입법의견서

발행일 2022. 12. 01.

국가사이버안보 기본법 제정안 (국가정보원공고 제2022-5호) 에 대한 의견서

국정원감시네트워크

민주사회를 위한 변호사모임, 민주주의법학연구회,
진보네트워크센터, 참여연대, 천주교인권위원회,
투명사회를 위한 정보공개센터, 한국진보연대

목차

.

목차 **2**

들어가며 **3**

1. 국정원 권한과 역할을 은폐하고 있는 국정원안 **4**

2. 국정원의 권한을 확대, 강화한 국정원안 **7**

3. 국가사이버보안의 실질적 컨트롤타워, 국정원 **9**

4. 사이버안보를 명분으로 한 국정원의 민간 사찰 우려 **11**

5. 국정원 개혁과 감독의 필요성 여전 **13**

들어가며

2022년 11월 8일, 국가정보원은 '국가사이버안보 기본법 제정(안)'(이하 국정원 2022년안)을 국가정보원공고 제2022-5호로 입법예고를 했다. 이 법안은 '국가사이버안보'와 관련한 국가정보원(이하 국정원)의 권한을 상세히 규정하고 있는데, 비밀정보기관인 국정원의 사이버보안 관련 권한을 인정하며 확대, 강화하고 있다.

국정원은 지난 2017년에도 '국가사이버안보법안'(이하 국정원 2017년안)을 국회에 제출했으며, 6개 시민사회단체들은 해당 법안에 대해 반대 입장을 담은 의견서를 발표한 바 있다. 국가사이버보안을 위한 조정과 대응은 필요하지만, 이는 비밀정보기관의 업무가 아니라, 일반 행정부처・기관들에서 투명성과 책무성을 갖고 이해관계자와의 참여와 협력을 통해 수행해야 하는 업무이기 때문이다.

네트워크 운영과 기술 개발은 주로 민간영역에서 이루어지고 있다. 그래서 미국, 영국, 일본 등 주요 선진국들에서도 사이버보안 정책의 수립과 집행과정에서 다양한 이해관계자의 참여와 민간의 자율성을 강조하며, 기본권의 보장, 네트워크의 개방과 혁신, 민주적 거버넌스를 핵심 가치로 내세운다.

그러나 국정원에 사이버보안 관련 권한을 지나치게 부여하거나 권한의 자의적 확대 해석과 집행 여지를 강화하면서 실질적 컨트롤타워 역할까지 맡기게 되면, 이해관계자들의 참여와 협력을 전제로 한 민주적 거버넌스의 가치와는 충돌이 있을 수밖에 없다. 국정원이 밀행성과 은밀성이라는 특성으로 움직여야 하는 비밀정보기관이기 때문이다. 더구나 국정원은 광범위하고 과도한 정보 수집과 대공수사권을 통해 불법적으로 국내 정치에 개입하고 민간인을 사찰해 왔다. 국정원에 대한 입법・사법・사회적 감독 체계도 여전히 미흡한 상황에서 국정원에 국가사이버보안 컨트롤타워까지 맡긴다면, 공공・민간 정보통신망에 대한 감시와 사찰로 인한 인권 침해를 우려할 수밖에 없다. 이같은 취지로 국정원감시네트워크는 2021년 12월 김병기 의원(더불어민주당)이 대표발의한 '국가사이버안보법안'(이하 김병기 의원안)에 대해서도 반대 의견을 표명한 바 있다.

국정원감시네트워크의 7개 시민사회단체는 국정원이 입법예고한 '국가사이버안보 기본법 제정(안)'에 대해서도 그동안 밝혀 온 취지와 아래와 같은 이유로 입법에 반대하는 의견을 제출한다.

1. 국정원 권한과 역할을 은폐하고 있는 국정원안

국정원 2022년안은 2017년안에 비해 그 내용을 간소화했다. 예를 들어, 책임기관, 지원기관, 사이버안보 전문기업 등 국정원을 정점으로 한 사이버보안 거버넌스 체제의 세부 규정과, 실태평가, 대응훈련, 탐지체계 등 사이버보안 활동과 관련된 구체적 조항들을 삭제했다. 이는 국정원의 관련 권한을 자의적으로 확대, 강화할 여지를 넓히면서도 법안에 대한 논란도 최소화하려는 의도로 보인다. 동시에 많은 규정들을 시행령에 위임함으로써 국정원은 오히려 자신의 의도에 맞게 세부 규칙을 정할 권한을 갖게 됐다.

