

「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법제기반 체계적 정비

Review of the New Government Action Plans on the
National Strategy for Cyber-Security

김한균

KICJ

「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법제기반 체계적 정비

연구책임자

김 한 균 한국형사·법무정책연구원 선임연구위원, 법학박사



목 차

국문요약 1

제1장

서론: 국정과제로서 사이버안보 법적 기반 체계적 구축 15

제1절 연구의 의의와 목적 17

- 1. 연구의 배경과 의의 17
- 2. 연구의 목적과 기대효과 19

제2절 연구의 구성과 방법 20

- 1. 연구의 구성체계 20
- 2. 연구의 방법 21

제2장

디지털 혁신 가속화에 따른 사이버안보 중요성과 정책문제 23

제1절 국가 사이버 안보 역량의 의미 25

- 1. 국가 사이버안보 역량의 국정과제로서의 중요성 25
- 2. 국가 사이버안보 역량 국정과제의 평가 27

제2절 국가 사이버 안보 역량강화 정책의 배경 28

- 1. 사이버범죄 발생 증가와 검거율 저하 28
- 2. 팬데믹 장기화로 인한 사이버안보 위험 심화 34
- 3. 북한의 국가기반시설 사이버공격 위협증가 34
- 4. 사이버안보 침해와 피해의 국제적 동향 36
- 5. 사이버범죄의 국가안보 문제화 37

제3장

국가 사이버안보 역량강화 정책의 발전 41

- 제1절 국가 사이버 안보 역량 강화 정책의 주요경과 43
 - 1. 2019년 국가사이버안보전략과 국가사이버안보기본계획 43
 - 2. 2017년 국가사이버안보법 정부법안 45
 - 3. 국제사회의 사이버안보 역량강화 의제 46
- 제2절 국내법제 변화와 사이버 안보 체제 정비 47
 - 1. 국내법제 개혁에 따른 사이버안보 체계 정비 47
 - 2. 국내법제 개혁에 따른 사이버범죄 수사체계 정비 48

제4장

사이버안보 체계와 제도 및 정책 정비 51

- 제1절 국정과제 이행과제와 사이버 안보 역량강화 전략 53
 - 1. 국정과제 목표와 기대효과 53
 - 2. 국정과제 주요내용별 10대 이행과제 54
- 제2절 국가사이버안보위원회 설치와 사이버안보 통제 체계 구축 55
 - 1. 대통령 직속 국가사이버안보위원회 55
 - 2. 사이버안보 국가 컨트롤 타워 57
- 제3절 사이버안보 유관기관 협력체계와 사이버안보 기본법제 58
 - 1. 사이버안보 유관기관 협력체계 58
 - 2. 국가사이버안보전략과 사이버안보 기본법제 60

제5장

경제안보와 국민안전을 위한 제도 및 정책 정비 65

- 제1절 사이버안보 민관 협력체계와 경제안보 67
 - 1. 경제안보와 사이버안보 67
 - 2. 사이버안보와 민관협력 68

제2절 디지털플랫폼 정부와 사이버안보 69

제3절 정보통신환경의 안전과 국민안전 71

제6장

사이버안보 기술 및 전문인력 확보를 위한 제도 및 정책 정비 73

제1절 사이버안보 기술역량의 고도화 75

제2절 사이버안보 전문인력 양성 76

제3절 사이버전 대비 강화 78

제7장

사이버안보 국제협력강화를 위한 제도 및 정책 정비 81

제1절 국가사이버안보 역량강화정책으로서 국제규범 수립 참여 83

1. 유럽평의회 사이버범죄 협약의 의미와 내용 83
2. 일본의 협약 가입 및 국내이행 사례 86
3. 한국의 협약 가입 필요성 86
4. 협약 가입을 위한 검토과제 87
5. 2022년 국회 협약 가입촉구 결의안 88
6. 유럽평의회 사이버범죄협약 선택의정서 가입검토 89
7. 유엔 차원의 정보통신기술의 범죄약용방지에 관한 국제조약
제정논의 참여 90

제2절 사이버안보 국제협력네트워크 강화 92

1. 유엔, 유럽연합 등 국제기구와 사이버안보 협력 네트워크 강화 92
2. 한·미 사이버범죄 공조 강화 93
3. 미국 CLOUD법 대응 93

제8장

결론: 국가사이버안보 역량강화의 법제 기반 정비과제 101

제1절 국가사이버안보 대응역량강화 국정과제 이행평가를 위한 지표 ...	103
1. 국정과제 이행 평가 지표의 의미	103
2. 국가 사이버안보 대응역량 강화과제 주요내용별 평가지표	104
제2절 국가사이버안보 대응역량강화 국정과제 이행을 위한 법제정비	
및 정책개발 과제	106
1. 세부과제 1: 대통령 직속 ‘국가사이버안보총괄’ 설치 및 컨트롤타워 운영체계를 갖춘다	106
2. 세부과제 2: 사이버안보 유관기관별 역할과 각급 기관간 협력 활성화 등을 규정한 법령 제정을 추진한다	107
3. 세부과제 3: 민관 합동 사이버협력체계 강화를 통해 핵심기술 보유기업·방산업체·국가기반시설 대상 위협과 공격 방지 및 대응조치를 적극 실행함으로써 경제 안보에 기여한다	107
4. 세부과제 4: 사이버공격으로부터 안전한 ‘디지털플랫폼’ 정부를 구현한다	107
5. 세부과제 5: 클라우드·스마트그리드 등 국민 생활에 밀접한 IT 환경의 안전성을 확보한다	108
6. 세부과제 6: 産·學·研·官 협력 아래 AI·양자통신 등 신기술 위협 대응 新기술 연구·개발을 적극 지원하여 사이버공격 탐지·차단·추적 시스템을 고도화한다	108
7. 세부과제 7: 사이버안보 국제공조 활성화 차원에서 국제사회의 사이버규범 수립에 적극 참여한다	109
8. 세부과제 8: 사이버위협에 맞서 글로벌 협력 네트워크를 확충한다 ...	110
9. 세부과제 9: 대학·특성화 교육 확대, 지역별 교육센터 설치 등 ‘10만 인재 양성’ 프로그램을 실행한다	110
10. 세부과제 10: ‘사이버 예비군’ 운영 등 사이버戰 인력을 확보한다 ...	111

참고문헌 113

Abstract 117

1. 서론

- 1.1. 새 정부는 “국가 사이버안보 대응역량 강화” (국정과제 101)를 국정과제의 하나로 제시함. 사이버안보가 별개의 독립된 국정과제로 선정된 경우는 최초임.
- 1.2. “국가 사이버안보 대응역량 강화” 국정과제의 목표는 전통적 국가안보 영역에서 경제안보·국민생활까지 확장 추세인 사이버안보 패러다임 구축 및 범정부 차원 협력체계 공고화, 사이버 방어체계 및 국제공조 시스템 강화를 통한 국가안보 및 사이버안전 환경 제공 등을 통해 사이버안보 기반 공고화로 제시됨.
- 1.3. 본 연구는 2022년 윤석열 정부 출범과 함께 중요 국정과제중 하나인 사이버안보 분야 정책 과제 이행 방향과 법제정비 필요성을 종합·분석하여 앞으로 추진해야 할 입법 및 정책과제와 국책연구기관의 연구지원 역할을 개괄적으로 제시함으로써 정부의 국정과제 이행에 선제적으로 기여하고자 기획됨.
- 1.4. 본 연구는 「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법제기반 체계적 정비를 위해 대처해야 할 문제점과 추진해야 할 과제를 분석, 제시함으로써, 특히 국가사이버안보 법제 도입논의에 선도적으로 기여할 뿐만 아니라, 정부의 국제사회 사이버규범 수립참여를 위한 연구자료를 지원하고자 함.

2. 디지털 혁신 가속화에 따른 사이버안보 중요성과 정책문제

- 2.1. 국가 사이버안보 역량이란 사이버공간의 급속한 발전과 사이버안보 위협의 증폭에 대응하여, 국민 안전과 국가 핵심 인프라 보호를 위해서, 국가전략적

2 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

차원에서 사이버공격 탐지·대응체계와 사이버범죄 방지·대응 법제를 비롯한 능동적인 대응 수단 확보를 목표로, 법제도·전문 인력·예산·민관협력·투자를 체계적으로 정비·구축·실행할 수 있는 총체적 국가역량을 뜻함.

2.2. 윤석열 정부의 국가사이버안보 관련 국정과제 체계

101. 국가 사이버안보 대응역량 강화	78. 세계 최고 네트워크 구축 및 디지털혁신 가속화	75. 초격차 전략기술 육성으로 과학기술 G5도약
<ul style="list-style-type: none"> ○ 전통적 국가안보 영역에서 경제안보·국민생활까지 확장 추세인 사이버안보 패러다임 구축 및 범정부 차원 협력체계 공고화, 사이버 방어체계 및 국제공조 시스템 강화를 통한 국가안보 및 사이버안전 환경 제공 등을 통해 사이버안보 기반 공고화 필요. ○ 윤석열 정부는 ‘국가사이버안보’ 설치 및 컨트롤타워 운영체계·기관별 역할 등을 규정한 법령 제정을 추진 ○ 윤석열 정부는 民官 합동 사이버협력체계 강화를 통해 국가반사설 대상 사이버공격으로부터 안전, ‘디지털플랫폼’ 정부 구현, 국민 생활에 밀접한 IT 환경의 안전성 확보를 추진 ○ 윤석열 정부는 産·學·研·官 협력아래 AI·양자통신 등 신기술위협 대응 기술개발 및 국제공조 활성화, 사이버위협에 대한 억지 역량 강화를 위해 국제사회의 사이버규범 수립에 적극 참여하고, 글로벌 협력 네트워크 확충을 추진 	<ul style="list-style-type: none"> ○ 5G·6G 네트워크 인프라를 고도화하고, 네트워크 안정성 및 사이버보안 대응력 확보로 튼튼하고 안전한 디지털 기반 강화 필요. ○ 윤석열 정부는 초연결 시대 디지털 안정성을 확보하고, 주요 안전관리의 디지털·지능화를 통해 국민 생활안전 강화 추진 ○ 윤석열 정부는 사이버보안 역량 강화를 위해 보안클러스터 모델의 확산과 10만 사이버보안 인재 양성을 추진. 	<ul style="list-style-type: none"> ○ 기술패권 경쟁시대, 글로벌 시장선도와 국익·안보 확보를 위해 필수적인 전략기술 육성에 국가적 역량을 결집함으로써 과학기술 5대 강국 도약 필요 ○ 윤석열 정부는 경제성장과 안보 차원에서 주도권 확보가 필수적인 전략기술(사이버보안)을 지정하여, 초격차 선도와 대체불가 기술확보를 목표로 집중 육성 추진. ○ 윤석열 정부는 초격차 R&D프로젝트에서 출연연을 전략기술 임무해결을 선도하는 핵심연구거점으로 지정하여 산학연과의 협동·융합연구 활성화 추진.

2.3. 새 정부는 사이버안보 분야 국가전략을 단지 사이버보안이나 범죄 분야의 방어적 현안에 한정 짓지 아니하고, 자유민주주의 가치와 지구촌 번영에 이바지하면서 국제사회에서 중추 역할을 담당하는 국가를 지향하는 국정목표 이행

과제의 하나로 자리매김하여, 사이버안보를 가치적 토대 위에 적극적 정책의 제로 설정하였다는 점에서 국가정책적으로 의미가 상당함.

2.4. '글로벌 중추국가' 역할 강화 과제와 관련하여 국제사회 평화안보·민주주의·인권·법치·비확산·기후변화·개발 분야 협력에 선도적 역할 수행하면서 규범 기반 국제질서 강화를 주도해 나가는 차원에서 사이버안보 분야의 규범기반 국제질서 정립 차원에까지 국정목표의 시야를 적극 확장했다는 점에서도 상당한 의미가 있음.

2.4. 국가 사이버 안보 역량강화 정책의 배경은 ①사이버범죄 발생 증가와 검거율 저하; ②팬데믹 장기화로 인한 사이버안보 위협 심화; ③북한의 국가기반시설 사이버공격 위협증가; ④사이버안보 침해와 피해의 국제적 동향; ⑤사이버범죄의 국가안보 문제화로 정리할 수 있음.

3. 국가 사이버안보 역량강화 정책의 발전

3.1. 2019년 「국가사이버안보전략」은 사이버위협을 안보위협으로 인식하여 모든 역량을 결집·대응할수 있도록 「국가안보전략」에 따라 수립된 최초의 전략임. 국가사이버안보전략은 사이버안보의 미래 비전과 목표를 제시하고 개인·기업·정부가 중점 추진해야 할 전략적 과제를 제시함.

3.2. 2019년 「국가사이버안보 기본계획」은 사이버위협 대응역량의 지속적 고도화, 국민들의 참여와 신뢰를 보장할 수 있는 사이버보안 문화 정착, 사이버안보를 위한 국제협력 내실화를 3대 기본과제로 제시함.

3.3. 2019년 수립된 국가사이버안보기본계획상 주요 과제중의 하나는 국가 사이버안보 역량 및 환경 변화 대응을 위한 법적기반 구축임.. 그러나 국가사이버안보의 기본법제 제정작업은 진전되지 못하고 있는 상태임.

4 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

- 3.4. 2015년 일본뿐만 아니라 2016년 중국도 국가전략과 국민안전 차원에서 사이버 안보기본법제를 갖추어 가고 있는데, 한국은 팬데믹 위기, 그리고 북한의 사이버 공격 위협에도 불구하고 여전히 논의 단계에 머물러 있음.
- 3.5. 사이버안보 국제환경 변화 요인 중 하나는 미국과 동맹국인 한국과 일본도 러시아와 중국, 북한 정부가 배후에 있는 사이버범죄조직의 공격 집중 대상이 되고 있다는 점임.
- 3.6. 국가전략적 차원에서 볼 때 사이버안보 시스템은 총괄적 통제기구가 부재한 상태이며, 공공 부문은 국가정보원, 민간 부문은 한국인터넷진흥원, 군은 사이버작전사령부 관할로 분장되어 있음.
- 3.7. 최근 팬데믹 상황에서 강조된 K-사이버 방역체계 구축 계획 역시 국가 사이버안보 거버넌스 정비 차원에서 이행될 필요가 있음.
- 3.8. 수사구조개혁에 따른 사이버범죄 분야 수사협력체계 정비 또한 중요한 정책현안임. 사이버범죄 대응과 수사를 담당하는 기관간 협력 네트워크와 정보보안사고 대응 체계와 더불어 사이버범죄 대응의 핵심체계를 구성하기 때문임.
- 3.9. 국가경쟁력의 중요한 부분으로서 사이버범죄 대응 관련 국가적 체계 정비는 국가정책적으로 중요한 문제라는 점을 고려한다면, 단순히 권력기관 개혁 차원에서 검경간의 갈등문제로 접근할 것이 아니라, 사이버범죄에 대응한 국가수사역량의 전략적인 목표와 효과를 종합적으로 고려한 사이버범죄 수사체계의 합리적 정비가 필요함.

4. 사이버안보 체계와 제도 및 정책 정비

4.1. 국가 사이버안보 대응역량 강화: 국정과제의 10대 세부과제

국정과제 주요내용	국정과제 세부과제
사이버안보 정책 체계 정비	세부과제 1 : 대통령 직속 '국가사이버안보총' 설치 및 컨트롤타워 운영체계를 갖춘다.
	세부과제 2 : 사이버안보 유관기관별 역할과 각급 기관간 협력 활성화 등을 규정한 법령 제정을 추진한다.
경제안보로서 사이버안보	세부과제 3 : 민간 합동 사이버협력체계 강화를 통해 핵심기술 보유기업·방산업체·국가기반시설 대상 위협과 공격 방지 및 대응조치를 적극 실행함으로써 경제 안보에 기여한다.
국민생활 안전	세부과제 4 : 사이버공격으로부터 안전한 '디지털플랫폼' 정부를 구현한다.
	세부과제 5 : 클라우드·스마트그리드 등 국민 생활에 밀접한 IT 환경의 안전성을 확보한다.
기술 고도화 및 국제협력 강화	세부과제 6 : 産·學·研·官 협력 아래 AI·양자통신 등 신기술 위협 대응 新 기술 연구·개발을 적극 지원하여 사이버공격 탐지·차단·추적 시스템을 고도화한다.
	세부과제 7 : 사이버안보 국제공조 활성화 차원에서 국제사회의 사이버규범 수립에 적극 참여한다.
	세부과제 8 : 사이버위협에 맞서 글로벌 협력 네트워크를 확충한다.
사이버 전문인력 양성	세부과제 9 : 대학·특성화 교육 확대, 지역별 교육센터 설치 등 '10만 인재양성' 프로그램을 실행한다.
	세부과제 10 : '사이버 예비군' 운영 등 사이버戰 인력을 확보한다.

4.2. 이제까지 국가 차원에서 범정부 역량을 집중할 수 있는 일원화된 사이버안보 공조체계 부재가 비판받아온 이유는 다수 정부 부처에 사이버안보 책임과 역할이 분산돼 명확한 사이버안보 거버넌스 체계를 확립하지 못했기 때문이다.

4.3. 사이버안보 정책시야가 북한에 한정되다 보니, 국제적인 사이버안보 규범 정립과 법 개정도 적극적이지 못했기 때문에 국가 사이버안보 정책에 대해서는 대통령실과 국가사이버안보위원회가 관장해야 함.

4.4. 위원회 형식이나 소속과 별개로, 사이버안보는 선택의 문제가 아닌 국가안보 및 국민안전에 직결된 필수적 과제라는 인식을 가지고 다양한 사이버 공격과 위협에 선제적이고 적극적으로 대응하기 위해서는 대통령 직속의 컨트롤타워

6 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

역할을 담당할 중심을 둘 필요가 있음.

- 4.5. 종래 기관에 역할과 권한을 부여하거나 기존 여러 기관에 분산되어 있는 기능을 통합해 조직을 신설하거나 컨트롤타워를 중심으로 한 체계정비는 필요함. 정보와 권한의 집중은 바람직스럽지 아니함은 물론이나, 이는 법적 제한조치가 기관간 견제구조를 통해 해소할 수 있는 문제이며, 권한과 기능은 분장되더라도 국가 사이버안보전략 차원에서 중장기적인 기획과 사안대응에서 통합조정 역할은 단일화되어야 하기 때문임.
- 4.6. 사이버안보의 국가전략적 접근에 있어서 체계적이고 효과적인 컨트롤타워 운영체계의 구축은 근거법과 제도 정비를 통해 이행해야 할 우선 과제이며, 종래 논의되었던 방안들과 제기되었던 사회적 의견들을 참고하여 행정부와 입법부가 책임성 있게 추진해야 할 것임.
- 4.7. 북한의 사이버위협과 주변국가들의 사이버보안전략 및 법제 시행, 4차산업혁명 기반인 사이버보안의 중요성을 고려할 때, 우리 정부도 사이버보안기본법제 논의를 신속히 마무리 짓고 제정과 후속작업에 노력해야 할 것임. 사이버공간의 법치국가적 규율과 국민안전 확보에 대한 국가적 책무를 다하기 위해서는 민관협력과 시민참여의 형식을 적극 수용할 필요가 있음.
- 4.8. 향후 국가사이버안보기본법제 제정추진에 있어서 특히 사이버공격에 대한 체계적 대응을 기획·조정할 컨트롤타워를 정하는 문제, 사이버공격 대응 책임기관, 지원기관, 수사기관의 권한과 직무 조정배분의 문제, 사이버위기대책협의 기구의 설치와 운영문제는 사이버범죄, 사이버보안침해사고, 사이버테러를 포괄하는 「국가 사이버안보 대응역량 강화」국정과제 차원에서 적극적으로 협의하여야 할 것임.

5. 경제안보와 국민안전을 위한 제도 및 정책 정비

- 5.1. 초연결성은 사이버공간의 형태와 민간기업 부문의 초국가적 영향력 확대의 양상으로 나타나고 있는 바, 사이버공격으로부터 국가기반시설과 민간기업 보호를 위해서는 현실 공간과 사이버공간, 민간부문과 정부의 협력이 필수적이다. 이는 사이버안보가 국가경제 안보의 차원에서도 핵심요소가 되었음을 의미함.
- 5.2. 2017년 정부법안에 따르면, 국가·지방자치단체 및 기업은 사이버안보가 국가안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하여 사이버공간을 보호하도록 노력하여야 한다(안 제3조 제2항)고 규정하여 민관 합동 사이버협력체계의 중요성을 확인함.
- 5.3. 디지털플랫폼 정부 구현에 있어서 사이버공격으로부터의 안전은 기본적 토대임. 물론 디지털플랫폼 정부 중점추진과제 중에 새로운 보안체계 구축도 포함되어 있어, 사이버보안체계 구축의 중요성도 더욱 높아지게 될 것임. 궁극적으로 디지털플랫폼 정부의 사이버안전 확보는 디지털플랫폼 정부에 대한 국민 신뢰 제고의 관건임.
- 5.4. 스마트그리드에 적용되고 있는 IT기술 중에 최근 주목받는 클라우드 컴퓨팅기술은 클라우드 제공자의 플랫폼을 이용하기 때문에 사이버 보안대책이 중요한 과제임. 스마트 그리드의 다양한 활용 가능성에도 불구하고 구조적 특징과 상호 운용성 표준의 부재로 인해 신뢰적인 인증이 보장되지 않으면, 네트워크의 신뢰성을 약화시키는 요인으로 작용하며, 보안 문제가 초래되기 때문임.

6. 사이버안보 기술 및 전문인력 확보를 위한 제도 및 정책 정비

- 6.1. 産·學·研·官 협력을 기반으로 사이버공격 탐지·차단·추적 시스템을 고도화하기 위해서는 민간부문과 정부 모두 정보보호 투자 확대를 통해 안전 확보가

8 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

우선되어야 한다는 인식을 갖추어야 하며, 인공지능 기반의 신기술 개발과 클라우드 서비스 전환 등 경쟁력 확보를 위해 민관협력이 뒷받침되어야 함.

6.2. 사이버보안 인재양성과 정부출연연구기관의 협동·융합연구 활성화 과제 외에 국정과제 추진과정에서 필요하고 가능한 범위에서 관련 정보는 국민에게 공개돼 사이버안보의 주체로서 인식하고 활동할 수 있도록 정책적 고려가 필요함. 이러한 국민인식 제고에 있어서 정부출연연구기관은 연구성과확산과 대국민 정보서비스의 역할도 담당할 수 있을 것임.

6.3. 사이버안보 관련 국내 정책추진과 국제협력과 규범체계 참여는 무엇보다도 국민의 자유와 인권보장을 명분으로 하는바, 오히려 국민 인권을 침해하거나 침해 우려를 낳지 않도록 사이버안보 대응 역량강화와 국민기본권 보장의 바람직한 균형점을 모색하기 위해서는 관련 정보의 공유와 국민참여를 통해 국민인식과 신뢰도를 개선하는 정책적 노력이 필요함.

6.4. 북한·러시아 등 주변 국가의 사이버전 능력 고도화와 전력 증강에 맞서 사이버전 역량을 강화하기 위해서는 전문인력 확보가 최우선 정책으로 추진되어야 할 것임.

7. 사이버안보 국제협력강화를 위한 제도 및 정책 정비

7.1. 사이버범죄에 대한 효율적인 국제공조 방안으로서 2001년 유럽 사이버범죄 방지 협약(Convention on Cybercrime)에는 2021년 현재 유럽 국가들을 비롯하여 전 세계 65개국이 비준하였는데, 우리나라는 가입추진단계에 있음.

7.2. 사이버범죄는 국경의 한계를 넘어 빠르게 확산될 수 있다는 특징이 있어 협약을 통한 국제공조의 필요성이 인정됨. 우리나라는 개별국가들과 형사사법공조 협약을 맺고는 있으나 자국의 이해관계가 큰 관련성이 없는 경우 타국 수사기

관의 적극적 공조가 쉽지 않고 많은 시간이 소요되는 것이 현실이므로 협약 가입이 필요함.

- 7.3. 협약은 통신데이터 또는 통신내용데이터의 실시간 수집 등을 의무화하고 있어 개인의 사생활 보호를 침해할 우려가 제기되고 있음.
- 7.4. 국내 정보자산을 다른 국가에서 접근할 수 있어 국가안보에 영향을 줄 수 있음. 그러나 협약상 통신데이터 또는 통신내용데이터의 실시간 수집 관련규정은 사이버범죄수사·소추·재판절차를 위한 조치로 한정하고 있어 개인정보 및 정보주권 침해가 일부의 우려만큼 크지는 않을 것임.
- 7.5. 협약에 따라 광범위하게 정보를 수집하고 제출명령에 응하기 위하여 인터넷서비스제공자의 정보저장시설 및 관리인력 증가로 경제적 부담이 초래될 수 있음. 그러나 협약으로 인하여 기업의 자료제출 의무를 법제화하면 자료제출로 발생할 수 있는 기업의 민형사상 책임이 면책될 수 있으며, 사이버수사 활성화로 인한 범죄 감소·예방으로 인터넷서비스제공자가 간접적으로 혜택을 받을 수도 있음.
- 7.6. 2001년 사이버범죄방지협약에 이어, 사이버공간상의 인종차별, 외국인혐오행위의 범죄화를 내용으로 하는 제1부가선택의정서에 이어, 클라우드소재 증거에 관한 제2부가선택의정서까지 갖추어지면 유럽평의회 사이버범죄방지협약은 사이버범죄에 관한 더욱 체계적인 국제기준이 될 것임.
- 7.7. 2019년 유엔 총회는 사이버범죄 분야의 새로운 국제규범으로서 정보통신기술의 범죄악용 방지에 관한 국제조약 (International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes) 제정을 위한 논의를 시작함.
- 7.8. 유엔의 새로운 조약 창설은 찬반논의와 서명비준 과정을 거쳐야 하는 것이나,

10 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

국제규범으로서의 중요성을 고려하건대, 그 제정 논쟁과 구체화 논의 과정을 면밀히 살피고 한국의 국익과 국제사회 지위를 고려한 일정한 관여 내지 참여가 필요함.

- 7.9. 유럽 사이버범죄방지협약과 달리 유엔 차원의 국제조약으로서 장차 사이버안보 분야 국제규범으로 자리잡을 가능성도 있으므로, 한국도 논의단계부터 적극적으로 참여함으로써 새로운 국제규범체계가 사이버범죄수사를 원활하게 함과 동시에 개인정보인권 보호와 균형을 맞추도록 선도적 역할을 맡아야 할 것임.
- 7.10. 유럽평의회 사이버범죄협약 체계부터 한미 사이버 안보 동맹에 이르기까지 국제 협력을 통한 외교적 전략적 사이버 안보 역량 강화, 사이버 공격에 대한 억지력 강화가 필요함.
- 7.11. 특히 유럽평의회 사이버범죄협약은 역대 정부에서 다양한 찬반논의와 후속과제에 대한 검토가 충분히 진행되어 왔으므로, 급변하는 세계적 사이버안보 정세를 고려해 가입을 더 이상 미루지 말고 적극 검토할 것이며, 이에 뒤따라 국내법 정비뿐만 아니라 유엔 차원의 규범체계 신설, 미국 등 주요동맹국과의 공조체계 강화를 위한 과제를 체계적으로 실행해 나가야 할 것임.
- 7.12. 한국 수사기관이 미국 등 외국 정보통신서비스제공자로부터 콘텐츠 데이터를 포함한 수사자료를 효과적으로 확보하기 위해서는 미국 정부와 행정협정을 체결하는 방안을 다각적으로 검토해 볼 필요가 있음.
- 7.13. 향후 미국과 CLOUD법상 행정협정을 체결하면 상호주의 원칙에 따라 한국 정보통신 기업이 보유 또는 관리하고 있는 데이터에 대해 미국이 직접 기업을 상대로 제공 요청을 할 수 있게 되므로 이에 따른 대비도 필요함.
- 7.14. 한국은 여전히 유럽평의회 사이버범죄협약 당사국도 아니고, 동 협약상 규정

의 국내적 이행과 관련하여 사이버범죄와 디지털 증거에 대한 실체법 및 절차법을 완비하지 못하고 있기 때문에, 현행 국제 기준에 맞는 실체법 및 절차법적 정비가 우선되어야 할 것임.

