



제429회 국회(정기회)
제 6 차 정 보 위 원 회

국가사이버안보법안 사이버안보 기본법안

검 토 보 고

〈국가사이버안보법안〉

■ 유용원의원 대표발의(의안번호 제2211450호)

〈사이버안보 기본법안〉

■ 김상훈의원 대표발의(의안번호 제2213722호)

2025. 11.

정 보 위 원 회

수석전문위원 김건오

목 차

I . 개요	1
1. 국가사이버안보법안	1
가. 제안경위	1
나. 제안이유	1
다. 주요내용	2
2. 사이버안보 기본법안	4
가. 제안경위	4
나. 제안이유	4
다. 주요내용	5
II . 검토의견	7
1. 총괄적 검토	7
(1) 제정안들의 입법취지 및 제안 배경	7
(2) 제정안들의 구성체계	17
2. 주요 조문별 검토	21
(1) 정의(안 제2조)	21
(2) 사이버안보 기본계획 등의 수립(안 제5조·제6조)	27
(3) 국가사이버안보위원회(안 제7조)	32

(4) 국가사이버안보센터(안 제8조)	35
(5) 통합보안관제의 구축(안 제10조)	37
(6) 사이버피해 조사(유용원의원안 제13조·제20조, 김상훈의원안 제13조·제21조)	40
(7) 사이버위기대책본부(안 제15조)	43
(8) 국회 정보위원회 보고(유용원의원안 제16조, 김상훈의원안 제19조)	45

I. 개 요

1. 국가사이버안보법안

가. 제안경위

- (1) 발의자 : 유용원 등 10인
- (2) 발의연월일 : 2025. 7. 11.
- (3) 회부연월일 : 2025. 7. 14.

나. 제안이유

국제 및 국가배후 해킹조직 등에 의하여 공공 및 민간 영역의 구분이 없이 동시다발적으로 광범위하게 발생하는 사이버공격으로 인한 국가안보와 국익 침해가 심각한 상황임.

그러나 우리의 국가적 대응활동은 각 부처별 소관 개별법령에 따라 제각각 분리, 독립 대응하고 있어 국가 사이버안보위협 상황 발생 시 범정부 차원의 종합적 대응에 한계가 있음. 또한 사이버기술의 발전으로 국가 안보 영역이 사이버공간으로 확장되었음에도 불구하고 사이버안보를 담보하기 위한 정책 방향 및 대응책을 수립·시행하는 기본 법조차 마련되지 않아 각 부처별 역할의 혼선, 업무영역의 중복 등 비효율화가 초래되고 있음.

따라서, 정부는 국가 사이버안보 정책 및 사업을 효율적으로 추진하기 위하여 대통령을 위원장으로 하고 민간전문가가 참여하는 국가사

이더안보위원회를 구성하고, 위기 시 국가 역량을 결집하여 신속한 사고 조사·위협정보 공유 등을 수행하는 통합대응 조직을 별도로 설치·운영하는 등 국가사이버안보 체계를 정립하고자 함. 또한, 각 부처의 소관사무 영역 보호책임을 명확히 하여 예방·대응활동을 강화하고, 범정부 차원의 협력을 공고화하여 국가 사이버안보 위협에 효과적으로 대응할 수 있도록 하고자 함.

다. 주요내용

가. 사이버공격에 대한 체계적이고 효과적인 예방 및 대응을 위하여 사이버안보에 관한 조직 및 운영체계에 대한 사항을 규정하고 국가 안전보장 및 국익보호에 이바지함(안 제1조).

나. 사이버안보와 관련된 국가의 정책 및 전략 수립에 관한 사항 등을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회를 두되, 위원회는 위원장을 포함하여 20명 이내의 위원으로 구성하고, 위원장은 대통령으로, 위원은 대통령령으로 정하는 중앙행정기관의 장, 국가안보실장, 국회 해당 상임위원회에서 추천한 사람 중에서 대통령이 위촉하는 사람, 민간 전문가 중에서 대통령이 위촉하는 사람으로 구성토록 하며, 과학기술정보통신부장관·국가정보원장이 간사위원이 됨(안 제7조).

다. 국가 차원의 종합적·체계적인 사이버안보 업무 수행과 효율적인 사이버공격·위협 대응을 위하여 국가정보원에 국가사이버안보센터

를 둠(안 제8조).

라. 사이버공격·위협 대응에 필요한 정보의 효율적인 배포, 공유 및 관리를 위하여 정보공유시스템을 구축·운영할 수 있도록 함(안 제11조).

마. 중앙행정기관등은 소관 영역에서 예방보안 점검·훈련, 안전한 정보통신기기등의 도입·활용, 위협 정보공유·신고 체계 구축·운영, 전문인력 확보·교육 등 예방·대응활동을 수행토록 하고, 정부는 국제협력 강화 및 공세적 대응조치 방안을 마련토록 함(안 제12조).

바. 책임기관의 장은 소관사무 영역에서 사이버공격으로 인한 피해가 발생한 때에는 신속하게 사고조사를 실시하여야 하고 그 결과를 관계 책임기관의 장 및 국가정보원장에게 통보하도록 함(안 제13조).

사. 국가정보원장은 사이버공격·위협에 대한 징후를 식별하거나 사이버공격·위협이 예상되는 경우에는 그 위협 수준, 발생 가능성 등을 판단하여 관심·주의·경계·심각 단계의 사이버위기 경보를 발령할 수 있도록 함(안 제14조).

아. 국가정보원장은 이 법에 따른 정부의 사이버안보 업무와 관련한 사항을 국회 정보위원회에 반기별로 보고하도록 함(안 제16조).

자. 제2조제5호다목에 해당하는 기관에 대한 사이버공격·위협 조사 및 사이버안보 실태 평가는 국방부장관이 업무를 수행하도록 함(안 제20조).

2. 사이버안보 기본법안

가. 제안경위

- (1) 발의자 : 김상훈 등 20인
- (2) 발의연월일 : 2025. 10. 27.
- (3) 회부연월일 : 2025. 10. 28.

나. 제안이유

사이버공격이 국가안보 및 국익에 심각한 위협으로 대두됨에 따라 2020년 12월 「국가정보원법」(법률 17646호)의 전부개정을 통해 국가정보원이 국제 및 국가 배후 해킹조직 등 사이버안보 정보 수집과 중앙행정기관 등에 대한 사이버공격 예방 및 대응 업무를 수행하도록 하였음.

그러나, 사이버안보 공격에 대한 공공과 민간 부문의 통합적 대응을 위한 체계가 갖추어지지 않아 광범위한 사이버공격에 효율적인 대처가 불가하다는 지적이 있음. 또한, 국가정보원의 사이버안보 정보 및 대응활동에 필요한 구체적인 절차가 확립되지 않아 사이버안보 공격에 대한 효과적인 대응이 어려운 측면이 있음.

이에 공공과 민간이 함께 협력하여 지속적으로 발생하는 사이버공격에 대한 사전탐지, 조기차단 등 능동적이고 효율적인 대처가 가능하게끔 대응체계를 마련하고, 사이버안보에 관한 국가의 전략 및 정책

수립을 통합적으로 추진할 수 있도록 함.

다. 주요내용

가. 국가안보를 위협하는 사이버공격을 예방하고 사이버안보에 관한 조직 및 운영체계에 대한 사항을 규정함으로써 국가의 안전보장과 이익보호에 이바지함(안 제1조).

나. 사이버안보 업무의 효율적이고 체계적인 추진을 위하여 3년마다 국가 차원의 전략 방향을 제시하는 사이버안보 기본계획을 수립함(안 제5조).

다. 사이버안보에 관한 국가의 전략 및 정책 수립에 관한 사항 등을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회를 두되, 위원회는 위원장을 포함하여 20명 이내의 위원으로 구성하고, 위원장은 국가안보실장으로, 위원은 국가정보원장, 과학기술정보통신부장관, 개인정보보호위원장 등 대통령령으로 정하는 중앙행정기관의 장, 국회 해당 상임위원회에서 추천한 사람 중에서 대통령이 위촉하는 사람 3명, 민간 전문가 중에서 대통령이 위촉하는 사람 3명으로 구성토록 하며, 과학기술정보통신부장관·국가정보원장이 간사위원이 됨(안 제7조).

라. 국가 차원의 종합적·체계적인 사이버안보 업무 수행과 효율적인 사이버공격·위협 대응을 위하여 국가정보원에 국가사이버안보센터를 둠(안 제8조).

- 마. 국가정보원장은 책임기관에 대한 사이버공격·위협을 즉시 탐지·대응하기 위하여 통합보안관제체계를 구축·운영함(안 제10조).
- 바. 국가정보원장은 사이버공격·위협 대응에 필요한 정보의 효율적인 배포, 공유 및 관리를 위하여 국가사이버위협정보공유시스템을 구축·운영함(안 제11조).
- 사. 책임기관의 장은 소관사무 영역에서 사이버공격으로 인한 피해가 발생한 때에는 신속하게 사고조사를 실시하여야 하고 그 결과를 관계 책임기관의 장 및 국가정보원장에게 통보함(안 제13조).
- 아. 국가정보원장은 책임기관에 대한 사이버공격·위협 징후를 식별하거나 사이버공격·위협이 예상되는 경우에는 체계적인 대응을 위하여 그 위협 수준, 발생 가능성 등을 판단하여 국가안보실장과 미리 협의한 후 관심·주의·경계·심각 단계의 사이버위기 경보를 발령할 수 있음(안 제14조).
- 자. 국가정보원장은 책임기관의 사이버안보 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등 사이버안보 실태를 평가할 수 있음(안 제17조).
- 차. 국가정보원장은 이 법에 따른 정부의 사이버안보 업무와 관련한 사항을 국회 정보위원회에 반기별로 보고함(안 제19조).
- 카. 「국군조직법」 제2조에 따른 각 군, 해병대, 합동참모본부에 대한 사이버피해 조사 및 사이버안보 실태 평가는 국방부장관이 수행함(안 제21조).

II. 검토의견

1. 총괄적 검토

(1) 제정안들의 입법취지 및 제안 배경

최근 공공 및 민간영역에 대한 구분 없이 국제 및 국가배후 해킹조직 등에 의한 사이버공격이 동시다발적으로 발생하고 있어 사회적 피해 규모가 급증함에 따라 이에 대한 대책 마련이 시급한 상황임.

2025년의 경우, SKT텔레콤 유심 정보 유출 사건(2025. 4.), SGI보증 보험 랜섬웨어 사태(2025. 7.), YES24 서비스 마비 사태(1차 2025. 6., 2차 2025. 8.), 롯데카드 개인신용정보 유출 사고(2025. 8.), KT 이용자 대상 무단 소액 결제 사태(2025. 8.) 등이 발생하였고, 2021년부터 2025년 8월까지 한국인터넷진흥원(KISA)에 접수된 기업 대상 정보침해 신고 건수는 총 6,447건이고, 개인정보 유출로 인한 행정처분은 총 451건으로 집계되었음.¹⁾

또한 북한 김수키 그룹에 의한 원격근무 공무원 등의 VPN 또는 원격접근시스템 인증 정보 탈취 후 정보 유출 시도 사례 등이 있었고, 전국 지방자치단체 대상 해킹시도는 4년간 5,000만건에 달하고, 군 전산망에 대한 해킹시도도 6년간 약 7만 4천여건 발생하고 있는 등 매년 증가하는 추세임.²⁾

1) 김진호, 「대한민국, 해킹 피해 급증과 범정부 대응 필요성」, 글로벌경제신문, 2025. 9. 23. <<https://www.getnews.co.kr/news/articleView.html?idxno=841660>>

2) 김기태, 「4년간 전국 지자체 대상 해킹 시도 4788만건… 15건은 실제 뚫려」, 뉴스1, 2025. 10.

< 최근 4년간 지방자치단체·군 대상 해킹시도 >

(단위: 건)

구 분	2022년	2023년	2024년	2025년
지방자치단체	8,003,265	9,422,885	11,580,455	18,879,073
군	9,048	13,514	14,419	12,368

※ 2025년의 경우 지방자치단체는 7월말까지, 군은 8월말까지 집계된 통계임.