또한 국정원 2022년안은 2017년안과 달리 여러 조항의 수행 주체를 '정부'로 하면서 명확히 규정하지 않음으로써 국정원의 실질적인 권한을 은폐하고 있다. 명확한 수행기관이 명시되어 있지 않을 경우, 2022년안의 주무부처인 국정원이 수행하겠다는 것으로 이해하는 게 합리적이다. 2022년안의 제5조는 정부로 하여금 사이버안보 기본계획을 수립・시행하도록 하고 있는데, 결국 국정원이 수행하겠다는 것으로 보인다. 사이버안보 위해자 추적 등 사이버위협을 무력화하기 위한 활동 방안과 공세적 대응조치 방안 마련을 위한 권한도 국정원이 수행하겠다는 것이다(제7조 제5항). 통합대응 조직을 국정원에 설치・운영할 수 있고, 국가사이버안보위원회의 통제를 받는다고 규정하고 있으나(제9조 제2항), 조직의 구성 및 운영에 관해 필요한 사항을 시행령에 위임(제9조 제3항)하면서 국정원의 민간 통제 권한을 강화하는 수단이 될 것으로 보인다. 사이버위기 경보의 발령(제10조)과 그에 따른 사이버위기대책본부의 구성(제11조)과 관련해 앞서 제11조 제1항에 '통합대응 조직'을 확대 운영할 수 있도록 열어두고, 제2항에서 국가안보실장이 대책본부장을 지명할 수 있게 해 국정원장이 대책본부장을 맡을 수 있는 법적 근거를 두고 있다.

2022년안에서 사이버위협 대응에 필요한 정보의 효율적인 공유 및 관리를 위한 국가 차원의 체계(예컨대, 김병기 의원안의 '사이버위협정보 공유센터')의 운영 권한(제8조)과 함께 사이버안보에 관련된 국내외 정보를 수집・종합 및 작성해 국회, 국가사이버안보위원회 및 대책본부 등에 보고・ 배포하는 주체를 국정원장으로 명시하고 있다는 점(제13조) 또한 관련 정보들이 국정원으로 모이는 구조를 법적으로 분명히 한 것이다. 사이버안보 관련 전문연구기관의 설립・운영(제14조)과 관련해서도 제14조 제2항에서 시행령으로 위탁기관이나 단체를 정할 수 있도록 했는데, 국정원 산하의 국가보안기술연구소가 그 역할을 맡게 될 가능성이 높다. 2022년안대로라면 전문연구기관을 신설한다고 하더라도 국정원의 통제 안에 놓일 수밖에 없다.

이런 권한은 2017년안에서는 국정원으로 명시했던 것들이다. 그 사이 국정원이 권한을 넓히려는 의지를 스스로 꺾은 게 아니라면, 2022년안은 오히려 자의적인 법 적용과 해석의 여지를 더 넓힌

것으로 봐야 한다.