8. 결론: 국가사이버안보 역량강화의 법제 기반 정비과제

- 8.1. 국가 차원에서 범정부 역량을 집중할 수 있는 일원화된 사이버안보 컨트롤타워는 효율적인 사이버안보 거버넌스 체계에 필수적임. 국가 사이버안보 정책에 대해서는 대통령실과 국가사이버안보위원회가 관장할 필요있음.
- 8.2. 사이버안보의 국가전략적 접근에 있어서 체계적이고 효과적인 컨트롤타워 운영체계의 구축은 국가사이버안보 기본법 제정을 통해 이행해야 할 우선 과제다. 입법 과정에서 종래 논의되었던 방안들과 제기되었던 사회적 의견들을 참고하여 행정부와 입법부가 책임성 있게 추진해야 함.
- 8.3. 국가사이버안보 기본법제의 핵심내용과 쟁점은 사이버공격에 대한 유관기관 협력과 체계적 대응을 기획·조정할 컨트롤타워를 정하는 문제, 사이버공격 대응 책임기관, 지원기관, 수사기관의 권한과 직무 조정배분의 문제, 사이버위기대책협의기구, 그리고 민관 합동 사이버협력체계의 구성과 운영방식이 될 것임.
- 8.4. 국가 사이버안보는 궁극적으로 국민안전을 목표로하므로, 종래 “국가사이버안보법” 명칭에서 오는 불필요한 오해를 피하고, 민관협력의 중요성을 강조하는 측면에서 법명을 “국민사이버안전법” 내지 “국민사이버안전기본법”으로 칭하는 대안이 있음.
- 8.5. 2017년 정부 국가사이버안보법안의 예에 따라 국가·지방자치단체 및 기업은 사이버안보가 국가안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하

12 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

여 사이버공간을 보호하도록 노력하여야 한다는 원칙적 규정에 이어 구체적 협력체계 구축을 위한 규정을 두어야 할 것임.

- 8.6. 디지털플랫폼정부위원회는 디지털플랫폼정부 구현과 디지털 혁신 산업 기반 조성을 위한 민간·정부 간 협업과 민간 참여 활성화, 공무원 및 국민의 디지털 역량 강화, 그리고 특히 디지털플랫폼정부의 안전한 개인정보 활용 등 안전성·신뢰성 확보, 차별 없는 디지털플랫폼정부 서비스 제공을 위한 환경의 조성, 디지털플랫폼정부 구현에 관한 국민 공감대 형성과 활용 확산 정책에 특히 주력해야 함.
- 8.7. 2010년 스마트그리드 국가로드맵의 경우 스마트그리드 특별법 제정 계획을 포함하고 있었으며, 이처럼 정보통신 안전환경을 위한 특별법 제정 논의에서는 기반시설 보호뿐만 아니라 개인정보 보호규정도 균형있게 반영되어야 할 것임.
- 8.8. 사이버보안 인재양성과 정부출연연구기관의 협동·융합연구 활성화 과제 외에 국정과제 추진과정에서 필요하고 가능한 범위에서 관련 정보는 국민에게 공개돼 사이버안보의 주체로서 인식하고 활동할 수 있도록 정책적 고려가 필요함.
- 8.9. 사이버안보 대응 역량강화와 국민기본권 보장의 바람직한 균형점을 모색하기 위해서는 관련 정보의 공유와 국민참여를 통해 국민인식과 신뢰도를 개선하는 정책적 노력이 필요함. 이러한 국민신뢰도 제고정책을 위해서는 정부출연연구기관이 연구성과확산과 대국민정보서비스를 통해 역할을 담당할 수 있도록 지원이 필요함.
- 8.10. 사이버범죄 뿐만 아니라 사이버위협에 대한 실증자료는 효과적인 사이버안보 대응전략 기획과 추진에 기본자료가 되므로 사이버 안보관련 통계기반 구축도 연구개발 과제의 하나로 고려되어야 할 것임.

- 8.11. 유럽 사이버범죄협약은 이미 역대 정부에서 다양한 찬반논의와 후속과제에 대한 검토가 충분히 진행되어 왔고, 2022년 국회에서도 동 협약에 조속히 가입할 것을 정부에 촉구하는 결의안도 제안된 바 있음. 새 정부는 급변하는 세계적 사이버안보 정세를 고려해 가입을 더 이상 미루지 말고 적극 검토해야 함.
- 8.12. 유엔 정보통신기술의 범죄악용 방지에 관한 국제조약은 장차 사이버안보 분야 국제규범으로 자리잡을 가능성도 있으므로, 한국도 논의단계부터 적극적으로 참여함으로써 새로운 국제규범체계가 사이버범죄수사를 원활하게 함과 동시에 개인정보인권 보호와 균형을 맞추도록 선도적 역할을 맡아야 할 것임.
- 8.13. 2021년 구성된 한미 사이버 워킹그룹의 효과적 운영을 통해 미국과 협력체계를 사이버안보 글로벌 협력네트워크의 핵심축으로 삼아야 할 것임.
- 8.14. 국가 사이버안보 대응역량 강화를 위해서는 전략기술로서 사이버보안 기술 산학연 협동·융합연구 활성화가 필수적이며, 법무정책 분야 국책연구기관으로서 한국형사·법무정책연구원 또한 전략기술 개발의 법제기반 정비와 법정책 개발에 관한 핵심연구거점으로서의 역할을 담당할 수 있음.
- 8.15. 북한·러시아 등 주변 국가의 사이버전 능력 고도화와 전력 증강에 맞서 사이버전 역량을 강화하기 위해서 사이버 예비군의 필요성은 역대 정부가 검토해 온 과제임. 우선적 과제로서 외국 제도 사례를 비교연구하여 도입 가능성과 활용 방안을 연구할 필요가 있음.

제 1 장

「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법적 기반 체계적 정비

서론: 국정과제로서 사이버안보 법적 기반 체계적 구축

제1장

서론: 국정과제로서 사이버안보 법적 기반 체계적 구축

제1절 | 연구의 의의와 목적

1. 연구의 배경과 의의

2022년 1월 미국 정부는 최근 주요 시설에 대한 사이버공격의 증가에 따라 사이버 안보역량의 중요성을 인식하고, 사이버 대응강화 전략으로서 국가 안보 지침 8 (National Security Memorandum 8)를 발표했다.¹⁾

동 지침 “국가안보로서 사이버안보, 국방부 및 정보체계”(Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems)은 국가안보국(NSA)의 국가안보체계(National Security Systems) 안전보장관련 감독조정 권한을 확대하였다.²⁾ 즉 국가안보국은 국가안보체계를 구성하는 모든 기관에 대하여 사이버안보 위협과 취약성에 대해 구속력 있는 조치를 부과할 수 있도록 하였다. 국가안보체계내 모든 기관은 사이버안보 위협 의심 사안, 특정 사이버안보 위협사안에 대한 대응조치 및 영향평가에 대해 국가안보국에 보고해야 한다. 또한 동 지침은 정보통신 민간기업이 확보한 사이버안보 침해 사안 정보를 정부와 공유할 수 있도록 체계를 구축하였다.

1) “President Biden Signs Cybersecurity National Security Memorandum” (<https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/> 2022년 8월 15일 최종검색)

2) Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (<https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/> 2022년 8월 15일 최종검색)

뿐만 아니라 2022년 7월 미국은 ‘반도체와 과학법(Chips and Science Act)’을 제정했다.³⁾ 동법은 첨단 산업 기술경쟁력 우위 확보를 위한 기술 개발 집중 투자를 목적으로 하며, 그 10대 핵심 기술에는 사이버보안도 포함된다. 동법의 제정은 강대국 기술 패권 경쟁이 치열해지면서, 국가 경쟁력이 첨단 산업 경쟁력에 좌우된다는 의미다.⁴⁾ 사이버 안보의 기술적 기반을 구축하기 위한 법제가 국가전략적 차원에서 정비되고 있는 최근 사례다.

한편, 2022년 5월 한미 정상회담에서는 사이버보안과 사이버범죄가 특히 강조되었다.⁵⁾ 양국이 사이버보안을 국가안보 차원에서 접근해야 한다는 인식을 같이 한 만큼 사이버안보 정책 이행은 더욱 강조될 것이다. 이를 뒷받침하는 상황이 바로 우크라이나 전쟁 사태다. 2022년 3월부터 8월 현재까지 사이버위기관보가 3단계(주의) 상태가 지속되고 있다. 현대 전쟁이 사이버 전쟁이 병행되는 ‘하이브리드 전쟁’ 양상으로 전개되면서 국가안보에 영향을 미칠 수 있기 때문이다.⁶⁾

또한 한미 양국 뿐만 아니라 국제사회에서 사이버위협으로 북한이 지목되는 경우가 더욱 빈발하고 있다. 코로나19 팬데믹 사태가 장기화되면서, 비대면·재택·원격 근무가 확산되고 이로 인해 사이버보안이 취약해진 상황을 북한이 악용하고 있는 것이다. 북한은 해커를 양성하고 관리하면서 외국까지 진출해 연 1조 원에 달하는 “사이버 외화벌이”를 하고 있다는 분석도 있다. 그러나 우리 정부는 사이버안보 분야 기본법제가 갖추어져 있지 않아서 범정부 차원의 컨트롤타워 구성이나 민관 사이버안보 협력도 한계가 있는 형편이다.⁷⁾

3) FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China (<https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/> 2022년 8월 15일 최종검색)

4) 10대 핵심기술은 인공지능, 고성능컴퓨팅 및 반도체, 양자 정보 과학, 로보틱스 및 첨단 제조업, 자연재해 예방 및 대비, 첨단 통신, 바이오기술 및 합성생물학, 데이터 및 사이버보안, 첨단 에너지(배터리, 원자력), 첨단 소재를 말한다. 경희건, 미국 ‘반도체와 과학법’의 정책적 시사점, 산업경제이슈 144호, 산업연구원, 2022, 2면.

5) “윤석열 대통령과 바이든 대통령은 사이버 적대세력 억지, 핵심 기반 시설의 사이버보안, 사이버 범죄 및 이와 관련한 자금세탁 대응, 가상화폐 및 블록체인 애플리케이션 보호, 역량 강화, 사이버 훈련, 정보 공유, 군 당국 간 사이버 협력 및 사이버 공간에서의 여타 국제안보 현안에 관한 협력을 포함하여, 지역 및 국제 사이버 정책에 관한 한미 간 협력을 지속 심화시켜 나가기로 했다.”(2022년 5월 21일 한-미 정상 공동성명)

6) <https://www.ddaily.co.kr/news/article/?no=238507>(2022년 8월 15일 최종검색)

7) <https://www.donga.com/news/article/all/20220811/114924535/1>(2022년 8월 15일 최종검색)

이런 상황에서 새 정부는 “국가 사이버안보 대응역량 강화” (국정과제 101)를 국정과제의 하나로 제시하였다. 사이버안보가 별개의 독립된 국정과제로 선정된 경우는 이번이 처음이다.

그런 만큼 “국가 사이버안보 대응역량 강화” 국정과제의 중요성은 한층 강조될 필요가 있으며, 전통적 국가안보 영역에서 경제안보·국민생활까지 확장 추세인 사이버안보 패러다임 구축 및 범정부 차원 협력체계 공고화, 사이버 방어체계 및 국제공조 시스템 강화를 통한 국가안보 및 사이버안전 환경 제공 등을 통해 사이버안보 기반 공고화가 목표로 제시된다.⁸⁾

이와 함께 새 정부는 국가사이버안보위원회 설치 및 컨트롤타워 운영체계·기관별 역할 등을 규정한 법령 제정부터 민관 합동 사이버협력체계 강화를 통한 국가기반시설 대상 사이버공격 방어, ‘디지털플랫폼’ 정부 구현, 국민 생활에 밀접한 사이버환경 안전성 확보 추진에 이르기까지 국가 사이버안보 대응역량을 폭넓게 이해하고 그에 상응한 추진전략과 과제를 설정하였다. 특히 사이버위협에 대한 억지 역량 강화를 위해 국제사회의 사이버규범 수립에 적극 참여하고, 글로벌 협력 네트워크 확충을 추진하는 내용도 국정과제에 포함시켰다.⁹⁾

2. 연구의 목적과 기대효과

따라서 본 연구는 2022년 윤석열 정부 출범과 함께 중요 국정과제중 하나인 사이버안보 분야 정책 과제 이행 방향과 법제정비 필요성을 종합·분석하여 앞으로 추진해야 할 입법 및 정책과제와 국책연구기관의 연구지원 역할을 개괄적으로 제시함으로써 정부의 국정과제 이행에 선제적으로 기여하고자 기획되었다.

“국가 사이버안보 대응역량 강화” (국정과제 101)는 본 국정과제 이행노력을 통해 범국가 사이버안보 역량을 결집하고 글로벌 사이버위협 신속 대응 및 예방체계 구축을 목표로 한다. 튼튼한 사이버안보 초석 아래 ‘더 안전한 대한민국’과 ‘첨단 IT 환경’이 조성될 수 있다는 것이다..¹⁰⁾

8) 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022년 5월, 170면.

9) 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022년 5월, 170면.

10) 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022년 5월, 170면.

20 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

본 연구는 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비를 위해 대처해야 할 문제점과 추진해야 할 과제를 분석, 제시함으로써, 특히 국가사이버안보 법제 도입논의에 선도적으로 기여할 뿐만 아니라, 우리 정부의 국제 사회 사이버규범 수립참여를 위한 연구자료를 지원하고자 한다.

나아가 한국형사·법무정책연구원의 사이버안보 법제분야 연구지원 핵심거점으로 서 역할을 다시 한번 정립함으로써, 향후 사이버안보분야 산-학-관 협력 연구사업에 도 적극 참여하고자 한다.

제2절 | 연구의 구성과 방법

1. 연구의 구성체계

본 연구의 목적은 국정과제로서 사이버안보 법적 기반 체계적 구축이다. 이를 위해서 제2장에서는 디지털 혁신 가속화에 따른 사이버안보 중요성과 정책문제를 설명한다. 즉 국가 사이버 안보 역량의 의와 국가 사이버 안보 역량강화 정책의 배경을 분석한다. 제3장에서는 국가 사이버 안보 역량 강화 정책의 주요경과를 정리하고, 국내법제 변화와 사이버 안보 체제 및 사이버범죄 수사체계 정비를 분석한다.

본문에 해당하는 제4장부터 제7장까지는 국정과제 「국가 사이버안보 대응역량 강화」의 주요내용을 분석, 재구성한 10대 세부과제별 정책현안과 과제를 논의한다.

제4장에서는 사이버안보 체계와 제도 및 정책 정비, 제5장에서는 제5장 경제안보와 국민안전을 위한 제도 및 정책 정비, 제6장에서는 사이버안보 기술 및 전문인력 확보를 위한 제도 및 정책 정비, 제7장에서는 사이버안보 국제협력강화를 위한 제도 및 정책 정비에 관하여 분석한다.

결론적으로 국가사이버안보 역량강화의 법제 기반 정비과제로서, 국가사이버안보 대응역량강화 국정과제 이행평가 지표, 국가사이버안보 대응역량강화 국정과제 이행을 위한 법제정비 및 정책개발 과제, 국정과제 핵심연구거점으로서 한국형사법무정책 연구원에 관하여 정책분석과 제안을 제시한다.

2. 연구의 방법

본 연구는 한국형사·법무정책연구원의 수사개발 정책연구과제로서 국가 사이버안보 역량 관련 사이버보안 및 사이버범죄 분야 국내외 주요 정책보고서, 연구논문 및 정책동향 문건들을 정리하고 분석한다.

특히 2022년 8월 1일, 「국가사이버안보 대응역량 강화 법정정책적 과제」를 주제로 국립외교원과 정책세미나를 공동개최하였다.¹¹⁾ 이는 새 정부 출범과 함께 주요 국정과제인 사이버안보 분야 제도 정비 및 정책 추진 과제를 논의하기 위해 기획되었다. 법무부, 외교부, 국가정보원, 대검찰청, 국가보안기술연구소 등 유관기관 정책 전문가들이 참가하여, 사이버안보 역량강화를 위한 국정과제 이행전략, 외교 분야 사이버안보 역량강화 전략, 사이버안보의 국제규범 발전 동향, 국가보안 분야 사이버 안보 위협대응 및 억지 분야 사이버안보 대응역량강화 방안 네 가지 주제의 발제와 법무부 국제형사과, 외교부 국제안보과, 대검찰청 사이버수사과, 국가정보원 사이버안보정책과가 참여한 토론을 통해, 국가사이버안보 대응역량 강화를 위한 국정과제 추진에 있어서 정부 유관부처간, 국책연구기관간 협업과 정책연구기반 조성의 필요성을 확인하였다.

11) [https://www.kicj.re.kr/gallery.es?mid=a10303000000&bid=0001\(2022년 8월 15일 최종검색\)](https://www.kicj.re.kr/gallery.es?mid=a10303000000&bid=0001(2022년 8월 15일 최종검색))

제 2 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

디지털 혁신 가속화에 따른 사이버안보 중요성과 정책문제

제2장

디지털 혁신 가속화에 따른 사이버안보 중요성과 정책문제

제1절 | 국가 사이버 안보 역량의 의미

1. 국가 사이버안보 역량의 국정과제로서의 중요성

가. 국가 사이버안보 역량의 개념

2017년 국가사이버안보법 정부법안 제2조 제4호는 “사이버안보”란 사이버공격으로부터 사이버공간을 보호함으로써 사이버공간의 기능을 정상적으로 유지하거나 정보의 안전성을 유지하여 국가의 안전을 보장하고 국민의 이익을 보호하는 것을 말한다 고 규정한다.

2020년 제정된 사이버안보 업무규정은 사이버안보에 관한 별도의 개념정의 규정을 두지는 아니하였으나, 제3조 제1항에서 국가정보원의 “사이버안보 업무”를 다음과 같이 규정한다.

첫째, 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포 업무 (사이버정보업무),

둘째, 중앙행정기관을 대상으로 하는 사이버 공격·위협에 대한 예방 및 대응 업무 (사이버공격예방·대응업무)가 그것이다. 즉 사이버안보는 사이버정보와 사이버공격 예방 및 대응이다.

이러한 법령상 개념은 사이버안보의 목적을 국가안전 보장과 국민 이익 보호로 설정하고, 대응의 대상을 사이버공격으로, 보호의 대상을 사이버공간으로 각각 규정한다. 사이버안보의 내용은 사이버공간의 정상적 기능과 정보의 안전성 유지다. 하지

26 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

만 국가 사이버안보 역량은 법적 개념보다 더 포괄적이고 전략적으로 규정될 필요가 있다.

즉 **국가 사이버안보 역량**이란 사이버공간의 급속한 발전과 사이버안보(cyber-security) 위협의 증폭에 대응하여, 국민 안전과 국가 핵심 인프라 보호를 위해서, 국가전략적 차원에서 사이버공격 탐지·대응체계와 사이버범죄 방지·대응 법제를 비롯한 능동적인 대응 수단 확보를 목표로, 법제도·전문 인력·예산·민관협력·투자를 체계적으로 정비·구축·실행할 수 있는 총체적 국가역량을 뜻한다.

나. 국정목표와 사이버안보 관련 국정과제

2022년 윤석열 정부 120대 국정과제 중 다섯 번째 국정목표는 “자유, 평화, 번영에 기여하는 글로벌 중추국가”다. 이는 국익·실용의 외교전략과 튼튼한 국방역량으로, 영향을 받는 국가에서 영향력을 행사하는 글로벌 중추국가로의 도약을 목표로 한다는 의미다.¹²⁾

이러한 목표의 구체적 내용 중 하나는 자유민주주의 가치를 지키고, 지구촌 번영에 기여함인데, 이와 관련하여 「**국가 사이버안보 대응역량 강화**」가 주요 국정과제로 제시된다. (국정과제 101)

뿐만 아니라, 국가적 차원의 사이버안보 종합역량 강화와 관련하여 「**세계 최고 네트워크 구축 및 디지털혁신 가속화**」(국정과제 78), 「**초격차 전략기술 육성으로 과학 기술 G5 도약**」(국정과제 75) 또한 포괄적으로 살펴볼 필요가 있겠다.

12) 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022년 5월, 17면.

[윤석열 정부의 국가사이버안보 관련 국정과제 체계]

101. 국가 사이버안보 대응역량 강화	78. 세계 최고 네트워크 구축 및 디지털혁신 가속화	75. 초격차 전략기술 육성으로 과학기술 G5도약
<ul style="list-style-type: none"> ○ 전통적 국가안보 영역에서 경제안보·국민생활까지 확장 추세인 사이버안보 패러다임 구축 및 범정부 차원 협력체계 공고화, 사이버 방어체계 및 국제공조 시스템 강화를 통한 국가안보 및 사이버안전 환경 제공 등을 통해 사이버안보 기반 공고화 필요. ○ 윤석열 정부는 ‘국가사이버안보촉’ 설치 및 컨트롤타워 운영체계·기관별 역할 등을 규정한 법령 제정을 추진 ○ 윤석열 정부는 민·官 합동 사이버협력체계 강화를 통해 국가 기반시설 대상 사이버공격으로부터 안전, ‘디지털플랫폼’ 정부 구현, 국민 생활에 밀접한 IT 환경의 안전성 확보를 추진 ○ 윤석열 정부는 産·學·研·官 협력아래 AI·양자통신 등 신기술 위협 대응 기술개발 및 국제공조 활성화, 사이버위험에 대한 억지 역량 강화를 위해 국제사회의 사이버규범 수립에 적극 참여하고, 글로벌 협력 네트워크 확충을 추진 	<ul style="list-style-type: none"> ○ 5G·6G 네트워크 인프라를 고도화하고, 네트워크 안정성 및 사이버보안 대응력 확보로 튼튼하고 안전한 디지털 기반 강화 필요. ○ 윤석열 정부는 초연결 시대 디지털 안정성을 확보하고, 주요 안전관리의 디지털·지능화를 통해 국민 생활안전 강화 추진 ○ 윤석열 정부는 사이버보안 역량 강화를 위해 보안클러스터 모델의 확산과 10만 사이버보안 인재 양성을 추진. 	<ul style="list-style-type: none"> ○ 기술패권 경쟁시대, 글로벌 시장선도와 국익·안보 확보를 위해 필수적인 전략기술 육성에 국가적 역량을 결집함으로써 과학기술 5대 강국 도약 필요 ○ 윤석열 정부는 경제성장과 안보 차원에서 주도권 확보가 필수적인 <u>전략기술(사이버보안)</u>을 지정하여, 초격차 선도 및 대체불가 기술확보를 목표로 집중 육성 추진. ○ 윤석열 정부는 초격차 R&D 프로젝트에서 <u>출연연을 전략기술 임무해결을 선도하는 핵심연구거점</u>으로 지정하여 산학연과의 협동·융합 연구 활성화 추진.

2. 국가 사이버안보 역량 국정과제의 평가

새 정부는 사이버안보 분야 국가전략을 단지 사이버보안이나 범죄 분야의 방어적 현안에 한정 짓지 아니하고, 자유민주주의 가치와 지구촌 번영에 이바지하면서 국제사회에서 중추 역할을 담당하는 국가를 지향하는 국정목표 이행과제의 하나로 자리매김하였다. 즉 사이버안보를 가치적 토대 위에 적극적 정책의제로 설정하였다는 점에서 국가정책적으로 의미가 상당하다.

뿐만 아니라 ‘글로벌 중추국가’ 역할 강화 과제와 관련하여 국제사회 평화안보·민

주주의·인권·법치·비확산·기후변화·개발 분야 협력에 선도적 역할 수행하면서 규범 기반 국제질서 강화를 주도 (국정과제 99: 국격에 걸맞은 글로벌 중추국가 역할 강화) 해 나가는 차원에서 사이버안보 분야의 규범기반 국제질서 정립 차원에까지 국정목표의 시야를 적극 확장했다는 점에서도 상당한 의미가 있다고 평가할 수 있다.

제2절 | 국가 사이버 안보 역량강화 정책의 배경

1. 사이버범죄 발생 증가와 검거율 저하

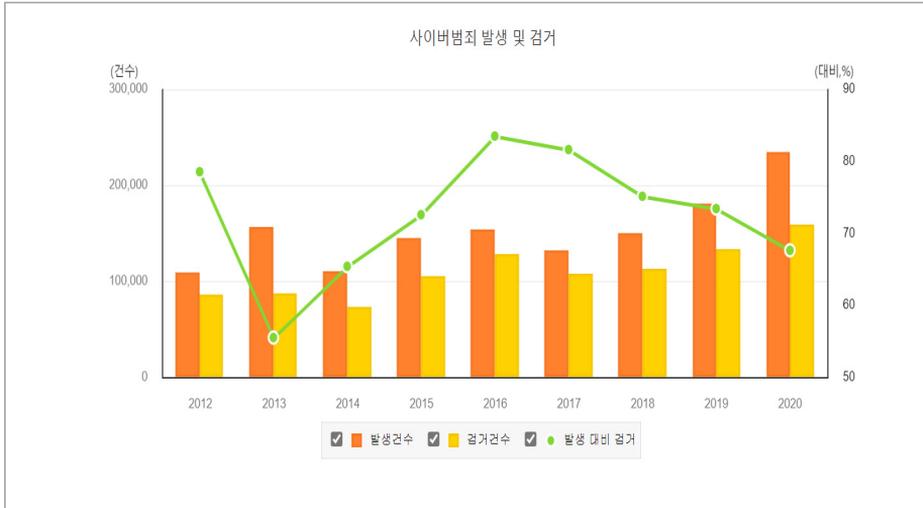
가. 사이버범죄의 통계적 현실

최근¹³⁾ 사이버범죄 발생 및 검거현황¹⁴⁾에 따르면, 사이버범죄는 계속 증가 추세에 있는데 비해, 최근 사이버범죄발생대비 검거율은 오히려 감소하고 있다. 사이버범죄 통계상 정보통신망이용범죄에 포함된 사이버 사기범죄의 비중이 가장 크다. 특히 사이버범죄는 첨단과학기술의 발전에 따라 관련 범죄 양상 또한 새로운 형태와 수법으로 변화하는 양상을 보이고 있다.

13) 2022년 8월 현재까지 경찰청 사이버범죄 통계자료와 e-나라지표상 사이버범죄 발생 및 검거 통계자료로 가장 최신 자료는 2021년 9월 발표된 2020년도까지의 통계로 한정된다.

14) 경찰청 사이버수사국 사이버수사기획과 사이버범죄 통계자료 2011-2020.

▶▶ [표 2-1] 사이버범죄 발생 및 검거율(2011~2020)



(단위: 건, %)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
발생건수	116,961	108,223	155,366	110,109	114,679	153,075	131,734	149,604	180,499	234,098
검거건수	91,496	84,932	86,105	71,950	104,888	127,758	107,489	112,133	132,559	157,909
발생 대비 검거율	78.2	78.5	55.4	65.3	72.5	83.5	81.6	75.0	73.4	67.5

나. 해킹범죄의 증가

정보통신망침해범죄의 증가 양상¹⁵⁾과 관련해서는, 정보통신망침해범죄(해킹, 서버 스거부공격, 악성프로그램) 유형 중에서 특히 해킹범죄가 지속적으로 증가하고 있다.

