.

넷째, 국정원에 의한 감시와 사찰, 인권 침해를 우려하지 않을 수 없습니다.

사이버 보안 업무의 경우 보안관제나 침해사고 분석 등의 과정에서 기업비

밀이나 이용자 개인정보 등이 유출되거나 악용될 위험성이 큽니다. 은밀한 감시와 사찰이 가능한 사이버 공간의 특성 상 국정원이 보안 업무를 담당하게 된다면, 권한 남용에 대한 우려가 더 커질 수 밖에 없습니다. 더구나 지금까지 국정원은 광범한 정보수집 권한과 수사권을 매개로 국내 정치에 개입하고 민간인을 사찰해 온 역사를 가지고 있습니다. 국정원에 대한 신뢰는 '앞으로 잘 하겠다'는 선언이 아니라 국정원을 감독할 수 있는 사법적, 입법적, 사회적 감독 체계가 전제되어야 합니다. 그러나 지난 2015년 국정원이 RCS라는 해킹 프로그램을 사용해왔음이 드러났음에도 불구하고, 이를 어떠한 용도로 사용해 왔는지에 대해 국회 조차도 사후검증에 실패한 바 있습니다. 이런 상황에서 국정원에 사이버 보안에 대한 막강한 권한을 부여할 수는 없는 노릇입니다.

어떠한 국가도 비밀정보기관이 국가 사이버 보안의 컨트롤타워를 담당하도록 하고 있지 않습니다. 예를 들어, 미국의 경우 백악관 산하에 사이버 보안국(Cybersecurity Directorate)과 사이버보안조정관(Cybersecurity Coordinator)을 두어 컨트롤타워 역할을 하고 있고, 국가기반시설의 사이버 보안은 국토안보부가 담당하고 있으며, 보안기술 표준과 관련한 업무는 상무부의 국립표준기술원(NIST) 등이 맡고 있습니다. 국내 사이버 보안 체제도 일반 행정부처에서 사이버 보안 관련 업무를 담당하고, 사이버 보안 관련 국정원의 역할은 해외정보전담기관으로서 자신이 취득한 사이버 보안 정보를 관련 부처에 제공하는 것으로 제한해야 합니다.

2. 국가사이버안보법(안) 조항별 문제점

사이버 보안 관련 국정원의 권한이 재검토되어야할 상황에서 이 법안은 입법될 필요가 없을 뿐만 아니라, 법체계적으로, 내용적으로 많은 문제점을 안고 있습니다.

(1) 용어의 모호성과 관련 법령과의 일관성 부족

이 법안에서 사용하고 있는 용어의 정의가 모호하여 자의적인 해석이 가능할 뿐만 아니라, 사이버 보안 관련 타 법령과의 일관성도 부족하여 오히려 법 적용의 혼란을 야기할 가능성이 큽니다.

- 동 법안은 '사이버안보'라는 용어를 법안의 제목과 본문에서 사용하고 있으며, 이를 "사이버공격으로부터 사이버공간을 보호함으로써 사이버공간의 기능을 정상적으로 유지하거나 정보의 안전성을 유지하여 국가의 안전을 보장하고 국민의 이익을 보호하는 것"이라고 정의(제2조 4호)하고 있습니다. 이는 국가사이버안전관리규정 제2조 3호에서 "사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태"로 규정한 '사이버안전'과 유사한 개념이지만 더욱 추상적으로 규정되어 있습니다. 예를 들어 정보의 기밀성·무결성·가용성 등은 ISO27000 국제표준에서도 규정하고 있지만, 정보의 안전성은 그 의미가 모호합니다. 또한, 이 개념은 '사이버 보안(Cyber Security)'과 유사한 의미로 보이지만, '안보'라는 용어를 사용함으로써 사이버 보안의 국가안보적 측면만을 왜곡해서 강조하고 있습니다. 이러한 용어 사용은 국정원의 권한을 합리화하기 위한 의도로 보이나, 사이버 보안, 정보 보안, 사이버 안전 등의 개념을 명확한 규정없이 혼용하는 것은 일관되고 체계적인 국내 사이버 보안 법제 구축에 저해가 될 뿐입니다.
- 동 법안은 2조 2호와 3호에서 '사이버 공격'과 '국가안보위협 사이버 공격'의 개념을 구분하고 있는데, '국가안보위협 사이버 공격'의 개념이 지나치게 폭이 넓어 사실상 '책임기관'으로 지정된 기관에 대한 사이버 공격은 그 규모나 파급력과 무관하게 모두 '국가안보위협 사이버 공격'으로 규정될 수 있습니다. 3호의 '나'는 정보통신기반시설과 공공기관을 '다'는 핵심기술보유 업체와 방위산업체를 의미하기 때문입니다. 또한, '가'의 경우는 북한을 지칭하는 것인데, 사이버 공격의 주체를 사전에 확인할 수 없고 사후에도 공격자를 특정하기 힘든 현실을 고려하면, 공격자가 북한이라는 '추정'을 근거로 폭넓게 해석

