입법의견서

발행일 2021.12.16.

국가사이버안보법안(김병기 의원 대표발의)에 대한 의견서

국정원감시네트워크

민들레_국가폭력피해자와 함께하는 사람들, 민주사회를 위한 변호사모임,
민주주의법학연구회, 진보네트워크센터, 참여연대, 천주교인권위원회,
투명사회를 위한 정보공개센터, 한국진보연대

목차

목차	2
들어가며	3
1. 총론	3
사이버보안은 정보기관의 업무로 적절하지 않음.	4
2. 법률안의 문제점	7
(1) 국정원의 컨트롤타워 역할의 문제점	7
(2) 민간 기업에 대한 사찰 및 통제	8
가. 책임기관을 민간기업으로 확대	8
나. 통합보안관제체계로의 연계의 문제점	10
다. 국정원법의 직무범위 이탈	11
(3) 정부부처 및 업계에 대한 국정원의 통제력 강화	12
(4) 사이버 조사권을 통한 내국인 사찰 우려	15
가. 전기통신 당사자의 임의 제공	16
나. 디지털정보확인조치의 문제점	17
(5) 용어의 모호성과 관련 법령과의 일관성 부족	20
(6) 정보통신기반보호법과의 충돌	22

들어가며

2021년 11월 4일, 더불어민주당 김병기 의원은 ‘국가사이버안보법안’(이하 김병기안)을 대표발의 하였습니다. 이 법안은 국가 사이버보안과 관련한 국가정보원(이하 국정원)의 권한을 상세히 규정하고 있는데, 국가정보원법에서 규정하고 있는 이상으로 그 권한을 확대, 강화하고 있습니다.

국정원은 지난 2017년 1월 3일, 같은 이름의 법안을 정부안으로 발의한 바 있으며, 이에 대해 우리 시민사회단체들은 [의견서](#)를 발표하여, 국정원의 사이버보안 권한은 시대착오적일 뿐만 아니라 인권 침해 우려가 있고 이해관계자 사이의 협력을 저해하는 등 오히려 국내 사이버보안에 부정적 영향을 미칠 수 있음을 우려한 바 있습니다. 김병기안은 당시 국정원이 발의한 법안보다 국정원의 권한을 훨씬 강화하였을 뿐만 아니라 새로운 권한도 부여하고 있는 바, 김병기안에 더욱 반대하지 않을 수 없습니다. 이에 아래와 같이 입법에 반대하는 의견을 제출합니다.

1. 총론

사이버보안은 정보기관의 업무로 적절하지 않음.

국정원은 그동안 명확한 법적 근거도 없이 사이버보안 관련된 정책 및 관리를 총괄·조정하고 국가사이버안전전략회의와 국가사이버안전센터를 운영하는 등 정책적, 실무적 측면에서 국내 사이버 보안의 컨트롤타워로서 역할해 왔다. 그동안 국정원이 사이버테러방지법이나 국가사이버안보법 등을 통해 자신의 사이버보안 권한에 대한 법적 근거를 마련하려고 했던 것도 이 때문이다. 결국 2020년 말에 개정된 국정원법은 '(공공) 기관 대상 사이버공격 및 위협에 대한 예방 및 대응'을 국정원의 직무로 규정하였다.

김병기안에서는 사이버보안과 관련한 국정원의 직무와 권한을 다음과 같이 더욱 구체적으로 규정하고 있는데, 2017년 발의된 국정원안보다 더욱 강화된 것이다.

사이버안보위원회 위원장 및 실무위원회 담당 (제5조)
국가사이버안보센터 운영 (제7조)
사이버안보 기본계획 수립·시행 (제9조)
책임기관을 대상으로 통합훈련 실시(제10조)
책임기관을 대상으로 사이버안보 활동에 대한 실태평가 실시, 평가 기준 배포, 개선대책에 대한 이행여부 확인, 사이버안보실태 합동평가단 구성·운영(제12조)
정보통신기기등에 대한 시험·분석·사실조회 등 검증 업무 수행(제13조)
통합보안관제체계 구축·운영, 책임기관에 대한 합동 보안관제 실시, 사이버안보 위협 탐지규칙정보의 배포(제14조)
사이버안보 위협행위의 대응에 필요한 조사 및 조치 실시, 책임기관의 장에게 필요한 조치 요청(제15조)
책임기관에 대하여 정보통신기기등의 운영제한 등 필요한 조치를 취해줄 것을 요청 또는 요구(제16조)
사이버안보 위기 경보 발령(제17조)
사이버안보 위기대책본부 구성(제18조)
사이버안보위협디지털정보 중 통신사실확인자료 또는 송·수신이 완료된 전기통신 내용을 제공하여 줄 것을 전기통신 당사자에게 요청(제19조)
국가안보를 위한 디지털정보확인조치 수행(제20조)
사이버안보위해자추적 권한(제23조)

그러나 지난 2017년 정부 발의 국가사이버안보법안에서 지적한 바와 같이, 사이버안보(보안) 기본계획의 수립, 사이버보안 실태 평가, 보안 관제 및 보안 사고에 대한 조사 및 대응, 위기 경보의 발령, 기술 연구 등 사이버보안 관련 업무는 해외정보기관으로서 국정원의 역할이 아니며, 역할이 되어서도 안된다. 국정원이 사이버보안 관련 권한을 보유할 경우 발생할 수 있는 문제점을 다시 한번 지적한다.

첫째, 사이버보안 업무는 정보기관의 업무로 부적절하다.