15) 경찰청 사이버범죄 통계자료 2014-2020

30 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

▶▶▶ [표 2-2] 정보통신망침해범죄 유형별 발생 및 검거건수(2014~2020)

(단위: 건)

구분		총계	해킹	서비스거부공격	악성프로그램	기타
2014	발생	2,291	1,648	26	130	487
	검거	846	540	16	69	221
2015	발생	3,154	2,247	40	166	701
	검거	842	524	19	74	225
2016	발생	2,770	1,847	192	137	594
	검거	1,047	537	164	98	248
2017	발생	3,156	2,430	43	167	516
	검거	1,398	990	28	122	258
2018	발생	2,888	2,178	20	119	571
	검거	902	584	14	50	254
2019	발생	3,638	2,664	35	270	669
	검거	1,007	556	14	189	248
2020	발생	4,344	3,176	25	169	974
	검거	911	548	10	81	272

또한, 정보통신망이용범죄의 증가¹⁶⁾ 양상과 관련해서 정보통신망이용범죄(사이버 사기, 사이버금융범죄, 개인위치정보침해, 사이버저작권침해) 유형 중 가장 많은 사이버 사기범죄는 범죄발생건수가 증가하는데 따라 검거율도 높아지고 있다. 반면 사이버금융범죄의 경우 높은 증가율에도 불구하고 검거율이 낮은 수준이다.

16) 경찰청 사이버범죄 통계자료 2014-2020

▶▶ [표 2-3] 정보통신망이용범죄 유형별 발생 및 검거건수(2014~2020)

(단위: 건)

구분	총계	사이버사기	사이버 금융범죄	개인위치 정보침해	사이버 저작권침해	기타	
2014	발생	88,519	56,667	15,596	939	14,168	2,149
	검거	56,461	40,657	6,567	635	7,198	1,404
2015	발생	118,362	81,849	14,686	609	18,770	2,448
	검거	86,658	68,444	7,886	296	8,832	1,200
2016	발생	121,867	100,369	6,721	2,410	9,796	2,571
	검거	103,271	89,364	4,034	2,125	5,616	2,033
2017	발생	107,271	92,636	6,066	413	6,667	1,489
	검거	88,779	80,740	2,632	298	4,134	975
2018	발생	123,677	112,000	5,621	246	3,856	1,954
	검거	93,926	87,714	2,353	142	2,467	1,250
2019	발생	151,916	136,074	10,542	179	2,562	2,559
	검거	112,398	105,651	3,387	78	1,772	1,510
2020	발생	199,594	174,328	20,248	241	2,183	2,594
	검거	134,696	127,233	4,621	95	1,493	1,254

특히 최근 한국 사회의 주요 현안 중 하나인 불법콘텐츠범죄의 증가¹⁷⁾ 동향과 관련해서 불법콘텐츠 범죄 유형인 사이버음란물(성착취물), 사이버도박, 사이버 명예훼손, 사이버스토킹 중에서 사이버성착취물과 사이버스토킹 범죄는 사이버범죄로서 뿐만 아니라 그 범죄양상과 범죄피해 현실에 비추어 가장 심각하고 정책적 노력이 요청되는 문제다.

무엇보다도 사이버성착취범죄는 디지털성범죄로서 국가대응전략¹⁸⁾의 중요한 현안이기도 하다. 디지털 성폭력은 디지털 기기 및 정보통신기술을 매개로 온·오프라인상에서 발생하는 젠더기반폭력을 폭넓게 지칭하며, 불법촬영, 비동의유포, 유포협박, 불법 합성(딥페이크) 등이 현행법상 성폭력범죄로서 처벌대상이 된다. 디지털 성폭력의 다양한 양상들은 점차 법률 제정과 개정을 통해 점차 성범죄로 규정되고 있다.¹⁹⁾

17) 경찰청 사이버범죄 통계자료 2014-2020

18) 관계부처 합동, 디지털 성범죄 근절대책, 2020

19)

성폭력처벌법

통신매체이용음란

- 2010년 4월 제정-제12조 2년이하 징역/500만원이하 벌금
- 2012년 12월 전부개정-제13조

32 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

		· 2020년 5월 일부개정-2년이하 징역/2천만원이하 벌금
카메라이용 불법촬영 등	불법촬영물 반포·판매·임대·공연전시·상영	· 2010년 4월 제정-제13조 1항 5년이하 징역/1천만원이하 벌금 · 2012년 12월 전부개정-제14조 1항 · 2018년 12월 일부개정- 5년이하 징역/3천만원이하 벌금
	의사에 반한 사후 반포·판매·임대·공연전시·상영	· 2012년 12월 전부개정-제14조 2항 신설 3년이하 징역/500만원이하 벌금 · 2018년 12월 일부개정- 5년이하 징역/3천만원이하 벌금 · 2020년 5월 일부개정-촬영 당시에는 촬영대상자의 의사에 반하지 아니한 경우에 자신의 신체를 직접 촬영한 경우를 포함.
	영리목적 정보통신망이용 유포	· 2010년 4월 제정-제13조 2항 7년이하 징역/3천만원이하 벌금 · 2012년 12월 전부개정-제14조 3항 · 2018년 12월 일부개정- 3년이상 징역
	불법촬영물 소지·구입·저장·시청	· 2020년 5월 일부개정- 제14조 4항신설 3년이하 징역/3천만원이하 벌금
	상습 불법촬영물범죄	· 2020년 5월 일부개정- 제1조 5항신설 2분의 1 가중
	미수범	· 제15조
허위영상물 반포 등	반포목적 편집·합성·가공	· 2020년 3월 일부개정-제14조의 2 1항 신설 5년이하 징역/5천만원이하 벌금
	편집물·합성물·가공물 반포	· 2020년 3월 일부개정-제14조의 2 2항 신설 5년이하 징역/5천만원이하 벌금
	영리목적 정보통신망이용 허위영상물 반포	· 2020년 3월 일부개정-제14조의 2 3항 신설 7년이하 징역
	상습 허위영상물범죄	· 2020년 5월 일부개정-제14조의 2 4항 신설 2분의 1가중
		미수범
불법촬영물 이용협박	촬영물이용협박	· 2020년 5월 일부개정-제14조의 3 1항 신설 1년이상 징역
	촬영물이용권리행사방해	· 2020년 5월 일부개정-제14조의 3 2항 신설 3년이상 징역
	상습 촬영물이용협박범죄	· 2020년 5월 일부개정-제14조의 3 3항 신설 2분의 1가중
		미수범
청소년성보호법		
아동 청소년 성착취물 제작배포 등	제작·수입·수출	· 2000년 2월 제정 제8조 (청소년이용음란물의 제작·배포등) 1항-5년이상 징역 · 2012년 12월 전부개정 제11조 1항 · 2020년 6월 일부개정 제11조(아동·청소년성착취물의 제작·배포등) 1항-무기 또는 5년이상징역
	상습제작·수입·수출	· 2020년 6월 일부개정 신설 제11조 7항-2분의1 가중
	제작·수입·수출 미수	· 2000년 2월 제정 제11조 4항 · 2012년 12월 전부개정 제11조 6항
	영리목적 판매·대여·배포·소지·운반·공연전시·상영	· 2000년 2월 제정 제8조 2항-7년이하 징역 · 2012년 12월 전부개정 제11조 2항-10년이하 징역 · 2020년 6월 일부개정 제11조 2항-5년이상 징역
	배포·공연전시·상영	· 2005년 12월 일부개정 신설 제8조3항-3년이하 징역 2천만원이하 벌금 · 2012년 12월 전부개정 제11조 3항-7년이하 징역 5천만원 이하 벌금 · 2020년 6월 일부개정 제11조 3항-3년이상 징역

불법콘텐츠범죄 유형 중 사이버음란물 범주는 감소에서 증가추세로 변화하였으나, 검거율은 매우 높게 나타나고 있다.

▶▶ [표 2-4] 불법콘텐츠범죄 유형별 발생 및 검거건수 (2014~2020)

(단위: 건)

구분		총계	사이버 음란물	사이버도박	사이버 명예 훼손·모욕	사이버 스토킹	기타
2014	발생	18,299	4,354	4,271	8,880	363	431
	검거	14,643	3,739	4,047	6,241	300	316
2015	발생	23,163	4,244	3,352	15,043	134	390
	검거	17,388	3,475	3,365	10,202	124	222
2016	발생	28,438	3,777	9,538	14,908	56	159
	검거	23,539	3,435	9,394	10,539	53	118
2017	발생	21,307	2,646	5,130	13,348	59	124
	검거	17,312	2,329	5,080	9,756	52	95
2018	발생	23,039	3,833	3,012	15,926	60	208
	검거	17,305	3,282	2,947	10,889	50	137
2019	발생	24,945	2,690	5,346	16,633	25	251
	검거	19,154	2,164	5,162	11,632	20	176
2020	발생	30,160	4,831	5,692	19,388	45	204
	검거	22,302	4,063	5,436	12,638	39	126

	배포목적 광고·소개	· 2020년 6월 일부개정 추가 제11조 3항-3년이상 징역
	제작알선	· 2000년 2월 제정 제8조 3항-1년이상 10년이하 징역 · 2007년 8월 일부개정 제8조 5항 · 2011년 9월 일부개정 제8조 6항 · 2012년 12월 전부개정 제11조 4항-3년이상 징역
	소지	· 2007년 8월 일부개정 신설 제8조 4항-2천만원이하 벌금 · 2012년 12월 전부개정 제11조 5항-1년이하 징역 2천만원이하 벌금
	구입·소지·시청	· 2020년 6월 일부개정 제11조 5항-1년이상 징역
정보통신망 이용아동성 착취대화	성적착취목적 정보통신망이용 성적 욕망·수치심·혐오감 유발대화·유인	· 2021년 3월 일부개정 제15조의2 1항 신설-3년이하 징역 3천만원이하 벌금
	16세미만대상 정보통신망이용 성적 욕망·수치심·혐오감 유발대화·유인	· 2021년 3월 일부개정 제15조의2 2항 신설-3년이하 징역 3천만원이하 벌금

2. 팬데믹 장기화로 인한 사이버안보 위협 심화

2020년 COVID-19 상황이 지속되면서 지능형 악성코드의 형태가 날로 심각해지고 있으며, 사이버안보 관련 주요 문제가 될 것으로 예상된다. 즉 COVID-19 팬데믹과 유사한 ‘사이버 팬데믹’ 가능성까지 제기되고 있는 상황이다.²⁰⁾

코로나 바이러스와 악성코드는 은밀하게 침투하고 복제 및 변종이 잦다는 유사한 특성이 있으며, 이는 인터넷 웜(Internet Worm)이나 이메일 피싱 형태, 트로이목마와 지능형 지속위협(APT) 공격에서 발견된다.²¹⁾ 또한 바이러스 변이 또는 변종처럼 암호형 바이러스도 나타나고 있다. 더욱 심각한 점은 팬데믹 사태에 따라 인터넷 사용과 사이버공간 활동이 증가하면서 해커들의 범죄 기회도 증가하고 있다는 문제다. 예를 들어 랜섬웨어 공격형태로서 ‘백신 제공’ 등 팬데믹 사태와 관련하여 사람들의 관심을 자극하는 문구를 넣어 배포된 악성 문자메시지도 크게 증가하였다.²²⁾

특히 팬데믹 상황에서 ① 비대면 학교수업에 따른 온라인 교육 플랫폼 취약, ② 재택근무 확대에 따른 회사 자료 외부 유출, ③ 개인 휴대 디지털기기의 취약성을 이용한 단말 정보 탈취 문제 등 다양한 사이버공간 내 범죄피해 위험성이 증가하였다. 또한 팬데믹 상황에서 비대면 의료 진료 환자 정보 침해, 웨어러블 시스템 해킹이나 환자 개인 정보 유출과 관련한 범죄피해 위험성도 증가하였다.²³⁾

3. 북한의 국가기반시설 사이버공격 위협증가

최근 북한의 사이버 공격 양상은 지능형지속위협(APT) 공격, 보안 메일 체크 프로그램으로 위장한 악성파일 유포와 같은 침해행위, 불특정 다수 대상 무차별적 사이버 공격과 테러행위가 자행되고 있다. 북한 관련으로 의심되는 사이버 범죄 내지 불법

20) “코로나19 닮은 ‘사이버 팬데믹’ 시대 온다
(<https://scienceon.kisti.re.kr/srch/selectPORSrchTrend.do?cn=SCTM00208118&dbt=SCTM> 2022년 8월 15일 최종검색)

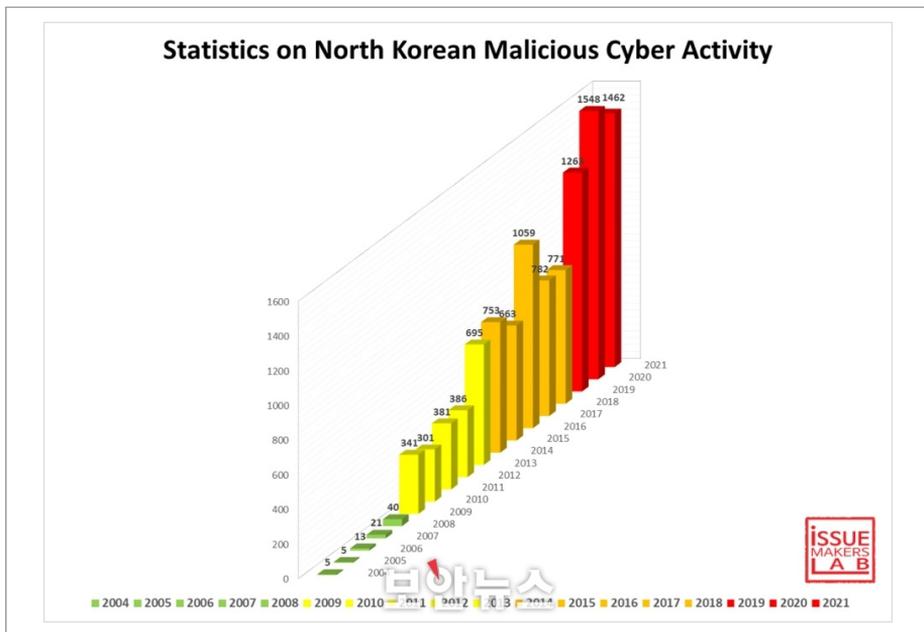
21) “사회 기반 시설 노리는 APT 단체의 공격이 점점 무서워지는 이유”
(<https://www.boannews.com/media/view.asp?idx=106113> 2022년 8월 15일 최종검색)

22) “코로나19 바이러스 사칭 스미싱 주의 안내”
(https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=35290 2022년 8월 15일 최종검색)

23) “코로나 사태에 사이버범죄 활개”
(<https://www.ajunews.com/view/20210731115916077> 2022년 8월 15일 최종검색)

행위는 2015~2019년까지 35건의 해킹으로 20억 달러에 달하는 범죄피해를 초래하였다. 북한은 2014년 소니픽처스 해킹을 시작으로 2018년 방글라데시 중앙은행이 뉴욕 미 연방준비은행에 개설한 계좌를 해킹해 8100만 달러를 탈취하고, 2009년에는 한국과 미국의 주요 기관을 마비시킨 디도스(DDoS) 공격을 자행한 것으로 알려져 있다.²⁴⁾

▶▶ [그림 2-1] 북한의 사이버공격동향(2004~2021)²⁵⁾



미국 국가정보국(DNI)은 중국과 러시아, 이란과 함께 북한을 사이버 위협국가로 지목한 바 있다. 위협국가는 의료시설에 랜섬웨어 등 악성 프로그램 공격을 가하고 백신 생산과 공급망, 송유관 기업을 위협하는 수준에 이르러 사이버안보 강화는 미국과 전 세계의 최우선 과제임으로 강조되고 있는 실정이다. 2017년 전 세계적으로 병원, 은행, 기업의 컴퓨터 네트워크를 마비시킨 '워너크라이' 사건에 대하여 미국과 유럽연

24) “북한 추정 사이버공격, 2004년부터 2021년까지 300배 이상 증가했다”

(<https://www.boannews.com/media/view.asp?idx=106606> 2022년 8월 15일 최종검색); “미 싱크탱크, 북한, 2005~2021년 사이버 공격 54회”

(<https://www.voakorea.com/a/6659422.html> 2022년 8월 15일 최종검색)

25) <https://www.boannews.com/media/view.asp?idx=106606> 2022년 8월 15일 최종검색

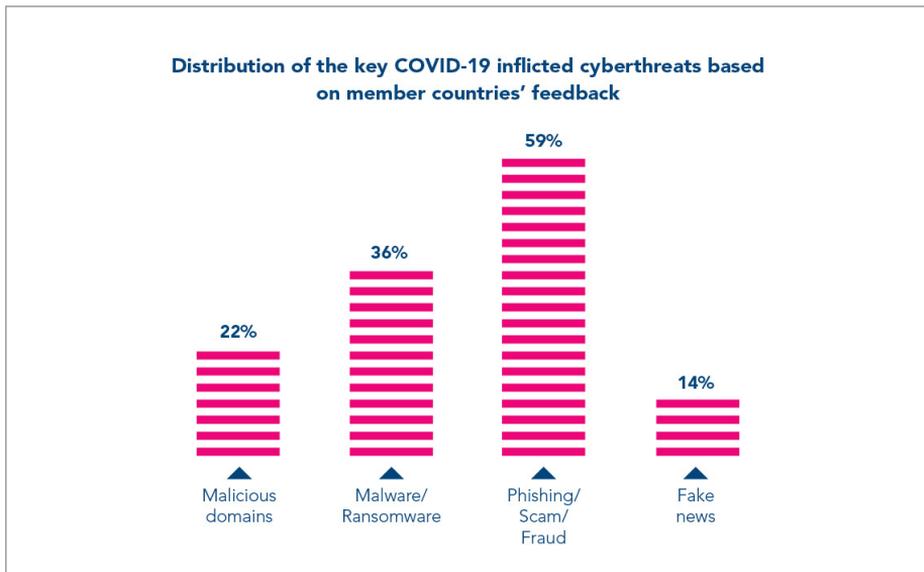
36 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

합(EU)은 공격의 배후로 북한을 지목하였다.²⁶⁾ 재래식 전략에 따른 군비경쟁에서 뒤처지는 북한에게 사이버 공격은 효과적 공격과 범행 수단으로 악용되고 있는 것으로 보인다.

4. 사이버안보 침해와 피해의 국제적 동향

COVID-19 팬데믹 이후 사이버범죄의 증가 양상과 관련해서는 국제적으로 COVID19의 영향이 가장 넓고 크게 미친 사이버범죄 유형은 피싱사기로 파악된다.

» [그림 2-2] 팬데믹 시기 사이버위협 동향²⁷⁾



랜섬웨어와 디도스 공격은 의료보건 기간시설에 대해 주로 자행되었는데 이는 가장 큰 피해를 가할 수 있는 취약지점으로서 범죄수익도 높게 기대되기 때문으로 판단된다. 정보탈취 말웨어(Data Harvesting Malware)로서 원격접근바이러스(Remote Access Trojan), 정보탈취 말웨어(info stealers), 스파이웨어 (spyware) 범죄가 증가하

26) 「미 국방부 '중국, 러시아, 북한 사이버 위협 극심」
(<https://www.bbc.com/korean/news-57140784> 2022년 8월 15일 최종검색)
27) INTERPOL report on cyberattacks during COVID-19, 2020

고 있으며, 의료정보에 대한 사회적 높은 관심을 기회로 “coronavirus” “COVID”와 같은 단어가 포함된 가짜 도메인(Malicious Domains)을 이용해 말웨어를 심거나 피싱에 악용하는 사례도 급증하고 있다. 2020년 상반기중 말웨어 범죄는 569% 증가했다.²⁸⁾

특히 가짜뉴스(Misinformation)의 급증은 사회불안을 조성할 뿐만 아니라 사이버 공격의 발미를 제공한다는 점에서 사이버보안의 중요 현안이 되고 있다. 인터폴 조사 대상국의 30%에서 COVID19 관련 가짜뉴스 문제가 지적되고 있다.²⁹⁾

사이버공격과 범죄의 피해 규모 또한 막대하다.³⁰⁾ 전 세계 사이버 범죄 피해 규모가 2020년 6조 9,390억 달러(약 7,754조 원)에서 2025년에는 10조 5,000억 달러(약 1경 1,745조 3,000억 원)로 증가될 것으로 예상된다.

2020년 미국 사이버범죄 피해 규모 역시 역대 최대로 파악된다. 미국 FBI 2020년도 인터넷 범죄 보고서에 따르면 2020년 사이버 범죄건수와 피해액 규모가 사상 최고치를 기록했다. FBI에 접수된 범죄피해 신고건수는 2019년보다 69% 증가하였으며, 피해 금액도 45억 달러에 달한다. 사이버 범죄 유형 중에서 비즈니스 이메일 사기(Business Email Compromise), 이메일 계정 사기(e-mail Account Compromise) 관련 신고 건수는 1만 9,369건이며 피해 총액은 19억 달러에 이른다. 피싱사기는 24만 1,342건이며 피해액은 5800만달러, 랜섬웨어 피해는 2,474건으로 피해액은 3100만 달러에 달한다. 신종 사이버 범죄로는 2020년 미 연방정부에 의한 코로나 지원과 구제 경제 안보법 도입 이후 개인 정보를 절취와 허위 실업 수당, 기업 구제지원금 허위 신청 등의 사례가 증가하고 있다.³¹⁾

5. 사이버범죄의 국가안보 문제화

2021년 미국 에너지 기간시설에 대한 랜섬웨어 공격 피해 발생 등 일련의 사건들로 인하여 사이버공간 미국, 중국, 러시아 등 국가간 충돌위험 증가하고 있다. 육·해·공·우주에 이은 ‘제5 전장’으로 불리는 사이버공간에서 일종의 새로운 냉전 가능성까지

28) INTERPOL report on cyberattacks during COVID-19, 2020

29) INTERPOL report on cyberattacks during COVID-19, 2020

30) CyberSecurity Ventures, Special Report: Cyberwarfare In The C-Suite, 2020

31) FBI 2020 Internet Crime Report, 2020

제기되는 실정이다.³²⁾

미국 국가핵안보국(NSA) 전산망 해킹, 미국 소프트웨어 업체 솔라윈즈의 솔루션 공급망을 통한 고객사 해킹, 미국 대형 보안 업체 파이어아이 해킹, 미국 재무부와 상무부 산하기관 이메일 해킹, 미국 최대 송유관 업체 콜로니얼 파이프라인 랜섬웨어 공격, 세계 최대 육류 공급 업체 JBS 미국 지사에 대한 랜섬웨어 공격의 배후로 러시아 정부가 지목된 바 있다.³³⁾

2021년 6월 미국 바이든 대통령이 푸틴 러시아 대통령과 정상회담에서 16개 분야 인프라 시설에 대한 해킹 금지 목록을 전달하면서 사이버 공격을 중단할 것을 경고하였다.³⁴⁾

한편 중국으로부터의 사이버 공격은 러시아와 달리 정보를 탈취하는 해킹에 초점이 맞춰져 있다고 알려져 있다. 2021년 마이크로소프트(MS) 익스체인지 서버 탈취 사건, 뉴욕 지하철 시스템 해킹 사건의 배후로 중국 정부가 지목된 바 있다.³⁵⁾

2020년 미국 법무부는 랜섬웨어에 대한 수사 대응을 테러에 준하는 수준으로 강화하였다. 법무부의 새 지침은 랜섬웨어를 비롯한 사이버범죄 사건에 관하여 법무부 ‘컴퓨터 범죄 및 지적재산국(CCIPS)’³⁶⁾으로 보고체계를 중앙화하고, 연방 검찰에 대하여 관련 모든 수사와 사건을 CCIPS와 국가안보·사이버 범죄 조정관’에 보고하고, 수사 개시부터 기소에 이르기까지 모든 과정을 보고하고 조율하도록 하였다.³⁷⁾ FBI는 “랜섬웨어 공격은 2001년 9·11 테러만큼 위협적이다”라고 경고하였다. 이는 랜섬웨어 수사 우선순위를 테러 수준으로 격상하고, 정부 부처뿐만 아니라 민간 기업과 시민도

32) “제5의 戰場… 美, 육·해·공·우주 이어 사이버 공간 중대 피해뎀 군사대응 선언”
(<http://news.kmib.co.kr/article/view.asp?arcid=0005162295&code=11141400> 2022년 8월 15일 최종검색)

33) “미 기업 200여개 랜섬웨어 공격당해…러 해킹그룹 소행 추정”
(<https://www.hankyung.com/international/article/202107034008Y> 2022년 8월 15일 최종검색)

34) “바이든 에너지 시설 등 16곳은 절대 해킹말라”
(https://www.chosun.com/international/international_general/2021/06/18/DZULZXMU6VH-EPBBU3ARWGNYSYDQ/ 2022년 8월 15일 최종검색)

35) “미국, 사상 처음으로 중국을 해킹 범인으로 공식 지목했다”
(<https://www.boannews.com/media/view.asp?idx=99222> 2022년 8월 15일 최종검색)

36) <https://www.justice.gov/criminal-ccips> (2022년 8월 15일 최종검색)

37) “미 법무부, 랜섬웨어 수사 테러 공격 수준으로 강화”
(https://www.voakorea.com/a/korea_korea-politics_us-ransomware-attack/6059213.html 2022년 8월 15일 최종검색)

대응책임을 분담해야 한다는 의미다.³⁸⁾

또한 2021년 5월 미국 대통령은 사이버 공격 대응 태세를 높이기 위해 행정명령(EO 14028)을 제정하였다. 그 주요내용은 정부와 민간 부문, 정보통신 서비스 기업이 사이버 위협 정보를 공유할 수 있도록 하고, 클라우드 서비스, 제로 트러스트 아키텍처(zero-trust architectures)³⁹⁾, 다단계 인증(Multi-Factor Authentication, MFA), 암호화 명령 관련 사이버보안 표준을 정부가 제시한다는 것이다. 소프트웨어 공급망 보안을 개선하고, 사이버보안 사고를 사후적으로 평가하기 위해 정부와 민간 전문가로 구성된 사이버보안 안전심의위원회를 구성한다. 그리고 정부 차원에서 엔드포인트 탐지 및 대응(Endpoint Detection and Response, EDR)⁴⁰⁾ 시스템을 활성화하고, 사이버보안 사고 탐지 시스템을 개선한다.⁴¹⁾

38) "F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat"
(<https://www.nytimes.com/2021/06/04/us/politics/ransomware-cyberattacks-sept-11-fbi.html>
2022년 8월 15일 최종검색)

39) 제로 트러스트는 신뢰하지 말고 항상 검증할 것이라는 원칙을 바탕으로 네트워크 세분화 및 엄격한 액세스 제어와 같은 네트워크 보안 방법론이다. 제로 트러스트 네트워크는 중요한 데이터, 자산, 애플리케이션 및 서비스로 구성되는 보호 범위를 정의하며, DAAS라고도 한다.
(<https://www.vmware.com/kr/topics/glossary/content/zero-trust.html> 2022년 8월 15일 최종검색)

40) 다양한 의심스러운 활동과 행동에 대해 네트워크상의 최종 사용자 하드웨어 디바이스를 감지해 인식된 위협을 자동으로 차단하도록 대응하고 추가 조사를 위해 포렌식 데이터를 저장하는 보안 도구를 말한다. (<https://www.itworld.co.kr/news/136271#csid823850a543e66e195d201bfa3a01df7> 2022년 8월 15일 최종검색)

41) Executive Order on Improving the Nation's Cybersecurity, 2021
(<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> 2022년 8월 15일 최종검색)

제 3 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

국가 사이버안보 역량강화 정책의 발전

제3장

국가 사이버안보 역량강화 정책의 발전

제1절 | 국가 사이버 안보 역량 강화 정책의 주요경과

1. 2019년 국가사이버안보전략과 국가사이버안보기본계획

2019년 4월 발표된 「국가사이버안보전략」은 사이버위협을 안보위협으로 인식하여 모든 역량을 결집·대응할수 있도록 「국가안보전략」에 따라 수립된 최초의 전략이다. 국가사이버안보전략은 사이버안보의 미래 비전과 목표를 제시하고 개인·기업·정부가 중점 추진해야 할 전략적 과제를 제시한다. 이를 통해 국가 전반의 사이버방어 능력이 제고되고, 사이버위협으로부터 사이버공간을 보호하여 국민 모두가 더 안심하고 향유할 수 있게 하는데 목표가 있다. ⁴²⁾

동 국가전략의 전략과제는 첫째, 국가 핵심 인프라 안전성 제고, 둘째, 사이버공격 대응역량 고도화, 셋째, 신뢰와 협력 기반 거버넌스 정립, 넷째, 사이버보안 산업 성장 기반 구축, 다섯째, 사이버보안 문화 정착, 여섯째, 사이버안보 국제협력 선도로 제시된다.