될 위험이 있습니다. 더구나 입법예고안에 비해 동 법안은 '그 지령을 받은 자가 하는 사이버 공격' 까지 포함하여, 자의적인 해석의 가능성을 더욱 넓히고 있습니다. 어떠한 사이버 공격이든 국정원이 '북한의 지령을 받았다' 는 명분으로 이 법령에서 규정한 권한을 이용하여 해당 정보통신망에 개입할 수 있게 됩니다.

2조(정의) 3. "국가안보위협 사이버공격"이란 다음 각 목의 어느 하나에 해당하는 사이버공격을 말한다. 가. 군사분계선 이북지역에 기반을 두고 있는 반국가단체의 구성원 또는 그 지령을 받은 자가 하는 사이버공격 나. 에너지·통신·교통·금융 등 국가기반체계 또는 전자정부를 운영하는 데 사용되는 사이버공간 등 국가적 사이버공간을 불법침입·교란·마비·파괴하는 사이버공격 다. 국가기밀, 군사기밀 또는 국가핵심기술 등 국가적으로 중요한 정보를 빼내거나 훼손하는 사이버공격

- 정보통신기반보호법은 "정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위" 를 '전자적 침해행위' 로 규정하고 있으나, 동 법안은 '사이버 공격' 으로 규정하여 법령간의 일관성이 없습니다. 한편, 정보통신망법은 '전자적 침해행위' 나 '사이버공격' 에 대한 정의규정 없이, 전자적 침해행위로 발생한 사태를 '침해사고' 로 정의하고 있습니다. 이 법안은 '국가안보위협 사이버공격' 이라는 새로운 용어를 사용함으로써 법령 사이의 혼란을 오히려 확대하고 있습니다.

⑵ 정보통신기반보호법과의 충돌

동 법안은 제6조 "「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설을 관리하는 기관" 을 책임기관으로 지정하고, 사이버 보안

관련 책임기관의 책임과 의무를 규정하고 있습니다. 그리고 제4조에서는 "사이버안보에 관하여는 다른 법률에 우선하여 이 법을 적용한다"고 하고 있습니다. 정보통신기반보호법은 국무총리 소속하에 정보통신기반보호위원회를 두고 있고, 공공부문의 기반시설의 경우 국가정보원이, 민간부문의 기반시설은 미래창조과학부가 관할하도록 하고 있습니다.

따라서 동 법에서 규정하고 있는 '국가 사이버안보 위원회'와 책임기관에 대한 국정원의 권한과, 정보통신기반보호법에 따른 '정보통신기반보호위원회' 및 민간부문의 기반시설에 대한 미래창조과학부의 권한이 충돌하거나, 혹은 정보통신기반보호법이 무력화될 수 있습니다. 이는 특히 민간부문의 사이버 보안에 이중, 삼중의 규제로 작용하여 오히려 부정적인 영향을 초래할 것입니다.

⑶ 국정원 권한 강화

동 법안은 국가사이버안전관리규정에 비해 적용 대상을 민간부문으로 확대하여 사이버 보안 관련 국정원의 권한을 강화하고 있으며, 입법예고안에 비해서도 국정원에게 더 많은 권한을 명확하게 부여하고 있습니다.

국가사이버안보법에 따른 국정원의 권한
- 국가 사이버안보 위원회에 상정할 안건을 미리 검토하고 위원회가 위임한 안건을 심의할 국가 사이버안보 실무위원회의 위원장을 국가안보실과 국가정보원의 공무원이 공동으로 수행함. (제5조 6항) - 지원기관의 지정, 지정 취소, 기술적 지원 실태 점검, 기술적 지원에 드는 비용의 전부 또는 일부 지원 권한 (제7조) - 사이버안보 연구기관의 설립, 혹은 지정 권한. (제9조) - 사이버안보 기본계획 수립·시행 권한(제10조) - 책임기관을 대상(국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관 및 민간부문 제외)으로 사이버 안보 실태평가 수행. 평가를 받은 책임기관의 장은 실태평가 결과에서 나타난 미비사항에 대해서는 개선 대책을 마

