



제418회국회(정기회)
제 6 차 국 방 위 원 회

통합방위법 일부개정법률안

검 토 보 고

〈통합방위 대상영역에 정보통신기반시설 추가〉

■ 김선교의원 대표발의(의안번호 제2204414호)

2024. 11.

국 방 위 원 회

수석전문위원 오 명 호

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
※ 참고자료	8

I. 제안경위

1. 발 의 자 : 김선교의원 등 11인
2. 발 의 일 : 2024. 9. 27.
3. 회 부 일 : 2024. 9. 30.

II. 제안이유 및 주요내용

현행법은 적(敵)의 침투·도발이나 그 위협에 대응하여 국가방위 요소를 통합·운용하기 위한 통합방위 대책을 수립·시행하는데 필요한 사항을 규정하는 것을 목적으로 하고 있음.

그런데 최근 국가 주요시설을 대상으로 정보의 탈취를 시도하거나 사회기반시설 운영의 교란·마비를 목적으로 사이버 공격을 시도하는 사례가 증가하고 있어 사이버공간을 국가안보 차원에서 방호하여야 할 필요성이 높아지고 있음에도 불구하고 현행법은 통합방위의 범위를 대한민국 국민 또는 영역으로 규정하고 있어 이에 대한 문제가 제기되고 있음.

이에 “침투”, “도발” 등 통합방위 대상에 대한 개념에 사이버공간을 포함하도록 명시함으로써 사이버안보에 대한 법·제도적 장치를 강화하려는 것임(안 제2조제9호 및 제10호).

Ⅲ. 검토의견

1. 통합방위 대상영역에 정보통신기반시설 추가

□ 개정안은 정의 규정에서 침투 및 도발의 통합방위 대상영역에 정보통신기반시설¹⁾을 추가하려는 것임(안 제2조제9호 및 제10호).

[신·구조문대비표]

현행	개정안
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. 1. ~ 8. (생략) 9. “침투”란 적이 특정 임무를 수행하기 위하여 대한민국 <u>영역</u> 을 침범한 상태를 말한다. 10. “도발”이란 적이 특정 임무를 수행하기 위하여 대한민국 <u>국민 또는 영역</u> 에 위해(危害)를 가하는 모든 행위를 말한다. 11. ~ 13. (생략)	제2조(정의) ----- -----. 1. ~ 8. (현행과 같음) 9. ----- ----- <u>영역</u> <u>또는 정보통신기반시설(「정보통신기반 보호법」 제2조제1호에 따른 정보통신기반시설을 말한다. 이하 같다)</u> ----- -----. 10. ----- ----- <u>국민, 영역 또는 정보통신기반시설</u> ----- -----. 11. ~ 13. (현행과 같음)

1) 「정보통신기반 보호법」 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “정보통신기반시설”이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.

□ 최근 사이버범죄와 테러가 급증하면서, 국민의 일상과 기업의 경제 활동이 위협받고 있으며, 조직화된 사이버공격이 국가 안보에 심각한 도전이 되고 있음. 사이버공격의 양상도 기밀절취·금전취득에서 기반시설 마비·파괴하는 사이버테러 등 다양화되고 있으며, 최근에는 사이버공격을 통해 전통적인 무력공격 수준의 피해를 발생시키는 사이버전쟁 발생 가능성²⁾도 점차 증대하고 있음.

□ 실제로, 최근 5년간('20~'24.10.) 군을 대상으로 한 유형별 사이버 침해시도 건수가 매년 1만건 이상으로 발생하고 있어 해킹이나 컴퓨터바이러스 등 사이버공격에 의한 국방정보 유출이나 파괴 등을 예방하기 위한 대비태세의 강화가 요구되고 있음.

[최근 5년간 군 대상 사이버 침해시도 현황]

구분	총계	홈페이지 침해시도	악성코드 탐지	해킹메일 탐지
'20	12,696	12,586	58	52
'21	11,600	11,511	34	55
'22	9,021	8,982	6	33
'23	13,499	13,482	1	16
'24.10.	10,564	10,488	0	76
계	57,380	57,049	99	232

2) 2022년 러시아의 우크라이나 침공 당시 우크라이나와 러시아측의 해커들이 양국의 언론사와 주요 관공서 사이트를 공격해서 다운시켰으며 딥페이크 기술을 이용해서 푸틴 대통령이 말하는 걸 흉내내 계엄령과 총동원령을 내렸다는 가짜 뉴스가 해킹된 지역 방송국과 라디오를 통해 살포된바 있음.