이에 따라 국가사이버안보전략 과제를 추진하기 위하여 범부처 차원에서 이행할 구체적인 실행계획을 담은 「국가사이버안보 기본계획」은 2019년 9월 확정되었다.⁴³⁾ 이는 최근 국제사회의 분쟁요인 급증, 5세대 이동통신(5G) 초연결 사회 진전에 따른 위협요인 확대 등 국가 사이버안보에 대한 위협이 증가함에 따라 과기정통부, 국정원,

42) 청와대 국가안보실, 국가 사이버안보전략, 2019년 4월, 10면.

43) 관계부처합동, 국가 사이버안보 기본계획, 2019년 9월

44 「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법제기반 체계적 정비

국방부 등 9개 기관은 정부, 기업 및 개인 모두가 참여하여 사이버보안을 강화하기 위한 체계적인 실행 방안을 마련한 것이다. 기본계획에 따라서 정부는 사이버안보 6대 전략과제를 뒷받침하기 위해 기관별 실행계획을 18개 중점과제, 100개의 세부과제로 종합하고 단계적으로 추진하게 된다.

기본계획에 따른 사이버범죄 대응기반 구축 3대 과제는 다음과 같다.

첫째, 사이버공격을 사전에 효율적으로 억지하고 사고발생시 신속하고 능동적으로 대응할 수 있도록 민·관·군 합동 대응체계를 강화하는 등 사이버위협 대응역량의 지속적 고도화를 추진한다.

둘째, 국민 모두가 사이버안보 중요성을 인식하고 실천하며 정책 수행 과정에서 기본권을 존중받고 국민들의 참여와 신뢰를 보장할 수 있는 사이버보안 문화를 정착시킨다.

셋째, 다양한 국제협력을 통한 파트너십을 강화하고 국제규범 형성을 주도하는 등 사이버안보를 위한 국제협력을 내실화한다.

특히 사이버위기 예방과 사이버공격 대응역량 강화를 위해서는 사이버공격 억지력 확보가 중요하다. 머신러닝 등을 활용한 보안위협 자동분석체계를 구축하고, 유관부처 합동 공격원점 규명 절차와 기준을 마련한다. 대규모 사이버공격 대비 태세 강화를 위해서는 중앙·지자체 차세대 보안시스템을 구축하고, 민·관·군 합동대응체계 개편 및 정기 합동훈련을 실시한다. 또한 포괄적·능동적 수단 확보를 위하여 우방국, 국제안보기구 등과 긴밀한 협조체계를 구축하고, 사이버전 대비 전략·전술을 개발한다. 사이버보안 인식 제고 및 실천 강화를 위해서는 ‘10대 정보보안 기본수칙’을 개발·보급하고 국민참여형 정보보호 캠페인을 지속 추진한다. 특히 기본권과 사이버안보의 균형을 고려하여, 정책 수립 과정에 민간 정책자문단을 구성·운영하고, 공격실태 공개, 세미나 등을 통해 정책 공감대를 확보하는 노력도 중요하다.

그리고, 사이버범죄 대응역량 제고를 위해서는 사이버범죄 대응조직·인력을 확대하고 유럽평의회 사이버범죄협약(European Convention on Cybercrimes) 가입 추진이 검토과제다. 사이버범죄 대응기관으로서 대검찰청의 경우 국제 사이버수사공조 전문부서 신설 및 전문인력 확충, 사이버위협 정보 분석·공유 체계 구축을 추진하고, 경찰청은 사이버범죄 대응강화 및 국제공조 전담조직 확대, 사이버위기 관리 전담조

직 신설 등 인프라 확충을 추진하며, 국가정보원 주요 국가 정보통신망 단계별 보안수준 강화, 첨단기술 보안 연구·개발 및 가이드라인 개발을 각각 추진하고 있다.

2. 2017년 국가사이버안보법 정부법안

2019년 수립된 국가사이버안보기본계획상 주요 과제중의 하나는 국가 사이버안보 역량 및 환경 변화 대응을 위한 법적기반 구축이다. 그러나 국가사이버안보의 기본법 제 제정작업은 진전되지 못하고 있는 상태다. 2015년 일본뿐만 아니라 2016년 중국도 국가전략과 국민안전 차원에서 사이버안보기본법제를 갖추어 가고 있는데, 한국은 팬데믹 위기, 그리고 북한의 사이버공격 위협에도 불구하고 여전히 논의 단계에 머물러 있는 것이다.

2017년 정부가 제출했던 ‘국가사이버안보법안’의 입법 추진 취지는 다음과 같이 정리할 수 있다.⁴⁴⁾

첫째, 이제까지 국가 차원의 사이버 위기 관리 등과 관련된 업무가 소관부처별로 이루어져 각 부처의 업무범위는 정보자산과 기반시설에 대한 침해사고 대응 및 복구에 한정되고 있다.

둘째, 현재 국정원이 사이버안보에 관하여 주도적인 역할을 하도록 규정하고 있는 「국가사이버안전관리규정」이 있으나 이는 국가 및 공공기관에만 적용되는 대통령훈령으로서 민간부문을 포함한 종합적이고 체계적인 대응의 근거 법령으로서는 미흡하다.

셋째, 국가정보원은 국내에서 사이버공격 등에 대한 분석 및 대응에 있어 최고의 기술력과 노하우가 있고, 대통령훈령에 따라 사이버안보 분야에서 국가정보원이 실제 주도적 역할을 수행하고 있다.

넷째, 우리나라는 세계최고로 발달된 정보통신기술 덕택에 업무나 생활 전 부문에서 편리성을 누리고 있지만, 역설적으로 그만큼 사이버공격의 대상이 확대되어 위험성도 커지고 있다.

다섯째, 사이버공간에서 우리나라는 다른 나라에서 공통적으로 받는 위험성 외에 북한이라는 변수가 하나 더 있기 때문에 더욱 더 다층적으로 안전장치가 필요하다고

44) 국회 정보위원회, 국가사이버안보법안【정부 제출】검토보고, 2017. 2. 9-10면.

볼 수 있다.

동 법안 제16조 내지 제17조에 따르면 국가정보원장이 사이버공격에 대한 체계적인 대응을 위하여 단계별 사이버위기정보를 발령하도록 하고, 중앙행정기관 및 시·도 등 상급책임기관의 장은 일정 단계 이상의 경보가 발령되거나 사이버공격으로 인하여 그 피해가 심각하다고 판단하는 경우에는 책임기관, 지원기관 및 수사기관이 참여하는 사이버위기대책본부를 구성·운영할 수 있도록 규정하였다.

따라서 향후 국가사이버안보기본법제 제정추진에 있어서 특히 사이버공격에 대한 체계적 대응을 기최조정할 컨트롤타워를 정하는 문제, 사이버공격 대응 책임기관, 지원기관, 수사기관의 권한과 직무 조정배분의 문제, 사이버위기대책협의기구의 설치와 운영문제는 사이버범죄, 사이버보안침해사고, 사이버테러를 포괄하는 국가사이버안보 입법정책 차원에서 논의되어야 할 것이다.

3. 국제사회의 사이버안보 역량강화 의제

2010년 유엔총회 결의안 65/230에 따라 회원국들의 역량강화와 기술지원을 통해 사이버범죄 대응역량을 강화하기 위한 사이버범죄대응 글로벌 프로그램 (Global Programme on Cybercrime)이 진행되고 있다. 45) 점증하는 사이버위협과 그 초국가적 특성을 감안하여 개발도상국 대상 지원과 민간기업과의 협력도 강조되고 있다. 46) 사이버안보는 국제 사회 공동체의 목표인 안보와 평화에 있어서 주요 의제로 자리잡게 되었다.

사이버안보 국제환경 변화 요인 중 하나는 미국과 동맹국인 한국과 일본도 러시아와 중국, 북한 정부가 배후에 있는 사이버범죄조직의 공격 집중 대상이 되고 있다는 점이다. 특히 미국은 사이버 공격 피해가 집중되는데, 보안 기업 NSHC의 다크웹상 범죄행위 감시 플랫폼에 따르면, 2019년 5월부터 1년간 랜섬웨어 공격을 당해 다크웹에 정보가 유출된 기업·기관이 전체 피해 건수의 53.7%에 달한다. 47) 전 세계 인터넷

45) Resolution adopted by the General Assembly on 21 December 2010: 65/230. Twelfth United Nations Congress on Crime Prevention and Criminal Justice

46) UNODC and the private sector partner to train cybersecurity professionals (<https://www.unodc.org/roseap/en/2021/06/private-sector-partner-cybersecurity-professionals/story.html> 2022년 8월 15일 최종검색)

트래픽을 저장하는 Root DNS 서버 대부분이 미국내 위치하기 때문에, 전 세계 트래픽의 70%가 미국을 거치므로 공격대상이 되는 것이다. 이에 따라 미국 정부는 사이버공격 대응을 위해 글로벌 협력 강화를 추진하고 있다. 2020년 12월 미국 연방수사국과 사이버보안국(CISA)은 영국 국립사이버보안센터(NCSC)와 유럽연합경찰기구(Europol), 국제적 정보통신 기업들과 함께 랜섬웨어 전담 조직을 설치하였다.⁴⁷⁾

제2절 | 국내법제 변화와 사이버 안보 체제 정비

1. 국내법제 개혁에 따른 사이버안보 체제 정비

국가전략적 차원에서 볼 때 사이버안보 시스템은 총괄적 통제기구가 부재한 상태이며, 공공 부문은 국가정보원, 민간 부문은 한국인터넷진흥원, 군은 사이버작전사령부 관할로 분장되어 있다. 최근 팬데믹 상황에서 강조된 K-사이버 방역체계 구축 계획 역시 국가 사이버안보 거버넌스 정비 차원에서 이행될 필요가 있다.

다만, 사이버안보 거버넌스 정비 문제에 있어서 중심적 역할을 맡아야 할 국가정보원은 대공 수사과정에서의 인권 침해 등 권한남용과 정치적 일탈 행위의 우려가 지속적으로 제기되어 왔다. 이에 따라 국가정보원이 다변화되고 있는 대외 위협으로부터 국가 안보를 수호하는 정보기관으로 변모해야 한다는 요청이 있었다. 직무범위를 명확히 하며 정보기관 본연의 직무수행에 집중하도록 함으로써 국가정보기관으로서의 위상을 재정립하기 위해 2020년 12월 국가정보원법이 개정되었다.

동법 제3조에 따르면 국가정보원은 운영에 있어 정치적 중립성을 유지하고, 이 법에서 정하는 정보의 수집 목적에 적합하게 정보를 수집하며, 수집된 정보를 직무 외의 용도로 사용하지 아니하도록 운영 원칙을 정해야 한다.(동조 제2항).

47) “다크웹 랜섬웨어 해커조직에 당한 최대 피해국은 미국”

(<https://www.boannews.com/media/view.asp?idx=99061> 2022년 8월 15일 최종검색)

48) “신홍 인프라 노리는 랜섬웨어...각국 사이버 방패 구축 분주”

(http://economychosun.com/client/news/view.php?boardName=C00&t_num=13611276 2022년 8월 15일 최종검색)

48 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

또한 동 개정법은 국가정보원의 직무 범위를 국외 및 북한에 관한 정보, 방첩, 대테러, 국제범죄조직에 관한 정보, 사이버안보 및 위성자산 정보 등의 수집·작성·배포, 보안 업무, 직무수행 관련 대응조치, 사이버 공격 및 위협에 대한 예방 및 대응, 정보 및 보안 업무의 기획·조정 등으로 명확히 하였다. (제4조).

이에 따라 국정원은 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포 업무를 맡게 되었다. 또한 '지역 화이트 해커 양성'을 통해 지역에서 발생할 수 있는 사이버 공격 및 위협을 차단할 기반을 구축하는 방안을 추진하게 된다. (동법 제4조)

또한 법개정으로 국내 정보 업무가 폐지됨에 따라 방첩, 대테러, 사이버, 우주정보 등과 관련한 업무 및 기능을 재정비하기 위해 산하 조직 및 역할을 새로운 업무에 맞게 조정하게 되었다. 2003년 '국가사이버안전센터'라는 이름으로 설립된 국가정보원 산하 사이버안전 전담조직은 2020년 개정 국가정보원법과 사이버안보업무규정 제정에 따라 2021년 '국가사이버안보센터'로 재정비되었다. 동시에 국가사이버안보센터는 1급 조직으로 격상되면서, 소프트웨어(SW) 공급망 보안 대책 마련을 포함해 국가·국제 사이버안보 체계 강화를 추진하게 된다. 이는 국제 사이버안보 협력 강화, 민간 사이버 위협 정보 공유 확대를 위한 역할과 중요성을 반영한 것으로 평가된다.

국가사이버안보센터는 국가사이버 안전 정책 총괄, 사이버 위기 예방 활동, 사이버 공격 탐지 활동, 사고 조사와 위협 정보 분석 업무를 담당하며, 조직강화에 따라 민·관 사이버안보 협력도 강화할 것으로 기대된다. 국제 사이버안보 협력 강화, 민간 정보 공유 확대, 지역 보안 사각지대 해소, SW 공급망 보안 대책 마련, 분야별·유형별 신 보안 모델 수립 전략 중심으로 역할 확대 추진도 이러한 노력의 일환이다. 국가정보원은 '집단 사이버 면역체계 구축'을 목표로 필요시 사이버 위협 정보를 외부와 공유한다는 전략에 따라 향후 국가사이버안보협력센터 설립도 검토하고 있다.

2. 국내법제 개혁에 따른 사이버범죄 수사체계 정비

사이버범죄의 기술적 범행특성과 국가차원의 피해규모를 고려할 때, 국가정책적으로 사이버범죄 수사기관이 충분한 역량을 갖추 수 있도록 표준적인 훈련 방법과 조직

구조를 개발하고 국제공조와 정보교류를 원활하게 하기 위한 법제도와 기술적인 협력 체계를 함께 구축해야 한다.

이에 따라·사이버 범죄 대응강화 및 국제공조 전담조직 확대, 사이버 위기관리 전담조직 신설 등 인프라 확충 등을 맡고 있는 경찰청은 2019년 사이버경찰 조직·인력 확충에 있어서 3개(대구·인천·경기) 지방청 사이버안전과 신설, 지방청 사이버수사, 디지털증거 분석관 및 경찰서 사이버수사관 증원 등을 했으며, 2020년부터 다크웹 불법 정보 추적시스템 고도화와 사이버국제공조팀을 운영하고 있다.⁴⁹⁾ 또한 대검찰청은 국제 사이버수사공조 전문부서 신설 및 전문인력 확충, 사이버위협 정보 분석·공유 체계 구축 업무 강화를 추진해 왔다.⁵⁰⁾

수사구조개혁에 따른 사이버범죄 분야 수사협력체계 정비 또한 중요한 정책현안이다. 사이버범죄 대응과 수사를 담당하는 기관간 협력 네트워크와 정보보안사고대응 체계와 더불어 사이버범죄 대응의 핵심체계를 구성하기 때문이다.

사이버범죄에 대응한 수사기관 네트워크는 인터폴과 유로폴 등 기존의 국제경찰 네트워크를 중심으로 각국의 전담 사이버경찰의 협력관계로 구성된다.⁵¹⁾ 한국 사이버범죄 수사경찰은 사이버범죄 대응 네트워크에서 세계적 수준의 역량을 인정받고 있다. 사이버범죄 수사기관으로서 경찰은 전문인력 채용 및 교육훈련 체계와 사이버범죄 예방부터 수사까지 가장 진화된 형태의 조직 구조를 갖추고, 많은 개발도상국에 사이버치안 역량을 전수하고 있을 정도로 뛰어난 역량을 갖추고 있기 때문이다.⁵²⁾

한편 수사구조개혁 이후 시행령 단계에서 검사의 직접수사 분야에 사이버범죄를 대형참사범죄에 포함시켜 검찰도 사이버범죄 수사를 지속하게 되었으나, 2022년 형사소송법령 개정으로 인하여 사이버범죄도 직접 수사 범위에서 배제될 것으로 보인다. 다만 국가경쟁력의 중요한 부분으로서 사이버범죄 대응 관련 국가적 체계 정비는

49) “정부, ‘국가사이버안보전략’ 수립 이후 1년간 무엇을 했나?”

(<http://www.atnnews.co.kr/news/articleView.html?idxno=39469> 2022년 8월 15일 최종검색)

50) 대검찰청 (<https://www.spo.go.kr/site/spo/02/10206010000002018100812.jsp> 2022년 8월 15일 최종검색)

51) “인터폴, 글로벌 사이버 위협 퇴치 위한 국제적 경찰 공조 도모”

(<https://www.ciokorea.com/t/21989/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4/201084#csidxe93157724746916a0f7865d9d02542d> 2022년 8월 15일 최종검색)

52) 동남아에 퍼진 ‘치안한류’...사이버수사 역량 강화에 한국 경찰 앞장

(<https://www.asiae.co.kr/article/2021052921332295440> 2022년 8월 15일 최종검색)

50 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

국가정책적으로 중요한 문제라는 점을 고려한다면, 단순히 권력기관 개혁 차원에서 검경간의의 갈등문제로 접근할 것이 아니다. 사이버범죄에 대응한 국가수사역량의 전략적인 목표와 효과를 종합적으로 고려한 사이버범죄 수사체계의 합리적 정비가 필요하다.

제 4 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

사이버안보 체계와 제도 및 정책 정비

제4장

사이버안보 체계와 제도 및 정책 정비

제1절 | 국정과제 이행과제와 사이버 안보 역량강화 전략

1. 국정과제 목표와 기대효과

「국가 사이버안보 대응역량 강화」 국정과제의 목표는 다음과 같다.⁵³⁾

첫째, 전통적 국가안보 영역에서 경제안보·국민생활까지 확장 추세인 국가배후조직 및 국제 해킹조직의 위협에 대응하는 사이버안보 패러다임을 구축한다.

국제적으로 국가 사이버안보 전략은 단순한 사이버위협, 사이버범죄 대응 차원에 그치지 않고 적극적 사이버 방어(active cyber defense) 차원에서 위협 탐지 및 사전예방적 차원의 안보조치 등 보다 적극적인 형태로 변화하는 추세다. 미래 사이버 안보 전략 구상은 적극적 사이버안보 패러다임 위에서 구축되어야 한다.⁵⁴⁾

둘째, 범정부 차원 협력체계 공고화, 사이버 방어체계 및 국제공조 시스템 강화를 통해 확고한 국가안보 태세 유지 및 국민·기업에 안전한 사이버환경을 제공한다.

국가안보와 국민안전을 모두 아우르는 사이버안보 개념은 국내적으로는 첨단 정보통신환경과 사이버 안전환경 조성을 통해서 구체적으로 실현될 것이다. 이와 더불어 사이버안보 관련 보편타당한 국제규범 정립 과정에 적극 참여하여 국제규범 및 모범 사례 확산을 선도하며, 사이버정책협의회 개최, 국제기구 파트너십 강화, 국제협약 가입 등을 통해 양·다자간 실질적인 협력과 공조체계를 구축함으로써 국제공조 환경

53) 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022년 5월, 170면.

54) 유지연, 국가 사이버 안보 전략 패러다임 변화에 대한 주요국 비교분석 연구, 국가정보연구 14 (1), 한국국가정보학회, 2021, 115면 이하.

54 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

도 갖추어야 할 것이다.⁵⁵⁾

셋째, 관련 산업·기술 경쟁력 제고, 인재 육성 등을 통해 사이버안보 기반을 공고하게 한다.

이는 사이버보안 투자확대, 보안인력 및 기술경쟁력 강화, 보안기업 성장환경 조성, 사이버보안 인식 제고 및 실천 강화, 그리고 기본권과 사이버안보의 균형을 통해 실현될 수 있다.⁵⁶⁾ 뿐만 아니라 점차 고도화되는 사이버 공격에 대응하기 위해 인공지능 기술을 접목한 사이버 보안 기술 발전이 진행되고 있다.⁵⁷⁾ 사이버보안에서 인공지능의 활용 또한 정책적으로 주목할 필요가 있다.

이로써 범국가 사이버안보 역량 결집, 글로벌 사이버위협 신속 대응 및 예방체계 구축 효과를 기하여, 튼튼한 사이버안보 초석 아래 ‘더 안전한 대한민국’과 ‘첨단 IT 환경’ 조성이 기대된다는 것이다.

2. 국정과제 주요내용별 10대 이행과제

「국가 사이버안보 대응역량 강화」국정과제의 주요 내용은 ① 사이버안보 정책 체계 정비; ② 경제안보로서 사이버안보; ③ 국민생활 안전; ④ 기술 고도화 및 국제협력 강화; ⑤ 사이버전문인력 양성 다섯 가지로 제시된다.

본 보고서에서는 이를 주제별로 재유형화하여 10대 세부과제로 정리해 본다.

▶▶▶ [표 4-1] 「국가 사이버안보 대응역량 강화」국정과제의 10대 세부과제

국정과제 주요내용	국정과제 세부과제
사이버안보 정책 체계 정비	세부과제 1 : 대통령 직속 ‘국가사이버안보총’ 설치 및 컨트롤타워 운영 체계를 갖춘다.
	세부과제 2 : 사이버안보 유관기관별 역할과 각급 기관간 협력 활성화 등을 규정한 법령 제정을 추진한다.
경제안보로서 사이버안보	세부과제 3 : 민관 합동 사이버협력체계 강화를 통해 핵심기술 보유기업·방산업체·국가기반시설 대상 위협과 공격 방지 및 대응조치를 적극 실행함으로써 경제 안보에 기여한다.

55) 청와대 국가안보실, 국가 사이버안보전략, 2019년 4월, 23면.

56) 청와대 국가안보실, 국가 사이버안보전략, 2019년 4월, 20-22면.

57) 김민진, 인공지능: 사이버보안 패러다임의 전환, 정보통신정책연구원, 2021

국정과제 주요내용	국정과제 세부과제
국민생활 안전	세부과제 4 : 사이버공격으로부터 안전한 '디지털플랫폼' 정부를 구현한다.
	세부과제 5 : 클라우드·스마트그리드 등 국민 생활에 밀접한 IT 환경의 안전성을 확보한다.
기술 고도화 및 국제협력 강화	세부과제 6 : 産·學·研·官 협력 아래 AI·양자통신 등 신기술 위협 대응, 新기술 연구·개발을 적극 지원하여 사이버공격 탐지·차단·추적 시스템을 고도화한다.
	세부과제 7 : 사이버안보 국제공조 활성화 차원에서 국제사회의 사이버 규범 수립에 적극 참여한다.
	세부과제 8 : 사이버위협에 맞서 글로벌 협력 네트워크를 확충한다.
사이버 전문인력 양성	세부과제 9 : 대학·특성화 교육 확대, 지역별 교육센터 설치 등 '10만 인재 양성' 프로그램을 실행한다.
	세부과제 10 : '사이버 예비군' 운영 등 사이버전 인력을 확보한다.

제2절 | 국가사이버안보위원회 설치와 사이버안보 통제 체계 구축

세부과제 1 : 대통령 직속 '국가사이버안보委' 설치 및 컨트롤타워 운영체계를 갖춘다.

1. 대통령 직속 국가사이버안보위원회

본 과제와 관련하여 종래 2017년 국가사이버안보법 정부법안 제5조에서 사이버안보와 관련된 국가의 정책 및 전략 수립에 관한 사항 등을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회를 두되, 위원장은 국가안보실장으로, 위원은 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관의 차관급 공무원 중 대통령령으로 정하는 사람과 사이버안보에 관하여 전문적인 지식과 경험을 갖춘 사람 중에서 국가안보실장이 임명하거나 위촉하도록 규정하였던 바 있다.

동 법안에서 대통령 직속으로 국가사이버안보위원회를 두고자 했던 취지는 공공

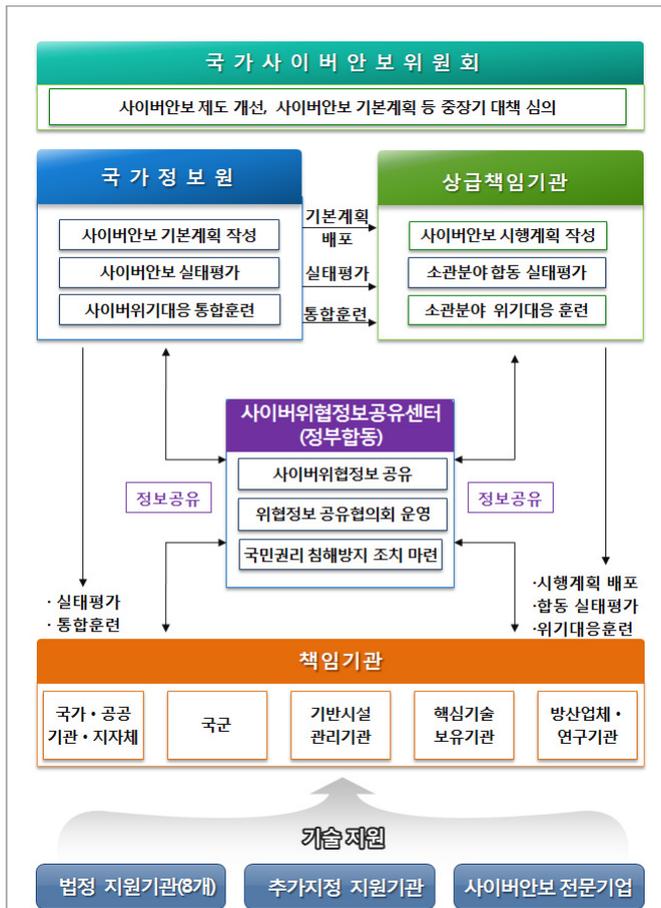
56 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

및 민간 영역의 구분이 없이 광범위하게 발생하는 사이버공격으로 인하여 막대한 경제적 피해와 사회 혼란이 유발되고 있기 때문에, 국가안보를 위협하는 사이버공격을 신속히 차단하고 피해를 최소화하기 위하여 국가사이버안보위원회를 설치하고, 국가사이버안보 관련 조직 및 운영을 체계적으로 정립하기 위함이었다.⁵⁸⁾

2020년 사이버안보 기본법안⁵⁹⁾에서는 사이버안보에 관한 중요한 사항을 심의하기 위하여 대통령을 의장으로 하는 국가사이버안보정책조정회의를 두도록 하였다.(안 제5조).

2021년 국가사이버안보법안⁶⁰⁾에서는 사이버안보를 위한 중요 사항을 심의하기 위

58) 국회 정보위원회, 국가사이버안보법안【정부 제출】검토보고, 2017. 2. 46면.



59) 의안번호 제1220호 (조태용의원 대표발의 2020. 6. 30)

60) 의안번호 제1314호 (김병기의원 대표발의 2021. 11.4.)