이와 같이 사이버 위협이 갈수록 동시다발적으로 광범위하게 발생하고 있으나, 국가 차원에서의 대응은 각 부처별 소관 개별법령에 따라 이루어짐에 따라 종합적인 대응에 한계가 있다는 점이 지적되고 있고,³⁾ 국가 안보 영역이 사이버공간으로 확장되었음에도 불구하고 사이버안보를 담보하기 위한 정책 방향 및 대응책을 수립·시행하도록 하는 기본법이 마련되지 않아 부처별 역할의 혼선, 업무영역의 중복 등 비효율이 발생하고 있다는 지적이 있음.

현재 우리나라의 국가 사이버안보 업무의 총괄·조정은 국가안보실(사이버안보비서관)이 수행하고 있고,

국가정보원은 「국가정보원법」, 대통령령인 「사이버안보 업무규정」, 대통령훈령인 「국가사이버안전관리규정」 등에 근거 각 소관부처와의 협력체계를 구축하여 ① 국가적인 사이버위기 대응과 ② 공공부문(중앙

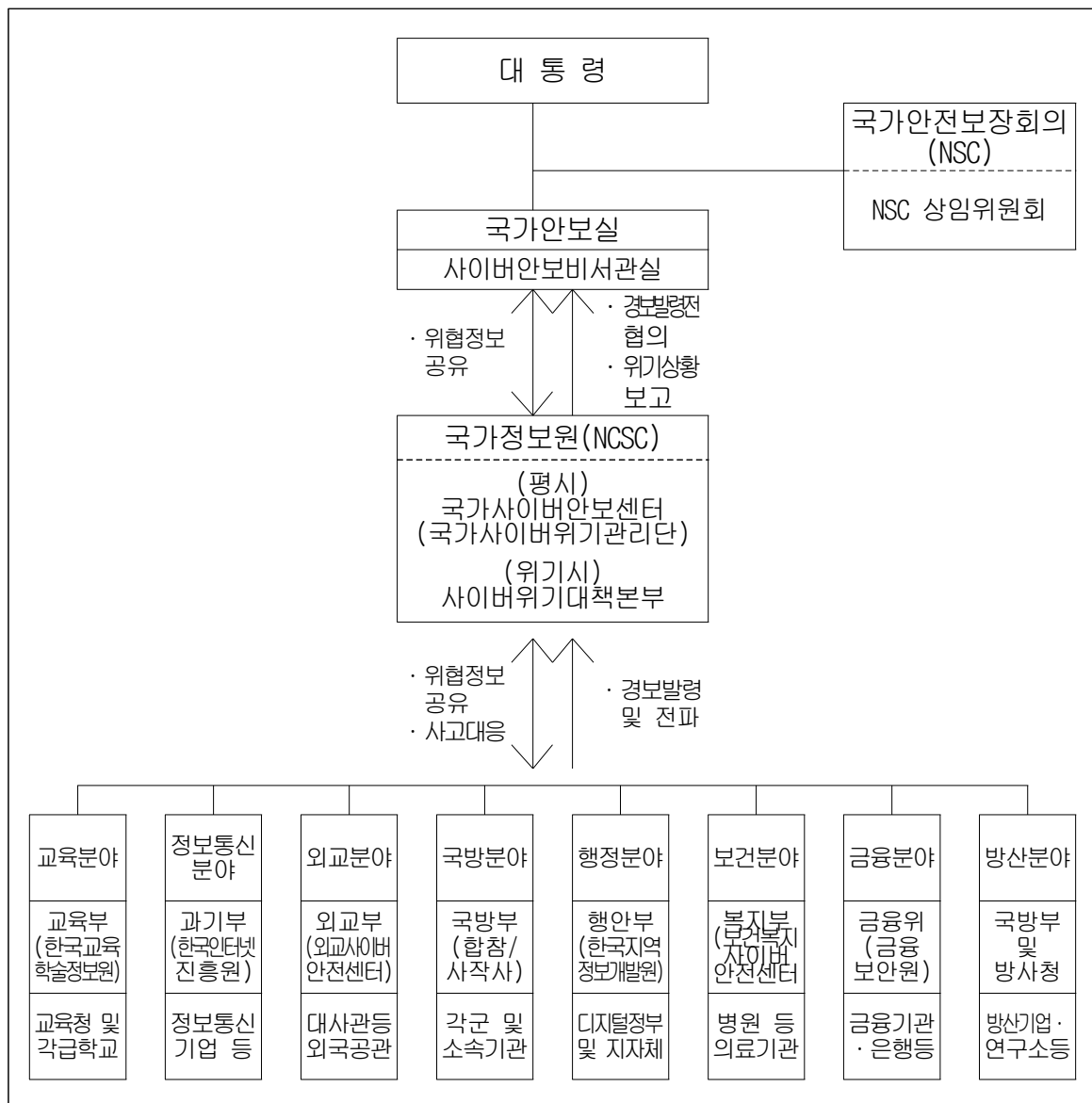
13. <<https://www.news1.kr/local/daejeon-chungnam/5938370>>, 이현호, 「[단독] 軍」 전산망 “해킹시도 6년간 약 7만4000건”...‘해킹메일’ 급증[이현호의 밀리터리!톡]», 서울경제, 2025. 10.

13. <<https://n.news.naver.com/mnews/article/011/0004542344?sid=100>>

3) 예를 들어, KT 무단 소액결제 사건의 경우 기업 해킹 사건이지만 피해가 곧바로 금전적 손실로 이어지면서 어느 부처가 주도해야 하는지 조율이 원활하지 않았다는 주장이 있음. (박형빈, 「[해킹 대란] ②국경 없는 해킹 공격...한국만 ‘칸막이 보안’», 연합뉴스, 2025. 9. 21., <https://www.yna.co.kr/view/AKR20250920028500017?section=search>)

행정기관, 지방자치단체와 그 소속기관, 공공기관 등)의 사이버공격 및 위협에 대한 예방 및 대응업무를 수행하고 있으며,
 민간부문 각 분야의 사이버보안 관련 업무는 소관 부처 유관 법률에 따라 소관 부처 또는 산하기관에서 개별적으로 수행하고 있는 상황임.

< 국가 사이버안보 수행체계 >



자료: 국가정보원 제출 자료

이에 제정안은 대통령을 위원장으로 하고 민간전문가가 참여하는 국가사이버안보위원회를 구성하고, 「사이버안보 업무규정」에 따라 국가정보원에 설치하고 있는 국가사이버안보센터, 통합보안관제 체제 등을 법률로 상향하는 등 국가사이버안보체계를 정립하여 국가 사이버안보 위협에 효과적으로 대응하려는 것으로 그 입법취지에 공감할 수 있음.

한편, 10월 22일 국가안보실을 중심으로 과학기술정보통신부, 금융위원회, 개인정보보호위원회, 국가정보원, 행정안전부 등 관계부처 합동으로 민간과 공공을 아우르는 ‘범부처 정보보호 종합대책’이 수립되어 발표되었는데,

이에 따르면 국가정보원의 조사·분석 도구를 민간과 공동 활용하도록 하고, 부처별로 파편화된 해킹 사고조사 과정을 체계화하여 One-Stop 신고체계 도입과 조사단별 투입시기 최적화 및 상호 정보공유를 강화하며, 민·관·군 합동 조직인 국가정보원 산하 국가사이버위기관리단과 정부 부처 간의 사이버 위협 예방·대응 협력을 강화하고, 국가 사이버안보 전략을 연내 수립할 계획인 점 등을 고려할 때 국가정보원의 역할 강화가 요구되는 측면이 있음.

이와 관련하여 해외 입법례를 살펴보면, 주요국은 사이버보안/정보기관 중심의 국가 사이버안보 체계를 운영하고 있고, 미국·일본은 사이버보안/정보기관의 역할을 확대하면서(미국: 국토안보부/CIA, 일본: 내각사이버시큐리티센터(현 국가사이버통괄실)/내각정보조사실) 민·관협력을 강화하는 법률을 시행 중에 있음.

< 사이버 안보 관련 해외 입법례 >

국가	법률	주요내용
미국	「사이버안보법」 (2015)	자발적 정보공유 프로세스 형성, 정부기관간·민간관 정보공유 강화, 연방정부 보안 향상, 인력 평가 등을 통한 사이버안보 강화
	「사이버인프라 보호청법」 (2018)	국토안보부 사이버안보 조직을 사이버인프라보호청(CISA)으로 개편·정비
일본	「사이버시큐리티기본법」 (2014)	사이버시큐리티본부 설치, 전략 및 기본시책 수립 시행, 행정기관 정보시스템에 대한 부정활동 감시, 정보공유 시책 강구
	「중요전자계산기 대상 부정행위 피해방지법」 (2025)	사이버안보 능력을 미국, 유럽 등 주요국 수준 이상으로 강화하기 위하여 ‘능동적 사이버 방어 체계’를 도입함 사이버공격에 대한 민관협력 강화, 통신정보를 활용한 사이버위협 탐지, 공격자의 서버 침입 무해화, 사이버안전보장 분야 조직 신설 등 4가지 목표를 설정함
영국	「정보서비스법」 (1994)	정보기관인 비밀정보국(SIS) 및 정보통신본부(GCHQ) 관련 사항 법제화
	「조사권한법」 (2016)	인터넷 및 통신에 대한 정보·수사기관의 조사·수사 권한을 정비
호주	「정보기관법」 (2001)	호주신호정보부(ASD)에 관한 사항 법제화
	「핵심인프라안보법」 (2018)	핵심 인프라에 대한 사이버보안 노력을 지원
독일	「연방정보기술 보안청법」 (1990)	연방정부의 보안 관련 정보수집과 조치 등 중심적 역할을 수행하는 연방정보기술보안청(BSI)의 설립근거와 임무를 법제화
	「독일 네트워크 정보보안(NIS) 지침 이행법」 (2017)	연방정보기술보안청의 역할 강화 및 정보기관과의 정보공유 확대, 원격의료·통신 등 주요 분야 사이버보안 강화
캐나다	「국가안보법」 (2017)	통신보안국(CSE)에 사이버안보 및 능동적인 사이버작전을 수행토록 광범위한 권한 부여, 보안정보부(CSIS)에 개인정보 수집 권한 부여

자료: 국가정보원에서 국회 정보위원회에 제출한 자료, 2025. 9., 한국인터넷진흥원, 「일본 의회, 「사이버 대응능력 강화법안」 통과(2025. 5. 16.)」, 2025.

다만, 제정안들에 대하여는 다음과 같은 신중 검토 필요 의견을 포함한 다양한 의견이 제시되고 있음을 심사시 고려할 필요가 있음.

우선 국가정보원은, 국제 및 국가배후 해킹조직 등의 사이버공격에 효과적으로 대응하기 위한 범정부 차원 협력 강화 등 동 법안의 제정 취지에는 공감하지만,

현행 국가정보원의 사이버안보 직무는 ① 사이버안보 정보 업무(국내외 전 영역), ② 사이버보안 업무(중앙부처·지방자치단체·공공기관 대상)으로 이루어져 있는데, 동 제정안은 사이버안보 정보 업무와 사이버보안 업무 공히 ‘책임기관’을 대상으로 이루어져 사이버보안 업무에 대하여 헌법기관, 軍, 일부 민간 중요기업까지 업무 범위가 확대되는 점을 고려할 필요가 있다는 의견을 제시하고 있음.

한편 정부는 국정과제에 따라 사이버공격에 대한 일원화된 대응체계와 능동적 방어활동 강화를 위해 정부차원의 심층 검토와 각계 의견을 반영하여 법률 제정 필요성과 방향을 연말까지 정할 계획이라는 것이 국정원의 입장임.

국회와 중앙선거관리위원회에서는 헌법기관이 소관 영역의 사이버안보 업무에 대해 대통령 소속인 국가정보원의 관리와 통제를 받는 효과를 가져오게 되어, 권력분립의 원칙과 헌법기관의 독립성이 침해될 우려가 있다는 취지의 의견을 제시하였음.