이스라엘-하마스 전쟁 개시와 함께 하마스의 공식 사이버 부대(Hamas Cyber Unit)는 물론 방글라데시, 모로코 등지의 친팔레스타인 해티비스트 그룹들, 러시아의 지원을 받는 해커 그룹들이 이스라엘의 정보망을 공격했고, 반대로 이스라엘 및 인도의 해커들이 팔레스타인 전산망을 공격하며 서로의 선전문구를 올려놓거나 사이트를 다운시키기도 함.

□ 이에 개정안은 적의 ‘침투’ 및 ‘도발’에 대한 통합방위의 대상영역에 정보통신기반시설을 추가하려는 것으로, 사이버공격의 양상이 사이버전쟁으로 확대될 가능성이 높아지는 상황 및 위협적인 사이버전력을 보유³⁾한 북한과 직접 대치하고 있는 우리나라의 안보환경을 고려할 때 개정안의 입법취지는 타당한 것으로 보임. 또한 현행법 제15조제1항⁴⁾에서 통합방위작전의 관할구역을 지상, 해상 및 공중으로만 구분하고 있어 사이버공간에 대한 침투 및 도발시 관할구역이 불분명한바, 개정안과 같이 사이버공간을 침투 및 도발의 대상영역으로 규정하면 관할구역이 명확해 지는 효과도 나타날 것으로 보임.

□ 다만, 개정안에 대해서는 다음과 같은 점을 함께 고려해야 할 것으로 보임.

첫째, 현행법은 현재 ‘침투’의 대상이 되는 영역으로 ‘대한민국의 영역’을 규정하고 있으나, 영역은 일반적으로 한 나라의 주권이 미치는 범위를 의미하므로 사이버공간도 대한민국의 주권이 미치는 범위 내에 있는 것으로 해석⁵⁾한다면 개정안과 같이 별도로

3) 하버드 케네디 대학의 벨퍼센터가 제공하는 ‘사이버국력지수(NCPI)’를 통해 파악된 북한의 종합적인 사이버 역량은 2022년 세계 14위를 차지하고 있으며 사이버 역량의 상당 부분이 사이버 공격 활동과 불법적인 금융 활동에 집중되어 있음.(북한의 사이버 위협 실태와 우리의 대응, 외교안보연구소, 2023.5.), 국정원은 북한 내 사이버인력을 8,400명 규모로 보고 있음.(’24.7.)

4) 「통합방위법」 제15조(통합방위작전) ① 통합방위작전의 관할구역은 다음 각 호와 같이 구분한다.

1. 지상 관할구역: 특정경비지역, 군관할지역 및 경찰관할지역
2. 해상 관할구역: 특정경비해역 및 일반경비해역
3. 공중 관할구역: 비행금지공역(空域) 및 일반공역

5) 정부는 2011년 ‘국가 사이버안보 마스터플랜’을 수립한바 있는데, 사이버공간을 영토·영공·영해에 이어 국가가 수호해야 할 또 하나의 ‘영역’으로 본 바 있음.

침투의 대상으로 사이버공간(정보통신기반시설)을 규정할 실익은 적어진다는 점을 고려할 필요가 있음.

둘째, 현행법은 현재 ‘도발’의 대상이 되는 영역으로 ‘대한민국 국민 또는 영역’을 규정하고 있으나, 사이버공간에 대한 도발은 궁극적으로 대한민국의 영역 내의 시설 마비, 정보 위조 등을 유발하고 이로 인해 국민의 재산권 등에 직·간접적으로 위해를 가한다는 점을 고려한다면 개정안과 같이 별도로 도발의 대상으로 사이버공간(정보통신기반시설)을 규정할 실익은 적어진다는 점을 고려할 필요가 있음.

□ 참고로, 정부는 현행법 체계 하에서 제56차(2023. 2.) 및 제57차(2024. 1.) 중앙통합방위회의를 개최해 사이버 공격, 테러 등에 대한 통합방위태세 구축에 대한 논의를 실시한 바 있음.

□ 개정안에 대해서 국방부는 다음과 같은 이유로 신중한 검토가 필요하다는 입장임.