하여 국가정보원장 소속으로 사이버안보위원회를 두도록 하였다.(안 제5조 및 제6조).

2021년 사이버보안기본법안⁶¹⁾에서는 사이버보안에 관한 중요한 사항을 심의·의결하기 위하여 대통령을 위원장으로 하는 국가 사이버보안 전략위원회를 두도록 하였다.(안 제5조)

새 정부에서는 대통령 직속으로 신설되는 3개 민관합동위원회에 국가사이버안보위원회가 포함될 계획이다. 이전 정부에서는 국가안보실 1차장 산하 사이버안보비서관이 새 정부에선 국가안보실 2차장 산하에 국방비서관과 함께 배치될 예정이다.

이제까지 국가 차원에서 범정부 역량을 집중할 수 있는 일원화된 사이버안보 공조체계 부재가 비판받아 왔다. 다수 정부 부처에 사이버안보 책임과 역할이 분산돼 명확한 사이버안보 거버넌스 체계를 확립하지 못했다는 것이다. 뿐만 아니라 사이버안보 정책시야가 북한에 한정되다 보니, 국제적인 사이버안보 규범 정립과 법 개정도 적극적이지 못했다. 그렇기 때문에 국가 사이버안보 정책에 대해서는 대통령실과 국가사이버안보위원회가 관장해야 한다.⁶²⁾

2. 사이버안보 국가 컨트롤 타워

그런데 최근 대통령실은 대통령직인수위원회에서 대통령 직속 위원회 신설 문제에 대해 위원회가 아닌 협의체·자문그룹 등의 형태로 재검토하고 있다. 이는 위원회보다는 더 신속적이고 효율적인 거버넌스를 설계해 개별적 국정과제들을 보완하겠다는 것이다. 국가 사이버 안보 대응 전략 강화를 위해 대통령 직속 사이버안보위원회를 설치하겠다는 국정과제는 과학기술정보통신부·국가정보원·국방부 등으로 분산된 사이버 보안 지휘 체계를 통합하는 컨트롤타워를 만들겠다는 취지였다. 대통령 직속 위원회 형식에 대해 대통령실은 사이버안보는 상황변화가 빠르기 때문에 오히려 위원회 같은 경직된 구조가 맞지 않을 수 있어서 더 탄력적 대응이 가능한 구조가 바람직하다는 것이다.⁶³⁾

61) 의안번호 제13670호 (윤영찬의원 대표발의, 2021.12.2.)

62) “새 정부 사이버안보, 民·官·學 세 박사 모두 맞아야”

(<https://biz.chosun.com/it-science/ict/2022/05/26/VOAK76GUCJACXKXMWNDWEWXQQQ>
/2022년 8월 15일)

63) 위원회 통폐합 기조에 맞춰...‘사이버안보’ 설치 재검토

그럼에도 위원회 형식이나 소속과 별개로, 사이버안보는 선택의 문제가 아닌 국가 안보 및 국민안전에 직결된 필수적 과제라는 인식을 가지고 다양한 사이버 공격과 위협에 선제적이고 적극적으로 대응하기 위해서는 대통령 직속의 컨트롤타워 역할을 담당할 중심을 둘 필요가 있다. 종래 기관에 역할과 권한을 부여하거나 기존 여러 기관에 분산되어 있는 기능을 통합해 조직을 신설하거나 컨트롤타워를 중심으로 한 체계정비는 필요하다. 정보와 권한의 집중은 바람직스럽지 아니함은 물론이나, 이는 법적 제한조치가 기관간 견제구조를 통해 해소할 수 있는 문제이며, 권한과 기능은 분장되더라도 국가 사이버안보전략 차원에서 중장기적인 기획과 사안대응에서 통합 조정 역할은 단일화되어야 하기 때문이다.

특히 장기화된 팬데믹 사태로 인해 사이버공간과 인프라 의존도가 심화하는 상황에서 사이버안보 위협에 대응하기 위해 모든 정부 기관이 대비체계를 점검하고 선제적으로 대응할 필요성이 그 어느 때보다도 높다. 따라서 사이버안보의 국가전략적 접근에 있어서 체계적이고 효과적인 컨트롤타워 운영체계의 구축은 근거법과 제도 정비를 통해 이행해야 할 우선 과제이며, 종래 논의되었던 방안들과 제기되었던 사회적 의견들을 참고하여 행정부와 입법부가 책임성 있게 추진해야 할 것이다.

제3절 | 사이버안보 유관기관 협력체계와 사이버안보 기본법제

세부과제 2 : 사이버안보 유관기관별 역할과 각급 기관간 협력 활성화 등을 규정한 법령 제정을 추진한다.

1. 사이버안보 유관기관 협력체계

본 과제와 관련하여 2017년 정부 국가사이버안보법안에 따르면 국가기관·지방자치단체 및 국가적으로 중요한 기술을 보유·관리하는 기관 등은 책임기관으로서 소관 사이버공간을 안전하게 보호하는 책임을 지도록 하고, 국가정보원장은 책임기관을

지원하기 위한 기술적 역량이 있는 기관 또는 단체를 지원기관으로 지정할 수 있도록 하였다. (안 제6조 및 제7조) 뿐만 아니라 기관간 협력 활성화를 위해서는 사이버위협 정보의 공유(안 제12조), 사이버공격으로 인한 사고의 통보 및 조사(안 제15조) 규정을 두었다.

특히 사이버위기대책본부의 구성(안 제16조 및 제17조)에 따르면 국가정보원이 사이버공격에 대한 체계적인 대응을 위하여 단계별 사이버위기경보를 발령하도록 하고, 중앙행정기관 및 시·도 등 상급책임기관은 일정 단계 이상의 경보가 발령되거나 사이버공격으로 인하여 그 피해가 심각하다고 판단하는 경우에는 책임기관, 지원기관 및 수사기관이 참여하는 사이버위기대책본부를 구성·운영할 수 있도록 규정하였다.

국정과제에서 제시한 국가사이버안보위원회가 컨트롤타워로서 기능을 하려면, 사이버안보 유관기관마다의 권한과 책임, 기관간 협력의 체계화와 효율화를 내용으로 하는 법적 기반이 뒷받침되어야 함은 물론이다.

2019년 국가사이버안보기본계획에서도 주요 과제중 하나가 국가 사이버안보 역량 및 환경 변화 대응을 위한 법적기반 구축이었지만, 국가사이버안보기본법제 제정추진이 되지 않았다. 다만 국회차원에서는 논의가 지속되었다.

2020년 사이버안보 기본법안⁶⁴⁾에서는 국가정보원 소속으로 국가사이버안보센터 설치를 제안하였다. (안 제7조). 국가정보원은 사이버안보업무의 효율적이고 체계적인 추진을 위하여 사이버안보 기본계획을 수립하고 (안 제8조) 국가차원의 사이버위협 정보의 효율적인 공유 및 관리를 위하여 사이버위협정보 공유센터를 구축운영하도록 하였다.(안 제11조). 국가정보원은 사이버공격에 대한 체계적인 대응을 위하여 사이버 위기경보를 발령할 수 있으며, 책임기관의 장은 피해 발생을 최소화하거나 피해복구 조치를 취해야 한다. (안 제14조)

2021년 국가사이버안보법안⁶⁵⁾에서도 국가정보원을 중심으로 하는 협력체계를 제안하였다. 즉 국가정보원 및 관계 기관·단체가 타 책임기관 소관사무 영역 보호활동을 지원하기 위한 정보를 상호 공유할 수 있도록 하고,(안 제11조) 국가정보원이 책임기관을 대상으로 사이버안보 위협행위로부터 소관사무 영역을 보호하는 활동에 대한

64) 의안번호 제1220호 (조태용의원 대표발의 2020. 6. 30)

65) 의안번호 제1314호 (김병기의원 대표발의 2021. 11.4.)

실태평가를 하거나 자체평가·대체평가를 할 수 있도록 하였다.(안 제12조). 사이버안보 위협행위에 신속하고 효율적으로 대응하기 위하여 통합보안관제체계를 중심으로 보안관제를 실시하고 피해 발생 시 필요한 조사 및 조치를 취하도록 하고,(안 제14조 및 제15조), 국가정보원은 사이버안보 위기 경보를 발령할 수 있고, 경계 이상의 경보 발령 시 사이버안보위기대책본부를 구성·운영하도록 하였다.(안 제17조 및 제18조).

이에 비해 2021년 사이버보안기본법안⁶⁶⁾에서는 과학기술정보통신부를 중심으로 하는 협력체계를 제안하였다.⁶⁷⁾

2015년 일본뿐만 아니라 2016년 중국도 국가전략과 국민안전 차원에서 사이버안보기본법제를 갖추어 가고 있는데, 한국은 팬데믹 위기, 그리고 북한의 사이버공격 위협에도 불구하고 여전히 논의 단계에 머물러 있다. 2015년 일본 사이버보안기본법제의 경우 국가적 사이버안보전략 추진과 총괄기구의 법적 근거를 마련하였다는 점, 사이버안보 관련 정책의 투명성 확보를 위해 일반국민 참여를 보장하였다는 점, 사이버보안분야에서의 국제협력 중요성을 인정하였다는 점, 그리고 정부주도보다는 민간분야에서 법제정논의가 시작되고 의원입법 형태로 법을 제정하였다는 점이 특징이다.

2. 국가사이버안보전략과 사이버안보 기본법제

특히 북한의 사이버위협과 주변국가들의 사이버보안전략 및 법제 시행, 4차산업혁명 기반인 사이버보안의 중요성을 고려할 때, 우리 정부도 사이버보안기본법제 논의

66) 의안번호 제13670호 (운영찬의원 대표발의, 2021.12.2.)

67) 공공·민간을 포괄하는 국가 차원의 사이버보안에 관한 업무를 효율적으로 수행하기 위하여 과학기술정보통신부 소속으로 사이버보안본부를 두고, (안 제6조) 과학기술정보통신부는 사이버보안에 관한 전략 및 기본방향을 정하는 사이버보안 기본계획을 수립·시행하고 중앙행정기관장은 기본계획에 따른 시행계획을 수립·시행하도록 하였다.(안 제7조). 또한 과학기술정보통신부는 정보통신망·서비스 및 기기등의 안전성·신뢰성을 확보하기 위한 사이버보안대책을 수립·운영할 수 있도록 지침을 제정·권고할 수 있으며(안 제10조), 공공분야 사이버보안 수준점검을 할 수 있도록 한다.(안 제11조) 과학기술정보통신부는 보안취약점에 관한 정보를 종합적으로 수집·분석, 관리할 수 있는 체계를 구축·운영할 수 있으며(안 제14조) 침해사고가 발생한 사실을 과학기술정보통신부장관 또는 관계 중앙행정기관의 장에게 알려야 하며(안 제17조), 과학기술정보통신부는 침해사고에 대한 원인분석 등 필요한 조사를 실시하여야 하고, 침해사고 대응, 복구 및 피해확산 방지를 위한 조치를 취할 수 있도록 하였다.(안 제20조 및 제22조). 과학기술정보통신부는 침해사고 탐지·대응을 위한 통합보안관제체계를 구축·운영하고, 사이버위협정보의 효율적인 공유 및 관리를 위한 공유센터를 구축·운영할 수 있도록 하였다.(안 제18조 및 제19조).

를 신속히 마무리 짓고 제정과 후속작업에 노력해야 한다. 무엇보다도 사이버공간의 법치국가적 규율과 국민안전 확보에 대한 국가적 책무를 다하기 위해서는 민관협력과 시민참여의 형식을 적극 수용하여 정부가 새롭게 정당성과 책임성을 가지고 사이버안보 기본법제를 추진해야 할 것이다.⁶⁸⁾

2017년 이후 국가 사이버안보 기본법제의 구조와 내용에 대한 논의들을 정리 비교해 보면 다음과 같다.

▶▶ [표 4-2] 사이버안보 기본법제안의 구조와 내용

주요내용	2017년 정부법안	2020년 사이버안보기본법안	2021년 국가사이버안보법안	2021년 사이버보안기본법안
사이버안보체계	<ul style="list-style-type: none"> 국가사이버안보위원회 : 안보실 국가사이버안보실무위원회 : 안보실·국정원(공동 운영) 국가사이버안보센터 설치 	<ul style="list-style-type: none"> 국가사이버안보정책조정회의 국가정보원 소속 국가사이버안보센터 	<ul style="list-style-type: none"> 국가정보원 소속 사이버안보위원회 	<ul style="list-style-type: none"> 대통령을 위원장으로 하는 국가 사이버보안 전략위원회 과학기술정보통신부 소속 사이버보안본부
사이버안보활동	<ul style="list-style-type: none"> 기본계획 수립·시행 : 국정원 시행계획 작성·배포 : '상급책임기관'(중앙부처, 광역지자체·교육청, 국회·법원 등) 실태평가 : 국정원(합동평가단 운영) 국가·공공분야 중 대통령령으로 정한 기관 대상 보안관제센터 설치 : 책임기관 사이버위협정보공유센터 설치 : 국정원 사고조사- 일반 사이버공격: '상급책임기관' - 안보위협 사이버공격 : 국정원 	<ul style="list-style-type: none"> 사이버안보 기본계획 수립 : 국정원 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터 구축·운영: 책임기관 국가차원의 사어비 위협정보의 효율적인 공유 및 관리를 위하여 사이버위협정보 공유센터 구축·운영: 국정원 사이버공격 사고 조사 실시 및 국가정보원 통보: 책임기관 사이버위기경보 발령: 국정원 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급 	<ul style="list-style-type: none"> 사이버안보 기본계획 수립 : 국정원 국가정보원 및 관계기관·단체의 정보 상호 공유 책임기관 실태평가 : 국정원 공급망 보안 위협 확인 시 국가안전보장 및 국민 안전 위협 최소화조치를 각 소관위원회에서 심의·조치 통합보안관제체계를 중심으로 보안관제 실시 사이버안보 위협에 악용되었거나 악용될 우려가 현저한 정보통신기기등의 운영주체에 대한 필요한 보호조치 요청 	<ul style="list-style-type: none"> 사이버보안 기본계획 수립·시행: 과기정통부 기본계획에 따른 시행계획 수립·시행: 중앙행정기관 사이버보안대책 수립·운영 지침제정·권고: 과기정통부 사이버보안에 적합한 설계·개발 장려·촉진 위한 지침의 개발·보급: 과기정통부 공공분야 사이버보안 수준점검: 과기정통부 보안취약점 정보를 종합적으로 수집·분석, 관리할 수 있는 체계 구축·운영 사이버보안 평가·

68) 김한균, 사이버보안 국가전략과 기본법제 - 일본의 2016년 개정 사이버보안기본법과 2015년 사이버보안전략, 형사정책연구소식 143, 한국형사정책연구원, 2017

62 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

주요내용	2017년 정부법안	2020년 사이버안보기본법안	2021년 국가사이버안보법안	2021년 사이버안보기본법안
	<ul style="list-style-type: none"> • 민간 분야 안보위협 사고조사시 합동조사팀 운영 • 대응훈련 : 상급책임기관(소관영역), 국정원(통합) • 경보발령 : 국정원, 중앙행정기관(분야별) • 대책본부 : 상급책임기관, 국정원(2개 이상 부처가 관련될 경우) • 전문기업 지정·관리 : 미래부 	<p>대응, 피해복구 등을 위하여 책임기관 및 지원 기관이 참여하는 사이버위기 대책본부 구성·운영</p>	<ul style="list-style-type: none"> • 사이버안보 위기 경보를 발령 및 경계 이상의 경보 발령 시 사이버안보위기 대책본부를 구성·운영: 국정원 • 국가정보원이 수집한 사이버안보 정보에 대해서 보고 받을 수 있고, 현장검증 및 조사 실시: 국회정보위원회 	<p>인증제도 도입·시행: 과기정통부</p> <p>사. 침해사고 원인분석 등 필요한 조사 실시 및 침해사고 대응, 복구 및 피해확산 방지 조치: 과기정통부</p> <ul style="list-style-type: none"> • 침해사고 탐지·대응을 위한 통합보안관제체계 구축·운영: 과기정통부 • 사이버위협정보의 효율적인 공유 및 관리를 위한 공유센터를 구축·운영: 과기정통부 • 수준별 경보 발령 및 경계 이상일 경우 대책본부를 구성·운영: 과기정통부
사이버안보기반조성	<ul style="list-style-type: none"> • 산업육성·인력양성·국제협력 • 벌칙 : 공유정보 부정사용, 자료삭제, 비밀 미엄수, 직무목적 외 사용(추가)시 5년 이하, 5천만원 미만 • 개인정보 처리 	<ul style="list-style-type: none"> • 사이버안보 전문업체 지정·관리 • 사이버안보에 필요한 기술개발·산업육성·인력양성 등 필요한 시책 추진 • 사이버 공격 기도에 관한 정보를 제공하거나 사이버공격을 가한 자를 신고한 자에 대하여 포상금 지급 • 직무상 비밀을 누설한 경우 5년 이하의 징역 또는 5천만원 이하의 벌금. 	<ul style="list-style-type: none"> • 국가보안기술연구소를 '사이버안보 전략기술원'으로 승격 	<ul style="list-style-type: none"> • 사이버보안 기반조성을 위하여 연구·개발, 표준화, 인력양성, 인식 제고 • 국제협력 • 사이버보안 산업 지원을 위한 시범사업 및 정보통신기술융합에 따른 사이버보안 촉진 사업 추진 • 자율적인 사이버보안 활동 촉진

그렇다면 현재까지 국가 사이버안보 대응역량 관련 기본법제를 갖추지 못하게 된 이유는 무엇인가?⁶⁹⁾

첫째, 정보통신망법, 정보통신기반 보호법, 전자금융거래법, 국가정보화기본법이

69) 국회 정보위원회, 국가사이버안보법안【정부 제출】검토보고, 2017. 2. 10-11면.

존재하기 때문에 사이버 위협에 대한 대응법제는 충분하다는 것이다.

둘째, 사이버안보는 국가안보보다 넓은 개념으로 사이버분야의 안보를 명분으로 하여 국정원이 민간에 대한 감시권한을 확대될 수 있다는 것이다.

셋째, 사이버안보는 국정원법에서 규정하고 있는 국정원의 직무범위를 벗어난다는 것이다.

그러나 사이버범죄, 사이버테러를 포함하여 초국가적인 다양한 양상의 사이버안보 위협에 대응하기 위해서는 현재 개별 법률들로서는 부족한 것이 사실이다. 사이버안보는 국가안보보다 더 넓거나 좁은 개념의 문제가 아니라 국민안전과 밀접한 국가전략 문제가 되었다.

또한 현행 국가정보원법 제4조 제1항 제1호 마. 국제 및 국가배후 해킹조직 등 사이버안보 및 위성자산 등 안보 관련 우주 정보는 국가정보원의 업무로 명시되어 있다. 국정원의 국가 사이버안보 직무와 권한을 국가 사이버안보대응역량 차원에서 강화하는 문제와 권한남용의 문제는 함께 고려해야 마땅하다. 하지만 권한남용의 문제는 대통령실 국가안보실 등 통제장치와 법적 제재 장치를 충분히 갖추면 해결될 문제이지, 사이버안보기본법제의 입법 자체를 못할 절대적 이유는 되지 못할 것이다.

따라서 향후 국가사이보안보기본법제 제정추진에 있어서 특히 사이버공격에 대한 체계적 대응을 기획·조정할 컨트롤타워를 정하는 문제, 사이버공격 대응 책임기관, 지원기관, 수사기관의 권한과 직무 조정배분의 문제, 사이버위기대책협의기구의 설치와 운영문제는 사이버범죄, 사이버보안침해사고, 사이버테러를 포괄하는 「국가 사이버안보 대응역량 강화」 국정과제 차원에서 적극적으로 협의하여 결실을 맺어야 할 것이다.

제 5 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

경제안보와 국민안전을 위한 제도 및 정책 정비

경제안보와 국민안전을 위한 제도 및 정책 정비

제1절 | 사이버안보 민관 협력체계와 경제안보

세부과제 3 : 민관 합동 사이버협력체계 강화를 통해 핵심기술 보유기업·방산업체·국가기반시설 대상 위협과 공격 방지 및 대응조치를 적극 실행함으로써 경제 안보에 기여한다.

1. 경제안보와 사이버안보

일반적으로 '경제 안보'란 국가의 권력과 부(wealth)를 유지하기 위하여 국가적 자원, 재원 및 시장에 충분히 접근하고 활용할 수 있는 수준을 의미한다. 그런데 2000년대 이후 세계화 진전과 함께 글로벌 공급망 확대를 통해 국가간 상호의존성과 초연결성이 증대되면서 새로운 형태로 경제와 안보간의 연계가 강화되는 방향으로 진화하고 있다.⁷⁰⁾

특히 초연결성은 사이버공간의 형태와 민간기업 부문의 초국가적 영향력 확대의 양상으로 나타나고 있는 바, 사이버공격으로부터 국가기반시설과 민간기업 보호를 위해서는 현실 공간과 사이버공간, 민간부문과 정부의 협력이 필수적이다. 이는 사이버안보가 국가경제 안보의 차원에서도 핵심요소가 되었음을 의미한다.

70) 이효영, 경제안보 개념과 최근 동향 평가, 2022, 국립외교원 외교안보연구소, 3-5면.

2. 사이버안보와 민관협력

2019년 국가사이버안보전략에 따르면 민관협력의 중요성은 개인, 기업, 정부 간의 상호 신뢰와 협력을 바탕으로 민·관 영역을 포괄하는 미래지향적인 사이버안보 수행 체계를 확립한다는 데 있다. 이를 활성화하기 위한 방안은 다음과 같다. 71)

첫째, 정부를 비롯한 모든 이해당사자가 사이버안보에 대한 역할과 책임을 분담하고 상호 협력하는 거버넌스 체계를 정립한다.

둘째, 정부는 개인과 기업이 국가적 비전을 공유하고 자체 역량을 제고하여 각각의 역할과 책임을 다할 수 있도록 지원한다.

셋째, 사이버안보 전략·정책 및 관련 주요 이슈를 심층 연구하기 위한 국내외 전문가 협력 네트워크를 구축한다.

넷째, 민간분야 사이버안보 사각지대 해소를 위해 대응체계 개선, 유관기관간 공조체계 강화 및 지원기관의 인력·예산 확충을 추진한다.

다섯째, 공공분야의 자체 보안관리 체계 구축을 위해 전담조직 및 전문 인력을 확대하고 민간분야와 협력체계를 활성화한다.

여섯째, 국방분야 정보통신망에 대한 사이버위협에 능동적으로 대응하기 위하여 국방 사이버안보 수행체계를 개선한다.

일곱째, 민·관·군 협력체계를 강화하고 국가차원에서 사이버안보 정책을 발굴·추진하기 위해 국가안보실이 컨트롤타워 역할을 수행한다.

2017년 정부법안에 따르면, 국가·지방자치단체 및 기업은 사이버안보가 국가안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하여 사이버공간을 보호하도록 노력하여야 한다(안 제3조 제2항)고 규정하여 민관 합동 사이버협력체계의 중요성을 확인한 바 있다. 실제로 동 법안은 구체적으로 제8조(사이버안보 전문기업), 제9조(사이버안보 연구기관) 규정도 두었다.

새 정부 출범 이후 국가정보원의 경우 2022년 7월 사이버보안 정책 발굴 및 개선방안 마련을 목표로 '사이버 안보 민관 합동 협의체'를 구성하여, 높아진 국가 사이버안보 역량 강화를 위한 민관 협업에 착수하였다. 협의체에는 국정원 사이버안보센터를

71) 국가안보실, 국가사이버안보전략, 2019, 18면.

비롯, 국내 주요 전문가들이 참여하여, 클라우드, 암호기술, 보안인증 3개 분과로 구성된다. 향후 인공지능·5G 등 정보통신분야 최신기술과 관련된 분과도 추가 개설할 예정이다.⁷²⁾

제2절 | 디지털플랫폼 정부와 사이버안보

세부과제 4 : 사이버공격으로부터 안전한 ‘디지털플랫폼’ 정부를 구현한다.

디지털플랫폼정부는 모든 데이터를 연결하는 디지털 플랫폼 위에서 국민·기업·정부가 함께 사회문제를 해결하고 새로운 가치를 창출하는 정부를 의미한다.⁷³⁾

새 정부는 세계 최고의 디지털플랫폼 정부 구현을 위해 대국민 선제적·맞춤형 서비스 제공, 인공지능·데이터 기반의 과학적 행정 구현, 국민·기업·정부 협력을 통한 혁신 생태계 조성 등을 추진한다.

이를 위해 2022년 7월 대통령 소속 ‘디지털플랫폼정부위원회’가 설치되었다. 동 위원회는 ‘모든 데이터가 연결되는 세계 최고의 디지털플랫폼정부 구현’ (국정과제 11) 추진을 주로 담당하며, ‘편안한 국민, 혁신하는 기업, 과학적인 정부’를 목표로 5대 중점 추진과제를 선정해 추진해 나간다. 그 구체적 계획은 다음과 같다.⁷⁴⁾

첫째, 국민과 기업이 단기간에 개선효과를 체감할 수 있는 혁신적 선도프로젝트를 추진한다.

둘째, 누구나 쉽게 한 번에 이용할 수 있도록 기관 간 정보 공유 확대 등을 통한 선제적 서비스를 제공한다.

셋째, 인공지능·데이터 기반 정책 의사결정 지원체계 구축, 정부의 일하는 방식

72) “국가정보원, 사이버안보 민관 합동 협의체 발족” 연합뉴스 2022년 7월 28일.

73) 디지털플랫폼정부위원회의 설치 및 운영에 관한 규정(대통령령 제32750호, 2022. 7. 1., 제정) 제1조 : 인공지능 등의 기술을 활용하여 다양한 데이터를 통합·연계 및 분석하는 디지털플랫폼을 기반으로 국민·기업 및 정부가 함께 사회문제를 해결하고 새로운 가치를 창출하는 정부를 구현한다.

74) 대한민국 정책브리핑, “세계 최고의 디지털플랫폼 정부 구현…혁신 생태계 조성한다” (<https://www.korea.kr/news/policyNewsView.do?newsId=148902945>)

혁신, 국가 현안·난제 해결을 위한 민관 협업을 활성화한다.

넷째, 정부는 데이터·핵심 기능을 플랫폼으로 제공하고, 민간이 창의적 서비스를 창출할 수 있는 혁신 생태계를 조성한다.

다섯째, 활용과 보안을 제고할 수 있는 새로운 보안체계 구축, 개인정보의 안전한 활용 기반을 강화하여 대국민 신뢰를 높인다.

이를 뒷받침하기 위해 2022년 7월 대통령령으로 디지털플랫폼정부위원회의 설치 및 운영에 관한 규정이 제정되었다.⁷⁵⁾ 그 주요내용은 다음과 같다.