또한, 과학기술정보통신부는 국가정보원 중심으로 거버넌스가 구축되고 통신사, 금융사 등 국민 전체의 주요정보를 다루는 분야가 법 적용 대상으로 포함되어 정보기관의 민간 사찰 우려 등 불필요한 사회적 논란이 발생할 우려⁴⁾가 있으며, 통합 대응 조직을 국가정보원에 설치하는 것은 사이버보안 기관과 정보기관을 분리하여 운영하는 미국(국토안보부/CIA)과 일본(내각사이버시큐리티센터(현 국가사이버통괄실)/내각정보조사실)의 흐름과도 불일치⁵⁾하고, 적용 범위 또한 제정 목적에 언급된 사이

4) 이에 대해 국정원은, 과기부의 국정원에 대한 ‘민간사찰 우려’는 사실과 다르며, 구체적 사실에 기반하지 않은 막연한 주장에 불과하다는 입장임. 국정원은 실제 사이버안보 활동에 있어서 문제된 사례가 전무하고, 법적 통제하에 필요 최소한의 개인정보를 취급하고 있다는 입장이며, 구체적으로 아래와 같은 근거를 제시하고 있음.

첫째, 국정원에 대한 오남용 통제 장치는 이미 완비되어 있고, 국가사이버안보센터 개소 이래 21년간 어떠한 민간사찰 관련 문제 사례도 발생하지 않았다는 입장임.

- 16대 대통령인 노무현 대통령의 지시에 따라 2004년 국가사이버안전센터를 개소한 이래 21년간 인권침해·권한남용 문제가 제기된 사례(소송, 고발, 민원, 진정 등)가 전무함.

- 2019년 UN 인권위 산하 ‘조셉 칸나타시’ 사생활권 특별보고관은 한국의 사생활 보호문제에 대한 방한 조사를 실시하면서, 한국 시민단체가 제기한 국정원의 사이버안보 활동을 내세운 민간사찰 가능성을 조사한 결과, 사실무근임을 확인하고 보고서에서 관련 내용을 삭제함.

- 「국가정보원법」 제3조(운영원칙), 제13조(직권남용 금지), 제14조(불법감청 금지), 제23조(처벌) 등 강력한 통제 장치가 법률에 완비되어 있음.

- 국회(정보위원회)도 「국가정보원법」 제4조제2항에 따라 국정원으로부터 정보활동기본지침을 보고받는 등 직무 외 민간감시·무분별한 정보수집 행위는 법적으로 불가능하다는 입장임.

둘째, 안보목적으로 수집하는 개인정보는 「개인정보보호법」 주요 조항들의 적용을 받지 아니한다는 입장임.

- 「개인정보보호법」 제58조는 국가안전보장과 관련된 정보분석 목적인 경우, 개인정보를 합법적으로 임의제출할 수 있도록 규정하고 있어 민간기업·관계기관으로부터 법적 절차에 따라 개인정보가 포함된 자료를 제공받아 취급하거나 분석할 수 있음.

- 다만, 법령에 따라 필요한 범위내 최소 기간·정보만을 처리토록 하여 개인정보의 안전한 관리대책을 마련토록 하고 있음.

- 개인정보보호위원회는 2016년 「국가 사이버안보 기본법」 제정안에 대해 “보안관제를 위하여 사이버공격을 탐지·대응 목적으로 IP주소·접근시간 등을 수집·이용하는 것은 국가안전보장에 관하여 처리될 수 있는 개인정보에 해당한다”라고 해석, 「사이버안보 업무규정」 제정(2020.12) 및 개정(2024.3)시 ‘개인정보 침해요인 평가’ 과정에서 개인정보 침해요인이 전무하다고 판단, 2024년 국정원의 해킹사고 조사시 「개인정보보호법」 제58조 예외에 따라 개인정보수집이 ‘가능하다’는 공식적인 유권해석(‘24.9)을 하였음.

- 정보통신기반시설 해킹사고가 발생하더라도, 국정원의 활동은 「국가정보원법」에 따른 국가배후 해킹조직 등의 사이버안보 정보 수집·분석과 이를 통한 국민안전 보호를 위한 대응조치이며, ‘기술지원’이 아니므로, 「정보통신기반보호법」 제7조제3항(국정원의 개인정보 시설 기술지원 금지)와는 무관하다는 입장임.

5) 이에 대해 국정원은, 과기부의 ‘세계적 추세 未부합’ 주장 역시 사실과 다르며, 구체적 사실에 기반하지 않는 막연한 주장에 불과하다는 입장임. 현대 사이버위협 대응의 ‘세계적 흐름’은 미국·일본 등의 ‘능동적 사이버방어 법안’ 사례에서 보듯, 위협행위자에 대한 정보수집·추적·무력

버안보로 한정되지 않고 일반적인 사이버공격·위협의 예방·대응까지 범위를 확대하여 규정하는 것은 국가정보원이 민·관을 사실상 통할 가능하다는 우려가 있다⁶⁾는 이유로 법 제정에 반대 입장을 보이고 있음.

아울러 과학기술정보통신부는 과거 국가정보원 중심 사이버안보 기본법안 등이 여러 차례 발의되어 왔으나, 민간 영역에 대한 과도한 개입 우려⁷⁾ 등으로 폐기되었음을 지적하며, 국가안보실의 단일화된 컨트롤타워로 국가안보실에 안보실장 주관의 사이버안보협의체를 두고,

화 등 ‘정보’ 활동의 중요성을 부각하고 있어, 사이버위협 대응기관과 정보기관을 분리하는 것이 세계적 흐름이라는 주장은 사실이 아니며, 과기부가 사례로 든 미국 국토안보부와 일본 내각사이버시큐리티센터(현 국가사이버통괄실) 역시 정보기관이자 보안기관으로서, 「정부조직법」에 따라 ‘정보’와 ‘보안’ 업무를 모두 수행 중인 국정원 국가사이버안보센터와 유사하다는 입장이며, 이래와 같은 논거를 제시하고 있음.

첫째, 미국 국토안보부는 국가안보·영토보안을 담당하는 부처로, 9.11 테러 당시 CIA·NSA·FBI 등 정보·보안기관에 대한 대대적 개편 과정에서 창설된 기관으로서, 「정부조직법」에 따라 국가안보에 관한 정보와 보안 업무를 수행하는 국정원과 매우 유사한 조직이며, 사이버인프라보호청(CISA)은 국토안보부의 소속 부서로서 ‘보안’ 업무를 수행하며, 또다른 소속기관인 국가사이버보안통신통합센터(NCCIC, ‘위협정보 수집·분석’)의 기능을 합친다면 국정원의 국가사이버안보센터와 유사한 조직이라는 입장임.

둘째, 일본 내각관방 산하 국가사이버통괄실 역시 국가 정보기관(‘사이버통신정보감리위원회’)의 승인을 받아 통신사업자로부터 위협정보를 수집·분석)이자 보안기관이며, 수행 기능은 국정원 국가사이버안보센터와 유사한 조직이라는 입장임.

셋째, 영국 역시 국가정보기관(GCHQ) 소속기관인 국가사이버안보센터(NCSC)에서 민·관 불문 국가 사이버안보 업무를 총괄 수행 중이라는 입장임.

위와 같이 미국·일본 등 주요국은 우리나라 국가정보원과 같이 ‘정보’와 ‘보안’ 업무를 모두 수행하는 기관이 사이버위협 대응을 수행하고, 전 세계 어느 나라든 우리나라 과학기술정보통신부와 같은 정보통신산업규제 부처(미국 FCC, 일본 디지털성, 영국 Ofcom, 호주 ACMA, 독일 BNetzA, 캐나다 ISED)가 사이버안보를 총괄하는 전례가 없다는 입장임.

- 6) 이에 대해 국정원은, 제정안이 규정하는 ‘사이버안보’ 직무 범위와 일치하는 기관은 없으며, 만약 ‘사이버안보’ 주관기관을 정해야 한다면 아래와 같은 논거에 따라 현행법상 가장 유사한 직무를 수행 중인 국정원이 적절하다는 입장임.

첫째, 제정안은 일반 사이버공격·위협을 포함한 국가 차원의 사이버안보를 강화하기 위한 것으로 ‘사이버안보’를 통상적인 사이버안보 정의보다 넓게 규정하는 측면이 있음에 따라, 해당 의미와 완전히 일치하는 직무 범위를 갖는 기관은 현재 없다는 입장임.

둘째, 이와 같은 상황에서 어느 기관이든 ‘사이버안보’ 업무를 수행해야 한다면, 현행 법률상 가장 유사한 직무를 가지고 있는 국정원이 적합하다는 의견임.

- 국정원은 「정부조직법」상 국내 유일하게 국가정보기관과 국가보안기관을 겸하고 있으며, 「국가정보원법」에 따라 ‘국제 및 국가배후 해킹조직 등 사이버안보’에 대한 정보를 수집·작성·배포하고, 이와 관련된 조치로서 국민 안전보호를 위한 대응조치를 수행하며, 「국가위기관리기본지침」에 따라 민관 영역을 불문하여 국가적 사이버위기 대응 주관기관 역할을 수행 중이라는 입장임.

- 7) 이에 대해 국정원은 각주 4)와 같은 입장임.

민·관·군 3축의 사이버안보 거버넌스를 구축하여 민은 과학기술정보통신부, 관은 국가정보원, 군은 국방부가 총괄하면서 유기적 협력을 강화하는 방향이 바람직하고, 사고 발생시 공격 양상 분석을 통해 단독 대응 또는 공동 대응 여부를 판단하여 민·관 협업 사고조사가 가능하다는 의견임.

국방부는 책임기관⁸⁾의 범위에 「국군조직법」에 따른 군 관련 조직이 포함되는 경우 국방부 외 기관이 국방부를 거치지 않고 군 조직에 대하여 직접적으로 통제가 가능해질 것을 우려하는 입장임.

이 밖에도 금융위원회는 제정안에서 정의하는 책임기관은 국가 사이버 안보 차원에서 중요성이 높은 기관으로 대부분의 민간 금융회사(약 500여개 社)를 책임기관에 포함하는 것은 과도한 측면이 있고, 현재 금융분야는 「전자금융거래법」과 「정보통신기반 보호법」 등에 따라 일원화된 체계로 사이버 위협에 대응 중인바, 중복규제에 따른 대응체계 혼선, 업무효율성 저하 등 우려가 있어 신중한 검토가 필요하다는 입장임.

민간부문의 경우, 한국인터넷기업협회⁹⁾에서는 민간 사업자인 집적정보통신시설 사업자 및 전자금융기반시설 사업자에게 정부와 동일한 의무를 부담하게 하는 것은 비용 등 현실적으로 상당한 부담이 발생할 수 있고, 통합보안관제체계 연계, 사이버안보 실태평가 등 조항에 대해 민간사업자의 영업비밀이 노출될 수 있음을 우려하는 의견을,

8) 사이버안보에 관한 업무를 수행하는 기관을 뜻함

9) 한국인터넷기업협회에서 국회 정보위원회에 제출한 자료, 2025. 8.

주한미국상공회의소(AMCHAM)은 책무 및 협조의무는 국가기관 및 공공기관 등 공적 주체로 한정하고, 민간 사업자에 대해서는 자율적 참여 및 협력 유도 중심으로 규정하는 방향으로 재검토를 요청하는 의견을,

참여연대 산하 국정원감시네트워크의 경우 국정원의 사이버보안 관련 권한이 헌법기관에까지 확대되는 것에 대하여 우려하는 의견을 제시하고 있음.¹⁰⁾

따라서 제정안에 대하여는 앞에서 살펴본 대로 사이버 공격에 대응한 범정부 차원의 협력 강화 등 제정안의 입법취지와 함께, 현행법 내에서의 해킹 등 사이버 보안 사고에 대한 대응 추진 실태 및 사이버안보 협력 현황 등에 대한 면밀한 분석과 아울러 범정부차원의 국가사이버안보체계 정립 필요성, 그리고 국회 등 헌법기관이 사이버보안 업무에 대해 국가정보원의 관리를 받는 경우 권력분립의 원칙과 헌법기관의 독립성 침해 우려, 국가정보원 중심 거버넌스 구축시 정보기관의 민간 사찰 우려 및 민간 영역에 대한 과도한 개입 우려 등에 따른 신중검토 필요 의견 등에 대한 종합적인 고려를 통해 입법정책적으로 결정할 사항으로 보임.