국정원 2022년안 (입법예고)	국정원 2017년안 (20대 국회 제출)
제5조(사이버안보 기본계획의 수립・시행) ① 정부는 사이버안보 전략 및 정책의 효율적・체계적 추진을 위하여 3년마다 제6조 제1항에 따른 국가사이버안보위원회의 심의를 거쳐 다음 각 호의 사항이 포함된 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립・시행한다.	제10조(사이버안보 기본계획의 수립 등) ① 국가정보원장은 사이버안보 업무를 효율적이고 체계적으로 추진하기 위하여 3년마다 위원회의 심의를 거쳐 다음 각 호의 사항이 포함된 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립・시행하여야 한다.
제7조(예방・대응활동) ④ 정부는 사이버위협에 대한 국제적 공동대응을 위하여 우방국과의 교류, 국제형사사법 공조 등 국제협력을 강화하여야 한다. ⑤ 정부는 사이버안보 위해자를 추적하는 등 사이버위협을 무력화하기 위한 활동 방안과 억지력을 확보하기 위한 사법・경제・외교적 제재 등 공세적 대응조치 방안을 마련하여야 한다. ⑥ 제1항 내지 제5항에 따른 예방・대응활동의 방법・절차 및 세부 내용 등에 필요한 사항은 대통령령으로 정한다.	제14조(사이버공격의 탐지 등) ① 국가정보원장은 국가적 사이버공간에 대한 사이버공격에 신속하고 효율적으로 대응하기 위하여 관계 중앙행정기관의 장과 협의하여 국가 차원의 사이버공격 탐지・대응체계를 구축・운영하여야 한다.
제8조(정보의 공유) ① 정부는 사이버위협 대응에 필요한 정보의 효율적인 공유 및 관리를 위한 국가 차원의 체계를 운영할 수 있다.	제12조(사이버위협정보의 공유) ① 다음 각 호의 정보를 공유하기 위하여 국가정보원장 소속으로 사이버위협정보 공유센터를 둔다.
제9조(통합대응 조직의 운영) ① 정부는 사이버위협으로 인한 사고가 발생하거나 이에 대비하기 위하여 국가 차원의 일원화된 통보·조사 등 대응체계를 구축・운영하여야 한다.	제15조(사이버공격으로 인한 사고의 통보 및 조사) ① 국가정보원장은 책임기관의 사이버공간에서 사이버공격으로 인한 사고가 발생하는 경우에 대비하여 국가 차원의 일원화된 통보 및 조사 체계를 구축・운영하여야 한다.

② 제1항의 체계를 구축하기 위하여 대통령령이 정하는 관계 중앙행정기관, 정보수사기관, 기업 등이 참여하는 통합대응 조직을 국가정보원에 설치・운영할 수 있고, 통합대응 조직은 위원회의 통제를 받는다. ③ 제2항의 통합대응 조직의 구성 및 운영에 관하여 필요한 사항은 대통령령으로 정한다.	
제10조(사이버위기 경보의 발령) ① 정부는 사이버위협에 대한 체계적인 대응을 위하여 관심·주의·경계·심각 단계의 사이버위기 경보(이하 “경보”라 한다)를 발령할 수 있다.	제16조(사이버위기경보의 발령 및 조치) ① 국가정보원장은 사이버공격에 국가 차원에서 체계적으로 대응하기 위하여 단계별 국가사이버위기경보(이하 “경보”라 한다)를 발령할 수 있다. 이 경우 국가정보원장은 경보의 발령 시점과 단계 등에 관하여 국가안보실장과 미리 협의하여야 한다.
제14조(전문연구기관 설립 등) ① 정부는 이 법에 따른 사이버안보 관련 업무를 효율적으로 수행하기 위하여 전문연구기관을 설립・운영할 수 있으며, 이에 필요한 사항은 따로 법률로 정한다.	제9조(사이버안보 연구기관) ① 국가정보원장은 사이버안보에 필요한 정책과 기술을 연구・개발하기 위하여 사이버안보 연구기관을 설립하거나, 다른 법령에 따라 설립된 기관 또는 기관 부설연구소를 관계 중앙행정기관의 장과 협의하여 사이버안보 연구기관으로 지정할 수 있다.

2. 국정원의 권한을 확대, 강화한 국정원안

국정원 2022년안은 20대 국회에 제출한 국정원 2017년안에 비해 그 내용을 간소화했음에도 불구하고, 국정원의 권한을 확대, 강화하는 내용은 세심하게 챙기고 있다. 어차피 국가사이버보안과 관련한 일상적인 활동은 정보통신기반 보호법이나 국가사이버안전관리규정에 포함되어 있는 내용이고 보다 구체적인 규정은 시행령을 통해 만들 수 있다. 그러나 사이버안보 위해자 추적, 위협정보의 공유 및 운영과 같이 국정원이 반드시 필요한 권한은 포함했다.

기존 국정원 2017년안에는 없던 새로운 권한도 추가됐다. 안전한 정보통신기기 활용 관련 권한, 사이버안보 위해자 추적 등 일부 내용은 김병기 의원안에 포함되어 있는 것을 거의 그대로 가져와서 해당 내용을 기정사실화 하려는 의도로 보인다.