첫째, 디지털플랫폼정부 실현을 위한 주요 정책 등에 관한 사항을 효율적으로 심의·조정하기 위하여 대통령 소속으로 디지털플랫폼정부위원회를 둔다. (제2조)

둘째, 위원회는 디지털플랫폼정부 구현을 위한 기본 방향, 국가전략의 수립·변경 및 시행, 중앙행정기관, 지방자치단체 및 공공기관의 주요 정책과 사업의 조정·평가 및 지원, 정책 추진상황 점검, 디지털 혁신 산업 기반 조성을 위한 민간·정부 간 협업과 민간 참여 활성화, 핵심 인프라 구축 및 운영, 정부의 일하는 방식 혁신에 관한 사항, 인공지능과 데이터를 활용한 과학적 정책의사결정 지원 등 디지털 국정 관리·운영, 혁신적인 공공서비스 제공, 데이터의 개방·연계·활용과 기술적 처리, 규제혁신, 법령의 제정·개정과 제도의 개선, 예산 등의 확보, 공무원 및 국민의 디지털 역량 강화, 안전한 개인정보 활용 등 안전성·신뢰성 확보, 교육·연구·조사 및 모니터링, 차별 없는 디지털플랫폼정부 서비스 제공을 위한 환경의 조성, 디지털플랫폼정부 구현에 따라 발생하는 문제의 예방 및 해결, 국민 공감대 형성과 활용 확산, 디지털플랫폼정부 구현을 위한 국제협력 및 해외진출에 관한 사항을 심의·조정한다. (제2조)

셋째, 위원회는 위원회의 업무를 전문적으로 수행하기 위하여 필요한 경우 분야별 분과위원회를, 또한 디지털플랫폼정부 구현에 관한 사항을 전문적으로 검토하기 위하여 관계 전문가로 구성된 자문단을 설치·운영할 수 있다. (제8조)

넷째, 위원회는 위원회의 업무를 수행하기 위하여 필요한 경우에는 관계 전문가의 의견을 듣거나, 관계 행정기관이나 그 밖의 기관·법인·단체 등에 자료 제출 또는 의견 제시 등의 협조를 요청하거나, 조사나 연구를 의뢰할 수 있고, 설문조사, 공청회 및 세미나 개최 등을 통하여 여론을 수렴할 수 있다. (제11조)

75) 대통령령 제32750호, 2022. 7. 1., 제정

정리하면, 디지털플랫폼 정부 구현에 있어서 사이버공격으로부터의 안전은 기본적인 토대가 된다. 물론 디지털플랫폼 정부 중점추진과제 중에 새로운 보안체계 구축도 포함되어 있어, 사이버보안체계 구축의 중요성도 더욱 높아지게 될 것이다. 궁극적으로 디지털플랫폼 정부의 사이버안전 확보는 디지털플랫폼 정부에 대한 국민 신뢰 제고의 관건이기도 할 것이다.

제3절 | 정보통신환경의 안전과 국민안전

세부과제 5 : 클라우드·스마트그리드 등 국민 생활에 밀접한 IT 환경의 안전성을 확보한다.

스마트그리드는 기존의 전력계통에 다양한 ICT기술을 접목시켜서 에너지 효율을 최적화하여 전력소비를 줄이고 효율적인 전력관리를 달성하는 것을 목적으로 한다.

일찍이 2010년 우리 정부는 「스마트그리드 국가로드맵」을 제시한 바 있다. 이는 2009년 제1차 녹색성장위원회 국가단위의 스마트그리드 구축계획의 성과다.⁷⁶⁾

이와 함께 2009년 8월 한국 스마트그리드 사업단이 구성되어 그린에너지 기술혁신

76) 산업통상자원부, 보도자료:스마트그리드 국가로드맵 확정 (2010.1.25.) 스마트그리드 국가로드맵의 주요내용은 ‘스마트그리드 구축을 통한 저탄소 녹색성장 기반 조성’을 비전으로 설정하고, 시범도시·광역시도 등 ‘先거점구축, 後확산전략’에 따라 2030년까지 국가단위의 스마트그리드 구축완료율 목표를 한다. 이를 위해 지능형 전력망, 소비자, 수송, 신재생, 서비스 등 5대 분야에 대한 단계별 기술개발 및 비즈니스 모델을 제시한다. 스마트그리드를 수출전략산업으로 육성하기 위한 정책과제 중에는 전기차 충전인프라 구축계획과 스마트그리드 특별법 제정 계획이 포함된다. 즉 정부는 전기차 보급대수에 맞추어 충전소를 ‘11년에 시범도시 200대를 시작으로 ’30년까지 27,000여대를 구축한다. 또한 기업의 속도감 있는 비즈니스 모델 개발을 제도적으로 지원하기 위해 “(가칭) 지능형 전력망 구축 및 지원에 관한 특별법”을 제정한다는 것이다. 정부는 스마트그리드의 성공적인 추진을 위해서는 민간 공동분담을 통해 ‘30년까지 총27.5조원이 소요될 것’이라고 전망하면서, 정부의 분담액은 2.7조원으로 초기에 핵심기술 개발 및 신제품 시장창출 지원, 공공인프라 구축에 지원하고, 기술개발 및 시장의 성숙도에 따라 단계적으로 지원을 감소하는 방향으로 추진한다는 것이다. 스마트그리드가 성공적으로 구축되는 2030년이 되면 총2억3천만톤의 온실가스 감축(누적치), 5만개의 일자리(연평균) 및 74조원의 내수창출(누적치)이 기대되며, 에너지 이용 효율 향상에 따라 47조원의 에너지 수입 비용(석유 4.4억배럴 상당, 누적치)과 3조2천억원의 발전소 투자비용(발전량 5,817MW 상당)도 절감될 것으로 전망하였다.

을 통한 신 성장동력 육성과 저탄소 녹색사회 구현을 위해 2030년까지 세계 최초로 국가단위의 스마트그리드 구축을 목표로 운영되고 있다. 또한 스마트그리드에 적용되고 있는 IT기술 중에 최근 주목받는 클라우드 컴퓨팅기술은 기존 IT자원을 크게 줄이면서 컴퓨팅기술의 효율을 개선할 수 있기 때문에 적극적인 활용이 필요하다.⁷⁷⁾

그런데 클라우드 제공자의 플랫폼을 이용하기 때문에 사이버 보안대책이 중요한 과제가 된다. 스마트 그리드의 다양한 활용 가능성에도 불구하고 구조적 특징과 상호운용성 표준의 부재로 인해 신뢰적인 인증이 보장되지 않으면, 네트워크의 신뢰성을 약화시키는 요인으로 작용하며, 보안 문제가 초래되기 때문이다.

따라서 안전한 IT 환경 확보 차원에서 정부가 스마트그리드 및 클라우드 관련 표준 제정과 관련 정책을 수립하여, 안전한 데이터 통신을 위한 보안 메커니즘을 구축해야 한다.⁷⁸⁾

77) 스마트 전력그리드 및 클라우드 컴퓨팅

(<https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=KAR2013066510>)

78) 이협건 외, 클라우드 기반 스마트 그리드 환경에서의 보안 이슈, 한국정보처리학회:학술대회논문집, 2010

제 6 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

사이버안보 기술 및 전문인력 확보를 위한 제도 및 정책 정비

제6장

사이버안보 기술 및 전문인력 확보를 위한 제도 및 정책 정비

제1절 | 사이버안보 기술역량의 고도화

세부과제 6 : 産·學·研·官 협력 아래 AI·양자통신 등 신기술 위협 대응 新기술 연구·개발을 적극 지원하여 사이버공격 탐지·차단·추적 시스템을 고도화한다.

2020년 제2차 정보보호산업 진흥계획⁷⁹⁾에 따르면 디지털 전환에 따른 정보보호 신시장 창출, 민간의 사이버 복원력 확보를 위한 정보보호 투자 확대, 지속 성장 가능한 정보보호 생태계 조성을 위한 과제가 중점 추진된다. 특히 '사이버 복원력'이란 사이버 공격에 의한 시스템이나 서비스의 피해를 최소화하고 장애 또는 사고가 발생하기 이전 상태로 혹은 그에 준하는 상태로 신속하게 돌아가려는 역량을 뜻한다.

이를 위해 ICT융합 제품·서비스에 대한 정보보호 강화를 위한 근거 마련 및 협력, 체계 구축을 위한 정보통신망법, 정보통신기반보호법 등 개정, 인공지능, 사물인터넷 등 보안 강화를 위한 관련 법 개정 및 개별법의 정보보호 기능 강화·연계를 위한 정보보호기본법 제정 등 정보보호 신산업 육성을 위한 법제 개선이 과제다. 즉 지능정보서비스 보안(지능정보화기본법), 5G+ 융합서비스 보안(정보통신망법), SW 개발보안(소프트웨어진흥법) 등에 따라 정보보호 기술개발 및 사업화 지원을 위한 법제를 개선하고, ICT융합 환경변화에 대응하여 현행 정보통신망법 등 정보보호법제를 정보보호 기본법을 중심으로 체계화하는 것이다. 사이버보안산업활성화와 관련해서는 융합

79) 과학기술정보통신부, 보도자료 2020년 7월 1일

산업별 보안정책 추진 협력체계 구축과 실무조직 운영을 통한 산업별 보안 강화가 목표다. 사이버보안 투자를 확대하고, 보안 인력·기술 경쟁력 강화를 위해 실전형 사이버훈련장 및 전문 교육과정 확대 운영, 사이버보안 R&D 예산 확대 추진이 과제다. 보안기업 성장환경 조성을 위해서는 정보보호 클러스터 운영 내실화, 우수제품 개발 기술지원 강화 및 맞춤형 수출 지원사업 추진이 과제다.

産·學·硏·官 협력을 기반으로 사이버공격 탐지·차단·추적 시스템을 고도화하기 위해서는 민간부문과 정부 모두 정보보호 투자 확대를 통해 안전 확보가 우선되어야 한다는 인식을 갖추어야 하며, 인공지능 기반의 신기술 개발과 클라우드 서비스 전환 등 경쟁력 확보를 위해 민관협력이 뒷받침되어야 한다.

제2절 | 사이버안보 전문인력 양성

세부과제 9 : 대학·특성화 교육 확대, 지역별 교육센터 설치 등 ‘10만 인재 양성’ 프로그램을 실행한다.

본 과제는 국정과제「세계 최고 네트워크 구축 및 디지털혁신 가속화」(국정과제 78) 내용 중 사이버보안 역량 강화를 위한 10만 사이버보안 인재 양성 추진과도 연결된다.

사이버공격 대응, 사이버보안 유지, 사이버전 수행, 사이버범죄 대처의 핵심 기반은 장비나 기술보다 전문인력임은 물론이다. 따라서 사이버안보 전문인력 양성은 국가적 차원에서 중장기정책 프로그램으로서 중점 추진되어야 할 것이다. 2019년 국가 사이버안보전략 수립 이후 과기정통부는 산학연 협업 기반 창업 환경 조성 및 해외진출 지원을 추진하였다. 특히 산학연 협업과 관련한 정부의 지원정책은 사이버공격과 범죄 대응 전문인력 양성에 중점을 두어야 할 것이며, 사이버보안 분야 창업환경조성과 해외진출지원 또한 중장기적으로 전문인력을 확충하고 전문가역량을 증진하는 정책 프로그램이 체계적이고 지속적으로 운영될 필요가 있다. 대통령도 7월 제11회 ‘정보보호의 날’ 기념식에서 대학과 대학원의 사이버 전공 과정을 확대하고 최정예 개발인

력과 화이트 해커 육성체계를 통해 10만 인재를 양성하겠다고 밝힌 바 있다.⁸⁰⁾

그리고 「초격차 전략기술 육성으로 과학기술 G5 도약」(국정과제 75)에 따르면, 경제성장과 안보 차원에서 주도권 확보가 필수적인 전략기술 중 하나로서 사이버보안을 지정하였다. 전략기술로서 초격차 선도 및 대체불가 기술확보를 목표로 집중 육성을 추진하기 위해 정부출연연구기관을 전략기술 임무해결을 선도하는 핵심연구거점으로 지정하여 산학연과의 협동·융합연구 활성화를 추진하는 방안 역시 국정과제의 내용으로 포함되어 있다.

특히 사이버범죄 대응을 위해서는 새로운 사이버범죄 유형과 범위에 선제적으로 대비하여야 하며, 사이버인프라의 발달과 함께 사이버범죄는 더욱 지능화되고 범죄대상에 따라서 첨단화·전문화 되고 있으므로, 사이버범죄 대응기법과 수단도 이에 대응한 연구개발이 필수적이다. 전자공격을 위한 EMP 공격(Electromagnetic Pulse attack) 방호시설 구축, 전파교란을 위한 GPS(Global Positioning System), 전자교란, 통신재밍, 양자 암호화(Quantum Cryptography)와 같은 고기밀성의 암호장비, 해킹 역추적 기술, 사이버공격의 원점지 식별 및 타격, 해외 국가 사이버범죄정책과 기법 수집 및 분석 등 전문적이고 경험적인 전문기술을 개발하고, 실무운용할 수 있도록 대비해야 할 것이다.⁸¹⁾ 나아가 정보통신기술의 발전과 사이버공간 확대에 따라 4차산업혁명의 인공지능, 사물인터넷, 무인이동수단 등 첨단기술을 활용하기 위한 기술 연구개발에 필요한 예산과 조직 확보가 적극 고려되어야 한다.

그리고, 사이버보안 인재양성과 정부출연연구기관의 협동·융합연구 활성화 과제 외에 국정과제 추진과정에서 한가지 더 고려할 점이 있다. 이제까지 사이버안보와 관련한 정부부처의 핵심사업들은 국가보안기술연구소, 한국인터넷진흥원, 한국전자통신연구원, 국방과학연구소 등 정부출연연구기관 중심으로 정보보호 관련 대학교, 업체 등과 협업을 통해 내부 네트워크 안에서만 진행되어 왔다. 필요하고 가능한 범위에서 관련 정보는 국민에게 공개돼 사이버안보의 주체로서 인식하고 활동할 수 있도록 정책적 고려가 필요하다. 이러한 국민인식 제고에 있어서 정부출연연구기관은 연구성과확산과 대국민정보서비스의 역할도 담당할 수 있을 것이다.

80) 동아일보 2022년 7월 13일자.

81) 함승현·박대우, 국가 사이버안보를 위한 정책 연구, 한국정보통신학회논문지 Vol. 21, No. 9, 2017, 1670면.

이는 국가적 차원에서 사이버안보 체계와 사이버침해 및 범죄 대응역량 확대강화 정책의 일차적 과제는 국민 기본권, 특히 프라이버시와 정보인권 침해 위험에 대한 우려에 효과적으로 대응해야 한다는 것이기 때문이다. 사이버안보 관련 국내 정책추진과 국제협력과 규범체계 참여는 무엇보다도 국민의 자유와 인권보장을 명분으로 하는바, 오히려 국민 인권을 침해하거나 침해 우려를 낳는 결과가 된다면 그 자체 모순이 아닐 수 없다. 따라서 사이버안보 대응 역량강화와 국민기본권 보장의 바람직한 균형점을 모색하기 위해서는 관련 정보의 공유와 국민참여를 통해 국민인식과 신뢰도를 개선하는 정책적 노력이 필요할 것이며, 이러한 노력에 있어서 인재양성과 연구 활성화 못지 않게 국책연구기관의 역할이 정책적으로 중요하게 고려되어야 마땅하다.

제3절 | 사이버전 대비 강화

세부과제 10 : ‘사이버 예비군’ 운영 등 사이버戰 인력을 확보한다.

사이버전은 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 초래할 수 있는 총체적인 가상 공간에서의 정보마비전을 추구하는 전쟁수행 방식이다. 사이버전쟁은 사이버 타격/방어전, 물리연계전, 사이버 첩보전, 사이버심리전의 유형으로 구분된다.⁸²⁾

2011년 이래 사이버전의 기획, 계획, 시행, 연구·개발 업무를 국군사이버사령부가 담당해 오고 있다. 국군사이버사령부는 국방 사이버전의 기획 및 계획 수립, 사이버전의 시행, 사이버전 전문인력의 육성과 기술 개발, 사이버전 유관기관 사이의 정보 공유 및 협조체계 구축 임무를 수행한다.⁸³⁾ 2019년 국가 사이버안보전략 수립 이래 국방부는 사이버전 대비 군사전략·전술 개발, 사이버전 능동대응기술 및 다단계 다중

82) 박찬수·박용석, 사이버전의 개념과 대응방안에 관한 연구, 한국정보통신학회 2014 추계종합학술대회 자료집, 2014

83) 국군사이버사령부령 [대통령령 제26101호, 2015. 2. 16., 일부개정] 제2조

위협 대응체계 확보와 관련하여 군 사이버전술훈련장 구축, 군 사이버 인력 교육체계 정립, 서울안보대화 사이버워킹그룹 운영, 전군 사이버안보 소양 교육 강화를 추진해 왔다.

2020년 미국 국방부 보고서에 따르면 북한의 사이버전 전력의 수준과 능력은 세계적 수준에 달해 있다. '121국'으로 알려진 북한 사이버전 지도국에서 대부분의 사이버 작전을 관할한다. 121국에는 약 6천 명의 사이버 요원이 있으며, 대부분은 대부분 벨라루스와 중국, 인도, 말레이시아, 러시아 등 해외에서 활동한다. 또한 적 전산망에 대한 감시와 취약점을 분석하는 약 1천600명의 해커로 이뤄진 안다리엘 그룹, 주로 금융 사이버 범죄를 수행하는 1천700명 규모의 블루노로프 그룹, 2016년 워너크라이 멀웨어로 미국을 포함해 전 세계를 상대로 공격을 펼친 라자루스 그룹도 121국 소속이다. 121국 산하 부대에서 탈취한 정보가 전투 부대에 하달되거나, 적 전산망 공격으로 전투 현장의 적을 무력화시킴으로써 사이버 영역과 전투 현장이 유기적으로 운용될 수 있다. 특히 121국 산하 '전자전 재밍연대(Electronic Warfare Jamming Regiment)'는 전파방해 부대가 2000년부터 한국과 미국의 통신과 레이더 체계에 대한 전자 체계를 교란하는 작전을 수행해 왔다.⁸⁴⁾ 2019년 미국 사이버보안 전문기관 Technolytics에 따르면, 북한 해커들의 네트워크 침투 능력이 러시아 다음으로 강력하다.⁸⁵⁾

또한 2019년 유엔 전문가 패널 보고서(2019 final report of the UN Panel of Experts investigating North Korean violations of UN sanctions)에 따르면, 북한의 사이버 공격 능력은 세계 최상위 수준이다. 북한이 사이버공격으로 20억 달러의 불법 수익을 올린 것으로 조사됐다.⁸⁶⁾

따라서 북한·러시아 등 주변 국가의 사이버전 능력 고도화와 전력 증강에 맞서

84) "미 국방보고서 북한 사이버·전자정보전 역량 일선 부대서도 운용"

(https://www.voakorea.com/a/korea-korea-politics_norkor-cyber-combat-capabilities/6036846.html 2022년 8월 15일 최종검색)

85) 권호천, 북한의 사이버전 전력 증강

(http://it.chosun.com/site/data/html_dir/2022/05/11/2022051102645.html 2022년 8월 15일 최종검색); "유엔 보고서 北 핵개발 가속화...가상화폐 해킹으로 600억원 훔쳐"

(<https://m.hankookilbo.com/News/Read/A2022020609000003401> 2022년 8월 15일 최종검색)

86) 2019 final report of the UN Panel of Experts Established Pursuant to Resolution 1874 (2009), investigating North Korean violations of UN sanctions, S/2019/171 (2019.3.5.) 48면 이하.

80 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

사이버전 역량을 강화하기 위해서는 전문인력 확보가 최우선 정책으로 추진되어야 할 것이다.

그런 점에서 북한에 비해 열세인 사이버전 인력문제 극복을 위해 2015년 국방부는 사이버 예비군의 창설을 검토한 바 있다. 사이버 예비군 대상은 사이버전을 수행해 온 전역 군인으로 구성될 수 있다. 미국의 경우 국토안보부에서 보안기술 전문가를 확보하기 위한 방안으로 사이버 예비군 제도를 제시한 바 있고, 영국은 합동사령부 내에 사이버 방어 담당 조직인 사이버 예비군을 운영하고 있다.⁸⁷⁾

대통령도 7월 제11회 ‘정보보호의 날’ 기념식에서 대칭 전력과 비대칭 전력의 ‘하이브리드전(戰)’으로 변모하는 전쟁 양상에 대응하기 위해 사이버 전력과 기술을 고도화해야 한다고 지적하였다. 이에 따라 군 전문분야 복무와 전역 후 취업과 창업을 연계하는 ‘사이버 탈피오트(Talpiot)⁸⁸⁾와 국가 비상 상황에서 민·관의 역량을 결집하기 위한 ‘사이버 예비군’ 창설 의지를 밝힌 바 있다.⁸⁹⁾

87) 엄정호, 사이버전을 대비한 사이버 예비군 운영 방안, 보안공학연구논문지 44호, 보안공학연구지원센터, 2015, 122면.

88) 이스라엘 군의 인재육성 프로그램 명칭으로서 ‘성취의 정점’을 의미한다. 1979년 제4차 중동전쟁 이후 군은 위기관리에 적극 대처하기 위해 탈피오트 인재양성 프로그램을 시작했다. 탈피온(Talpiot)이라 불리는 인재들은 학업성적뿐 아니라 인성·지도력·협동심, 사고력을 키우기 위해 고강도의 문제해결식 교육을 받게 된다. 이스라엘이 방위산업, 특히 사이버보안 분야에서도 인공지능(AI)을 앞세워 앞서갈 수 있는 이유다. (손영동, “스타트업”과 “탈피오트”, 사이버 강국 이스라엘의 키워드, 중앙일보 2017년 8월 8일)

89) 동아일보 2022년 7월 13일자.

제 7 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

사이버안보 국제협력강화를 위한 제도 및 정책 정비

제7장

사이버안보 국제협력강화를 위한 제도 및 정책 정비

제1절 | 국가사이버안보 역량강화정책으로서 국제규범 수립 참여

세부과제 7 : 사이버안보 국제공조 활성화 차원에서 국제사회의 사이버규범 수립에 적극 참여한다.

1. 유럽평의회 사이버범죄 협약의 의미와 내용

사이버범죄에 대한 효율적인 국제공조 방안으로서 유럽평의회(Council of Europe) 주도로 2001년 유럽 사이버범죄 방지 협약(Convention on Cybercrime) (일명 '부다페스트협약')이 제정되어 2021년 현재 유럽 국가들을 비롯하여 전 세계 65개국이 비준하였는데,⁹⁰⁾ 우리나라는 줄곧 가입검토단계에 머물러 있다가, 2022년 8월 현재 곧 가입 신청 가능성이 높다.

가. 국제수사공조 대상 사이버범죄 규정

- 불법접속(제2조)
- 불법감청(제3조)
- 데이터 침해(제4조)
- 시스템 방해(제5조)
- 장치의 오용(제6조)

90) <https://www.coe.int/en/web/cybercrime/the-budapest-convention>(2022년 8월 15일 최종검색)

84 「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

- 컴퓨터를 이용한 위조(제7조) 및 사기(제8조)
- 아동성착취물 관련 범죄(제9조)
- 저작권 및 저작인접권 침해(제10조)

나. 사이버범죄 관련 전자적 증거수집 관련 절차규정

- 저장된 컴퓨터데이터가 손괴 또는 변경될 수 있다고 판단될 경우 이를 보존하도록 강제하는 권한을 수사기관에 부여(제16조)
- 수사기관이 사이버범죄의 통신경로 확인을 위하여 다수의 인터넷서비스제공자(ISP)에게 인터넷 접속기록 등의 통신데이터에 대한 신속한 보존명령을 내리고 충분한 통신데이터를 제출받을 수 있도록 권한 부여(제17조)
- 협약당사국 수사기관에게는 자국 내 사람에게 컴퓨터시스템이나 저장매체에 저장되어 있는 컴퓨터 데이터를 제출하도록 명령하고, 인터넷서비스제공자에게 가입자정보를 제출하도록 명령할 수 있는 권한 부여(제18조)
- 수사기관은 저장되어 있는 컴퓨터데이터에 대하여 수색과 압수를 할 수 있어야 함.(제19조)
- 수사기관은 신속한 수사 및 증거자료 수집을 위해 인터넷 접속기록 등 통신데이터를 실시간으로 수집하거나 인터넷서비스제공자에게 수집할 의무 부과(제20조).
- 중대한 범죄와 관련될 때에는 수사기관이 통신데이터뿐만 아니라 실제 이용자의 통신내용데이터(콘텐츠 데이터)를 실시간으로 수집하거나 인터넷서비스제공자에게 수집할 의무를 부과할 수 있도록 권한 부여(제21조)

다. 사이버범죄 국제공조와 관련 규정

- 당사국 법에 따라 최소 1년 이상의 구금형 또는 그 이상의 중범죄인 경우 범죄인 인도(제24조)
- 형사사법공조의 일반원칙(제25조)
- 자발적 정보제공(제26조)
- 사법공조의 요청국과 피요청국 간에 별도의 국제협약이 없는 경우에 대한 사법공조 요청절차(제27조)
- 피요청국이 요청국의 요청에 따라 정보 또는 자료를 제공할 때 비밀유지 및 사용제한의 조건을 부가(제28조)
- 협약당사국이 다른 협약당사국에게 저장된 컴퓨터데이터의 신속한 보존을 요청(제29조)
- 통신데이터의 전달 요청.(제30조) 피요청국은 요청 사유가 정치범죄와 관련되거나 통신데이터의 제공이 자국의 주권, 안보, 공공질서 등을 침해할 가능성이 있다고 판단할 경우 거절가능.

유럽평의회 사이버범죄협약 주요 규정을 요약 정리하면 다음과 같다.

▶▶ [표 7-1] 사이버범죄 처벌 및 수사관련 주요 규정

처벌	전자증거	국제공조
<ul style="list-style-type: none"> ① 불법접속(제2조) ② 불법감청(제3조) ③ 데이터 침해(제4조) ④ 시스템 방해(제5조) ⑤ 장치의 오용(제6조) ⑥ 컴퓨터를 이용한 위조(제7조) 및 사기(제8조) ⑦ 아동성착취물 관련 범죄(제9조) ⑧ 저작권 및 저작권접권 침해(제10조) 	<ul style="list-style-type: none"> ① 저장된 컴퓨터데이터가 손괴 또는 변경될 수 있다고 판단될 경우 이를 보존하도록 강제하는 권한을 수사기관에 부여(제16조) ② 수사기관이 사이버범죄의 통신행로 확인을 위하여 다수의 인터넷서비스제공자(ISP)에게 인터넷 접속기록 등의 통신데이터에 대한 신속한 보존명령을 내리고 충분한 통신데이터를 제출받을 수 있도록 권한 부여(제17조) ③ 협약당사국 수사기관에게는 자국 내 사람에게 컴퓨터시스템이나 저장매체에 저장되어 있는 컴퓨터데이터를 제출하도록 명령하고, 인터넷서비스제공자에게 가입자정보를 제출하도록 명령할 수 있는 권한 부여(제18조) ④ 수사기관은 저장되어 있는 컴퓨터데이터에 대하여 수색과 압수를 할 수 있어야 함.(제19조) ⑤ 수사기관은 신속한 수사 및 증거자료 수집을 위해 인터넷 접속기록 등 통신데이터를 실시간으로 수집하거나 인터넷서비스제공자에게 수집할 의무 부과(제20조). ⑥ 중대한 범죄와 관련될 때에는 수사기관이 통신데이터뿐만 아니라 실제 이용자의 통신내용데이터(콘텐츠 데이터)를 실시간으로 수집하거나 인터넷서비스제공자에게 수집할 의무를 부과할 수 있도록 권한 부여(제21조) 	<ul style="list-style-type: none"> ① 당사국 법에 따라 최소 1년 이상의 구금형 또는 그 이상의 중범죄인 경우 범죄인 인도(제24조) ② 형사사법공조의 일반원칙(제25조) ③ 자발적 정보제공(제26조) ④ 사법공조의 요청국과 피요청국 간에 별도의 국제협약이 없는 경우에 대한 사법공조 요청절차(제27조) ⑤ 피요청국이 요청국의 요청에 따라 정보 또는 자료를 제공할 때 비밀유지 및 사용제한의 조건을 부가(제28조) ⑥ 협약당사국이 다른 협약당사국에게 저장된 컴퓨터데이터의 신속한 보존을 요청(제29조) ⑦ 통신데이터의 전달 요청.(제30조)

2. 일본의 협약 가입 및 국내이행 사례

일본의 협약 가입 및 이행 입법 사례를 비교해 보면, 일본 정부는 2001년 협약 서명, 2004년 국회 비준에 이어 2011년 협약 이행을 위한 형법 및 형사소송법 개정을 완료하였다.⁹¹⁾

개정법에 따르면, 부정지령 전자적 기록작성죄 신설(형법 제168조의 2, 제168조의 3), 음란물반포 구성요건 확대(형법 제175조 개정), 봉인 등 파기죄 처벌대상 확대(형법 제96조 개정), 강제집행방해죄 처벌대상 확대(형법 제96조의 2 개정, 제96조의 3 신설), 직업적 강제집행방해자 대상 규정(형법 제96조의 5 신설)이 정비되었다. 협약 제6조의 장치오용죄와 관련하여 전자계산기 손괴 등 업무방해의 미수범 처벌 규정 신설(형법 제234조의2 제2항), 종래 소유자의 동의 없이 서버 컴퓨터 자료를 복사 또는 저장매개체를 압수하거나 원격지의 컴퓨터 안에 저장되어 있는 자료의 압수는 허용되지 않았으나, 개정을 통하여 협약 제18조 및 제19조 이행입법이 조치된 것이다.