국가사이버안보법안은 사이버 ‘안보’라는 표현을 사용하고 있으나, 사실상 그 내용은 사이버 보안(Security) 업무와 다르지 않다. 특정 사이버 공격이 국가안보에 영향을 미칠 수 있으나 사이버 보안 업무 전체를 국가안보적 시각에서 바라보는 것은 오히려 사이버 보안 정책에 부정적인 영향을 미칠 수 있다. ‘국가안보’의 특성상 사이버 보안 정책이 통제위주로 추진될 수 있으며 기본권과 자율성을 제약할 가능성이 크기 때문이다. 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 일반화되었다. 이런 상황에서 여전히 국정원이 과거의 관행대로 ‘암호자재’의 관리 업무를 담당하는 것은 적절하지 않다. 사이버 보안이 개인의 정보보안에서부터 인터넷 상의 사기나 해킹 등 민간 부문의 사이버 보안이 대부분을 차지하는 것을 고려할 때 국정원이 국내 사이버 보안의 컨트롤타워 역할을 맡는 것은 과도한 직무범위 설정이라고 아니할 수 없다.

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

주지하다시피, 정보기관으로서 국정원은 여타 정부부처에 비해 언론이나 국회에 의한 감독과 견제 기능이 약할 수밖에 없다. 조직, 인력, 예산, 사업 등 모든 측면에서 투명하게 공개되지 않기 때문이다. 실제로 국내 사이버 보안 관련하여 국정원이 수행하고 있는 정책 자료, 사업 내용, 예산 등이 투명하게 공개되고 있지 않다. 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 된다.

셋째, 사이버 보안을 위한 이해관계자와의 협력과 민간의 자율성을 저해한다.

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

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

사이버 보안 업무의 경우 보안관제나 침해사고 분석 등의 과정에서 기업비밀이나 이용자 개인정보 등이 유출되거나 악용될 위험성이 크다. 은밀한 감시와 사찰이 가능한 사이버 공간의 특성 상 국정원이 보안 업무를 담당하게 된다면, 권한 남용에 대한 우려가 더 커질 수 밖에 없다. 더구나 지금까지 국정원은 광범한 정보수집 권한과 수사권을 매개로 국내 정치에 개입하고 민간인을 사찰해 온 역사를 가지고 있다. 국정원에 대한 신뢰는 '앞으로 잘 하겠다'는 선언이 아니라 국정원을 감독할 수 있는 사법적, 입법적, 사회적 감독 체계가 전제되어야 한다. 비록 지난 2020년 말 국정원법이 개정되었음에도 불구하고, 국정원에 대한 사회적 감독 체계는 여전히 미흡하다. 이런 상황에서 국정원에 사이버 보안에 대한 막강한 권한을 부여할 수는 없다.

어떠한 국가도 정보기관이 국가 사이버 보안의 정책적, 실무적 차원에서 컨트롤타워를 담당하도록 하고 있지 않다. 국내 사이버 보안 체제도 과학기술정보통신부 혹은 (가칭)사이버 보안청 등 일반 행정부처에서 사이버 보안 관련 업무를 담당하도록 하고, 고위급 거버넌스 기구에서 부처간 협의가 이루어질 수 있도록 하며, 사이버 보안 관련 국정원의 역할은 해외정보전담기관으로서 사이버 보안 관련 정보의 수집으로 제한해야 한다.

2. 법률안의 문제점

이 법안은 법 체계적으로도, 내용적으로도 다음과 같은 많은 문제점을 갖고 있다.

(1) 국정원의 컨트롤타워 역할의 문제점

김병기안 (2021년)	국정원안(2017년)
<p>제5조(사이버안보위원회) ① 사이버안보에 관한 중요 사항을 심의하기 위하여 <u>국가정보원장</u> 소속으로 사이버안보위원회(이하 “위원회”라 한다)를 둔다.</p> <p>③ 위원회의 <u>위원장은 국가정보원장</u>이 되고, 위원회의 위원은 다음 각 호에서 정한 사람으로 한다.</p>	<p>제5조(국가사이버안보위원회) ① 사이버안보에 관한 다음 각 호의 사항을 심의하기 위하여 <u>대통령</u> 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다.</p> <p>③ 위원회의 <u>위원장은 국가안보실장</u>이 되고, 위원은 다음 각 호의 사람 중에서 국가안보실장이 임명하거나 위촉한다.</p>
<p>제7조(국가사이버안보센터의 설치) ① 국가차원의 종합적이고 체계적인 사이버안보 업무 수행을 위하여 국가정보원장 소속으로 국가사이버안보센터를 둔다.</p>	없음

지난 2017년에 국정원이 발의한 ‘국가사이버안보법안’은 그나마 형식적으로는 국가안보실장이 위원장을 맡는 대통령 소속 국가사이버안보위원회가 최고 컨트롤타워 역할을 하도록 하였다. 그런데 김병기안은 아예 국가정보원장이 위원장이 되는 사이버안보위원회를 국정원 내에 설치하도록 하고 있다. 나아가 국정원안에서는 포함되지 않았던, 국가사이버안보센터의 설치를 규정하고 있다. 국가사이버안보센터는 실무적인 차원에서 핵심적인 역할을 하고 있는 곳으로, 법적 근거없이 지금까지 운영되어 왔던 ‘국가사이버안전센터’를 법제화하려는 것이다.

그러나 국정원이 국가 사이버보안의 컨트롤타워 역할을 맡는 것이 적절한 것인지 의문이다. 앞서 언급한 것처럼 국정원이 사이버보안 관련 업무를 담당하는 것 자체가 부적절할 뿐 아니라, 부처간 조정의 역할을 맡아야 할 지위에 있는 것도 아니다. 국가사이버안보위원회는 비단 기술적인 보안

대책을 수립하는 기관이 아니라, 사이버범죄에 대한 수사, 국제 협력, 사이버 국방전략, 민간 이해관계자와의 협력 등 여러 정부부처간 조정 역할을 담당해야 하는 기관이다. 해외정보기관인 국정원이 유관 부처의 하나로 참여할 수는 있겠으나, 컨트롤타워 역할을 담당하는 것은 매우 부적절하다. 또한 이는 국정원이 일종의 상급기관으로 군림해 온 지금까지의 부적절한 관행을 지속시킬 위험성이 있다.