국정원 2022년안 (입법예고)	국정원 2017년안 (20대 국회 제출)
제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 4. “정보통신기기등”이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기·설비·소프트웨어 및 정보통신서비스를 말한다.	없음 ※ 참고 : 김병기 의원안 제2조 5. “정보통신기기등”이란 정보의 수집・가공・저장・검색・송신・수신 및 그 활용과 관련되는 기기・설비・소프트웨어 및 정보통신서비스를 말한다.
제3조(국가 등의 책무) ② 국가와 지방자치단체는 안전한 정보통신기기등이 개발・생산・유통될 수 있도록 시책을 강구하고, 안전한 정보통신기기등을 도입・활용하여야 한다.	없음
제7조(예방・대응활동) ⑤ 정부는 사이버안보 위해자를 추적하는 등 사이버위협을 무력화하기 위한 활동 방안과 억지력을 확보하기 위한 사법・경제・외교적 제재 등 공세적 대응조치 방안을 마련하여야 한다.	없음 ※ 참고 : 김병기 의원안 제13조(공급망 보안위협 예방) ① 국가정보원장은 국내에 공급되었거나 공급 예정인 정보통신기기등이 국제 및 국가배후 해킹조직에 의해 악용되어 초래될 수 있는 사이버안보에 대한 위협(이하 “공급망

	보안위협”라 한다)을 확인・견제・차단하기 위하여 해당 정보통신기기등에 대한 시험・분석・사실조회 등 검증 업무를 수행할 수 있다. 제16조(보호조치의 이행) ① 상급책임기관의 장은 사이버안보 위협행위에 악용되었거나 악용될 우려가 현저한 정보통신기기등을 인지한 경우, 소관사무 영역에서 해당 정보통신기기등을 운영・관리하는 책임기관에 대하여 관계 법령이 정하는 행정권한의 범위 내에서 필요한 조치(이하 “보호조치”라 한다)를 취하여야 한다. 제23조(사이버안보위해자추적) ① 국가정보원장은 국외・북한에 존재하는 사이버안보위협디지털정보가 사이버안보 위협행위의 확인・견제・차단에 필요하고 다른 방법으로는 접근이 어려운 경우에 한하여 대통령의 승인을 받아 사이버안보위해자추적을 할 수 있다.
제8조(정보의 공유) ① 정부는 사이버위협 대응에 필요한 정보의 효율적인 공유 및 관리를 위한 국가 차원의 체계를 운영할 수 있다.	제12조(사이버위협정보의 공유) ① 다음 각 호의 정보를 공유하기 위하여 국가정보원장 소속으로 사이버위협정보 공유센터를 둔다.

3. 국가사이버보안의 실질적 컨트롤타워, 국정원

국정원의 2022년안에서는 대통령 소속으로 국가사이버안보위원회를 두고 국가안보실장이 위원장을 맡도록 하고 있으나, 이번 안대로라면 일상적이고 실질적인 조정의 역할은 여전히 국정원이 맡을 것으로 보인다. 이는 2017년안에서도 마찬가지였다.

2022년안에서 국가사이버안보위원회의 안건을 사전에 검토하고 마련하기 위해 실무위원회를 두도록 하고 있다. 2017년안에서는 실무위원회의 위원장을 '국가안보실과 국가정보원의 공무원 중에서 소속 기관의 장이 지명하는 사람이 공동으로' 맡도록 했는데, 2022년안에서는 세부 규정을 삭제한 것이다. 국정원이 세부 규정의 빈 자리를 자의적으로 해석해 권한을 확대, 강화해 온 과거 사례에 비춰볼 때, 실무위원회의 위원장을 국정원이 맡을 것으로 보인다.

앞서도 언급했듯 2022년안에 따르면, 사이버위협정보의 공유를 위한 컨트롤타워도 국정원이 맡게 될 것이다(제8조). 국정원은 사고가 발생하거나 대비하기 위한 국가 차원의 일원화된 통보・조사 등의 대응체계 구축을 위한 통합대응 조직도 운영할 것이며(제9조), 사이버위기경보의 발령도 조정하게 된다(제10조). 이 모든 권한을 '국정원'에 명시적으로 부여한 2017년안과 달리 2022년안에서는 '국가 차원의 체계' 운영 주체를 '정부'로 표현함으로써 은폐하고 있는 게 문제다.