또한 전자통신회선으로 접속하고 있는 기록매체로부터의 복사(형사소송법 제99조 개정), 기록명령부 압류(형사소송법 제99조의 2 신설), 전자적 기록에 관련한 기록매체 압류 집행방법 정비(형사소송법 제110조의 2 신설), 통신이력의 전자적 기록 보존요청 규정 정비(형사소송법 제197조 개정)가 이행입법조치 내용이다.

3. 한국의 협약 가입 필요성

그렇다면, 한국의 가입 필요성에 대하여 긍정적 검토 논거⁹²⁾는 다음과 같다.

첫째, 사이버범죄는 국경의 한계를 넘어 빠르게 확산될 수 있다는 특징이 있어 협약을 통한 국제공조의 필요성이 인정된다.

91) 이범룡, 사이버 범죄 조약과 일본의 법안 정비, CLIS Monthly, 2003(4), 정보통신정책연구원, 2003, 39-41면.; 김영란, 사이버범죄조약 대응을 위한 일본의 형사법개정안 연구, 외국경찰동향, 경찰대학, 2010, 381-419면.

92) 긍정적 입장의 문헌으로는 김한균·김성은·이승현, 「사이버범죄방지를 위한 국제공조방안 연구 - 유럽사이버범죄방지협약을 중심으로」, 대검찰청 연구보고서, 2008; 신용우, 「유럽 사이버범죄 방지 협약」 체결 현황과 우리나라의 입법·정책적 대응방향, 국회입법조사처, 2020; 윤해성·라광현, 사이버범죄협약(일명 '부다페스트' 조약) 가입을 위한 선결과제, 가천법학, 제40호, 2019; 이창수, "초국가적 사이버범죄에 대한 국제공조 활성화방안과 그 선결과제," 형사법의 신동향 21, 대검찰청, 2009

둘째, 우리나라는 개별국가들과 형사사법공조 협약을 맺고는 있으나 자국의 이해관계가 큰 관련성이 없는 경우 타국 수사기관의 적극적 공조가 쉽지 않고 많은 시간이 소요되는 것이 현실이므로 협약 가입이 필요하다.

셋째, 협약상 통신데이터 또는 통신내용데이터의 실시간 수집 관련규정은 사이버범죄수사·소추·재판절차를 위한 조치로 한정하고 있어 개인정보 및 정보주권 침해가 일부의 우려만큼 크지는 않다.

넷째, 협약으로 인하여 기업의 자료제출 의무를 법제화하면 자료제출로 발생할 수 있는 기업의 민형사상 책임이 면책될 수 있으며, 사이버수사 활성화로 인한 범죄감소·예방으로 인터넷서비스제공자가 간접적으로 혜택을 받을 수도 있다.

이에 반해 가입에 신중해야 한다는 검토입장의 논거⁹³⁾는 다음과 같다.

첫째, 협약은 통신데이터 또는 통신내용데이터의 실시간 수집 등을 의무화하고 있어 개인의 사생활 보호를 침해할 우려가 있다.

둘째, 협약에 따라 광범위하게 정보를 수집하고 제출명령에 응하기 위하여 인터넷서비스제공자의 정보저장시설 및 관리인력 증가로 경제적 부담이 초래될 수 있다.

셋째, 국내 정보자산을 다른 국가에서 접근할 수 있어 국가안보에 영향을 줄 수 있다.

4. 협약 가입을 위한 검토과제

결론적으로 긍정론의 장점과 신중론의 단점을 종합적으로 고려하여 가입 여부를 판단하되, 가입에 뒤따라 국내법제 정비과제도 함께 검토해야 할 것이다.⁹⁴⁾

첫째, 협약 제6조의 장치의 오용과 관련하여 현행법상 불법감청 목적 등의 컴퓨터프로그램 제조 등에 대한 처벌규정, 감청데이터의 판매, 유포 등의 행위 처벌규정 신설이 필요하다.

93) 신중론 입장의 문헌으로는 신용우, 「유럽 사이버범죄 방지 협약」 체결 현황과 우리나라의 입법·정책적 대응방향, 2020:박희영 외, 사이버범죄협약 이행입법연구, 대검찰청, 2015; 전현욱·이자영, 사이버범죄협약과 형사절차상 적법절차원칙 : 저장된 데이터의 보존 및 일부 공개를 중심으로, 형사정책연구 25(2), 한국형사정책연구원, 2014

94) 신용우, 「유럽 사이버범죄 방지 협약」 체결 현황과 우리나라의 입법·정책적 대응방향, 2020, 5-6면.; 김상배 외, 디지털 경제 시대를 위한 미래 국가인터넷 전략 연구, 한국인터넷진흥원, 2021, 64-65면.

둘째, 협약 제12조는 협약을 위반한 자연인이 속한 법인의 법적 책임을 정하고 있는데, 협약 제7조와 제8조의 컴퓨터 관련 위조·사기 범죄에 대응하는 양벌규정 신설이 필요하다.

셋째, 협약 제16조의 컴퓨터데이터 보존과 관련하여 데이터가 쉽게 삭제될 수 있다는 휘발성을 고려하여 형사소송법상 별도의 보존명령 신설이 필요하다.

넷째, 협약 제17조의 통신데이터 보존 및 일부 제출과 관련하여 범죄수사를 위한 통신사실 확인자료제공 절차(통신비밀보호법 제13조), 전기통신사업자의 협조의무 및 통신사실확인자료의 제공·보관의무(제15조 의2와 동법 시행령 제41조)를 규정하고 있는데, 통신비밀보호법상 통신사실확인자료는 협약에서 규정하는 통신데이터와 일치하지 않아 보완이 필요하다.

다섯째, 협약 제18조의 컴퓨터데이터 제출명령과 관련하여 통신사실 확인자료제공 절차(통신비밀보호법 제13조) 보완 필요하고, 가입자정보 제출명령과 관련하여 통신자료 제공 규정(전기통신사업법 제83조제3항)은 강제적 조치 보완이 필요하다.

여섯째, 협약 제19조제2항은 압수·수색 대상자의 컴퓨터 시스템에서 정보통신망으로 연결된 다른 컴퓨터 시스템에 접속하는 원격수색을 허용하는 조항인데, 현행법상 원격수색을 명시적으로 허용하는 조항은 없으며 강제처분법정주의에 따라 명문화가 필요하다.

일곱째, 협약 제20조의 통신데이터 실시간 수집·기록과 관련하여 범죄수사를 위한 통신사실 확인자료제공 절차(통신비밀보호법 제13조)는 실시간이 아닌 이미 저장되어 있는 과거의 통신데이터의 수집에 관한 조항이므로 개정이 필요하다.

여덟째, 협약 제21조의 통신내용데이터 실시간 수집·기록과 관련하여 통신비밀보호법 제5조상 통신감청대상범죄에 협약 제2조 내지 제10조에 규정된 범죄 중 중요성·파급력이 큰 범죄를 포함시킬 필요가 있다.

5. 2022년 국회 협약 가입촉구 결의안

유럽 사이버범죄 협약 가입이 진전되지 않고 있는 상황에서 2022년 4월 국회에 가입 촉구결의안이 상정된 사실은 의미가 상당하다.

동 결의안의 배경은 우리나라뿐만 아니라 전 세계적으로 사이버범죄가 증가하고 있으며, 특히 N번방 사건으로 인해 성착취물에 대한 심각성을 다시 한 번 확인하게 되었다는 현실적 고려가 있다. 디지털 성범죄의 경우 인터넷을 통해 시간과 국경을 초월하는 초국가적 성격을 갖고 있으며, 컴퓨터 자료의 무형성과 휘발성으로 인하여 수사와 증거 수집, 피해 복구 등에 있어서 어려움이 있기 때문이다.⁹⁵⁾

따라서 동 협약 가입으로 초국가적 신속하고 긴밀한 국제공조를 통해 디지털 성범죄를 근절하는 계기가 될 수 있을 것으로 보아, 대한민국 국회는 사이버범죄에 대한 효율적인 국제공조 방안으로서 제안된 「유럽 사이버범죄 방지 협약」에 조속히 가입할 것을 정부에 건의하고, 대한민국 국회는 디지털 성범죄 근절을 위하여 형사사법을 비롯한 법적·제도적 장치를 정비할 것을 촉구하고자 제안하게 된 것이다.⁹⁶⁾

동 결의안이 주목한 점은 디지털 성범죄의 가장 큰 문제 중 하나가 해외 서버를 통해 피해 영상물이 유포된다는 것인데 이 때문에 사이버범죄 수사에 있어서 국가간 형사사법공조를 신속하게 구축하는 것이 매우 시급하다는 현실적 문제다. 무엇보다도 한국은 개별국가들과 형사사법공조 협약을 맺고 있지만, 해당 국가와 이해관계가 크지 않은 경우에는 적극적인 수사 공조가 쉽지 않소, 공조가 이루어진다고 하더라도 수사 협조에 장기간 소요되는 등, 단기간에 피해가 확산되는 디지털 성범죄 특성에 비추어, 대응 공백이 발생할 수밖에 없는 것이 현실이다. 따라서 초국가적으로 신속하고 긴밀한 국제공조를 할 수 있고, 디지털 성범죄에 대한 수사 대응력을 강화할 수 있으며, 이를 통해 디지털 성범죄 예방 및 근절의 계기를 만들 수 있다는 것이다.⁹⁷⁾

6. 유럽평의회 사이버범죄협약 선택의정서 가입검토

2021년 유럽평의회 사이버범죄방지협약 당사국들은 클라우드 소재 전자증거 확보, 상호사법공조의 효과성 증진, 서비스기업과의 직접 협력, 정보보호 안전조치 내용의 클라우드 소재 증거(evidence in the cloud) 선택의정서 (Second Additional Protocol to the Convention on Cybercrime) 안을 확정하였다.⁹⁸⁾ 2001년 사이버범죄방지협약

95) 유럽 사이버범죄 방지 협약 가입 촉구 결의안 (의안번호 15339호 2022. 4. 20)

96) 유럽 사이버범죄 방지 협약 가입 촉구 결의안 (의안번호 15339호 2022. 4. 20)

97) 유럽 사이버범죄 방지 협약 가입 촉구 결의안 (의안번호 15339호 2022. 4. 20)

98) "Second Additional Protocol to the Cybercrime Convention adopted by the Committee of

에 이어, 사이버공간상의 인종차별, 외국인혐오행위의 범죄화를 내용으로 하는 제1부 가선택의정서에 이어, 클라우드소재 증거에 관한 제2부가선택의정서까지 갖추어지면 유럽평의회 사이버범죄방지협약은 사이버범죄에 관한 더욱 체계적인 국제기준이 될 것이다.

제2선택의정서의 내용적 특징은 상호사법공조를 통한 사용자 정보 요청절차의 간소화를 통한 수사효율성 강화라는 점이다.⁹⁹⁾ 이와 관련하여 국제제출명령(international production orders), 사법당국간 직접협력(direct cooperation between judicial authorities in mutual legal assistance requests), 공조수사(joint investigations), 영어사용요건(requests in English language), 증인, 피해자, 전문가 오디오 및 비디오청문(audio/video hearing of witnesses, victims and experts), 긴급 사법공조절차(emergency MLA procedures) 규정을 두었다는데 있다. 또한 타국관할 서비스제공기업과의 직접 협력을 통해 사용자정보요청, 보존요청, 긴급요청을 가능하게 하며, 기존 초국가적 데이터접근 실무에 대하여 안전조치를 강화하고 절차규정을 명확히 하였다.

그러나 프라이버시의 침해, 또다른 한편으로는 통신망의 통합적 기능을 저해하지 않을지에 대한 우려가 있다. 반면 유럽평의회 제2선택의정서를 통한 사이버범죄에 특화된 상호사법공조 개선프로그램의 마련이 미국의 CLOUD법에 비해 좀 더 인권존중적인 대안이 될 가능성도 있다.¹⁰⁰⁾

7. 유엔 차원의 정보통신기술의 범죄악용방지에 관한 국제조약 제정논의 참여

2019년 12월 27일, 유엔 총회는 사이버범죄 분야의 새로운 국제규범으로서 정보통신기술의 범죄악용 방지에 관한 국제조약(International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes)

Ministers of the Council of Europe”<https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe> (2022년 8월 15일 최종검색)

99) 박재성, 사이버범죄 국제조약의 동향 - 부다페스트 협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로, 저스티스 185호, 한국법학원, 2021, 254면.

100) 박재성, 사이버범죄 국제조약의 동향, 265-266면.

제정을 논의하기 위해 전문가들로 구성된 특별위원회 설치를 결의하였다.¹⁰¹⁾

2019년 결의안의 문제의식은 정보통신기술은 새로운 범행수단으로 악용되어 범죄 수준과 복잡성을 증가시키고, 인공지능을 포함한 첨단기술은 그 악용의 위험성과 함께 정보통신기술의 범죄적 악용을 방지하거나 대처하는 수단으로서의 가능성도 인정되며, 디지털 공간에서 자행되는 범죄발생율과 다양성의 증가는 국가 기간시설과 기업의 안전 뿐만 아니라 개인의 삶의 질에도 영향을 미치고 있고, 인신매매를 비롯한 다양한 범죄자들이 범행에 정보통신기술을 악용하고 있다는 것이다. 이에 따라 동 결의안의 목표는 범죄 목적의 정보통신기술 악용에 맞선 국가들간의 조정협력 증진의 필요성을 강조하며, 이는 개발도상국가의 요청에 따라 기술적 지원을 제공하고, 범죄 방지, 탐지, 수사과 기소를 포함한 국가기관의 전반적 대응역량을 증진하며, 국내법제 및 기본체계를 개선한다는 데 있다.¹⁰²⁾

기존 유럽평의회 사이버범죄방지협약의 국제조약화에 찬성하는 가입국 및 한국은 이에 반대하였으나, 종래 유럽평의회 조약과 별개의 사이버범죄 분야 국제조약의 신설을 주장해온 러시아, 중국 등이 다수의 입장이었다.¹⁰³⁾ 찬성 입장은 유럽평의회 협약이 유럽을 중심으로 이루어졌기 때문에, 개발도상국들의 입장이 반영되지 못한 점, 국가주권 침해적 요소가 있다는 점을 비판하였다. 이에 맞서 반대 입장은 새로운 유엔 국제조약이 러시아, 중국 등과 같이 인터넷에 대한 국가통제를 강화하려는 국가들에 의해 정부의 통제와 재제를 강화하기 위한 시도라는 점을 비판하였다.¹⁰⁴⁾

유엔의 새로운 조약 창설은 찬반논의와 서명비준 과정을 거쳐야 하는 것이나, 국제규범으로서의 중요성을 고려하건대, 그 제정 논쟁과 구체화 논의 과정을 면밀히 살피고 한국의 국익과 국제사회 지위를 고려한 일정한 관여 내지 참여가 필요할 것이다. 유럽 사이버범죄방지협약과 달리 유엔 차원의 국제조약으로서 장치 사이버안보 분야

101) UN General Assembly, Proposed outline and modalities for the further activities of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/A.C.291/2 (15 June 2020)

102) Countering the use of information and communications technologies for criminal purposes, UN General Assembly Resolution 74/247 (27 December 2019)

103) 박재성, 사이버범죄 국제조약의 동향, 267면.

104) 정명현, 유엔 사이버범죄 대응 국제조약의 논의동향과 전망, 국제법 동향과 실무 제62호, 2021, 외교부, 15-16면.

국제규범으로 자리잡을 가능성도 있으므로, 한국도 논의단계부터 적극적으로 참여함으로써 새로운 국제규범체계가 사이버범죄수사를 원활하게 함과 동시에 개인정보인 권 보호와 균형을 맞추도록 선도적 역할을 맡아야 할 것이다.¹⁰⁵⁾

제2절 | 사이버안보 국제협력네트워크 강화

세부과제 8 : 사이버위협에 맞서 글로벌 협력 네트워크를 확충한다.

1. 유엔, 유럽연합 등 국제기구와 사이버안보 협력 네트워크 강화

유럽평의회 사이버범죄협약 체계부터 한미 사이버 안보 동맹에 이르기까지 국제 협력을 통한 외교적 전략적 사이버 안보 역량 강화, 사이버 공격에 대한 역지력 강화가 필요하다. 특히 유럽평의회 사이버범죄협약은 역대 정부에서 다양한 찬반논의와 후속 과제에 대한 검토가 충분히 진행되어 왔으므로, 급변하는 세계적 사이버안보 정세를 고려해 가입을 더 이상 미루지 말고 적극 검토할 것이며, 이에 뒤따를 국내법 정비뿐만 아니라 유엔 차원의 규범체계 신설, 미국 등 주요동맹국과의 공조체계 강화를 위한 과제를 체계적으로 실행해 나가야 할 것이다.

또한 외교부는 우리나라가 아시아협력동반자국(Asian Partners for Co-operation) 자격¹⁰⁶⁾으로 참여하는 유럽안보협력기구(OSCE)와 공동으로 아시아-유럽지역의 사이버안보 협력을 위해 지역 간 다자안보 협력 경험을 공유하고 상호 신뢰 구축에 노력하고 있다.¹⁰⁷⁾

외교부는 사이버안보, 테러·폭력적 극단주의, 신기술안보 등 초국경적 안보 위협 대응을 논의하기 한-OSCE 사이버안보 컨퍼런스(Inter-Regional Conference on

105) 같은 취지로는 박재성, 사이버범죄 국제조약의 동향, 278-279면.

106) “외교부, 유럽안보협력기구와 초국경 도전에 '다자 차원의 대응' 협의” (<https://cm.asiae.co.kr/article/nationaldefense-diplomacy/2020101318220523791> 2022년 8월 15일 최종검색)

107) 외교부 보도자료, 유럽안보협력기구 및 아시아협력동반자국과 새로운 안보 위협 대응 논의 (2021.9.22)

Cyber/ICT Security)를 개최해 왔다. 2021년 6월 컨퍼런스에서도 최근 국제 사이버안보 환경이 코로나19 상황을 악용한 행위자들에 의해 영향을 받고 있다고 지적하며, 이에 대응하기 위해 다양한 이해관계자를 포함하는 국제협력 필요성이 재차 강조된 바 있다. 또한 국제 사이버안보 증진을 위한 민·관 협력의 필요성, 사이버안보 정책 결정 과정에서 성평등적 접근이 필요성도 지적되었다.¹⁰⁸⁾

2. 한·미 사이버범죄 공조 강화

2021년 7월 국가사이버안보정책조정회의에서 점증하는 글로벌 사이버 위협과 관련해 한미 간 공동대처 및 협력체계를 강화하기 위해 '한미 사이버 워킹그룹' 출범이 결정된 바 있다. 이는 한미 정상회담 합의사항 이행 조치로서 관계 부처가 참여하는 한미 사이버 워킹그룹을 출범시켜 미국과 협력체계를 강화하기 위함이다.¹⁰⁹⁾

2021년 9월 미국 국가안보회의(NSC)는 한국과 랜섬웨어 워킹그룹 첫 회의를 개최함으로써, 랜섬웨어를 비롯한 사이버 범죄 퇴치에서 협력강화를 통해 한미 동맹의 힘을 보여준 것이라고 평가된다. 미국은 NSC에 랜섬웨어 대응 전담조직을 두고 랜섬웨어 공격 방어는 물론 사건 발생 시 수사기관의 공격자 추적, 은닉 범죄수익 환수 등을 위한 국제공조를 강화하고 있다. ¹¹⁰⁾

3. 미국 CLOUD법 대응

가. 입법 배경

클라우드 컴퓨팅(cloud computing) 환경에서는 데이터가 여러 지역의 서버에 분산되어 저장되기 때문에 초국가적 조직범죄 및 사이버범죄 수사 목적의 초국경적 자료 접근(cross-border access to data)의 현실적 중요성이 커지면서 법정책상 변화가 요

108) <https://www.osce.org/secretariat/490955> (2022년 8월 15일 최종검색)

109) “사이버안보정책조정회의’ 개최 사이버 안보는 선택 아닌 필수”

(<http://www.polinews.co.kr/m/article.html?no=491459> 2022년 8월 15일 최종검색);

靑, 사이버안보정책조정회의 개최...한미 사이버 워킹그룹 출범

(<https://www.etnews.com/20210716000051> 2022년 8월 15일 최종검색)

110) “한미 랜섬웨어 퇴치 손잡았다...첫 워킹그룹 회의 개최”

(<https://www.mk.co.kr/news/world/view/2021/09/880185/> 2022년 8월 15일 최종검색)

청된다. 특히 저장 데이터(data at rest)는 이메일, 소셜 네트워크 및 클라우드에 저장되고 있는 다양하고 광범한 자료인데, 각 국 수사기관이 필요로 하는 증거자료는 대부분 미국법관할내 미국 정보통신기업들에 소재하는 상황에서 수사기관이 범죄 발생지에서 발부된 영장이나 법적 절차를 통해서는 해당 저장데이터 또는 이전데이터에 대한 접근이 어려운 문제가 발생한다. 이에 따라 범죄자들의 소셜 네트워크 서비스 및 글로벌 기업의 이메일 서비스 이용이 증가하면서 각국 경찰에서는 관련 데이터의 소재지 국가에 공조를 요청하기 보다는 주로 미국기업인 Google, Facebook, Microsoft 등 통신서비스 제공자에게 직접 데이터 제공을 요청하고 있다. 그런데 수사기관이 국제형사사법공조절차를 거치지 않고 역외에 위치한 데이터에 접근하는 실무가 늘어나고 있는 상황에서 그 적법성뿐만 아니라, 시민의 프라이버시 보호 문제가 제기될 수 밖에 없다.¹¹¹⁾

나. CLOUD법의 주요내용

2018년 제정된 “합법적 국외 데이터 활용근거법(Clarifying Lawful Overseas Use of Data Act, 약칭 CLOUD Act)”¹¹²⁾은 클라우드컴퓨팅 환경에서 전자증거와 관련해 기존의 사법공조체계와 개인정보 보호법제로는 한계가 있다는 인식을 바탕으로, 미국 내 정보통신서비스제공자가 보유 또는 관리하고 있는 통신 내용, 트래픽 데이터, 가입자 정보 등에 대해서 정부기관이 실제 데이터가 저장된 위치에 관계없이 제공 요청을 할 수 있도록 명시한 입법이다. ¹¹³⁾

동법은 통신정보법(Stored Communication Act)상 집행 명령이 다른 국가에 저장되어 있는 특정 데이터에도 도달할 수 있음을 규정하였다. 다만 개인정보보호 및 시민의 자유를 침해할 수 있다는 우려와 관련하여 법 집행 요청 시 통신정보법에 규정된 법률 적용 대상 주체와 데이터의 유형에만 한정하였다. 즉 전자 통신 및 클라우드

111) 송영진, 미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018, 150면. ; 김상배 외, 디지털 경제 시대를 위한 미래 국가인터넷 전략 연구, 한국인터넷진흥원, 2021, 66-67면

112) <https://www.justice.gov/dag/cloudact> (2022년 8월 15일 최종검색)

113) U.S. Department of Justice, “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,” White Paper (April 2019)

저장 문서 내용과 기록 전송과 사용자 계정 정보 등 통신 관련 데이터 접근만 허용할 뿐 다른 유형의 개인 데이터 혹은 비즈니스 데이터에 대한 접근은 허용하지 아니한다.

이러한 입법조치는 고객 정보를 비공개로 유지할 의무가 있는 IT기업의 경우, 자국의 법 집행 기관에게 협조할 의무와 해당 국가의 데이터 보호법을 준수해야 할 의무 사이 법률적 딜레마를 법적으로 해결하고자 함이다.

CLOUD법은 기존 국제형사 사법공조 절차에 대한 대안으로써 미국과 해외국가가 행정협정(executive agreement)을 체결할 경우, 양국 수사기관이 이에 근거하여 광범위한 데이터를 상호 공유할 수 있도록 규정한다.¹¹⁴⁾ 동법 규정(저장통신정보법 제 2523조 신설)은 초국가적 정보 제공요청을 위한 미국과 외국 정부 간의 행정 협정(executive agreement)의 법적 근거가 된다. 이에 따라 미국 정보통신서비스 제공자가 기존 저장통신정보법을 위반하지 않고 행정협정에 따라 외국 정부의 정보 제공요청에 응할 수 있게 된다. 동법 제2523조는 해당 외국 정부 국내법 체계와 실무가 데이터 수집과 관련하여 프라이버시를 실제법적·절차법적으로 유효하게 보장하는 법적 요건을 충족하는 경우, 미국 연방법무부가 해당 외국정부와 행정 협정을 체결할 수 있는 권한을 부여한다.¹¹⁵⁾

이에 따른 절차는 다음과 같다.

첫째, 미국 법무부와 국무부는 관련 데이터 수집 활동에 관하여 해당 외국 정부가 ‘프라이버시와 시민적 자유의 강력한 실제적이고 절차적인 보호’ (robust substantive and procedural protections for privacy and civil liberties)를 제공한다고 서면으로 확인하여야 한다.

둘째, 해당 외국 정부는 ‘미국인에 관한 정보의 획득, 보유 및 전달’ (the acquisition, retention, and dissemination of information concerning United States persons)을 최소화하는 절차를 채택해야 한다.

행정협정(executive agreement)은 둘 이상 국가 정부수반사이의 협정으로서 입법부에 의한 조약비준절차를 거치지 않는다. 법적으로 구속력있는 조약과 달리 정치적

114) 맹정환, “해외 클라우드컴퓨팅 법제도 동향- 미국 CLOUD Act와 해외 클라우드 저장 정보에 대한 접근권 및 국외 이동 제한 문제를 중심으로”, 클라우드컴퓨팅 산업진흥법제도 연구, 정보통신산업진흥원, 2019, 8-9면.

115) 송영진, 미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점, 160-161면.

구속력을 가질 뿐임. 미국에서 행정협정은 연방대통령의 전속고유권한으로서 미국헌법상 행정협정은 의회 절대다수 기준을 요하는 본래적 의미의 국제조약으로 인정되지는 않지만, 미국과 협정대상국가 모두에 대한 구속력이 인정된다. 행정협정에 따라 해당 외국 정부는 영장으로 미국 관할권의 적용을 받는 서비스제공자에게 전자적 증거를 제시하도록 요청할 수 있게 된다.¹¹⁶⁾

동 영장은 해당 국가의 국내법을 준수하여 발급되고, 합리적 정당성에 근거하며, 테러를 포함한 중범죄 수사에 관련되고, 미국인 이외 외국인을 대상으로 한다. 정보통신서비스제공자는 고객 데이터를 저장할 지역을 선택할 때 데이터센터가 미국과 행정협정을 체결한 국가에 소재하게 할 것인지 결정하게 된다. 행정협정 체결로 정보통신서비스제공자는 법집행 목적의 초국경적 데이터 접근 요청에 있어서 미국과 제3국 사이의 의무의 충돌 위험을 면하게 될 수 있는 것이다.