(2) 민간 기업에 대한 사찰 및 통제

김병기안은 국정원이 공공기관 뿐만 아니라 민간의 정보통신망에도 자신의 권한을 행사할 수 있도록 열어두고 있다. 김병기안은 '사이버안보 위협행위'(제2조 제4호)에 국가핵심기술 등 산업기술을 전자적으로 부정하게 취득하는 사이버공격행위를 포함하고 있다. 무엇보다 정보통신기반시설, 국가핵심기술 보유기관, 방위산업체, 집적정보통신시설사업자, 전자금융기반시설 운영사업자 등 주요 민간기업을 이 법의 관할 대상에 포함하고 있는데, 이는 2017년 국정원안에 비해서도 그 관할범위가 확대된 것이다. 나아가 시행령을 통해 국정원은 언제든지 책임기관의 범위를 확대할 수 있기 때문에, 주요 민간기업들이 국정원의 관할 대상이 될 수 있다. 이에 따라 민간기업에 대한 국정원의 사찰이 가능해지고 이러한 정보 수집을 근거로 민간기업을 통제할 우려가 있다.

가. 책임기관을 민간기업으로 확대

김병기안 (2021년)	국정원안 (2017년)
<ol style="list-style-type: none"> 1. 국회 · 법원 · 헌법재판소 · 중앙선거관리위원회 회의 행정사무를 처리하는 기관 및 그 소속 기관 2. 중앙행정기관 및 그 소속 기관 3. 특별시 · 광역시 · 특별자치시 · 도 · 특별자치도(이하 “시·도”라 한다)와 시 · 군 · 자치구 및 그 소속 기관, 시 · 도 교육청과 교육지원청 및 그 소속 기관 4. 「국군조직법」에 따른 각 군, 합동참모본부, 국방부 직할 부대 및 직할 기관 	<ol style="list-style-type: none"> 1. 국회 · 법원 · 헌법재판소 · 중앙선거관리위원회 회의 행정사무를 처리하는 기관 및 그 소속 기관 2. 중앙행정기관 및 그 소속 기관 3. 특별시 · 광역시 · 특별자치시 · 도 · 특별자치도(이하 “시·도”라 한다)와 시 · 군 · 자치구 및 그 소속 기관, 시 · 도 교육청과 교육지원청 및 그 소속 기관 4. 「국군조직법」에 따른 각 군, 합동참모본부, 국방부 직할 부대 및 직할 기관

<p>5. 「지방공기업법」 제49조에 따른 지방공사 및 같은 법 제76조에 따른 지방공단</p> <p>6. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관</p> <p>7. 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설을 관리하는 기관</p> <p>8. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따라 지정된 국가핵심기술을 보유·관리하는 기관</p> <p>9. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 조 제10호에 따른 전문연구기관</p> <p>10. 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 보유한 기관</p> <p>11. 「전기통신사업법」 제6조에 따른 기간통신사업의 등록을 받은 자와 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설사업자</p> <p>12. 「전자금융거래법」 제2조제21호에 따른 전자금융기반시설을 운영하는 기관이나 단체 또는 사업자</p> <p>13. 그 밖에 사이버안보 위협으로부터 소관사무 영역 보호가 필요한 기관 또는 단체 중에서 대통령령으로 정한 기관 또는 단체</p>	<p>5. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관</p> <p>6. 「지방공기업법」 제49조에 따른 지방공사 및 같은 법 제76조에 따른 지방공단</p> <p>7. 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설을 관리하는 기관</p> <p>8. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따라 지정된 국가핵심기술을 보유·관리하는 기관</p> <p>9. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 조 제10호에 따른 전문연구기관</p> <p>10. 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 보유한 기관</p>
---	---

책임기관으로 지정된다는 것은 아래와 같은 여러 의무가 부과되며 국정원의 감독 하에 놓이게 된다는 의미이다. 즉, 민간 기업 역시 국정원의 요청에 따라 임직원을 파견하고, 관련 자료를 제출하거나 공유해야 하며, 자신의 보안관제센터를 국정원의 통합보안관제체계와 연계해야 한다. 국정원이 요구하는 여러 조치들을 이행해야 하는 것은 물론이다.

사이버안보위원회의 요청에 따른 자료 제출 (제6조 제2항)

국가사이버안보센터의 운영을 위하여 필요한 경우, 소속 공무원 또는 임직원의 파견 등 협조 (제7조 제2항)

사이버안보 위협행위로부터 소관사무 영역을 안전하게 보호, 이를 위한 전담조직 설치 (제8조)

사이버안보 위협 대응훈련 또는 국정원과의 통합훈련 실시 (제10조)

사이버안보 관련 정보의 공유(제11조)

사이버안보 실태평가 실시, 그 결과에 따라 국정원에 개선대책 통보 (제12조)

공급망 보안위험에 대한 심의 결과에 따라 (상급책임기관의 경우) 소관사무 영역에서 관계 법령에 따른 행정처분 등 적절한 대응조치 (제13조)

사이버안보 위협행위를 즉시 탐지·대응을 하기 위한 보안관제센터를 국정원의 통합보안관제체계와 연계하여 구축·운영(제14조 제2항)

탐지규칙정보를 국정원으로부터 제공받아 탐지 결과를 국정원에 제공(제14조 제3항)

사이버안보 위협행위로 피해 발생시 국정원에 즉시 통보, 국정원이 요청한 조치의 집행(제15조)