련하여 국가정보원장에게 통보하도록 함. (제11조)
- 사이버위협정보 공유센터 운영 (제12조)
- 책임기관의 사이버공간을 대상으로 사이버위기 대응 통합훈련 실시(제13조)
- 국가 차원의 사이버공격 탐지·대응체계 구축·운영(제14조)
- 사이버 공격에 대한 국가 차원의 일원화된 통보 및 조사 체계 구축·운영(제15조)
- 단계별 국가사이버위기경보 발령(제16조)
- 2개 이상의 상급책임기관에 대책본부를 구성하여야 하는 경우, 국정원이 대책본부 구성·운영(제17조)

- 국가사이버안전관리규정이 적용대상을 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망으로 한정하고 주요정보통신기반시설에 대해서도 정보통신기반보호법을 우선 적용하도록 한 반면, 동 법안은 책임기관으로 '국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관'과 주요정보통신기반시설, 국가핵심기술을 보유·관리하는 기관, 방위산업체 등도 포함하고 있습니다.
- 지원기관의 지정도 입법예고안에서는 국가사이버안보위원회가 하도록 되어 있었지만, 국회발의안은 국정원이 하도록 하고 있습니다. 또한, 지원기관의 지정뿐만 아니라, 지정 취소, 기술적 지원 실태 점검, 기술적 지원에 드는 비용의 전부 또는 일부 지원 권한도 부여하고 있습니다.
- 입법예고안에서는 국가사이버안보위원회가 심의·의결 권한이 있었지만, 국회발의안에서는 심의 권한만을 갖고 있고, 심의 내용도 입법예고안보다 축소되어 있습니다. 반면, 국가정보원은 사이버 안보 기본계획의 수립·시행 주체이며, 기본계획에 포함될 내용도 사이버안보의 정책 목표와 추진방향, 사이버안보와 관련된 제도 및 법령의 개선 등 보다 상세히 규정되어 있습니다. 법안에 따르면 국가사이버안보위원회는 심의기구일 뿐, 사실상 국가 사이버안보 콘트롤타워로서의 역할은 국정원에 부여하고 있음을 알 수 있습니다.
- 국회에 발의된 법안은 입법예고안보다 국정원의 권한을 강화하고 보다 명확하게 규정하고 있습니다. 예를 들어, 사이버위협정보공유센터는 국무조정실장(입법예고안)에서 국정원(국회발의안) 소속으로 변경되었고,

사이버공격 탐지・대응체계의 구축・운영 주체도 '정부'(입법예고안)에서 국정원(국회발의안)으로 명시되었습니다. 또한, 어차피 국정원이 주체가 아니었고 이미 타 법령에서 다루고 있는 산업육성, 인력양성, 교육홍보, 국제협력 관련 조항은 삭제된 반면, 사이버안보 연구기관 설립 및 지정 등 연구에 대한 권한은 원래 정부(입법예고안)로 되어있으나 국정원(국회발의안)이 권한을 갖는 것으로 명확하게 못을 박고 있습니다.

	입법예고안	국회발의안
지원기관의 지정	국가사이버안보위원회	국정원
사이버위협정보공유센터	국무조정실장 소속	국정원 소속
사이버공격 탐지・대응체계의 구축・운영 주체	정부	국정원
사이버위기 대응 훈련 실시	정부	상급책임기관 / 국정원
사이버위기대책본부의 구성	정부	상급책임기관 / 국정원

앞서 지적했듯이, 국가사이버안전관리규정에 근거한, 사이버 보안 관련 국정원의 권한도 재검토가 필요한 상황에서 국정원의 권한을 법으로 뒷받침하고, 그 권한을 확대하는 것은 어불성설입니다.

⑷ 정부부처 및 업계에 대한 국정원의 통제력 강화

국정원은 국정원법 1항 5호에서 규정하고 있는 기획・조정 권한을 통해 다른 행정부처의 상급 감독기관으로 군림해왔다는 비판을 받아 왔습니다. 그래서 수사권과 함께 국정원의 기획・조정 권한의 폐지가 국정원 개혁 방안의 하나로 제시되어 왔습니다. 그러나 이 법안은 다른 행정부처, 공공기관, 보안 업계 및 학계 등에 대한 국정원의 권한을 강화함으로써, 이들 기관에 대한 국정원의 통제력을 강화시키고 있습니다. 이러한 권한을 바탕으로 국정원은 자신과 권력자의 이익에 위해 이들 기관에 부당한 영향력을 행사할 우려가 있습니다.