참고로, 제정안들과 관련하여서는 제18대 국회에서부터 사이버안보 관련 법안의 제정시도가 있었고 2022년 11월에는 국가정보원의 「국가

10) 참여연대, 「[성명] 국정원 사이버보안 권한, 헌법기관 확대 반대한다」, 2024. 11. <<https://www.peoplespower21.org/government/1981096?cat=653&paged=0>>

사이버안보 기본법 제정(안)」 입법예고 등이 있었으나, 민간에 대한 감시와 사찰의 우려,¹¹⁾ 국가정보원을 사이버안보 기본계획의 수립 기관으로 하는 데 대한 관련 기관의 우려 등이 있어 현재까지 제정논의가 계속되어온 바 있음.

< 사이버안보 관련 법안 발의 연혁(제18대국회 ~ 제21대국회) >

발의 대수	제명	대표발의자	발의일
제18대	국가 사이버위기관리법안	공성진의원	'08. 10. 28.
제19대	국가 사이버안전 관리에 관한 법안	하태경의원	'13. 3. 26.
제19대	국가 사이버테러 방지에 관한 법률안	서상기의원	'13. 4. 9.
제19대	사이버위협정보 공유에 관한 법률안	이철우의원	'15. 5. 19.
제19대	사이버테러 방지 및 대응에 관한 법률안	이노근의원	'15. 6. 24.
제19대	국가 사이버테러 방지에 관한 법률안	서상기의원	'16. 2. 22.
제20대	국가 사이버안보에 관한 법률안	이철우의원	'16. 5. 30.
제20대	국가사이버안보법안	정부	'17. 1. 3.
제21대	사이버안보 기본법안	조태용의원	'20. 6. 30.
제21대	국가사이버안보법안	김병기의원	'21. 11. 4.
제21대	사이버보안 기본법안	윤영찬의원	'21. 12. 2.

자료: 국회 의안정보시스템 검색

(2) 제정안들의 구성체계

유용원의원이 대표발의한 제정안의 법률 제명은 「국가사이버안보법안」(이하 “유용원의원안”이라 함)으로, 본칙 21조와 부칙으로 구성되어

11) 국정원감시네트워크, 「국가사이버안보 기본법 제정안(국가정보원공고 제2022-5호)에 대한 의견서」, 2022. 12. 참고

있고, 김상훈의원이 대표발의한 제정안의 법률 제명은 「사이버안보 기본법안」(이하 “김상훈의원안”이라 함)으로 5개의 장과 본칙 25조, 부칙으로 구성되어 있는데,

두 제정안은 일부 조문을 제외하고는 상당 부문 조문 제목과 내용이 유사한 측면을 보이고 있음.

제정안들의 주요 내용을 살펴보면,

첫째, 정의 규정에서는 “사이버공간”, “사이버공격·위협”, “사이버안보”, “사이버위기”, “책임기관” 등의 용어를 정의하고,

둘째, 사이버안보 업무를 효율적이고 체계적으로 수행하기 위한 국가 차원의 전략 방향을 제시하는 사이버안보 기본계획과 이에 따른 연도별 시행계획을 규정하며,

셋째, 사이버안보 수행을 위한 주요 전략·정책 등의 심의기구로 “국가사이버안보위원회”를 설치하고,

넷째, 사이버안보 활동을 수행하는 기관으로 국가정보원에 “국가사이버안보센터”를 두며,

다섯째, 국가정보원장은 책임기관에 대한 보안관제를 위하여 통합 보안관제체계를 구축·운영하도록 하며, 책임기관의 장은 소관사무 영역에 대한 보안관제를 위하여 보안관제센터를 구축·운영하도록 하고,

여섯째, 국가정보원장은 사이버공격·위협 대응에 필요한 정보의 배포·

공유 등을 위하여 정보공유시스템을 구축·운영할 수 있도록 하며,

일곱째, 책임기관의 장은 소관사무 영역에서 사이버공격 등으로 인한 피해가 발생한 경우 사고조사를 실시하고 위협행위자의 사이버공격으로 인한 피해가 발생한 경우 국가정보원장으로 하여금 조사할 수 있도록 하며,

여덟째, 국가정보원장은 사이버공격·위협에 따른 징후를 식별하거나 위협이 예상되는 경우에는 경보를 발령할 수 있도록 하고, 사이버위기 대책본부를 구성·운영할 수 있도록 하며,

아홉째, 국가정보원장으로 하여금 책임기관의 사이버안보 실태 평가를 실시할 수 있도록 하는 것임.

< 제정안의 조문체계 >

유용원의원안	김상훈의원안
제1조(목적) 제2조(정의) 제3조(국가 등의 책무) 제4조(다른 법률과의 관계)	제1장 총칙 제1조(목적) 제2조(정의) 제3조(국가 등의 책무) 제4조(다른 법률과의 관계)
제5조(사이버안보 기본계획의 수립·시행) 제6조(연도별 시행계획) 제7조(국가사이버안보위원회)	제2장 사이버안보 기본계획 등 제5조(사이버안보 기본계획의 수립·시행) 제6조(연도별 시행계획) 제7조(국가사이버안보위원회)

제8조(국가사이버안보센터) 제9조(기관 간 협력체계 구축) 제10조(통합보안관제체계의 구축 등) 제11조(정보의 공유) 제12조(예방·대응활동) 제13조(사이버피해 조사 등) 제14조(사이버위기 경보의 발령) 제15조(사이버위기대책본부) 제17조(사이버안보 실태 평가)	제3장 사이버안보 활동 제8조(국가사이버안보센터) 제9조(기관 간 협력체계 구축) 제10조(통합보안관제체계의 구축 등) 제11조(정보의 공유) 제12조(예방·대응활동) 제13조(사이버피해 조사 등) 제14조(사이버위기 경보의 발령) 제15조(사이버위기대책본부) 제16조(사이버안보 전문업체의 지정·관리) 제17조(사이버안보 실태 평가)
제16조(국회 정보위원회 보고) 제19조(비밀 엄수의 의무) 제20조(사이버공격·위협 조사 등에 대한 특례)	제4장 보칙 제18조(국제협력) 제19조(국회 정보위원회 보고) 제20조(비밀 엄수의 의무) 제21조(사이버피해 조사 등에 대한 특례) 제22조(벌칙 적용 시의 공무원 의제)
제21조(벌칙)	제5장 벌칙 제23조(벌칙) 제24조(양벌규정) 제25조(과태료)
부칙(공포 후 6개월 이후 시행)	부칙(공포 후 6개월 이후 시행)

2. 주요 조문별 검토

(1) 정 의(안 제2조)

유용원의원안	김상훈의원안
제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 1. “사이버공간”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 <u>정보통신망(이하 “정보통신망”이라 한다)의</u> 정보 처리 영역을 말한다. 2. “사이버공격·위협”이란 해킹, 컴퓨터 바이러스, 서비스 거부 등 전자적 방법으로 사이버공간을 침입·교란·마비·파괴하거나, 정보를 위조·변조·훼손·절취하는 행위 또는 활동 및 그와 관련된 위협을 말한다. 3. “사이버안보”란 <u>북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인 등 위협행위자들이 행하는 사이버공격을 확인·견제·차단하고 그에 필요한 대응조치를 강구·이행함으로써 국가의 안전보장과 국민의 사이버공간 활동에 지장을 초래하지 아니하는 것</u>을 말한다. 4. “사이버위기”란 <u>사이버공격으로 인하여 국가기반시설의 핵심기능이 훼손·정지·무력화되거나 국가기밀 등 중요한 정보가 대량으로 유출되어 국가안보와 이익에 위해로운 결과를 초래하거나 국민의 사이버공간 활동에 지장을 초래하는 것</u>을 말한다.	제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 1. “사이버공간”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 <u>정보통신망의</u> 정보 처리 영역을 말한다. 2. “사이버공격·위협”이란 해킹, 컴퓨터 바이러스, 서비스 거부 등 전자적 방법으로 사이버공간을 침입·교란·마비·파괴하거나, 정보를 위조·변조·훼손·절취하는 행위 또는 활동 및 그와 관련된 위협을 말한다. 3. “사이버안보”란 <u>사이버공격·위협으로부터 사이버공간을 보호함으로써 사이버공간의 기능을 정상적으로 유지하거나 정보의 안전성을 유지하여 국가의 안전을 보장하고 국민의 이익을 보호하는 것</u>을 말한다. 4. “사이버위기”란 <u>사이버공격·위협으로 인하여 국가기반시설의 핵심기능이 훼손·정지·무력화되거나 국가기밀 등 중요한 정보가 대량으로 유출되어 국가안보나 그 밖에 국가의 중대한 이익을 해치거나 국민의 사이버공간 활동에 지장을 초래하는 것</u>을 말한다.

5. “책임기관”이란 사이버안보에 관한 업무를 수행하는 다음 각 목의 기관을 말한다.

가. 국회, 법원, 헌법재판소, 선거관리위원회, 감사원, 국가인권위원회, 고위공직자범죄수사처, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다)과 그 소속 기관, 시·도 및 그 소속 기관, 교육청 및 그 소속 기관

나. 「국가정보원법」 제4조제1항제4호다목의 공공기관

다. 「국군조직법」에 따른 각 군, 합동참모본부, 국방부 직할 부대 및 직할 기관

라. 「전기통신사업법」 제6조에 따른 기간통신사업의 등록을 받은 자와 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설사업자

마. 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설을 관리하는 기관

바. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따라 지정된 국가핵심기술을 보유·관리하는 기관

사. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 조 제10호에 따른 전문

5. “책임기관”이란 사이버안보에 관한 업무를 수행하는 다음 각 목의 기관을 말한다.

가. 국회, 법원, 헌법재판소, 선거관리위원회, 감사원, 국가인권위원회, 고위공직자범죄수사처, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 특별시·광역시·특별자치시·도·특별자치도(이하 “시·도”라 한다) 및 그 소속 기관, 시·도 교육청 및 그 소속기관

다. 「공공기관의 운영에 관한 법률」에 따른 공공기관과 「지방공기업법」에 따른 지방공사 및 지방공단

나. 「국군조직법」 제2조에 따른 각 군, 해병대, 합동참모본부

라. 「전기통신사업법」 제6조에 따라 기간통신사업을 경영하는 자와 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설 사업자

마. 「정보통신기반 보호법」 제5조제1항에 따른 주요정보통신기반시설을 관리하는 기관

바. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관

사. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 조 제10호에 따른 전문

연구기관 아. 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 보유한 기관 자. 「전자금융거래법」 제2조제21호에 따른 전자금융기반시설을 운영하는 기관이나 단체 또는 사업자 차. 그 밖에 사이버공격·위협으로부터 소관사무 영역 보호가 필요한 기관 또는 단체 중에서 대통령령으로 정한 기관 또는 단체	연구기관 아. 「전자금융거래법」 제2조제21호에 따른 전자금융기반시설을 운영하는 기관이나 단체 또는 사업자 자. 그 밖에 사이버공격·위협으로부터 소관사무 영역 보호가 필요한 기관 또는 단체 중에서 대통령령으로 정하는 기관 또는 단체 6. “지원기관”이란 책임기관의 사이버안보 업무를 지원하는 다음 각 목의 기관 또는 업체를 말한다. 가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원 나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원 다. 「민법」 제32조에 따라 금융위원회의 허가를 받아 설립된 금융보안원 라. 제16조에 따라 지정한 사이버안보 전문업체
--	---

1) 사이버공간(안 제2조제1호)

제정들안은 “사이버공간”을 “「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망¹²⁾의 정보 처리 영

12) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

역”으로 정의하고 있음.

사이버공간이란 용어는 일반적으로 통용되고 법률 상에서도 별다른 정의 없이 사용되고 있는 입법례¹³⁾가 있으나, 법률상 명확한 정의는 없었던 것으로 파악되는데, 제정안에서 사이버공간의 정의를 새롭게 규정하는 것은 사이버공간이 사이버공격의 대상이 되고, 국가적으로 보호하여야 하는 또 다른 영역으로 인정되고 있는 추세를 반영하기 위한 것으로 보임.