(상급책임기관의 경우) 사이버안보 위협행위에 악용되었거나 악용될 우려가 현저한 정보통신기기등을 인지한 경우, 소관사무 영역에서 해당 정보통신기기등을 운영·관리하는 책임기관에 대하여 보호조치 시행(제16조 제1항)

국정원의 요구에 따라 정보통신기기등의 운영제한 등 필요한 조치 이행(제16조 제2항)

사이버안보 위기경보 단계별로 사이버안보 위협행위에 대한 대비태세를 강화하는 등 필요한 조치 이행(제17조)

사이버안보 위기대책본부장의 요청에 따라 대책본부에 참여 (제18조)

나. 통합보안관제체계로의 연계의 문제점

특히 보안관제센터를 ‘통합보안관제체계와 연계하여 구축·운영’하도록 요구하는 것을 우려하지 않을 수 없다. 김병기안은 국정원이 통합보안관제체계를 이용하여 책임기관에 대한 보안관제를 실시할 수 있도록 하고 있다. 민간 책임기관의 정보통신망에 접근하여 트래픽을 분석할 수 있도록 열어두고 있는 것이다. 이 과정에서 국정원은 민간의 정보통신망에 대한 상세한 정보를 습득하고 때로는 영향력을 행사할 수 있게 될 것이다. 설사 해당 민간업체가 외부의 기술적 도움이 필요하다고 하더라도 어디에 요청할 것인지는 해당 업체가 판단할 문제이며, 국정원에 마음대로 접근할 수 있는 권한을 부여하는 것은 큰 문제다.

또한 법안에서는 ‘사이버안보’라고 표현하고 있지만 사실상 ‘사이버보안(Cyber Security)’과 관련한 모든 것이 대상이 될 수 있다. 특정한 사이버보안 사건 혹은 조치가 국가안보에 영향을 미치는지 여부는 결국 국정원의 자의적인 판단에 맡겨져있기 때문이다. 모든 것이 연결되고 빠르게 전파될 수 있는 사이버공간에서 아무리 작은 사건이라도 국가안보와 연결되거나 영향을 미칠 수 있다고 간주하는 것은 어려운 일이 아닐 것이다.

다. 국정원법의 직무범위 이탈

이처럼 국정원의 권한을 민간기업으로 확대하는 것은 국정원법을 벗어나는 것이다. 국정원법 제4조 제1항 제4호는 ‘사이버공격 및 위협에 대한 예방 및 대응’ 직무의 대상을 아래와 같이 규정하고 있다. 전술한 바와 같이, 시민사회단체는 제4호의 사이버보안 업무가 국정원의 직무가 되어서는 안된다고 생각하지만, 김병기안과 같이 주요 민간기업으로 책임기관을 확대하는 것은 국정원법에서 규정한 직무범위조차 넘어서는 것이다.

제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응

가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회

나. 지방자치단체와 그 소속기관

다. 그 밖에 대통령령으로 정하는 공공기관

(3) 정부부처 및 업계에 대한 국정원의 통제력 강화

국정원은 구 국정원법 제3조 제1항 제5호(개정 국정원법 제4조 제1항 제5호)에서 규정하고 있는 기획·조정 권한을 통해 다른 행정부처의 상급 감독기관으로 군림해왔다는 비판을 받아 왔다. 그래서 수사권과 함께 국정원의 기획·조정 권한의 폐지가 국정원 개혁 방안의 하나로 제시되어 왔다. 그러나 김병기안은 다른 행정부처, 공공기관, 보안 업계 및 학계 등에 대한 국정원의 권한을 강화함으로써, 이들 기관에 대한 국정원의 통제력을 강화시키고 있다. 이러한 권한을 바탕으로 국정원은 자신과 권력자의 이익에 위해 이들 기관에 부당한 영향력을 행사할 우려가 있다.

김병기안 (2021년)	국정원안(2017년)
<p>제12조(보호활동에 관한 평가) ① 국가정보원장은 <u>책임기관을 대상으로</u> 사이버안보 활동에 대한 실태평가(이하 “사이버안보 실태평가”라 한다)를 매년 1회 이상 실시하여야 한다.</p> <p>④ 국가정보원장은 사이버안보 실태평가 결과를 해당 기관에게 통보하고, 해당 기관은 결과를 통보받은 날로부터 2개월 이내에 국가정보원장에게 개선대책을 통보하여야 한다.</p>	<p>제11조(사이버안보 실태평가) ① 국가정보원장은 <u>제6조제1항제2호부터 제6호까지의 책임기관 중에서 대통령령으로 정하는 책임기관을 대상으로</u> 사이버안보를 위한 업무수행체계 구축, 사이버공격 예방 및 대응활동 등에 관한 실태평가(이하 “실태평가”라 한다)를 할 수 있다.</p> <p>③ 국가정보원장은 실태평가의 결과를 평가 받은 책임기관의 장에게 통보하여야 한다.</p> <p>④ 평가를 받은 책임기관의 장은 실태평가 결과에서 나타난 미비사항에 대해서는 개선 대책을 마련하여 국가정보원장에게 통보하여야 한다.</p>

이미 국정원은 공공기관에 대한 정보보안 관리실태 평가를 시행하고 있지만, 이 법안은 이에 대한 국정원의 권한을 보다 명확히 부여해주고 있다. 현재까지 국정원은 구 국정원법 제3조 2항, 전자정부법 제56조 3항, 정부업무평가기본법 제14조, 21조, 22조, 국가사이버안전관리규정 제9조 4항에 의거하여 정보보안 관리실태 평가를 수행하고 있지만, 법에 관련 사항이 구체적으로 규정되어 있지 않고 국가사이버안전관리규정은 훈령일 뿐이었다. 그러나 김병기안은 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 있다.