- 이미 국정원은 공공기관에 대한 정보보안 관리실태 평가를 시행하고 있지만, 이 법안은 이에 대한 국정원의 권한을 보다 명확히 부여해주고 있습니다. 현재까지 국정원은 국정원법 제3조 2항, 전자정부법 제56조 3항, 정부업무평가기본법 제14조, 21조, 22조, 국가사이버안전관리규정 제9조 4항에 의건하여 정보보안 관리실태 평가를 수행하고 있지만, 법에 관련 사항이 구체적으로 규정되어 있지 않고 국가사이버안전관리규정은 훈령일 뿐입니다. 그러나 이 법안은 사이버안보(정보보안) 실태평가에 대한 국정원의 권한을 명시하고 있을 뿐만 아니라, 실태평가 결과를 국정원이 책임기관에게 통보하고, 책임기관은 개선 대책을 마련하여 국정원에게 통보하도록 규정하는 등 실태평가와 관련한 국정원의 역할을 더 구체화하고 있어, 행정기관에 대한 국정원의 통제력을 강화하고 있습니다.
- 한편, '국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관'과 주요정보통신기반시설, 국가핵심기술을 보유·관리하는 기관, 방위산업체 등은 국정원에 의한 실태평가 대상에서는 제외되는 등 일부 예외가 있지만, 기본계획에 따른 시행계획 이행, 사이버위협정보의 공유, 사이버위기 대응 통합훈련, 보안관제센터의 설치, 사이버공격에 관한 사항 통보 등 제반 영역에서 동 법안의 적용을 받게 됨으로써 국정원의 통제 하에 들어가게 됩니다. 예를 들어, 국정원이 수립하는 기본계획에 따라 작성된 상급책임기관의 시행계획에 따라야 하며, 국정원이 지휘하는 사이버위기 통합훈련에 참여해야 하고, 사이버위협정보를 제공해야 합니다. 법안에는 '제공할 수 있다'고 되어 있지만, 대통령령이 정하는 바에 따라 제공할 수 있도록 되어 있고, 비밀정보기관인 국정원과의 권력 관계상 사실상 의무조항으로 작용하게 될 가능성이 큽니다.
- 한국인터넷진흥원 등 공공기관 및 보안 업체 등에 대한 국정원의 통제력은 더욱 커질 것입니다. 이들은 '지원기관'으로 규정되어 있는데(제7조), 국정원은 이들 지원기관의 지정, 지정 취소, 기술적 지원 실태 점검, 기술적 지원에 드는 비용의 전부 또는 일부 지원 권한을 가지고 있기 때문입니다.
- 법안은 국정원이 사이버안보 연구기관을 설립하거나, 기존의 기관 또는

연구소를 연구기관으로 지정할 수 있도록 하고 있습니다. (제9조) 이에 따라 연구에 필요한 예산도 책정될 것이고, 이를 통해 국정원은 보안기술업계 및 학계에 대한 통제력을 확대할 수 있을 것입니다. 즉, 정부의 보안정책에 비판적인 기술계 및 학계의 연구자들에 대한 지원은 하지 않고, 자신의 입맛에 맞는 연구자들만 지원하는 방식으로 국내 사이버 보안 정책의 연구와 토론을 왜곡할 수 있게 됩니다. 이미 국내 보안업계와 학계에 대한 국정원의 영향력은 큰 것으로 알려져 있지만, 국정원이 연구비를 어떻게 사용하는 지는 투명하게 공개되어 있지 않습니다. 입법예고안의 '국가사이버안보법 제정안 비용추계서 미첨부사유서'에서는 "제9조제1항의 사이버안보 연구기관의 설립에 따라서도 추후 재정소요의 변화가 발생할 수 있다"고 하면서도, "그러나 관련 기관·조직들의 운영 및 사업내역은 국가안전보장에 관한 사항으로서 그 재정소요 첨부가 곤란한 한계가 있다" 고 하고 있습니다. 국정원이 관할하게 되면서 사이버 보안 분야가 모두 '국가안전보장' 에 관한 사항으로서 비공개가 되는 폐단을 여기서도 볼 수 있습니다. 투명성과 책임성 등 민주적 조직원리에 맞지 않는 이러한 운영은 국내 사이버 보안의 실효성과 사이버 보안 산업 발전이라는 측면에서도 도움이 되지 않습니다.