2) 사이버안보(안 제2조제3호)

유용원의원안은 “사이버안보”를 “북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인 등 위협행위자들이 행하는 사이버공격을 확인·견제·차단하고 그에 필요한 대응조치를 강구·이행함으로써 국가의 안전보장과 국민의 사이버공간 활동에 지장을 초래하지 아니하는 것”으로 정의하고 있는데,

이는 「국가정보원법」 제4조제1항제1호마목에서 국가정보원의 직무를 “국제 및 국가배후 해킹조직 등 사이버안보”에 해당하는 정보의 수집·작성·배포로 규정하고, 같은 조 제1항제3호에서 “제1호 및 제2호의 직무수행에 관련된 조치로서 국가안보와 국익에 반하는 북한, 외국 및

1. “정보통신망”이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

13) 「전산산업발전법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

6. “사이버전사회”란 인터넷 등 정보통신망을 활용하여 사이버 공간에서 개최하는 전사회로서 산업통상부령으로 정하는 조건에 해당하는 것을 말한다.

외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·전제·차단하고, 국민의 안전을 보호하기 위하여 취하는 대응 조치”로 규정하고 있는 것을 고려한 것으로 보임.

한편, 김상훈의원안은 “사이버안보”를 사이버공격·위협으로부터 사이버공간을 보호하는 것에 초점을 두면서 사이버공격·위협을 행하는 주체에 대하여는 별도로 규정하고 있지 않은데, 이는 제명에 “안보”를 명시하고 있는 법률¹⁴⁾¹⁵⁾에서 안보를 위협하는 주체들보다는 안전보장이 이루어지고 있는 상태를 강조하고 있음을 반영한 것으로 보임.

3) 책임기관(안 제2조제4호)

제정안들은 “책임기관”을 “사이버안보에 관한 업무를 수행하는 기관”으로 정의하면서, ① 국회, 법원, 헌법재판소, 선거관리위원회, 중앙행정기관과 그 소속기관, 지방자치단체와 그 소속 기관, 교육청과 그 소속기관, ② 공공기관(과 지방공사 및 지방공단), ③ 「국군조직법」에 따른 각 군, 합동참모본부 등 군기관, ④ 기간통신사업자, 집적정보통신시설사업자, ⑤ 주요정보통신기반시설을 관리하는 기관, ⑥

14) 「경제안보를 위한 공급망 안정화 지원 기본법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “경제안보”란 국내외에서 발생하였거나 발생할 가능성이 있는 경제·통상·정치·외교적 상황 변화나 자연재해 등에도 불구하고 국내의 생산, 소비, 유통 등 국가 및 국민의 전반적인 경제활동에 필수적인 품목, 서비스, 기술 등이 원활히 유입되고, 부적절하게 해외로 유출되지 아니하도록 함으로써 국가의 안전보장이 유지되고 국가 및 국민의 경제활동에 지장이 초래되지 아니하는 상태를 말한다.

15) 「국가자원안보 특별법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. “자원안보”란 핵심자원의 가격 안정화와 중단 없는 공급이 이루어질 수 있도록 공급망의 안정적인 유지와 관리를 저해하는 요인에 대비하고, 그 요인에 대한 대응능력을 갖추어 국가의 안전보장과 국민경제 활동에 지장을 초래하지 아니하는 상태를 말한다.

국가핵심기술을 보유·관리하는 기관(또는 기업체), ⑦ 방위산업체, 전문 연구기관(또는 방위산업기술을 보유한 기관), ⑧ 전자금융기반시설을 운영하는 기관이나 단체 또는 사업자, ⑨ 그 밖에 사이버공격·위협으로부터 소관사무 영역 보호가 필요한 기관 또는 단체중에서 대통령령으로 정하는 기관 또는 단체로 나열하고 있음.

현행법령에 따르면 국가정보원은 「국가정보원법」, 대통령령인 「사이버안보 업무규정」, 대통령훈령인 「국가사이버안전관리규정」 등에 근거하여 각 소관부처와의 협력체계를 구축하여 ① 국가적인 사이버위기 대응과 ② 공공부문(중앙행정기관, 지방자치단체와 그 소속 기관, 공공기관 등)의 사이버공격 및 위협에 대한 예방 및 대응업무를 수행하고 있으며, 민간부문 각 분야의 사이버보안 관련 업무의 경우 소관 부처 유관 법률에 따라 소관 부처 또는 산하기관에서 개별적으로 수행하고 있는 상황인바,

제정안은 공공부문과 민간부문 중 사이버공격에 대한 체계적이고 효과적인 예방·대응이 필요한 기관을 “책임기관”으로 정의하여 보안관제, 예방·대응활동, 실태평가 등을 통합적으로 실시할 수 있도록 하려는 것으로 보임.

다만 이와 관련하여 한국인터넷기업협회, 주한미국상공회의소¹⁶⁾ 등에서 책임기관의 범위 불명확, 사이버안보 정책 협조 의무에 대한 부담, 사업자의 영업비밀 노출 우려 등을 이유로 신중한 검토가 필요하다는 의견을 제출한 바 있음.

(2) 사이버안보 기본계획 등의 수립(안 제5조·제6조)

유용원의원안	김상훈의원안
제5조(사이버안보 기본계획의 수립·시행) ① <u>정부는 이 법의 목적을 효율적으로 달성하기 위하여 3년마다 국가 차원의 전략 방향을 제시하는 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립하여야 한다.</u> ② 기본계획은 제7조에 따른 국가사이버안보위원회의 심의를 받아 확정한다. 기본계획을 변경하는 경우에도 또한 같다. ③ 기본계획에는 다음 각 호의 사항이 포함되어야 한다. 1. 사이버안보의 정책 목표와 추진방향 2. 사이버안보와 관련된 제도 및 법령의 개선 3. 사이버공격·위협의 예방 및 대응체계 4. 사이버안보 관련 교육·홍보·인력양성 및 국제협력 5. 사이버안보 관련 연구 및 기술개발	제5조(사이버안보 기본계획의 수립·시행) ① <u>정부는 사이버안보 업무의 효율적이고 체계적인 추진을 위하여 3년마다 국가 차원의 전략 방향을 제시하는 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립하여야 한다.</u> ② 기본계획은 <u>국가정보원장이 「정부조직법」 제2조에 따른 중앙행정기관(이하 “중앙행정기관”이라 한다)의 장과 협의하고,</u> 제7조에 따른 국가사이버안보위원회의 심의를 거쳐 확정한다. 기본계획을 변경하는 경우에도 또한 같다. ③ 기본계획에는 다음 각 호의 사항이 포함되어야 한다. 1. 사이버안보의 정책 목표와 추진방향 2. 사이버안보와 관련된 제도 및 법령의 개선 3. 사이버공격·위협의 예방 및 대응체계 4. 사이버안보 관련 교육·홍보·인력양성 및 국제협력 5. 사이버안보 관련 연구 및 기술개발

16) 주한미국상공회의소에서 국회 정보위원회에 제출한 자료, 2025. 10.

6. 사이버안보 정책 추진에 필요한 재원의 조달·운용 및 인력 확보방안 7. 그 밖에 사이버안보를 위하여 대통령령으로 정하는 사항 ④ 제1항부터 제3항까지에서 정하는 사항 외에 기본계획의 수립 <u>절차</u> 등에 관하여 필요한 사항은 대통령령으로 정한다.	6. 사이버안보 정책 추진에 필요한 재원의 조달·운용 및 인력 확보방안 7. 그 밖에 사이버안보를 위하여 대통령령으로 정하는 사항 ④ 제1항부터 제3항까지에서 정하는 사항 외에 기본계획의 수립 등에 필요한 사항은 대통령령으로 정한다.
제6조(연도별 시행계획) ① 국회·법원·헌법재판소·중앙선거관리위원회, 중앙행정기관, 시·도 및 시·도 교육청의 장은 기본계획에 따라 연도별 시행계획(이하 “<u>시행계획</u>”이라 한다)을 작성하여 국가정보원장에게 통보하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 대책·계획에 이미 반영하여 시행 중에 있거나 반영하기로 국가정보원장과 협의한 사항에 대하여는 시행계획을 작성하지 아니할 수 있다. 1. 「정보통신기반 보호법」 제5조제1항에 따른 보호대책 및 같은 법 제6조제1항에 따른 보호계획 2. 「개인정보 보호법」 제9조에 따른 기본계획 및 같은 법 제10조에 따른 시행계획 3. 그 밖에 개별 법령에 따라 소관사무 영역을 보호하는 사항이 포함된 대책·계획으로 대통령령이 정한 사항 ② 시행계획의 작성 방법·절차 및 세부 내용 등에 관하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.	제6조(연도별 시행계획) ① 국회·법원·헌법재판소·중앙선거관리위원회, <u>감사원, 국가인권위원회, 고위공직자범죄수사처</u>, 중앙행정기관 및 그 소속 기관, 시·도 및 시·도 교육청의 장은 기본계획에 따라 연도별 시행계획(이하 “<u>시행계획</u>”이라 한다)을 작성하여 국가정보원장에게 통보하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 대책·계획에 이미 반영하여 시행 중에 있거나 반영하기로 국가정보원장과 협의한 사항에 대하여는 시행계획을 작성하지 아니할 수 있다. 1. 「정보통신기반 보호법」 제5조제1항에 따른 보호대책 및 같은 법 제6조제1항에 따른 보호계획 2. 「개인정보 보호법」 제9조에 따른 기본계획 및 같은 법 제10조에 따른 시행계획 3. 그 밖에 개별 법령에 따라 소관사무 영역을 보호하는 사항이 포함된 대책·계획으로 대통령령이 정한 사항 ② 시행계획의 작성 방법·절차 및 세부 내용 등에 관하여 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.

1) 사이버안보 기본계획의 수립(안 제5조)

제정안들은 정부로 하여금 사이버안보 업무의 효율적이고 체계적인 추진을 위하여 국가 차원의 전략 방향을 제시하는 사이버안보 기본계획(이하 “기본계획”이라 함)을 3년마다 수립하도록 하면서, 사이버안보 기본계획에 포함되어야 하는 사항을 규정하고 있음.

현행법령을 살펴보면, 「사이버안보 업무규정」 제17조(사이버안보 업무 관련 전략 등의 연구·개발)¹⁷⁾에서 국가정보원장으로 하여금 사이버안보 업무의 수행에 필요한 전략·정책 및 기술을 연구·개발 할 수 있도록 하고 있으나, 해당 전략이 국가 차원의 전략인지 여부와 구체적인 내용에 대하여는 규정하고 있지 않고,

「전자정부법」에서는 중앙사무관장기관의 장으로 하여금 전자정부의 구현·운영 및 발전을 위하여 5년마다 전자정부기본계획을 수립하도록 하며, 「지능정보화 기본법」에서는 정부로 하여금 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획을 수립하도록 하고 있으나, 해당 계획들은 사이버보안이나 정보보호를

17) 「사이버안보 업무규정」 제17조(사이버안보 업무 관련 전략 등의 연구·개발) ① 국가정보원장은 사이버안보 업무의 수행에 필요한 전략·정책 및 기술을 연구·개발할 수 있다.
② 국가정보원장은 제1항에 따른 연구·개발을 위하여 다음 각 호의 어느 하나에 해당하는 기관을 전문기관으로 지정할 수 있다.
1. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따라 설립된 연구기관
2. 「민법」 제32조에 따라 설립된 비영리법인으로서 사이버안보 관련 학회 또는 학술단체
③ 제2항에 따른 전문기관을 지정하기 위하여 필요한 지정기준·절차 및 지정방법 등 세부 사항은 국가정보원장이 정한다.
④ 국가정보원장은 제2항에 따라 지정된 전문기관의 업무 수행을 위하여 그 필요한 경비의 전부 또는 일부를 예산의 범위에서 지원할 수 있다.

주된 목적으로 하고 있지 않다는 점을 고려할 때,¹⁸⁾

사이버안보 업무의 전략 방향을 제시하고자 하는 기본계획의 수립은 그 취지에 공감할 수 있음.

다만, 제정안들은 기본계획의 수립 주체를 “정부”로 하면서 주무 부처·기관을 명시하지 않고 있어 어느 기관에서 기본계획을 수립하여야 하는지 명확하지 않은 문제가 있어, 이를 명확하게 할 필요가 있다고 생각됨.