그나마 2017년 국정원안에서는 '1. 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관' 및 민간 업체는 제외하고 행정기관, 공공기관만을 대상으로 하고 있었는데, 김병기안은 모든 책임기관을 대상으로 실태평가를 하도록 하고 있다. 이제 국회 등을 포함한 모든 책임기관이 국정원의 통제 하에 들어가게 되는 것이다. 앞서 언급한 바와 같이 책임기관에게는 여러 의무가 부과되며 국정원의 감독을 받게 된다. 이는 군 역시 마찬가지인데, 국방부 역시 책임기관이며 제37조에 따라 제12조에 따른 보호활동에 대한 평가 및 제15조에 따른 사이버안보 위협에 대한 조사만 국정원 대신 국방부장관이 직접 수행할 수 있을 뿐이다. 즉, 국방부 역시 책임기관의 다른 의무를 수행해야 하며 국정원의 감독을 받게 된다.

김병기안 (2021년)	국정원안(2017년)
<p>제15조(사이버안보 위협행위에 대한 조사) ① 책임기관의 장은 소관사무 영역에서 사이버안보 위협행위로 인한 피해가 발생한 때에는 국가정보원장에게 즉시 통보하여야 한다.</p> <p>② 국가정보원장은 제1항에 따른 통보를 받은 경우에는 사이버안보 위협행위의 대응에 필요한 조사 및 조치를 실시하여야 한다.</p>	<p>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.</p> <p>② 책임기관의 장은 소관 사이버공간에서 사이버공격으로 인한 사고가 발생한 경우에는 피해를 최소화하는 조치를 하고, 그 사실을 다음 각 호의 구분에 따른 사람에게 통보하여야 한다. 이 경우 국가안보위협 사이버공격에 관한 사항은 국가정보원장에게 함께 통보하여야 한다.</p> <p>1. 상급책임기관: 국가정보원장. 이 경우 특별시장·광역시장·특별자치시장·도지사·특별자치도지사(이하 “시·도지사”라 한다)는 행정자치부장관에게, 시·도 교육감은 교육부장관에게 함께 통보하여야 한다.</p> <p>2. 시·군·자치구: 해당 시·군·자치구를 관할구역으로 하는 시·도지사</p>

	<p>3. 교육지원청: 해당 교육지원청을 관할하는 시·도 교육감</p> <p>4. 그 밖의 책임기관: 해당 책임기관을 관리·감독하는 상급책임기관의 장</p> <p>③ 상급책임기관의 장은 제2항제2호부터 제4호까지의 통보(국가안보위협 사이버공격에 관한 통보는 제외한다)를 받은 경우 신속히 사이버공격으로 인한 사고의 그 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 하여야 한다. 이 경우 해당 기관의 장은 필요하면 지원기관의 장에게 기술적 지원을 요청할 수 있다.</p> <p>④ 국가정보원장은 다음 각 호의 경우(제6조제1항제1호에 따른 책임기관 소관 사이버공간에서 사이버공격으로 인한 사고가 발생한 경우에 대해서는 해당 기관의 장이 요청하는 경우로 한정한다)에는 지체 없이 사이버공격으로 인한 사고의 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 하여야 한다. 이 경우 민간 분야 책임기관을 대상으로 사고 조사를 할 때에는 대통령령으로 정하는 바에 따라 관계 중앙행정기관, 수사기관 및 지원기관으로 구성된 합동조사팀을 운영하여야 한다.</p> <p>1. 제2항 각 호 외의 부분 후단에 따라 국가안보위협 사이버공격에 관한 통보를 받은 경우</p> <p>2. 제2항제1호에 따른 통보를 받은 경우</p> <p>3. 국가안보위협 사이버공격으로 인한 사고가 발생하였으나 제2항 각 호 외의 부분 후단에 따른 통보를 받지 못한 경우</p>
--	---

2017년 국정원안의 경우 사이버공격으로 인한 사고의 통보는 상급기관으로, 국가안보위협 사이버공격에 대한 통보는 동시에 국정원에도 하도록 하였다. 김병기안은 사이버안보 위협행위로 인한 피해가 발생한 경우 국정원에 즉시 통보하도록만 규정하고 있는데, 사이버안보 위협행위가

명확한 기준없이 사실상 모든 보안사고를 포함할 수 있다는 점에서 국정원이 모든 종류의 보안 사고에 개입할 수 있다.

또한 김병기안에서는 사이버보안 사고의 조사 과정에 대해서 구체적으로 규정하고 있지 않은데, 조사 과정은 일종의 수사와 유사한 과정으로서 해당 기관의 민감한 정보에 접근할 수 있어 자칫 영장주의의 잠탈이 우려된다. 이러한 우려 때문에 현재 정보통신기반보호법에서도 국정원이 ‘금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니’하도록 규정하고 있다. (정보통신기반보호법 제7조 3항) 집권여당과 다른 정당이 지방자치단체 등을 운영할 경우 국정원이 민감한 정보에 접근 가능할 때의 위험성은 더 커질 수 밖에 없다. 또한 2017년 국정원안에서는 “민간 분야 책임기관을 대상으로 사고 조사를 할 때에는 대통령령으로 정하는 바에 따라 관계 중앙행정기관, 수사기관 및 지원기관으로 구성된 합동조사팀을 운영”하도록 하고 있지만, 김병기안에서는 이러한 형식적인 견제 조치조차 규정하지 않고 있다.