- 이 법안은 2개 이상의 상급책임기관에 사이버위기대책본부를 구성해야 하는 경우 국정원이 대책본부를 구성, 운영하도록 하고 있으며(제17조 1항), '국가안보위협 사이버공격' 에 대해서는 책임기관의 통보가 없더라도 사고조사를 할 수 있도록 하고 있습니다. (제15조 4항) 사이버 보안 사고의 조사 과정은 일종의 수사와 유사한 과정으로서 해당 기관의 민감한 정보에 접근할 수 있어 자칫 영장주의의 잠탈이 우려됩니다. 이러한 우려 때문에 현재 정보통신기반보호법에서도 국정원이 '금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니' 하도록 규정하고 있습니다. (정보통신기반보호법 제7조 3항) 집권여당과 다른 정당이 지방자치단체 등을 운영할 경우 국정원이 민감한 정보에 접근 가능할 때의 위험성은 더 커질 수 밖에 없습니다. "민간 분야 책임기관을 대상으로 사고 조사를 할 때에는 대통령령으로 정하는 바에 따라 관계 중앙행정기관, 수사기관 및

지원기관으로 구성된 합동조사팀을 운영" 하도록 하고 있지만, 현실적인 권력 관계상 국정원의 권한 남용을 제대로 견제할 수 있을지 보장하기 힘듭니다.

- 국방분야에 대해서는 실태평가 및 사고조사 등을 국방부가 수행하도록 함으로써 일정한 예외를 인정하면서도 국가안보에 필요하다고 판단되거나 국정원이 요청하면 관련 내용을 국정원에게 통보하도록 함으로써(제20조) 국정원을 민, 관, 군의 상급기관으로 위치시키고 있습니다. 국정원은 '요청만 하면' 국방관련 정보에도 접근할 수 있기 때문입니다.

(5) 국정원의 민간 사찰과 감시의 위험성

이 법안은 국가핵심기술을 보유·관리하는 기관, 방위산업체 등을 책임기관으로 규정함으로써 국정원의 사이버 보안 권한을 국가정보통신망에서 민간부문으로 확대하고 있습니다. 이에 따라 민간부문의 정보통신망에 대한 국정원의 사찰과 감시의 가능성이 우려됩니다. 민간부문의 책임기관도 동 법안에 따라 국정원이 관할하는 다양한 정책이나 조치들을 이행해야 하고, 위협정보공유 및 사고 조사 등의 과정에서 자신이 보유하고 있는 정보들을 국정원에 제공하거나 정보통신망에 대한 국정원의 접근을 허용해야 하기 때문입니다.

또한, '국가안보위협 사이버 공격'의 개념이 지나치게 폭이 넓어 사실상 '책임기관'으로 지정된 이들 민간 기관에 대한 사이버 공격이 그 피해의 규모와 상관없이 '국가안보위협 사이버 공격'으로 규정될 수 있고, 이 경우 국정원은 해당 기관의 요청이 없이도 사고 조사를 할 수 있으며, 이를 명분으로 해당 기관의 정보통신망에 접근하여 민감한 정보들에 영장이 없이도 접근할 수 있습니다.

무엇보다 심각한 문제는 이 법안이 개인정보보호법을 우회하여 사이버 보안을 명분으로 정보주체의 동의나 영장 없이도 개인정보에 자의적으로 접근할 수 있다는 것입니다. 제14조는 "보안관제센터는 사이버공격 탐지·대응에

필요한 범위에서 「개인정보 보호법」 제2조제1호에 따른 개인정보를 수집·이용할 수 있다"고 규정하고 있으며, 제21조에서는 "사이버안보를 위하여 처리되는 개인정보는 「개인정보 보호법」 제58조제1항에 따라 같은 법이 적용되지 아니하는 개인정보로 본다"고 규정하고 있습니다. 그러나 '사이버공격 탐지·대응에 필요한 범위' 및 '사이버안보를 위하여 처리되는 개인정보'는 지나치게 폭이 넓은 규정으로 사실상 '사이버 보안을 위해서'라는 이유만 들이대면 개인정보를 자유롭게 수집·처리할 수 있도록 허용하는 것이나 마찬가지입니다. 이는 정보주체의 동의권 및 영장주의 원칙을 훼손하는 것이며, 특정 이용자에 대한 국정원의 사찰, 감시의 위험성을 우려할 수밖에 없습니다.