국정원 2022년안 (입법예고)	국정원 2017년안 (20대 국회 제출)
제5조(사이버안보 기본계획의 수립・시행) ① 정부는 사이버안보 전략 및 정책의 효율적・체계적 추진을 위하여 3년마다 제6조 제1항에 따른 국가사이버안보위원회의 심의를 거쳐 다음 각 호의 사항이 포함된 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립・시행한다.	제10조(사이버안보 기본계획의 수립 등) ① 국가정보원장은 사이버안보 업무를 효율적이고 체계적으로 추진하기 위하여 3년마다 위원회의 심의를 거쳐 다음 각 호의 사항이 포함된 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립・시행하여야 한다.
제6조(국가사이버안보위원회) ① 사이버안보에 관한 다음 각 호의 사항을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다. ③ 위원회의 위원장은 국가안보실장으로 한다.	제5조(국가사이버안보위원회) ① 사이버안보에 관한 다음 각 호의 사항을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다.

④ 위원회에 상정할 안건을 미리 검토하고 위원회가 위임한 사항을 처리하기 위하여 위원회에 사이버안보 실무위원회(이하 “실무위원회”라 한다)를 둘 수 있다.	③ 위원회의 위원장은 국가안보실장이 되고, 위원은 다음 각 호의 사람 중에서 국가안보실장이 임명하거나 위촉한다. ⑤ 위원회에 상정할 안건을 미리 검토하고 위원회가 위임한 안건을 심의하기 위하여 위원회에 국가 사이버안보 실무위원회(이하 “실무위원회”라 한다)를 둔다. ⑥ 실무위원회의 위원장은 국가안보실과 국가정보원의 공무원 중에서 소속 기관의 장이 지명하는 사람이 공동으로 된다.
제8조(정보의 공유) ① 정부는 사이버위협 대응에 필요한 정보의 효율적인 공유 및 관리를 위한 국가 차원의 체계를 운영할 수 있다.	제12조(사이버위협정보의 공유) ① 다음 각 호의 정보를 공유하기 위하여 국가정보원장 소속으로 사이버위협정보 공유센터를 둔다.
제9조(통합대응 조직의 운영) ① 정부는 사이버위협으로 인한 사고가 발생하거나 이에 대비하기 위하여 국가 차원의 일원화된 통보·조사 등 대응체계를 구축・운영하여야 한다. ② 제1항의 체계를 구축하기 위하여 대통령령이 정하는 관계 중앙행정기관, 정보수사기관, 기업 등이 참여하는 통합대응 조직을 국가정보원에 설치・운영할 수 있고, 통합대응 조직은 위원회의 통제를 받는다. ③ 제2항의 통합대응 조직의 구성 및 운영에 관하여 필요한 사항은 대통령령으로 정한다.	제15조(사이버공격으로 인한 사고의 통보 및 조사) ① 국가정보원장은 책임기관의 사이버공간에서 사이버공격으로 인한 사고가 발생하는 경우에 대비하여 국가 차원의 일원화된 통보 및 조사 체계를 구축・운영하여야 한다.
제10조(사이버위기 경보의 발령) ① 정부는 사이버위협에 대한 체계적인 대응을 위하여 관심·주의·경계·심각 단계의 사이버위기 경보(이하 “경보”라 한다)를 발령할 수 있다.	제16조(사이버위기경보의 발령 및 조치) ① 국가정보원장은 사이버공격에 국가 차원에서 체계적으로 대응하기 위하여 단계별 국가사이버위기경보(이하 “경보”라 한다)를 발령할 수 있다. 이 경우 국가정보원장은 경보의 발령 시점과 단계 등에 관하여 국가안보실장과 미리 협의하여야 한다.