(4) 사이버 조사권을 통한 내국인 사찰 우려

김병기안은 국정원이 내국인이 보유하고 있는 정보통신망과 컴퓨터, 그리고 디지털 정보를 당사자도 모르게 들여다볼 수 있도록 허용하고 있다. 이는 내국인에 대한 사찰을 중단하고 국정원이 해외정보기관의 역할에 충실하도록 개정한 국정원법 개정의 취지를 거슬러, 사실상 국정원이 과거와 같이 국내외 막론하고 사찰할 수 있는 권한을 유지하겠다는 것이나 다름없다.

가. 전기통신 당사자의 임의 제공

제19조(전기통신 당사자의 임의 제공) ① 누구든지 처분권한 있는 자의 동의 없이 국내디지털정보보관자가 보관하는 사이버안보위협디지털정보를 열람 또는 취득하여서는 아니 된다. 다만, 다음 각 호의 경우에는 해당 법령에 정하는 바에 따른다.

1. 이 법과 형사소송법, 군사법원법, 통신비밀보호법 등에 따른 절차에 의하여 적법하게 열람 또는 취득하는 경우

2. 「개인정보 보호법」 제58조에 따라 수집 또는 제공 요청되는 개인정보

3. 그 밖에 다른 법령에 따라 처분권한 있는 자의 동의 없이도 열람 또는 취득이 가능한 정보 또는 자료

② 국가정보원장은 사이버안보 정보수집에 필요한 조사(「국가정보원법」 제5조제2항0 따른 조사를 포함한다)를 실시하는 경우, 사이버안보위협디지털정보 중 통신사실확인자료 또는 송·수신이 완료된 전기통신 내용을 제공하여 줄 것을 전기통신 당사자(일방 또는 쌍방을 말한다. 이하 같다)에게 요청할 수 있다.

③ 제1항에 따른 요청을 받은 전기통신 당사자는 「통신비밀보호법」 제3조제1항 본문의 규정에도 불구하고 해당 통신사실확인자료 또는 전기통신 내용을 국가정보원장에게 제공할 수 있다.

우선, 제19조는 국정원이 법원의 허가 없이도 전기통신 당사자로부터 디지털 정보를 제공받을 수 있도록 허용하고 있다. 제1항은 ‘「개인정보 보호법」 제58조에 따라 수집 또는 제공 요청되는 개인정보’의 경우 해당 디지털정보의 보관자 및 정보주체의 의사와 무관하게, 혹은 인지없이도 개인정보를 수집할 수 있도록 하고 있다. 그러나 개인정보보호법 제58조는 ‘국가안전보장과 관련된 정보 분석’이라는 명분 하에 국정원이 개인정보보호법을 포괄적으로 면제받을 수 있도록 보장하고 있어 시민사회의 비판을 받아온 조항이다. 김병기안은 여기서 더 나아가 이를 보유하고 있는 자의 동의없이도 취득할 수 있도록 하고 있는 것이다. 사실상 국정원이 개인정보를 정보주체나 보유자의 동의나 인지없이 수집할 수 있도록 열어놓고 있다.

제2항에서는 사이버안보 정보수집에 필요한 조사를 할 때, 통신사실확인자료나 송·수신이 완료된 전기통신 내용을 제공해줄 것을 요청할 수 있도록 하고 있다. 다시 말해 네이버, 카카오

등의 서버에 저장되어 있는 이메일이나 메신저 대화 내용 등을 해당 업체에 요구할 수 있다. 여기서 사이버안보 정보수집에 필요한 조사는 「국가정보원법」 제5조제2항에 따른 조사를 포함한다고 하는데, 국정원법에 따른 조사의 개념조차 명확하지 않은데, 그것보다 폭넓은 것으로 규정되어 있는 ‘사이버안보 정보수집에 필요한 조사’의 개념은 무엇인지 의문이다.

통신비밀과 관련한 자료라면 이미 통신비밀보호법에 따라 수집하면 될 것인데 제19조 제2항의 규정을 둔 것은 번거롭게 통신비밀보호법을 따르지 않고 사업자에게 바로 요청하겠다는 것이나 다름없다. 요청을 받은 전기통신 당사자가 해당 자료를 ‘제공할 수 있다’로 규정하고 있어 제공의 의무를 부여하고 있는 것은 아니지만 국정원이 요청할 경우 사업자들이 과연 이를 거부할 수 있을지 의문이다. 설사 거부한다고 하더라도 제20조에 따라 국정원은 자료의 제출을 강제할 수 있다. 나아가 통신비밀보호법은 통신사실확인자료 및 전기통신내용의 ‘실시간’ 감청을 규율하고 있는 것과 달리, 이 법안은 통상의 경우 압수수색 영장이 필요한 ‘송·수신이 완료된 전기통신 내용’까지 다루고 있어 훨씬 폭이 넓다. 이제 법원의 허가서나 영장도 없이 손쉽게 통신 관련 자료를 취득할 수 있도록 하겠다는 것이다.

나. 디지털정보확인조치의 문제점

국정원은 전기통신 당사자로부터 디지털정보를 임의제출 받지 못할 경우, 고등법원 수석판사의 허가를 받아 디지털정보의 제출을 강제할 수 있다. 그러나 이는 국정원에 ‘사이버안보’로 이름표만 바꿔달고, 국내 정보 수집권한과 수사권을 부여하는 것이나 마찬가지다.

제20조(국가안보를 위한 디지털정보확인조치) ① 국가정보원장은 사이버안보 위협행위에 직접적으로 관련되고 국내디지털정보보관자가 보관하고 있는 사이버안보위협디지털정보에 대한 정보수집이 필요한 경우로서 다른 방법으로는 수집이 어려운 경우에 한정하여 고등법원 수석판사의 허가를 받아 디지털정보확인조치를 할 수 있다.