첫째, 전·평시 북한의 사이버공격 위협 증대에 따라 사이버공간에 대한 국가 차원의 방호를 위해 법·제도적 장치를 강화하고자 하는 개정안의 취지에는 동의하나, 통합방위사태 선포에 따라 통합방위본부장 또는 지역군사령관(시·도 경찰청장)이 수행하는 통합방위작전체계와 국가안보실을 컨트롤타워로 하는 現 국가 사이버안보 수행체계가 상충되어 관계기관과의 협의가 필요함.

*** 국가사이버안보 기본계획**

국가안보실 - 컨트롤타워, 주관기관 - 국가정보원 / 국방·외교 등 8개 분야 구분

둘째, 통합방위작전은 적의 침투·도발에 대하여 물리적인 영역에서 이루어지는 반면 사이버 대응은 침투·도발의 주체가 불분명하고 특정 영역에 국한되지 않으며, 통합방위 작전지휘관(지역군사령관, 시·도 경찰청장)의 사이버 대응 역량 및 전문기관 통제능력에도 제한이 있음.

셋째, 개정안은 사이버공간을 ‘정보통신기반시설’로 지칭하고 있으나 해당 용어는 그 의미가 명확하지 않아 설비·장비 등 여러가지 의미로 해석될 수 있는바, 법 적용 시 혼란이 발생할 수 있음.

□ 개정안에 대해서 국정원 및 경찰청도 다음과 같은 이유로 신중한 검토가 필요하다는 입장임.

국정원: 신중검토 필요	경찰청: 신중검토 필요
개정안은 사이버공간을 ‘정보통신기반시설’로 지칭하고 있는데, ‘정보통신기반시설’이라는 용어는 시스템·시설 등 통신기반설비의 의미가 강하고 안보·국방 법률에 사용하기는 부적절하고, 「통합방위법」 개정으로 별도의 업무수행 체계가 시행될 경우, 「국가정보원법」 및 「국가사이버안전관리규정」 등에서 규정하고 있는 <u>現 국가사이버안보 수행체계와의 충돌</u> 이 발생할 수 있음.	現 정부는 「국가사이버안전관리규정」 및 「국가사이버 안보 전략」 등에 의하여 ‘국가안보실’이 컨트롤타워 역할을 수행하도록 개선하고 ‘국가사이버위기관리단’도 신설하였는바, 「통합방위법」상의 지역 중심 통합방위 대응은 현행 대응체계와 상충됨.

문 의 처
02)6788-5308

※ 참고자료

○ 국가사이버안보 기본계획 (p.17)

- 안보실은 국가 사이버안보 관련 업무 전반을 조율하고, 중장기 정책방향을 수립·검토하는 최상위 컨트롤타워 역할을 수행
- 국정원은 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보를 수집·작성·배포하고, 북한·외국 등의 안보침해행위에 대한 확인·견제·차단과 국민안전 보호 대응조치를 수행하며, 국가사이버안보센터 내에 국가사이버위기관리단을 설치하여 유관부처, 전문기관·기업 등과 실시간 위협정보 공유 및 사이버위기에 대비·대응
- 각 부처는 개별 법령에 근거하여 각 분야별 보안·보호 활동을 수행

○ 국가위기관리기본지침 (제95조)

사이버안보 위협에 대해 국가안보실은 총괄 조정·통제, 공공분야 국가정보원, 민간분야는 과학기술정보통신부, 국방분야 국방부가 주관기관이 된다.

○ 국가사이버안전관리규정 (제5조, 제18조)

제5조(국가사이버안전정책 및 관리) ① 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다.
② 국가정보원장은 제1항에 따른 총괄·조정 업무를 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관의 장과 협의하여 국가사이버안전기본계획을 수립·시행한다.
③ 국가정보원장은 제2항에 따른 국가사이버안전기본계획을 원활하게 추진하기 위하여 관계 기관에 예산 반영 등에 관한 협조를 요청할 수 있다.

제18조(안전성 확인 등에 대한 특례) ① 제9조, 제12조 및 제13조에도 불구하고 국방분야의 사이버안전과 관련한 다음 각호에 대하여는 국방부장관이 그 업무를 수행한다.

1. 제9조제4항의 규정에 의한 안전성 확인
2. 삭제
3. 제12조제1항의 규정에 의한 사고통보
4. 제13조제1항의 규정에 의한 사고조사

② 국방부장관은 제1항의 규정에 의한 업무를 수행함에 있어 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.