4. 사이버안보를 명분으로 한 국정원의 민간 사찰 우려

국정원 2022년안은 국정원이 민간영역을 감시, 사찰할 수 있도록 열어두고 있다. 우선 제2조의 정의 규정이 모호해 국정원의 자의적으로 확대 해석할 수 있다. 제2조 제2호는 "사이버공격"을 "해킹, 컴퓨터 바이러스, 서비스 거부 등 전자적 방법으로 사이버공간을 불법침입・교란・마비・파괴 하거나, 정보를 빼내거나 훼손하는 등의 행위"로 정의하고 있으며, 제2조 제4호는 "사이버안보"를 "국제 및 국가배후 해킹조직과 북한, 외국 및 외국인・외국단체・초국가행위자 또는 이와 연계된 내국인의 국가안보와 국익에 반하는 사이버공격 행위 또는 활동(이하 "사이버위협"이라 한다)을 확인・견제・차단하고 이에 필요한 대응조치를 강구함으로써 국가의 안전을 보장하고 국익을 보호하는 것"으로 정의하고 있다. 제6조 제1항 제3호는 국가사이버안보위원회의 심의사항 중 하나로 "사이버안보 위해자 및 배후 국가・단체에 대한 대응조치에 관한 사항"을 포함하고 있으며, 제7조 제5항은 정부(국정원)가 "사이버안보 위해자를 추적하는 등 사이버위협을 무력화하기 위한 활동 방안과 억지력을 확보하기 위한 사법・경제・외교적 제재 등 공세적 대응조치 방안 마련"하도록 의무화하고 있다.

이와 같이 2022년안에서의 개념 정의는 (1) 사이버공격, (2) 사이버위협, (3) 사이버안보, (4) 사이버안보 위해자로 확장되고 있는데, 사이버안보의 기본적인 대상행위가 되는 '사이버공격'의 개념에 (ㄱ) 전자적 방법이기만 하면 모든 수단이 포함될 수 있고, (ㄴ) 사이버공간에 대한 불법침입・교란・마비・파괴 뿐 아니라 '정보'에 대한 탈취와 훼손, 더 나아가 여기에 규정되어 있지 않은 다른 행위 태양까지 모두 포괄된다(~ 등의 행위). 즉 수단과 행위의 측면에서 그 한계가 명확하게 제시되어 있지 않아 자의적 해석과 적용・집행이 가능하다. 여기에 '국익'이라고 하는 매우 추상적인 요건과 사이버공격 '활동'이라는 상당히 포괄적인 표현을 결부해 '사이버위협'과 '사이버안보' 개념을 정의하고, '위해자'라는 규범적・가치평가적 문구까지 더해 '사람'을 특정하고 있다. 내국인에 대한 제한적 요건으로는 '연계'라는 요소 밖에 없다. 따라서 사이버안보를 명목으로 민간인과 민간영역 정보통신망에 대한 감시와 사찰을 할 수 있다는 우려가 제기될 수밖에 없다. 이는 내국인 사찰을 금지하고자 한, 지난 정부 때 국정원 개혁의 취지를 거스르는 것이다.

예방 및 대응 활동도 "사이버위협을 무력화하기 위한 활동", "억지력을 확보하기 위한 사법・경제・외교적 제재 등 공세적 대응조치 방안" 등으로 추상적이고 포괄적으로 규정하고 있어, 국정원의 권한을 세세하게 규정하고 있는 김병기 의원안보다 오히려 국정원에게 강력한 권한을 부여하고 있다.

국정원 2022년안 (입법예고)

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

2. “사이버공격”이란 해킹, 컴퓨터 바이러스, 서비스 거부 등 전자적 방법으로 사이버공간을 불법침입·교란·마비·파괴하거나, 정보를 빼내거나 훼손하는 등의 행위를 말한다.

3. “사이버안보”란 국제 및 국가배후 해킹조직과 북한, 외국 및 외국인・외국단체・초국가행위자 또는 이와 연계된 내국인의 국가안보와 국익에 반하는 사이버공격 행위 또는 활동(이하 “사이버위협”이라 한다)을 확인·견제·차단하고 이에 필요한 대응조치를 강구함으로써 국가의 안전을 보장하고 국익을 보호하는 것을 말한다.

제6조(국가사이버안보위원회) ① 사이버안보에 관한 다음 각 호의 사항을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다.