여기서 ‘국내디지털정보보관자’라 함은 “내국인 또는 국내 기관·법인·단체로서, 사이버안보위협디지털정보 또는 사이버안보위협디지털정보가 저장된 정보저장매체의 소유자, 소지자 또는 보관자”를 의미한다. (제2조 제8호) 즉, 내국인 누구나를 대상으로 국정원이 디지털

정보 수집을 하도록 허용하고 있는 것이다. 이는 국정원을 해외정보수집기관으로 하고자 한 국정원법 개정의 취지에서 벗어난다.

또한 국정원에게 어떠한 이유로 이러한 권한을 부여해야 하는지 의문이다. 사이버안보 위협행위 혹은 정보통신망 침해행위는 불법일 것이므로 수사기관이 적법절차에 따라 수사를 하면 될 것이다. 만일 불법 행위와 연계되지 않은 디지털정보라면 수사기관이든 국정원이든 접근할 수 있도록 강제해서는 안될 것이다. 어떠한 경우이든 국정원에게 이러한 권한을 줄 이유가 없다. 그런데 수사권이 없는 국정원이 수사기관보다 간소한 절차를 통해 관련 정보에 접근할 수 있도록 하는 이유는 무엇일까. 고등법원 수석판사의 허가를 거친다고는 하지만, 그 이전에 정보기관인 국정원에 이러한 권한을 부여할 이유가 없다.

사이버안보 위협행위와 직접적으로 관련된 것인지 여부도 자의적이기 짝이 없다. 예를 들어, 제2조 제4호 가목의 경우 어떠한 사이버공격 행위 또는 활동을 조사하기 이전에 ‘국제 및 국가배후 해킹조직 등’에 의한 것인지 어떻게 알 수 있는지 의문이다. 나목의 경우 공공기관을 대상으로 하는 사소한 정보보안 침해행위가 모두 사이버안보 위협행위로 규정될 수 있다. 여기서도 개념만 ‘사이버안보’라는 표현을 사용했을 뿐, 모든 종류의 정보보안 침해행위가 대상이 될 수 있다.

4. “사이버안보 위협행위”란 국가안보와 국익에 반하는 다음 각 호의 어느 하나에 해당하는 행위 또는 활동을 말한다.

가. 국제 및 국가배후 해킹조직을 비롯하여 「국가정보원법」 제4조제1항제3호에 따른 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인[이하 “사이버안보위해자(危害者)”라 한다]이 행하는 사이버공격 행위 또는 활동

나. 「국가정보원법」 제4조제1항제4호 각 목의 기관을 대상 사이버공격 및 위협 행위 또는 활동

다. 「전자정부법」 제56조제3항에 따라 보안조치를 이행하여야 하는 정보통신망에서 전자문서에 대한 위조·변조·훼손·유출 행위 또는 활동

라. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조에 따른 국가핵심기술 또는 국가연구개발사업으로 개발한 산업기술 또는 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 전자적 수단을 통해 부정하게 취득하는 사이버공격행위 또는 활동

마. 그 밖에 「국가정보원법」 등 개별 법령에 따라 국가정보원의 직무에 관련되고 전자적 수단으로 이루어진 안보침해행위 또는 활동

고등법원 수석판사의 허가 절차가 현실적으로 제대로 된 통제 기능을 할 수 있을지도 의문이지만, 국정원은 제20조 제7항에 따라 아예 고등법원 수석판사의 허가없이도 디지털정보확인조치를 할 수 있다. 물론 “집행 후 지체 없이 제2항부터 제6항까지의 규정에 의하여 고등법원 수석판사에 허가청구를 하여야 하며, 그 긴급 디지털정보확인조치를 한 때부터 36시간 이내에 고등법원 수석판사의 허가를 받지 못한 때에는 열람 또는 취득한 정보를 지체 없이 폐기”하도록 하고 있지만, 이후 열람 또는 취득한 정보를 폐기하더라도 정보로서의 가치가 없어지는 것은 아니다. 어차피 수사기관이 아닌 국정원이 취득한 자료는 이후 재판 절차에 사용하기 위한 목적이라기 보다는 정보 수집 자체가 목적일 것이기 때문이다.

제21조(디지털정보확인조치의 집행 등)

⑥ 국가정보원장은 정보통신서비스 영역에서 처리되는 사이버안보위협디지털정보에 대하여 제21조제1항 또는 제7항에 따른 디지털정보확인조치를 집행한 경우에는, 집행한 날부터 30일 이내에 그 집행의 대상이 된 정보통신서비스의 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제4호에 따른 정보통신서비스 이용자를 말한다. 이하 같다)에게 디지털정보확인조치를 집행한 사실과 그 일자 등을 서면으로 통지하여야 한다.

⑦ 제6항에도 불구하고 다음 각 호의 어느 하나에 해당하는 사유가 있는 때에는 그 사유가 해소될 때까지 통지를 유예할 수 있다.

1. 디지털정보확인조치를 통지할 경우 국가의 안전보장·공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때
2. 디지털정보확인조치를 통지할 경우 사람의 생명·신체에 중대한 위험을 초래할 염려가 현저한 때

⑨ 국가정보원장은 제7항의 사유가 해소된 때에는 그 사유가 해소된 날부터 30일 이내에 제6항의 규정에 의한 통지를 하여야 한다.

제21조 제6항은 디지털정보확인조치의 집행 대상이 된 정보통신서비스 이용자에게 집행 사실과 일자 등을 서면으로 통지하도록 하고 있다. 통신비밀보호법에서와 마찬가지로, 여기서도 집행의 이유가 빠져있다.

정보통신서비스 이용자는 자신이 집행 대상이 되었다는 사실을 영구적으로 통지받지 못할 수도 있다. 제21조 제7항은 특정 사유로 통지를 유예할 수 있고 제7항은 사유가 해소된 때에는 그 사유가 해소된 날부터 30일 이내에 통지하도록 하고 있지만, 국정원은 사유가 해소되지 않았다는 이유로 영구적으로 통지하지 않을 수 있기 때문이다. 이러한 문제를 해소하기 위해서는 특정 기간 이후로는 반드시 통지하도록 하여 디지털정보확인조치의 남용을 방지할 필요가 있다.