3. 국내 사이버 보안 정책 개선 방안

이 법안이 '사이버 안보'라는 용어를 사용하고 있는 것 자체가 현재 국정원이 장악하고 있는 사이버 보안 체제의 폐단을 드러냅니다. 사이버 보안을 '사이버 안보'로 왜곡하여 자신의 관할 영역의 확대를 시도하고 있는 것입니다. 이제 국정원이 담당하고 있는 국내 사이버 보안 정책과 체제에 대한 전면적인 개혁이 필요합니다. 다음과 같은 몇 가지 정책 방안을 제안합니다.

(1) 체계적인 사이버 보안 전략의 수립

지금까지 수차례 사이버 안보 종합대책이 세워졌지만, 이는 사이버 보안 '전략'이라기 보다는 '종합대책' 수준이었습니다. 또한, 대규모 사이버 보안 사고가 발생할 때마다 임시방편적으로 만들어졌기에, 종종 과거에 내놓은 대책의 재탕이었습니다. 또한, 용어에서 드러나듯이, 사이버 보안에 대한 전체적 관점이 아닌, '국가안보'에 편향된 관점으로 수행되었습니다.

사이버 보안 전략은 우리 사회가 추구하는 가치에 기반하여, 그러한 가치와

원칙을 지키기 위한 제반 이슈들을 종합적으로 다룰 필요가 있습니다. 주요 선진국들은 사이버 보안을 위한 원칙으로 인터넷의 개방성과 혁신, 프라이버시권을 비롯한 인권 존중, 공공과 민간의 협력, 투명하고 민주적인 거버넌스, 국제협력과 신뢰 등의 원칙을 강조하고 있습니다. 우리의 사이버 보안 전략도 이러한 가치에 기반하여 수립될 필요가 있습니다. 비밀정보기관인 국정원이 주된 역할을 담당하는 현재의 사이버 보안 체제가 이러한 가치와 양립할 수는 없습니다.

⑵ 국정원 개혁과 사이버 보안 권한의 이양

국정원에 대한 불신은 단지 과거 국정원의 민간인 사찰과 정치 개입의 역사에 기인하는 것만은 아닙니다. 여전히 국정원에 대한 사법적, 입법적 감독체제가 부재하기 때문입니다. 국정원이 해킹 프로그램인 RCS를 사용해왔음을 인정했음에도 불구하고, 실제 어떠한 목적으로 어떻게 사용해왔는지 국회는 검증하는데 실패함으로써, 이러한 감독 체제가 부재하다는 것을 역설적으로 보여주었습니다. 만의 하나 국정원이 RCS를 민간인 사찰을 위해 사용하지 않았다고 하더라도, 사회적 감시와 견제 장치가 미흡한 기관은 언제든 자신의 권한을 남용 할 가능성을 배제할 수 없습니다.

국정원 권한 남용의 근본 원인으로 지적되고 있는 수사권, 기획·조정 권한은 폐지되어야 하고, 국정원은 전문적인 해외정보 수집기관으로 거듭나야 합니다. 그리고 정보기관에 대한 입법, 사법 기관의 감독체제가 마련되어야 합니다. 이것이 국정원이 신뢰를 회복할 수 있는 방도입니다.

국가 정보통신망의 사이버보안에 대한 책임, 정보보호시스템에 대한 인증, 암호 인증 등 현재 국정원이 담당하고 있는 사이버 보안 관련 역할도 일반 행정부처(예를 들어, 미래창조과학부, 국민안전처, 혹은 사이버보안청과 같은 별도의 부처 신설 등)로 이관되어야 합니다. 세계 어느 나라에서도 비밀정보기관이 사이버 보안의 실질적인 컨트롤타워 역할을 맡고 있는 나라는 없습니다. 정보기관의 역할은 자신들이 수집한 사이버 위협 등과 관련한 정

보들을 타 정부부처 및 관련 민간 기관과 공유하고 기술적으로 지원하는 것에 제한하고 있습니다. 국정원 역시 해외정보수집기관으로서 이러한 역할에 머물러야 할 것입니다.

(3) 사이버 보안 관련 법제의 체계적인 개편

현재 사이버 보안 관련 법령들은 용어의 정의도 통일되어 있지 않고, 중복적인 내용도 많습니다. 이런 상황에서 국가사이버안보법과 같이 또 하나의 유사 법령을 제정하는 것은 기존의 혼란을 가중시킬 뿐입니다. 합의된 사이버 보안 전략에 기반하여 관련 법령이 체계성과 상호 일관성을 갖도록 정비되어야 합니다. 또한, 사이버 보안 정책의 수립과 집행은 공개적이고, 관련 이해관계자들의 자유로운 참여와 협력에 기반하여 이루어져야 합니다.