1. 사이버안보와 관련한 전략・정책・법령 및 예산에 관한 사항
2. 사이버안보 기본계획 등 중장기 대책에 관한 사항
3. 사이버안보 위해자 및 배후 국가·단체에 대한 대응조치에 관한 사항
4. 그 밖에 위원회의 위원장이 부의하거나 위원이 제출한 사항

제7조(예방・대응활동)

⑤ 정부는 사이버안보 위해자를 추적하는 등 사이버위협을 무력화하기 위한 활동 방안과 억지력을 확보하기 위한 사법・경제・외교적 제재 등 공세적 대응조치 방안을 마련하여야 한다.

5. 국정원 개혁과 감독의 필요성 여전

국정원 2022년안의 제12조 및 제13조에서도 국회의 감독 권한을 일정하게 부여했으나, 국회의 전문성과 자원한 한계를 고려할 때 그 실효성은 제한적일 것으로 보인다. 비단 사이버보안 업무의 감독 때문이 아니라 국정원 업무 전반에 대한 국회의 감독 권한이 강화될 필요가 있다.

거의 예산 전체가 '특수활동비'로 가려지거나 정부 각 행정부처・기관들의 예산 속으로 숨겨지면서 비밀주의로 일관해 왔던 국정원 예산 구조부터 개혁하고 국회의 예산 심의부터 한층 강화해야 한다. 국정원 직원에 대한 직무감찰, 회계검사, 적법활동 여부 등의 감찰업무를 수행할 '정보감찰관' 신설, 국회 정보위원회 산하에 정보・인권분야의 전문가로 구성한 <전문가형 정보기관 감독기구>(옴부즈맨 등) 설치・운영, 「국회법」 제54조2 제1항의 단순위헌 결정에 따른 국회 정보위원회 회의의 공개 등은 매우 시급한 과제들이다.

무엇보다 국정원감시네트워크를 비롯해 시민사회가 오랫동안 주장해 왔듯, 국정원의 사이버보안 권한은 타 부처로 이관되어야 한다. 국가사이버보안 업무는 비밀정보기관의 업무가 아니기 때문이다. 적어도 비밀정보기관에 대한 민주적 통제가 이루어지고 있는 주요 선진국들에서는 정책적・실무적 차원에서 국가사이버보안의 컨트롤타워를 비밀정보기관들에 맡기지 않는다. 국내 사이버보안 관련 업무도 과학기술정보통신부나 (가칭)사이버보안청 등 일반 행정부처에서 총괄하도록 해야 한다. 사이버보안과 관련한 국정원의 역할은 해외정보전담기관으로서 관련 정보 수집으로만 제한적으로 수행하도록 해야 한다.

국정원이 사이버보안 업무를 수행할 경우 투명성과 책무성을 담보하기 힘들다. 비밀정보기관이기 때문이다. 사이버보안과 관련해 반드시 필요한 민간의 이해관계자들과의 원활한 소통과 협력관계를 구축하기도 힘들다. 국정원에 의한 민간 사찰과 우려가 끊임없이 제기될 수밖에 없다. 투명성과 책무성을 담보할 수 없는 국정원 같은 비밀정보기관에서 사이버보안 전략과 정책이 민주적으로 수립될 것이라 기대할 수도 없고, 가능하지도 않다.

물론 국가사이버보안과 관련된 기본법의 제정은 필요하다. 사이버보안 관련 현행 법률들도 체계적으로 개정할 필요가 있다. 사이버보안 컨트롤타워도 필요하다. 다만 이를 위해서는 국정원이 갖고 있던 사이버보안 권한의 이전이 반드시 전제되어야 한다. 문재인 정부에서 미완에 그친 국정원 개혁과 감독의 강화는 여전히 더는 미룰 수도 없고, 미루어서도 안 될 시급한 과제다.

국정원감시네트워크 입법의견서

국가사이버안보 기본법 제정**(**안**)**
(국가정보원공고 제**2022-5**호**)**에 대한 의견서

발행일 2022. 12. 01.
발행처 국정원감시네트워크
담당
- 진보네트워크센터 오병일 대표 02-774-4551
- 참여연대 장동엽 선임간사 02-723-5302 tsc@pspd.org

※ 이 자료는 웹사이트에서 다시 볼 수 있습니다.