참고로 유사 입법례인 「전자정부법」과 「지능정보화 기본법」에서는 중앙사무관장기관의 장, 과학기술정보통신부장관을 각각 기본계획의 수립 주체로 명시하고 있음.¹⁹⁾

18) 「전자정부법」의 경우 제4조(전자정부의 원칙) 중 “정보시스템의 안전성·신뢰성의 확보”, 「지능정보화 기본법」의 경우 지능정보화 종합계획의 내용 중 “정보보호, 정보격차 해소” 등이 있으나, 이러한 내용이 각 계획의 주된 내용이라고 보기는 어려운 측면이 있음.

19) 「전자정부법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

4. “중앙사무관장기관”이란 국회 소속 기관에 대하여는 국회사무처, 법원 소속 기관에 대하여는 법원행정처, 헌법재판소 소속 기관에 대하여는 헌법재판소사무처, 중앙선거관리위원회 소속 기관에 대하여는 중앙선거관리위원회사무처, 중앙행정기관 및 그 소속 기관과 지방자치단체에 대하여는 행정안전부를 말한다.

제5조(전자정부기본계획의 수립) ① 중앙사무관장기관의 장은 전자정부의 구현·운영 및 발전을 위하여 5년마다 제5조의2제1항에 따른 행정기관등의 기관별 계획을 종합하여 전자정부 기본계획을 수립하여야 한다.

「지능정보화 기본법」 제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획(이하 “종합계획”이라 한다)을 3년 단위로 수립하여야 한다.

② 종합계획은 과학기술정보통신부장관이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 “전략위원회”라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

2) 연도별 시행계획(안 제6조)

제정안들은 국회·법원·헌법재판소·중앙선거관리위원회, 중앙행정기관, 시·도 및 시·도 교육청 등의 장으로 하여금 기본계획에 따라 연도별 시행계획을 작성하여 국가정보원장에게 통보하도록 하고 있음.

이에 대하여 국회사무처는 국회가 소관 영역 사이버안보 업무에 대한 연도별 시행계획을 작성하여 대통령 소속인 국가정보원장에게 통보하도록 하는 것은 소관 영역 사이버안보 업무에 대하여 국가정보원의 관리와 통제를 받는 효과를 초래할 가능성이 있어, 권력분립의 원칙과 헌법기관의 독립성이 침해될 우려가 있고,

「전자정부법」 제56조제4항²⁰⁾은 국회 등 헌법기관의 경우 해당 헌법기관의 장이 필요하다고 인정하는 경우에만 국가정보원장이 안정성을 확인한 보안조치를 하고 국가정보원장에게 그 이행 여부를 확인할 수 있도록 규정하고 있는 점을 감안할 필요가 있다는 의견임.

20) 「전자정부법」 제56조(정보통신망 등의 보안대책 수립·시행) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다.

② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다.

③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안정성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.

④ 제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다.

(3) 국가사이버안보위원회(안 제7조)

유용원의원안	김상훈의원안
제7조(국가사이버안보위원회) ① 사이버안보에 관한 중요사항을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다. ② 위원회는 다음 각 호의 사항을 심의한다. 1. 사이버안보와 관련한 전략·정책·법령 및 예산의 개선에 관한 사항 2. 제5조에 따른 사이버안보 기본계획에 관한 사항 등 중장기 대책 수립 및 추진에 관한 사항 3. 사이버안보 피해자 및 배후 국가·단체에 대한 대응조치에 관한 사항 4. 사이버안보 관련 정책 및 기관 간 역할조정에 관한 사항 5. 그 밖에 위원장이 회의에 부치는 사항 ③ 위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다. <u>이 경우 제4항제2호 및 제3호에 해당하는 사람 3명이 각각 포함되어야 한다.</u> ④ 위원장은 <u>대통령이</u> 되고, 위원은 다음 각 호의 사람이 된다. 1. 대통령령으로 정하는 관계 중앙행정기관의 장 2. <u>국가안보실장</u> 3. 국회 해당 상임위원회에서 추	제7조(국가사이버안보위원회) ① 사이버안보에 관한 중요사항을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다. ② 위원회는 다음 각 호의 사항을 심의한다. 1. 사이버안보와 관련한 전략·정책·법령 및 예산의 개선에 관한 사항 2. 제5조에 따른 사이버안보 기본계획 수립 등 중장기 대책 수립 및 추진에 관한 사항 3. 사이버안보 피해자 및 배후 국가·단체에 대한 대응조치에 관한 사항 4. 사이버안보 관련 정책 및 기관 간 역할 조정에 관한 사항 5. <u>제17조에 따른 사이버안보 실태 평가에 관한 사항</u> 6. 그 밖에 위원장이 회의에 부치는 사항 ③ 위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다. ④ 위원장은 <u>국가안보실장이</u> 되고, 위원은 다음 각 호의 사람이 된다. 1. <u>과학기술정보통신부장관</u> 2. <u>국가정보원장</u> 3. <u>개인정보 보호위원회 위원장</u> 4. 대통령령으로 정하는 관계 중앙행정기관의 장 5. 국회 해당 상임위원회에서 추

천한 사람 중에서 대통령이 위촉하는 사람 4. 사이버안보에 관하여 전문적인 식견을 갖춘 사람 중에서 대통령이 위촉하는 사람 ⑤ 위원회에 간사위원 2명을 두며, 간사위원은 과학기술정보통신부장관, 국가정보원장이 된다. ⑥ 위원회는 제2항의 사항을 미리 검토하고 관계 기관 사이의 협조 사항을 정리하기 위하여 위원회에 사이버안보실무위원회(이하 "실무위원회"라 한다)를 둔다. ⑦ 제6항에 따른 실무위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하되, 위원장은 국가정보원장이 된다. ⑧ 제1항부터 제7항까지에서 정한 사항 외에 위원회, 실무위원회의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.	천한 사람 중에서 대통령이 위촉하는 사람 <u>3명</u> 6. 사이버안보에 관하여 전문적인 식견을 갖춘 사람 중에서 대통령이 위촉하는 사람 <u>3명</u> ⑤ 위원회에 간사위원 2명을 두며, 간사위원은 과학기술정보통신부장관과 국가정보원장이 된다. ⑥ 위원회는 제2항의 사항을 미리 검토하고 관계 기관 사이의 협조 사항을 정리하기 위하여 위원회에 사이버안보실무위원회(이하 "실무위원회"라 한다)를 둔다. ⑦ 실무위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하되, 위원장은 국가정보원장이 된다. ⑧ 제1항부터 제7항까지에서 정한 사항 외에 위원회, 실무위원회의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.
---	---

제정안들은 사이버안보에 관한 중요사항을 심의하기 위하여 대통령 소속으로 국가사이버위원회를 두도록 하면서, 위원회로 하여금 ① 사이버안보와 관련한 전략·정책·법령 및 예산의 개선에 관한 사항, ② 사이버안보 기본계획 수립 등 중장기 대책 수립 및 추진에 관한 사항, ③ 대응조치에 관한 사항, ④ 사이버안보 관련 정책 등 기관간 역할 조정에 관한 사항, ⑤ 그 밖에 위원장이 회의에 부치는 사항 등을 논의하도록 규정하고 있는데, 이는 국가사이버위원회를 설치함으로써 부처간 이해관계를 조정하고 전문가의 식견이 반영될 수 있도록 하려는 것으로 생각됨.

다만, 현행 「국가안전보장회의법」 제7조의2(상임위원회)²¹⁾에 따른 상임위원회에서 국가안전보장에 관련되는 대외정책·군사정책 및 국내 정책에 관한 사항을 협의할 수 있도록 규정하고 있음을 고려할 필요가 있을 것으로 보임.

이와 관련하여 행정안전부는 「행정기관 소속 위원회의 설치·운영에 관한 법률」 제7조²²⁾는 이미 설치되어 있는 위원회와 성격과 기능이 중복되는 위원회의 설치를 제한하고 있으며, 성격·기능이 유사하거나 관련이 있는 위원회를 하나의 위원회와 분과위원회·전문위원회 체계로 연계하여 설치·운영토록 규정하고 있는 점을 고려할 때, 새로운 위원회의 설치보다는 정부내 회의체 등을 활용하는 것이 바람직할 것으로 보여 신중한 검토가 필요하다는 의견을 제시하였음.²³⁾

21) 「국가안전보장회의법」 제7조의2(상임위원회) ① 회의에서 위임한 사항을 처리하기 위하여 상임위원회를 둔다.

② 상임위원회는 위원 중에서 대통령령으로 정하는 자로 구성한다.

③ 상임위원회의 구성과 운영, 그 밖에 필요한 사항은 대통령령으로 정한다.

「국가안전보장회의 운영 등에 관한 규정」 제8조(상임위원회의 구성 등) ① 법 제7조의2에 따라 상임위원회는 위원장 1명과 8명의 위원으로 구성한다. <개정 2014. 4. 22., 2024. 4. 9.>

② 상임위원회의 위원장은 국가안보실장이 된다.

③ 상임위원회의 위원은 외교부장관, 통일부장관, 국방부장관, 국가정보원장, 대통령비서실장, 사무처장, 국가안보실의 제2차장 및 제3차장이 된다.

④ 국무조정실장은 상임위원회에 출석하여 발언할 수 있다.

제9조(상임위원회의 기능) 상임위원회는 안보회의의 위임에 의하여 국가안전보장에 관련되는 대외정책·군사정책 및 국내정책에 관한 사항을 협의한다.

22) 「행정기관 소속 위원회의 설치·운영에 관한 법률」 제7조(중복 위원회의 설치 제한 등) ① 행정기관의 장은 그 기관 또는 관련 기관 내에 설치되어 있는 위원회와 성격과 기능이 중복되는 위원회를 설치·운영하여서는 아니 된다.

② 행정기관의 장은 성격·기능이 유사하거나 관련이 있는 복수의 위원회를 하나의 위원회와 분과위원회, 전문위원회 등의 체계로 연계하여 설치·운영하여야 한다. <신설 2015. 8. 11.>

③ 행정기관의 장은 불필요한 위원회가 설치되지 아니하도록 소관 정책에 관한 각계 전문가의 의견을 종합적으로 반영하기 위하여 위원회를 통합하여 설치·운영하도록 노력하여야 한다.

23) 국가정보원에서 국회 정보위원회에 제출한 자료, 2025. 9.

(4) 국가사이버안보센터(안 제8조)

유용원의원안	김상훈의원안
제8조(국가사이버안보센터) ① 국가차원의 종합적·체계적인 사이버안보 업무 수행과 효율적인 사이버공격·위협 대응을 위하여 국가정보원에 국가사이버안보센터를 둔다. ② 제1항에 따른 국가사이버안보센터에 사이버안보에 관한 사항을 전문적으로 검토하고 <u>위원회의</u> 원활한 업무 수행을 지원하기 위하여 관계 전문가로 구성된 자문단을 설치·운영할 수 있다. ③ 국가정보원장은 사이버안보를 위한 대응조치로서 사이버공격·위협 탐지·대응, 사이버공격 사고조사 등을 위하여 민관합동 통합대응체계를 구축·운영할 수 있다. ④ 국가정보원장은 제1항에 따른 국가사이버안보센터의 운영을 위하여 필요한 경우에는 책임기관의 <u>장에게</u> 소속 공무원 또는 임직원의 파견 또는 겸임을 요청할 수 있다. ⑤ 그 밖에 <u>국가사이버안보센터의</u> 구성·운영 등에 관한 사항은 대통령령으로 정한다.	제8조(국가사이버안보센터) ① 국가차원의 종합적·체계적인 사이버안보 업무 수행과 효율적인 사이버공격·위협 대응을 위하여 국가정보원에 국가사이버안보센터를 둔다. ② 제1항에 따른 국가사이버안보센터에 사이버안보에 관한 사항을 전문적으로 검토하고 <u>위원회 및 실무위원회의</u> 원활한 업무 수행을 지원하기 위하여 관계 전문가로 구성된 자문단을 설치·운영할 수 있다. ③ 국가정보원장은 사이버안보를 위한 대응조치로서 사이버공격·위협 탐지·대응, 사이버공격 사고조사 등을 위하여 민관합동 통합대응체계를 설치·운영할 수 있다. ④ 국가정보원장은 제1항에 따른 국가사이버안보센터의 운영을 위하여 필요한 경우에는 책임기관의 <u>장 및 지원기관의 장에게</u> 소속 공무원 또는 임직원의 파견 또는 겸임을 요청할 수 있다. ⑤ 그 밖에 <u>국가사이버안보센터 및 통합대응체계의</u> 구성·운영 등에 관한 사항은 대통령령으로 정한다.