(5) 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 크다.

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 공격 행위를 말한다.

3. “사이버안보”란 사이버공격을 확인·견제·차단하고 이에 필요한 대응조치를 강구함으로써 국가의 안전을 보장하고 국익 및 국민의 안전을 보호하는 것을 말한다.

4. “사이버안보 위협행위”란 국가안보와 국익에 반하는 다음 각 호의 어느 하나에 해당하는 행위 또는 활동을 말한다.

가. 국제 및 국가배후 해킹조직을 비롯하여 「국가정보원법」 제4조제1항제3호에 따른 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인[이하 “사이버안보위해자(危害者)”라 한다]이 행하는 사이버공격 행위 또는 활동

나. 「국가정보원법」 제4조제1항제4호 각 목의 기관을 대상 사이버공격 및 위협 행위 또는 활동

다. 「전자정부법」 제56조제3항에 따라 보안조치를 이행하여야 하는 정보통신망에서 전자문서에 대한 위조·변조·훼손·유출 행위 또는 활동

라. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조에 따른 국가핵심기술 또는 국가연구개발사업으로 개발한 산업기술 또는 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 전자적 수단을 통해 부정하게 취득하는 사이버공격행위 또는 활동

마. 그 밖에 「국가정보원법」 등 개별 법령에 따라 국가정보원의 직무에 관련되고 전자적 수단으로 이루어진 안보침해행위 또는 활동

김병기안은 ‘사이버안보’라는 용어를 법안의 제목과 본문에서 사용하고 있다. 이를 “사이버공격을 확인·견제·차단하고 이에 필요한 대응조치를 강구함으로써 국가의 안전을 보장하고 국익 및 국민의 안전을 보호하는 것”이라고 정의(제2조 제3호)하고 있는데, 국가사이버안전관리규정 제2조 제3호에서 ‘사이버안전’을 “사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태”로 규정한 것과 비교하면 더욱 추상적이다. 또한, ‘사이버 공격’이 국가안보에 관련이 있든 없든 모든 종류의 네트워크 보안을 침해하려는 행위임을 고려하면, ‘사이버안보’ 개념 역시 ‘사이버 보안(Cyber Security)’과 유사한 의미로 보이는데, ‘안보’라는 용어를 사용함으로써 사이버 보안의 국가안보적 측면만을 왜곡해서 강조하고 있다. 이러한 용어 사용은 국정원의 권한을 합리화하기 위한 의도이지만, 이처럼 사이버 보안의 개념을 왜곡하고 사이버 보안, 정보 보안, 사이버 안전 등의 개념을 명확한 규정없이 혼용하는 것은 일관되고 체계적인 국내 사이버 보안 법제 구축에 저해가 될 뿐이다.

이 법안은 제2조 제2호와 제4호에서 ‘사이버 공격’과 ‘사이버안보 위협행위’ 개념을 구분하고 있다. 김병기안의 ‘사이버안보 위협행위’는 2017년 국정원안에서는 ‘국가안보위협 사이버 공격’이라는 용어로 표현되었다. 어떻게 표현하든 ‘사이버안보 위협행위’의 개념은 지나치게 폭이 넓어 사실상 ‘책임기관’으로 지정된 기관에 대한 사이버 공격은 그 규모나 파급력과 무관하게 모두 ‘사이버안보 위협행위’로 규정될 수 있다. 또한, ‘가’의 경우는 사이버 공격의 주체를 사전에 확인할 수 없고 사후에도 공격자를 특정하기 힘든 현실을 고려하면, 공격자가 가목에 포함된 행위자라는 ‘추정’을 근거로 폭넓게 해석될 위험이 있다.

다른 법률과의 일관성도 부족하고 오히려 혼란을 확대할 위험도 있다. 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 규정하고 있다. 정보통신망법은 ‘전자적 침해행위’나 ‘사이버공격’에 대한 정의규정 없이, 전자적 침해행위로 발생한 사태를 ‘침해사고’로 정의하고 있다. 이 법안은 ‘사이버안보 위협행위’라는 새로운 용어를 사용함으로써 법령 사이의 혼란을 오히려 확대하고 있다.

(6) 정보통신기반보호법과의 충돌

김병기안은 제8조 제1항 제7호에서 “「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설을 관리하는 기관”을 책임기관으로 규정하고 있다. 그리고 제4조에서는 “사이버안보에 관하여는 다른 법률에 우선하여 이 법을 적용한다”고 하고 있다.

정보통신기반보호법은 국무총리 소속하에 정보통신기반보호위원회를 두고 있고, 공공부문의 기반시설의 경우 국가정보원이, 민간부문의 기반시설은 미래창조과학부가 관할하도록 하고 있다. 따라서 이 법안에서 규정하고 있는 ‘사이버안보위원회’ 및 책임기관에 대한 국정원의 권한과, 정보통신기반보호법에 따른 ‘정보통신기반보호위원회’ 및 민간부문의 기반시설에 대한 미래창조과학부의 권한이 충돌하거나, 혹은 정보통신기반보호법이 무력화될 수 있다.

국정원감시네트워크

입법의견서

국가사이버안보법안(김병기 의원 대표발의)에 대한
의견서

발행일 2021. 12. 16

발행처 국정원감시네트워크

담당 진보네트워크 오병일 대표 02-774-4551

참여연대 이은미 간사 02-723-53020 tsc@pspd.org

※ 본 자료는 [웹사이트](#)에서 다시 볼 수 있습니다.