제정안들은 국가차원의 종합적·체계적인 사이버안보 업무 수행과 효율적인 사이버공격·위협 대응을 위하여 국가정보원에 사이버안보센터를 두고, 사이버안보센터에 사이버안보에 관한 사항을 전문적으로 검토하고

안 제7조에 따른 국가사이버안보위원회의 원활한 업무 수행을 지원하기 위하여 관계 전문가로 구성된 자문단을 설치·운영할 수 있도록 규정하고 있는데,

국가정보원장으로 하여금 민관합동 통합대응체계를 설치·운영할 수 있도록 하고, 국가사이버안보센터의 운영을 위하여 필요한 경우에는 책임기관(또는 지원기관)의 장에게 소속 공무원 또는 임직원의 파견 또는 겸임을 요구할 수 있도록 하려는 것으로 보임.

이를 통해 현재 대통령령인 「사이버안보 업무규정」 제4조(국가사이버안보센터)²⁴⁾에 근거하여 운영되고 있는 국가사이버센터가 법률에 근거한 조직이 됨에 따라 관련 부처 간의 협력을 구하기 용이해지고, 법적 안정성이 확보되는 효과가 기대되는 측면이 있음.

다만, 현행 「사이버안보 업무규정」 제4조제4항은 국가정보원장이 국가사이버안보센터의 운영을 위하여 필요한 경우 국가기관이나 그 밖의 관계 기관 또는 단체의 공무원 또는 임직원의 파견 등 협조를 요청할 수 있도록 규정하고 있는데, 제정안은 “책임기관”의 장에게 공무원 또는 임직원의 파견 또는 겸임을 요구할 수 있도록 규정하고 있어 협력요청

24) 「사이버안보 업무규정」 제4조(국가사이버안보센터) ① 국가정보원장은 사이버안보 업무를 효율적으로 수행하기 위하여 국가사이버안보센터를 둘 수 있다.

② 제1항에 따른 국가사이버안보센터에는 제6조의2제4항에 따른 민관합동 통합대응체계를 구축·운영하기 위한 전담조직을 둘 수 있다.

③ 제1항에 따른 국가사이버안보센터에 사이버안보에 관한 사항을 전문적으로 검토하기 위하여 관계 전문가로 구성된 자문단을 설치·운영할 수 있다.

④ 국가정보원장은 제1항에 따른 국가사이버안보센터의 운영을 위하여 필요한 경우 법 제5조 제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체(이하 “국가기관 등”이라 한다)의 장에게 소속 공무원 또는 임직원의 파견 등 협조를 요청할 수 있다.

의 범위가 줄어들지는 측면이 있는 것으로 보임.

이와 관련하여 한국인터넷기업협회, 주한미국상공회의소 등 민간 기관에서는 국가정보원장이 “책임기관”의 장에게 임직원의 파견 또는 겸임을 요청할 수 있도록 하는 것은 기관 운영상의 부담이 따르는 것으로, 임직원의 파견 또는 겸임 요청의 요건을 보다 구체화하거나 인력 공백에 대한 비용 보전 등을 추가할 필요가 있다는 입장임.

(5) 통합보안관제의 구축(안 제10조)

유용원의원안	김상훈의원안
제10조(통합보안관제체계의 구축 등) ① 국가정보원장은 책임기관에 대한 사이버공격·위협을 즉시 탐지·대응[이하 “보안관제(保安管制)”라 한다]하기 위하여 통합보안관제체계를 구축·운영하여야 한다. ② 책임기관의 장은 소관사무 영역에 대한 보안관제를 위하여 제1항에 따른 통합보안관제체계와 연계된 보안관제센터를 구축·운영하여야 한다. 다만, 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 아니하고 다른 기관의 보안관제센터를 활용할 수 있다. ③ 국가정보원장은 제1항에 따른 통합보안관제체계를 이용하여 각 책임기관의 장과 합동으로 해당 책임기관에 대한 보안관제를 실시하거나 사이버안보 위협을 탐지할 수 있는 기술정보를 배포할 수 있다.	제10조(통합보안관제체계의 구축 등) ① 국가정보원장은 책임기관에 대한 사이버공격·위협을 즉시 탐지·대응[이하 “보안관제(保安管制)”라 한다]하기 위하여 통합보안관제체계를 구축·운영하여야 한다. ② 책임기관의 장은 소관사무 영역에 대한 보안관제를 위하여 제1항에 따른 통합보안관제체계와 연계된 보안관제센터를 구축·운영하여야 한다. 다만, 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 아니하고 다른 기관의 보안관제센터를 활용할 수 있다. ③ 국가정보원장은 제1항에 따른 통합보안관제체계를 이용하여 각 책임기관의 장과 합동으로 해당 책임기관에 대한 보안관제를 실시하거나 사이버공격·위협을 탐지할 수 있는 기술정보를 배포할 수 있다. ④ 국가정보원장은 제3항에 따른

④ 제1항부터 제3항까지에서 정하는 사항 외에 보안관제센터의 <u>설치·운영</u> 및 그 밖에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.	<u>보안관제를 위하여 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다.</u> ⑤ 제1항부터 제4항까지에서 정하는 사항 외에 <u>통합보안관제체계 및 보안관제센터의 구축·운영</u> 및 그 밖에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.
---	---

현행 「사이버안보 업무규정」 제14조(통합보안관제)²⁵⁾는 국가정보원장으로 하여금 중앙행정기관등²⁶⁾에 대한 보안관제를 실시하기 위하여 통합보안관제체제를 구축·운영하도록 하고 있고, 중앙행정기관의 장은 해당 기관의 보안관제를 위하여 통합관제센터와 연계된 보안관제센터를 설치·운영하거나 다른 기관의 보안관제센터를 활용할 수 있도록 하고 있음.

- 25) 「사이버안보 업무규정」 제14조(통합보안관제) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 즉시 탐지·대응[이하 “보안관제(保安管制)”라 한다]하기 위하여 통합보안관제체계를 구축·운영해야 한다.
- ② 중앙행정기관등의 장은 해당 기관의 보안관제를 위하여 제1항에 따른 통합보안관제체계와 연계된 보안관제센터를 설치·운영해야 한다. 다만, 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 않고 다른 기관의 보안관제센터를 활용할 수 있다.
- ③ 국가정보원장은 제1항에 따른 통합보안관제체계를 활용하여 각 중앙행정기관등의 장과 합동으로 해당 중앙행정기관등에 대한 보안관제를 실시할 수 있다.
- ④ 국가정보원장은 제3항에 따른 보안관제를 위하여 법 제5조제1항에 따라 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다.
- ⑤ 제1항부터 제4항까지에서 규정한 사항 외에 보안관제센터의 설치·운영 및 그 밖에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.
- 26) ① 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회, ② 지방자치단체와 그 소속기관, ③ 그 밖에 대통령령으로 정하는 공공기관을 뜻함.

제정안들은 국가정보원이 실시하는 통합보안관제체계의 범위를 중앙 행정기관 등에서 헌법기관, 민간기관을 포함하는 책임기관에까지 확장하려는 것으로,

사이버위협이 공공·민간 구분 없이 동시다발적·전방위적으로 발생한다는 점에서 사이버위협 탐지 체계를 국가 차원으로 확대하려는 취지에 공감할 수 있음.

다만, 국회사무처는 헌법기관 영역의 보안관제를 국가정보원에서 실시하도록 하는 것은 소관 영역 사이버안보 업무에 대하여 국가정보원의 관리와 통제를 받는 효과를 초래할 수 있어 권력분립의 원칙과 헌법기관의 독립성이 침해될 우려가 있는 점을 고려할 필요가 있다는 의견²⁷⁾을 제시하였고,

한국인터넷기업협회는 정부와 민간사업자 사이에 통합보안관제체계를 연계하여 구축하는 경우 시스템 운용 과정에서 국가-민간 통신망 연결에 따라 서비스 성능과 안전성이 저해될 우려가 있고, 민간사업자의 영업비밀이 유출될 우려가 있는 점이 문제될 수 있다는 의견을 제기하고 있는 점 등을 종합적으로 고려할 필요가 있어 보임.

27) 국회사무처에서 국회정보위원회로 제출한 자료, 2025. 8.

(6) 사이버피해 조사(유용원의원안 제13조·제20조, 김상훈의원안 제13조·제21조)

유용원의원안	김상훈의원안
제13조(사이버피해 조사 등) ① 책임기관의 장은 소관사무 영역에서 <u>사이버공격으로</u> 인한 피해가 발생한 때에는 신속하게 사고조사를 실시하여야 하고 그 결과를 관계 책임기관의 장 및 국가정보원장에게 통보하여야 한다. 다만, 제2조제3호에 따른 위협행위자의 <u>사이버공격으로</u> 인한 피해가 발생한 때에는 지체 없이 국가정보원장에게 통보하여야 한다. ② 국가정보원장은 제1항에 따른 통보를 받은 경우에는 사이버공격·위협 대응에 필요한 조사 및 조치를 실시하여야 한다. ③ 국가정보원장은 제2항에 따른 조사 및 조치를 위하여 필요한 경우 관계 책임기관의 장 및 대통령령으로 정하는 전문기관·단체의 장에게 기술적 지원을 요청할 수 있다. ④ 국가정보원장은 피해의 복구 및 확산 방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다. ⑤ 누구든지 제2항 및 제3항에 따른 조사를 완료하기 전에 사이버공격·위협과 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.	제13조(사이버피해 조사 등) ① 책임기관의 장은 소관사무 영역에서 <u>사이버공격·위협으로</u> 인한 피해가 발생한 때에는 신속하게 사고조사를 실시하고, 그 결과를 관계 책임기관의 장 및 국가정보원장에게 통보하여야 한다. <u>다만, 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인 등의 사이버공격으로</u> 인한 피해가 발생한 때에는 그 사실을 지체 없이 국가정보원장에게 통보하여야 한다. ② 국가정보원장은 제1항에 따른 통보를 받은 경우에는 사이버공격·위협 대응에 필요한 조사 및 조치를 실시하여야 한다. ③ 국가정보원장은 제2항에 따른 조사 및 조치를 위하여 필요한 경우 관계 책임기관의 장, <u>지원기관의 장</u> 및 대통령령으로 정하는 전문기관·단체의 장에게 기술적 지원을 요청할 수 있다. ④ 국가정보원장은 피해의 복구 및 확산 방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 <u>요청받은</u> 책임기관의 장은 특별한 사유가 없으면 이에 따라야 한다. ⑤ 누구든지 제2항에 따른 조사를 완료하기 전에 사이버공격·위협과 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

⑥ 그 밖에 조사 및 조치에 관하여 필요한 사항은 대통령령으로 정한다.	⑥ 그 밖에 조사 및 조치에 관하여 필요한 사항은 대통령령으로 정한다.
제20조(사이버공격·위협 조사 등에 대한 특례) ① 제13조 및 제17조에도 불구하고 제2조제5호다목에 해당하는 책임기관에 대한 다음 각 호의 업무는 국방부장관이 수행한다. 1. 제13조에 따른 사이버공격·위협 조사 2. 제17조에 따른 사이버안보 실태 평가 ② 국방부장관은 제1항에 따른 업무를 수행할 때에 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.	제21조(사이버피해 조사 등에 대한 특례) ① 제13조 및 제17조에도 불구하고 제2조제5호나목에 해당하는 책임기관에 대한 다음 각 호의 업무는 국방부장관이 수행한다. 1. 제13조에 따른 사이버피해 조사 2. 제17조에 따른 사이버안보 실태 평가 ② 국방부장관은 제1항에 따른 업무를 수행할 때에 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

현행 「사이버안보 업무규정」 제16조(사고 조사)²⁸⁾는 중앙행정기관 등에 대한 사이버공격·위협으로 사고가 발생한 경우 국가정보원장이 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있도록 하고, 사고 조사 결과 유출된 것으로 판단되는 자료에 대하여

28) 「사이버안보 업무규정」 제16조(사고 조사) ① 국가정보원장은 중앙행정기관 등에 대한 사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있다. 다만, 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 조사를 실시할 수 있다. <개정 2024. 3. 5.>
② 제1항에도 불구하고 국가정보원장 또는 국방부장관은 중앙행정기관 등에 대한 사이버공격·위협으로 인한 사고가 국제 및 국가배후 해킹조직 등의 위해 행위에 해당되지 않거나, 그 밖의 경미한 사고라고 판단될 경우 해당 중앙행정기관 등의 장이 자체적으로 조사하게 할 수 있다.
③ 국가정보원장은 제1항 및 제2항에 따른 조사 결과 해당 사고로 유출된 것으로 판단되는 자료에 대하여 해당 중앙행정기관 등의 장과 합동으로 국가안보, 국익 및 정부 정책에 미치는 영향을 평가할 수 있다.
④ 국가정보원장은 해당 중앙행정기관 등의 장에게 제3항에 따른 국가안보, 국익 및 정부 정책에 미치는 영향을 최소화하기 위하여 필요한 조치를 할 것을 요청할 수 있다.
⑤ 국가정보원장은 사이버보안 업무의 수행과 관련하여 필요한 경우 중앙행정기관 등의 장에게 제1항 단서 및 제2항에 따른 조사 결과, 제4항에 따른 조치 결과의 제출을 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관 등의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

해당 중앙행정기관의 장과 합동으로 국가안보, 국익 및 정부 정책에 미치는 영향을 평가할 수 있도록 하며, 해당 중앙행정기관의 장에게 해당 사항에 따른 필요한 조치를 할 것을 요청할 수 있도록 하고 있음.

또한, 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대하여는 국방부장관이 조사를 실시 할 수 있도록 하고, 사고가 국제 및 국가배후 해킹조직 등의 위해 행위에 해당하지 않거나 그 밖의 경미한 사고라고 판단될 경우 해당 중앙행정기관의 장이 자체적으로 조사할 수 있도록 예외 규정을 두고 있음.

제정안의 제13조 및 제20조·제21조는 국가정보원이 실시하는 사고 조사의 범위를 중앙행정기관 등에서 헌법기관, 민간기관을 포함하는 책임 기관에까지 확장하려는 것으로,

최근 사이버공격·위협이 공공과 민간의 구분 없이 동시다발적으로 발생함에 따라 그 피해 역시 전방위적으로 확산하고 있어 사고에 대한 조사 권한을 국가 차원으로 확대하려는 취지에 공감할 수 있음.

다만, 현행 규정은 국가정보원장의 사고 조사 실시를 임의규정으로 두고 사고가 국제 및 국가배후 해킹조직 등의 위해 행위에 해당하지 않거나 경미한 사고인 경우 해당 중앙행정기관의 장으로 하여금 자체적으로 조사할 수 있도록 규정하고 있는 반면,

제정안에서는 사고 조사 실시를 강행규정으로 하고 중앙행정기관에 대한 위임 규정은 두고 있지 않아 국가정보원이 모든 사고의 조사를 실시할 수

있는지에 대한 검토가 필요할 것으로 생각되며, 국회사무처의 제시 의견과 같이 국가정보원장이 헌법기관 대하여 조사를 실시할 수 있도록 하는 것에 대하여는 권력분립의 원칙과 헌법기관의 독립성 침해 우려를 고려한 입법적 검토가 수반되어야 할 것으로 생각됨.

(7) 사이버위기대책본부(안 제15조)

유용원의원안	김상훈의원안
제15조(사이버위기대책본부) ① 정부는 제14조에 따른 경계 또는 심각단계의 경보가 발령된 경우 사이버공격·위협에 대한 원인분석, 긴급대응, 피해복구 등 신속한 국민안전 보호조치를 수행하기 위하여 사이버위기대책본부(이하 “대책본부”라 한다)를 구성·운영할 수 있다. ② 대책본부의 장(이하 “대책본부장”이라 한다)은 국가정보원장이 되며, 대책본부장은 대책본부의 업무를 총괄하고 필요하다고 인정하면 사이버위기대책본부회의를 소집할 수 있다. 다만, 민간에 대한 부문별 경보가 발령된 경우에는 과학기술정보통신부장관이 대책본부장의 권한을 행사한다. ③ 대책본부장은 제1항에 따른 대책본부를 구성·운영하기 위하여 책임기관 및 대통령령으로 정하는 기관·단체의 장에게 참여를 요청할 수 있다. ④ 그 밖에 대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.	제15조(사이버위기대책본부) ① 정부는 제14조제1항에 따른 경계 또는 심각단계의 경보가 발령된 경우 사이버공격·위협에 대한 원인분석, 긴급대응, 피해복구 등 신속한 국민안전 보호조치를 수행하기 위하여 사이버위기대책본부(이하 “대책본부”라 한다)를 구성·운영할 수 있다. ② 대책본부의 장(이하 “대책본부장”이라 한다)은 국가정보원장이 되고, 대책본부장은 대책본부의 업무를 총괄하며 필요하다고 인정하는 경우에는 사이버위기대책본부회의를 소집할 수 있다. 다만, 민간에 대한 부문별 경보가 발령된 경우에는 과학기술정보통신부장관이 대책본부장의 권한을 행사한다. ③ 대책본부장은 대책본부의 구성·운영을 위하여 책임기관, 지원기관 및 그 밖에 대통령령으로 정하는 기관·단체의 장에게 참여를 요청할 수 있다. ④ 그 밖에 대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

현행 「사이버안보 업무규정」 제6조의2(사이버안보정보 업무 수행 관련 대응조치 등) 제4항²⁹⁾은 국가정보원장으로 하여금 국가안보나 국익에 반하는 활동으로부터 국민의 안전을 보호하기 위한 대응조치로서 국가안보실장과 협의하여 위기상황을 관리하기 위한 민관합동 통합대응체계를 구축·운영할 수 있도록 하면서, 같은 규정 제4조제3항³⁰⁾은 민관합동 통합대응체계를 구축·운영하기 위한 전담조직을 국가사이버안보센터에 둘 수 있도록 하고 있음.

제정안들은 정부로 하여금 경계 또는 심각단계의 경보가 발생된 경우 국민안전 보호조치를 수행하기 위하여 사이버위기대책본부를 구성·운영할 수 있도록 하고, 대책본부의 장은 국가정보원장이 되며 필요하다고 인정하는 경우에는 사이버위기대책본부회의를 소집할 수 있도록 하고, 대책본부장으로 하여금 대책본부의 구성·운영을 위하여 책임기관 및 대통령령으로 정하는 기관·단체의 장에게 참여를 요청할 수 있도록 하면서, 민간에 대한 부문별 경보가 발령된 경우에는 과학기술정보통신부장관이 대책본부장의 권한을 행사하도록 하고 있음.

이는 현행 「사이버안보 업무규정」 상 민·관 합동 대응을 위한 대

29) 「사이버안보 업무규정」 제6조의2(사이버안보정보 업무 수행 관련 대응조치 등) ① ~ ③ (생략)

④ 국가정보원장은 국가안보나 국익에 반하는 활동으로부터 국민의 안전을 보호하기 위한 대응조치로서 국가안보실장과 협의하여 위기상황을 관리하기 위한 민관합동 통합대응체계를 구축·운영할 수 있다.

③·④ (생략)

30) 「사이버안보 업무규정」 제4조(국가사이버안보센터) ① (생략)

② 제1항에 따른 국가사이버안보센터에는 제6조의2제4항에 따른 민관합동 통합대응체계를 구축·운영하기 위한 전담조직을 둘 수 있다.

③·④ (생략)

응체계를 사이버위기대책본부로 명명하여 법률로 상향함과 동시에, 현행 규정으로는 명확하지 아니하였던 본부 구성 요건, 참여 요청의 근거 등을 명확하게 하려는 취지로 생각됨.

다만 국방부는 대책본부장을 국가정보원장이 아니라 국가안보실장이 지명하도록 할 필요가 있다는 의견을 제시하였고, 경찰청은 국가안보실장이 대책본부장이 되어야 한다는 의견을 제시하였음.

(8) 국회 정보위원회 보고(유용원의원안 제16조, 김상훈의원안 제19조)

유용원의원안	김상훈의원안
제16조(국회 정보위원회 보고) ① 국가정보원장은 이 법에 따른 정부의 사이버안보 업무와 관련한 사항을 국회 정보위원회에 반기별로 보고하여야 한다. ② <u>국가정보원장은 제1항에도 불구하고 사이버안보 업무와 관련한 사항이 군사·외교·대북 관계의 국가기밀에 관한 사항으로서 그 보고로 인하여 국가 안위에 중대한 영향을 미치는 경우에는 그 사유를 밝히고 보고를 거부할 수 있다. 이 경우 국회 정보위원회는 그 의결로써 국가정보원장의 소명을 요구할 수 있으며, 소명을 요구받은 날부터 7일 이내에 국가정보원장의 소명이 없는 경우에는 보고를 거부할 수 없다.</u> ③ 국가정보원장은 국가 기밀에 속하는 사항에 관한 보고에 대하여 이를 공개하지 아니할 것을 요청할 수 있다.	제19조(국회 정보위원회 보고) ① 국가정보원장은 이 법에 따른 정부의 사이버안보 업무와 관련한 사항을 국회 정보위원회에 반기별로 보고하여야 한다. ② 국가정보원장은 국가 기밀에 속하는 사항에 관한 보고에 대하여 이를 공개하지 아니할 것을 요청할 수 있다.

제정안들은 국가정보원장으로 하여금 정부의 사이버안보 업무와 관련된 사항을 국회 정보위원회에 반기별로 보고하도록 하고 있는데, 이는 「국가정보원법」 제15조(국회에의 보고 등), 제17조(국회에서의 증언 등)³¹⁾과 관련된 내용의 조항으로, 국가사이버안보센터, 통합관제체제 등을 국가정보원이 운영함에 따라 불거질 수 있는 우려를 경감시키고, 국회 정보위원회의 사이버안보 업무에 대한 민주적 통제권을 강화하기 위한 취지로 이해됨.

다만, 「국가정보원법」 제17조제2항은 국가정보원장이 국회 정보위원회에서 자료의 제출, 증언 또는 답변을 거부하는 경우 국회 정보위원회 등은 그 의결로서 ‘국무총리’의 소명을 요구할 수 있도록 하고 있어, 유용원의원안 제16조제2항 중 소명을 요구하는 대상을 ‘국가정보원장’에서 ‘국무총리’로 수정하여 법적 체계성을 확보할 필요가 있어 보임.

문 의 처

02)6788-5614

31) 「국가정보원법」 제15조(국회에의 보고 등) ① 원장은 국가 안전보장에 중대한 영향을 미치는 상황이 발생할 경우 지체 없이 대통령 및 국회 정보위원회에 보고하여야 한다.

② 원장은 국회 정보위원회가 재적위원 3분의 2 이상의 찬성으로 특정사안에 대하여 보고를 요구한 경우 해당 내용을 지체 없이 보고하여야 한다.

제17조(국회에서의 증언 등) ① 원장은 국회 예산결산 심사 및 안건 심사와 감사원의 감사가 있을 때에 성실하게 자료를 제출하고 답변하여야 한다. 다만, 국가의 안전보장에 중대한 영향을 미치는 국가 기밀 사항에 대하여는 그 사유를 밝히고 자료의 제출 또는 답변을 거부할 수 있다.

② 원장은 제1항에도 불구하고 국회 정보위원회에서 자료의 제출, 증언 또는 답변을 요구받은 경우와 「국회에서의 증언·감정 등에 관한 법률」에 따라 자료의 제출 또는 증언을 요구받은 경우에는 군사·외교·대북관계의 국가 기밀에 관한 사항으로서 그 발표로 인하여 국가 안위(安危)에 중대한 영향을 미치는 사항에 대하여는 그 사유를 밝히고 자료의 제출, 증언 또는 답변을 거부할 수 있다. 이 경우 국회 정보위원회 등은 그 의결로써 국무총리의 소명을 요구할 수 있으며, 소명을 요구받은 날부터 7일 이내에 국무총리의 소명이 없는 경우에는 자료의 제출, 증언 또는 답변을 거부할 수 없다.

③ 원장은 국가 기밀에 속하는 사항에 관한 자료와 증언 또는 답변에 대하여 이를 공개하지 아니할 것을 요청할 수 있다.