다. CLOUD법제 검토과제

2022년 현재 미국은 영국, 호주 등과 클라우드법상의 협정체계를 구축하고 있다.¹¹⁷⁾

CLOUD법상 행정협정의 의미와 과제는 다음과 같다.¹¹⁸⁾

116) 정상익, 미국헌법상의 행정협정, 세계헌법연구, 16(1), 2010, 331면.

117) Joint Statement by the United States and the United Kingdom on Data Access Agreement (July 21, 2022); Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (October 3, 2019); Materials conveyed to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement (December 4, 2019); Supplementary letter conveyed to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement (January 16, 2020); U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (October 3, 2019); Joint US-EU Statement on Electronic Evidence Sharing Negotiations (September 26, 2019); Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (December 15, 2021); Materials conveyed to U.S. Congress in Support of U.S.-Australia CLOUD Act Agreement (December 22, 2021) ; United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime (December 15, 2021); Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (October 7, 2019) <https://www.justice.gov/dag/cloudact> (2022년 8월 15일 최종검색)

118) 김상배 외, 디지털 경제 시대를 위한 미래 국가인터넷 전략 연구, 2021, 68-69면.

첫째, CLOUD법상 행정협정은 일정한 중범죄수사사안에서 미국 정보통신서비스기업(CSP)이 외국수사기관에 직접 전자데이터를 제공하는데 있어서 국내법적 제한을 완화한 것이다.

둘째, CLOUD법상 행정협정 자체는 미국에 본사를 둔 CSP로 하여금 외국정부의 법적 조치에 구속되도록 의무를 창설하거나, 외국정부가 법적 관할권을 행사하도록 하는 조치가 아니다.

셋째, CLOUD법상 행정협정은 높은 수준의 프라이버시보호와 법치주의 준수를 요구한다.

넷째, CLOUD법상 행정협정은 상호사법공조 법체계상의 부담을 경감시켜주며, CSP로 하여금 미국과 상대국법 저촉위험없이 외국수사기관의 데이터요청에 응할 수 있게 하고, 미국 정부로서도 사법공조요청에 따른 자원을 필요한 사법공조에 효과적으로 집중할 수 있도록 해 줄 것이다.

다섯째, CLOUD법상 행정협정은 encryption-neutral이다. 정부로 하여금 암호해제(decryption)나 법적 권한 없는 해제명령의 근거가 될 수 없으며, 암호해제는 별개의 사안으로서 정부와 기업, 당사자간 협의가 필요하다.

결론적으로, CLOUD법의 정책적 의미와 과제를 정리해 보면 다음과 같다.¹¹⁹⁾

첫째, CLOUD 법에 따른 행정협정을 통한 수사공조 협력체계는 외국에 소재한 데이터 접근을 위한 기존 사법공조절차 이용 관행으로부터 새로운 발전 가능성을 보여준다.

둘째, CLOUD법은 행정협정 당사자인 외국 정부로부터 프라이버시와 시민적 자유의 일정한 수준을 요구함에도 미국 법집행당국의 데이터 접근 권한을 강화한 것이다.

셋째, 수사기관은 미국 기업의 해외 서버에 존재하는 데이터에도 더 용이하게 접근할 수 있는 권한을 갖게 되며, 미국 기업은 타국 사용자가 해외 서버에 저장한 데이터라도 해당국의 프라이버시보호법제와 무관하게 이를 제공해야 한다.

넷째, IT기업이 보유한 데이터와 개인정보에 대한 정부의 침해위험 우려가 제기되는 반면 데이터 주권을 둘러싼기업과 정부의 갈등, 혹은 국가 간 갈등은 앞으로 증기할 가능성이 높기 때문에 CLOUD 법은 미국 기업에게 데이터 국외 반출의 근거를 제공함

119) 김상배 외, 디지털 경제 시대를 위한 미래 국가인터넷 전략 연구, 2021, 69-70면

으로써 외국 정부의 규제나 압력을 회피하는 방안을 마련해줄 수 있다.

다섯째, CLOUD법에 대한 가장 큰 우려는 프라이버시와 인권침해 가능성인바, 이는 종래 형사사법공조체계가 제공해 온 데이터 프라이버시에 대한 보호장치에 대한 우회로가 허용됨으로써 보호정도가 약화될 수 밖에 없기 때문이다.¹²⁰⁾

여섯째, CLOUD법을 통해 외국 수사기관의 경우 미국 시민이 아닌 한, 미국내 거주자가 아닌한 종래 미국 프라이버시보호법 요건을 따르지 않고서도 데이터에 접근할 수 있게 된다. 행정협정에 따른 역외 데이터접근 제도는 정치적 도구화될 수도 있게 되므로, 행정협정 상대국이 인권침해국가임에도 동맹국 고려때문에 행정협정이 가능한 상황이 문제될 수 있다.

일곱째, 국내에서도 CLOUD법은 수사기관이 클라우드 기업의 해외 서버에 저장된 메일, 문서, 기타 통신 자료 등을 열람할 수 있도록 권한을 부여하고 있어 현지 당국이 합법적으로 우리 국민의 정보를 감시할 수 있다는 우려가 있다. 해외 클라우드 사업자는 클라우드 서비스를 제공할 때 개인정보보호 등 국내 관련 법규를 따르지 않을 수 있고, 이 경우 국내법에 따라 개인정보가 보호받지 못할 수 있다.

여덟째, 국내 클라우드 법제 시스템에 대해서는 미국 CLOUD법에 따른 미국정부의 데이터 제공 요청에 반드시 따라야 하는 것은 아니며, 고객 또는 가입자가 미국인이 아니며 미국에 거주하지 않고, 요구된 데이터 공개로 인해 사업자가 해당국가 법을 위반할 중대한 위험이 있는 경우, 기업은 미국 정부의 데이터 요구에 대한 각하 또는 변경을 법원에 청구할 수 있다.

아홉째, 개인신용정보·고유식별정보는 클라우드 활용 여부와 상관없이 국내 개인정보보호법·신용정보법 등 개인정보보호 법령에 따라 보호되고 법령 위반시 행정제재 및 형사처벌로 규율된다.

라. CLOUD법 정책적 검토과제

그렇다면 한미간 CLOUD법 관련 협력체계 추진에 있어서 검토할 사항은 다음과 같다.¹²¹⁾

120) 한국인터넷진흥원, 미국 클라우드법(CLOUD ACT)의 주요 내용 및 전망, 2018, 185면.

121) 김상배 외, 디지털 경제 시대를 위한 미래 국가인터넷 전략 연구, 2021, 71-72면.; 송영진,

첫째, 최근 한국 수사기관에서 직접 미국의 서비스제공자를 대상으로 영장을 집행하는 사례가 증가하고 있지만, 가입자정보나 로그기록 정도에 한정되는데, 이는 이메일 내용과 같은 콘텐츠 데이터의 경우, 해당 미국기업은 공식적인 형사사법공조절차를 통할 것을 요구하기 때문이다.

둘째, 따라서 한국 수사기관이 미국 등 외국 정보통신서비스제공자로부터 콘텐츠 데이터를 포함한 수사자료를 효과적으로 확보하기 위해서는 미국 정부와 행정협정을 체결하는 방안을 다각적으로 검토해 볼 필요가 있다.

셋째, 선결과제는 한국이 CLOUD법상 “자격 있는 외국 정부(qualifying foreign government)” 요건충족 여부에 대한 검토다.

넷째, 향후 미국과 CLOUD법상 행정협정을 체결하면 상호주의 원칙에 따라 한국 정보통신 기업이 보유 또는 관리하고 있는 데이터에 대해 미국이 직접 기업을 상대로 제공 요청을 할 수 있게 되므로 이에 따른 대비도 필요하다.

다섯째, 외국 수사기관의 데이터 제공 요청에 대응할 구체적인 법제나 가이드라인이 마련되어야 한다.

여섯째, 한국은 아직까지 유럽평의회 사이버범죄협약 당사국도 아니고, 동 협약상 규정의 국내적 이행과 관련하여 사이버범죄와 디지털 증거에 대한 실체법 및 절차법을 완비하지 못하고 있기 때문에, 현행 국제 기준에 맞는 실체법 및 절차법적 정비가 우선되어야 할 것이다.

미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점, 164-165면.

제 8 장

「국가사이버안보 대응 역량강화」국정과제 이행을 위한 법제기반 체계적 정비

결론: 국가사이버안보 역량강화의 법제 기반 정비과제

제8장

결론: 국가사이버안보 역량강화의 법제 기반 정비과제

본 연구는 새 정부 국정과제중 하나인 사이버안보 분야 정책 과제 이행 방향과 법제정비 필요성에 따라 향후 추진해야 할 입법 및 정책과제와 국책연구기관의 연구 지원 역할을 제시함으로써 정부의 국정과제 이행에 선제적으로 기여하고자 기획되었다.

따라서 결론적으로 국정과제 「국가 사이버안보 대응역량 강화」의 다섯가지 주요내용, 즉 사이버안보 정책 체계 정비, 경제안보로서 사이버안보, 국민생활 안전, 기술 고도화 및 국제협력 강화, 사이버 전문인력 양성별로 이행성과 평가지표를 제안하고, 이어서 「국가 사이버안보 대응역량 강화」이행을 위한 10대 세부과제별로 입법적, 정책적 이행을 위해 개발하고 추진해 나가야할 구체적 과제를 제안한다.

제1절 | 국가사이버안보 대응역량강화 국정과제 이행평가를 위한 지표

1. 국정과제 이행 평가 지표의 의미

현행 정부업무평가는 정부의 주요정책, 규제혁신, 정부혁신, 정책소통, 적극행정 등 부문별 평가를 통해 국정 통합 관리 및 국정성과 제고를 위해 각 기관이 국정과제 추진과 국정성과 창출을 위해 역점 추진하는 주요 정책을 중심으로 평가하여 기관의 정책성과와 책임성을 제고하는데 목적이 있다.¹²²⁾

특히 새 정부 출범, 국제정세 및 세계경제 변동가능성 등 정책환경 변화에 따른 각 기관의 적절한 대응노력을 평가하는 취지는 「국가 사이버안보 대응역량 강화」과제 이행 노력에 있어서 고려가 필요하다. 평가 이전에 국정과제 추진노력에 있어서 중점을 두어야 할 정책지점을 파악하는데 평가지표가 상당한 의미가 있기 때문이다.

2022년 정부업무평가 계획¹²³⁾에 따르면, 주요정책, 규제혁신, 정부혁신, 정책소통, 적극행정 등 부분별로 평가한다. 국가 사이버안보 대응역량 강화 국정과제의 다섯 개 주요내용별로 평가지표로서 고려가능한 요소들은 ① 이행노력(입법노력), ② 정책효과(국민체감효과, 장기적 효과), ③ 국민만족/체감도(기관 소관 주요정책에 대한 국민만족도 조사), ④ 혁신성과 (국민참여, 부처간 협업, 디지털 기반 업무효율화), ⑤ 정책소통성과 (언론 및 온라인 소통성과) 지표일 것이다.

2. 국가 사이버안보 대응역량 강화과제 주요내용별 평가지표

가. 사이버안보 정책 체계 정비

- ① 이행노력: 국가사이버안보기본법 제정 및 유관법령 개정
- ② 혁신성과: 국가사이버안보기본법안 초안과정에서 일반시민, 시민단체, 민간기업 의견수렴, 유관기관간 협의 실적
- ③ 정책소통성과: 국가사이버안보기본법 제정의 필요성과 기대효과 홍보실적

나. 경제안보로서 사이버안보

- ① 이행노력: 국가사이버안보기본법 제정 및 유관법령 개정
- ② 정책효과: 국가기반시설 및 주요 기업 사이버안전도 향상 효과
- ③ 혁신성과: 민관 합동 사이버협력체계 운용 실적

122) 국무조정실, 정부업무평가제도 (https://www.evaluation.go.kr/web/page.do?menu_id=25 2022년 8월 15일 최종검색)

123) 국무조정실, 2021년도 정부업무평가 시행계획(안), 2022

다. 국민생활 안전

- ① 이행노력 : 디지털플랫폼 정부 구현, 클라우드 및 스마트그리드 보안을 위한 관련 법령 제정 및 개정
- ② 혁신성과 : 디지털플랫폼정부위원회 운영 실적, 인공지능·데이터 기반 정책 의사결정 지원체계 구축실적
- ③ 정책소통성과 : 개인정보의 안전한 활용에 대한 홍보강화를 통해 국민 신뢰도 향상

라. 기술 고도화 및 국제협력

- ① 이행노력 : 유럽평의회 사이버범죄협약 가입 및 국내이행법령 제정·개정
- ② 혁신성과 : 사이버안보 분야 양자간·다자간 협력체계 운영 실적
- ③ 정책소통성과 : 사이버보안 연구개발 지원과 연구성과 확산 실적

마. 사이버 전문인력 양성

- ① 정책효과 : 사이버특성화 교육 프로그램 및 지역 교육센터 설치 실적
- ② 국민만족/체감도 : 인재양성 프로그램에 대한 만족도
- ③ 혁신성과 : 전문인력 양성 및 확보를 위한 부처간 협업

제2절 | 국가사이버안보 대응역량강화 국정과제 이행을 위한 법제정비 및 정책개발 과제

1. 세부과제 1: 대통령 직속 ‘국가사이버안보총’ 설치 및 컨트롤타워 운영체계를 갖춘다

- ① 국가 차원에서 범정부 역량을 집중할 수 있는 일원화된 사이버안보 컨트롤타워는 효율적인 사이버안보 거버넌스 체계에 필수적이다. 국가 사이버안보 정책에 대해서는 대통령실과 국가사이버안보위원회가 관장할 필요가 있다.
- ② 현재 위원회 형식이나 소속에 대한 논의가 진행 중이다. 사이버안보는 선택의 문제가 아닌 국가안보 및 국민안전에 직결된 필수적 과제라는 인식하에 다양한 사이버 공격과 위협에 선제적이고 적극적으로 대응하기 위해서는 대통령 직속의 컨트롤타워 기구를 둘 필요가 있다.
- ③ 정보와 권한의 집중은 바람직스럽지 아니함은 물론이나, 이는 법적 제한조치가 기관간 견제구조를 통해 해소할 수 있다. 권한과 기능은 분장되더라도 국가 사이버안보전략 차원에서 중장기적인 기획과 사안대응에서 통합조정 역할은 전담 위원회를 둬야 바람직할 것이다.
- ④ 사이버안보의 국가전략적 접근에 있어서 체계적이고 효과적인 컨트롤타워 운영체계의 구축은 국가사이버안보 기본법 제정을 통해 이행해야 할 우선 과제다. 입법 과정에서 종래 논의되었던 방안들과 제기되었던 사회적 의견들을 참고하여 행정부와 입법부가 책임성 있게 추진해야 할 수 있도록 다양하고 광범위한 청문회와 자문이 필요할 것이다.

2. 세부과제 2: 사이버안보 유관기관별 역할과 각급 기관간 협력 활성화 등을 규정한 법령 제정을 추진한다

- ① 국가사이버안보 기본법제의 핵심내용과 쟁점은 사이버공격에 대한 유관기관 협력과 체계적 대응을 기획·조정할 콘트롤타워를 정하는 문제, 사이버공격 대응 책임기관, 지원기관, 수사기관의 권한과 직무 조정배분의 문제, 사이버위기대책 협의기구, 그리고 민관 합동 사이버협력체계의 구성과 운영방식이 될 것이다.
- ② 국가 사이버안보는 궁극적으로 국민안전을 목표로하므로, 종래 “국가사이버안보법” 명칭에서 오는 불필요한 오해를 피하고, 민관협력의 중요성을 강조하는 측면에서 법명을 “국민사이버안전법” 내지 “국민사이버안전기본법”으로 칭할 수 있을 것이다.

3. 세부과제 3: 민관 합동 사이버협력체계 강화를 통해 핵심기술 보유기업·방산업체·국가기반시설 대상 위협과 공격 방지 및 대응조치를 적극 실행함으로써 경제 안보에 기여한다

국가 사이버안보 역량이란 사이버공간의 급속한 발전과 사이버안보 위협의 증폭에 대응하여, 국민 안전과 국가 핵심 인프라 보호를 법제도·전문 인력·예산·민관협력·투자를 체계적으로 정비·구축·실행할 수 있는 총체적 국가역량을 뜻한다.

따라서 2017년 정부 국가사이버안보법안의 예에 따라 국가·지방자치단체 및 기업은 사이버안보가 국가안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하여 사이버공간을 보호하도록 노력하여야 한다는 원칙적 규정에 이어 구체적 협력체계 구축을 위한 규정을 두어야 할 것이다.

4. 세부과제 4: 사이버공격으로부터 안전한 ‘디지털플랫폼’ 정부를 구현한다

- ① 디지털플랫폼 정부 구현에 있어서 사이버공격으로부터의 안전은 기본적 토대가 된다. 따라서 새 정부의 디지털플랫폼정부위원회는 특히 디지털플랫폼정부 구

현을 위한 규제혁신, 법령의 제정·개정과 제도의 개선정책에 있어서 디지털플랫폼정부 구현을 위한 핵심 인프라 구축 및 운영, 인공지능과 데이터를 활용한 과학적 정책의사결정 지원 등 디지털 국정 관리·운영, 디지털플랫폼정부 구현에 따라 발생하는 문제의 예방 및 해결에 관한 사항에 주력해야 한다.

- ② 궁극적으로 디지털플랫폼 정부의 사이버안전 확보는 디지털플랫폼 정부에 대한 국민 신뢰 제고의 관건이기도 하다. 따라서 디지털플랫폼정부위원회는 디지털플랫폼정부 구현과 디지털 혁신 산업 기반 조성을 위한 민간·정부 간 협업과 민간 참여 활성화, 공무원 및 국민의 디지털 역량 강화, 그리고 특히 디지털플랫폼정부의 안전한 개인정보 활용 등 안전성·신뢰성 확보, 차별 없는 디지털플랫폼정부 서비스 제공을 위한 환경의 조성, 디지털플랫폼정부 구현에 관한 국민 공감대 형성과 활용 확산 정책에 특히 주력해야 한다.

5. 세부과제 5: 클라우드·스마트그리드 등 국민 생활에 밀접한 IT 환경의 안전성을 확보한다

스마트그리드에 적용되고 있는 IT기술 중에 최근 주목받는 클라우드 컴퓨팅기술은 클라우드 제공자의 플랫폼을 이용하기 때문에 사이버 보안대책이 중요한 과제다. 현행 스마트도시 조성 및 산업진흥 등에 관한 법률의 경우 제21조(개인정보 보호), 제22조(스마트도시기반시설의 보호) 규정을 두고 있다. 2010년 스마트그리드 국가로드맵의 경우 스마트그리드 특별법 제정 계획을 포함하고 있었다. 이처럼 정보통신 안전환경을 위한 특별법 제정 논의에서는 기반시설 보호뿐만 아니라 개인정보 보호규정도 균형있게 반영되어야 할 것이다.

6. 세부과제 6: 産·學·研·官 협력 아래 AI·양자통신 등 신기술 위협 대응 新 기술 연구·개발을 적극 지원하여 사이버공격 탐지·차단·추적 시스템을 고도화한다

- ① 사이버보안 인재양성과 정부출연연구기관의 협동·융합연구 활성화 과제 외에

국정과제 추진과정에서 필요하고 가능한 범위에서 관련 정보는 국민에게 공개돼 사이버안보의 주체로서 인식하고 활동할 수 있도록 정책적 고려가 필요함.

- ② 사이버안보 대응 역량강화와 국민기본권 보장의 바람직한 균형점을 모색하기 위해서는 관련 정보의 공유와 국민참여를 통해 국민인식과 신뢰도를 개선하는 정책적 노력이 필요하다. 이러한 국민신뢰도 제고정책을 위해서는 정부출연연구기관이 연구성과확산과 대국민정보서비스를 통해 역할을 담당할 수 있도록 지원이 필요하다.
- ③ 사이버범죄 관련 통계는 현재 경찰청 사이버범죄 통계자료에 한정되어 있으며, 신속한 업데이트가 되고 있지 못하다. 사이버범죄 뿐만 아니라 사이버위협에 대한 실증자료는 효과적인 사이버안보대응전략 기획과 추진에 기본자료가 된다. 따라서 사이버 안보관련 통계기반 구축도 연구개발 과제의 하나로 고려되어야 할 것이다.

7. 세부과제 7: 사이버안보 국제공조 활성화 차원에서 국제사회의 사이버규범 수립에 적극 참여한다

- ① 사이버공간상의 인종차별, 외국인혐오행위의 범죄화를 내용으로 하는 제1부가선택의정서에 이어, 클라우드소재 증거에 관한 제2부가선택의정서까지 갖추어지면 유럽평의회 사이버범죄방지협약은 사이버범죄에 관한 더욱 체계적인 국제기준이 될 것이다. 이미 역대 정부에서 다양한 찬반논의와 후속과제에 대한 검토가 충분히 진행되어 왔다. 2022년 국회에서도 동 협약에 조속히 가입할 것을 정부에 촉구하는 결의안도 제안된 바 있다. 새 정부는 급변하는 세계적 사이버안보 정세를 고려해 가입을 더 이상 미루지 말고 적극 검토해야 한다.
- ② 유럽 사이버범죄협약 가입에 뒤따를 국내법 정비뿐만 아니라 유엔 차원의 규범체계 신설, 미국 등 주요동맹국과의 공조체계 강화를 위한 과제를 체계적으로

실행해 나가야 한다.

- ③ 유엔 정보통신기술의 범죄악용 방지에 관한 국제조약은 장차 사이버안보 분야 국제규범으로 자리잡을 가능성도 있으므로, 한국도 논의단계부터 적극적으로 참여함으로써 새로운 국제규범체계가 사이버범죄수사를 원활하게 함과 동시에 개인정보인권 보호와 균형을 맞추도록 선도적 역할을 맡아야 할 것이다.

8. 세부과제 8: 사이버위협에 맞서 글로벌 협력 네트워크를 확충한다

사이버위협과 공격, 그 위협과 피해가 글로벌화되면서 유럽평의회 사이버범죄협약 체계부터 한미 사이버 안보 동맹에 이르기까지 국제 협력을 통한 외교적 전략적 사이버 안보 역량 강화, 사이버 공격에 대한 억지력 강화가 필요하다.

특히 2021년 구성된 한미 사이버 워킹그룹의 효과적 운영을 통해 미국과 협력체계를 사이버안보 글로벌 협력네트워크의 핵심축으로 삼아야 한다.

9. 세부과제 9: 대학·특성화 교육 확대, 지역별 교육센터 설치 등 ‘10만 인재 양성’ 프로그램을 실행한다

- ① 국가 사이버안보 대응역량 강화를 위해서는 전략기술로서 사이버보안 기술 산학연 협동·융합연구 활성화가 필수적이다.¹²⁴⁾

법무정책 분야 국책연구기관으로서 한국형사·법무정책연구원 또한 전략기술 개발의 법제기반 정비와 법정책 개발에 관한 핵심연구거점으로서의 역할을 담당할 수 있다. 한국형사·법무정책연구원은 지난 20년간 사이버안전, 사이버범죄, 사이버테러 관련 법제 및 정책연구를 수행해 왔다.¹²⁵⁾

124) 국정과제 75 「초격차 전략기술 육성으로 과학기술 G5 도약」에 따르면, 경제성장과 안보 차원에서 주도권 확보가 필수적인 전략기술을 지정하여, 초격차 선도 및 대체불가 기술확보를 목표로 집중 육성하는데 목표가 있다. 동 과제의 주요 내용에는 출연연·대학 등을 전략기술 임무해결을 선도하는 핵심연구거점으로 지정하여 산학연과의 협동·융합연구 활성화가 포함되어 있다. 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022년 5월, 130면.

125) 한국형사정책연구원의 사이버안보 분야 연구성과로는 김한균 외, 동북아 사이버범죄 및 보안 지역협력방안, 2015; 김한균 외, 사이버범죄방지 가상포럼(VFAC) 사업 정책성과 연구, 2015; 김한균 외, 한·미 사이버테러 대응정책 협력방안 연구, 2015; 강석구, 사이버범죄 관련 법령정

- ② 10만 인재 양성과 특성화 교육 못지 않게 필요하고 가능한 범위에서 관련 정보를 국민에게 공개하고 사이버안보의 주체로서 교육할 수 있도록 정책적 고려가 필요하다. 사이버안보 사업에서도 다양한 정부출연연구기관의 참여확대를 통해 이를 뒷받침 할 수 있다.

10. 세부과제 10: ‘사이버 예비군’ 운영 등 사이버戰 인력을 확보한다

북한·러시아 등 주변 국가의 사이버전 능력 고도화와 전력 증강에 맞서 사이버전 역량을 강화하기 위해서 사이버 예비군의 필요성은 역대 정부가 검토해 온 과제다. 미국의 경우 국토안보부에서 보안기술 전문가를 확보하기 위한 방안으로 사이버 예비군 제도를 제시한 바 있고, 영국은 합동사령부 내에 사이버 방어 담당 조직인 사이버 예비군을 운영하고 있다. 우선 기초과제로서 외국 제도 사례를 비교연구하여 도입 가능성과 활용 방안을 연구할 필요가 있다.

비 방안, 2013; 윤해성 외, 사이버 테러의 동향과 대응 방안에 관한 연구, 2012; 이원상, 클라우드 컴퓨팅 환경에서의 사이버범죄와 대응방안 연구, 2012; 이원상 외, 사이버범죄의 새로운 유형과 형사정책적 대안연구, 2010; 강석구, 사이버안전체계 구축에 관한 연구, 2010; 정완, 사이버공간상 인권침해범죄에 대한 법제도적 통제방안 연구, 2007; 정완, 사이버범죄 방지를 위한 국제공조방안, 2005; 백광훈, 사이버범죄에 대한 ISP의 형사책임, 2003; 이영준, 사이버범죄방지조약에 관한 연구, 2001; 백광훈, 사이버범죄방지조약에 관한 연구, 2001; 이민식, 사이버공간에서의 범죄피해에 관한 연구, 2000.

참고문헌

- 국무조정실, 2021년도 정부업무평가 시행계획(안), 2022
- 국회 정보위원회, 국가사이버안보법안【정부 제출】검토보고, 2017
- 경희건, 미국 '반도체와 과학법'의 정책적 시사점, 산업경제이슈 144호, 산업연구원, 2022
- 김민진, 인공지능: 사이버보안 패러다임의 전환, 정보통신정책연구원, 2021
- 김상배 외, 디지털 경제 시대를 위한 미래 국가인터넷 전략 연구, 한국인터넷진흥원, 2021
- 김영란, 사이버범죄조약 대응을 위한 일본의 형사법개정안 연구, 외국경찰동향, 경찰대학, 2010
- 김한균, 사이버보안 국가전략과 기본법제 - 일본의 2016년 개정 사이버보안기본법과 2015년 사이버보안전략, 형사정책연구소식 143, 한국형사정책연구원, 2017
- 김한균·김성은·이승현, 「사이버범죄방지를 위한 국제공조방안 연구 - 유럽사이버범죄 방지협약을 중심으로」, 대검찰청 연구보고서, 2008
- 관계부처합동, 국가 사이버안보 기본계획, 2019
- 관계부처 합동, 디지털 성범죄 근절대책, 2020
- 맹정환, “해외 클라우드컴퓨팅 법제도 동향 - 미국 CLOUD Act와 해외 클라우드 저장 정보에 대한 접근권 및 국외 이동 제한 문제를 중심으로”, 클라우드컴퓨팅 산업진흥법제도 연구, 정보통신산업진흥원, 2019
- 박재성, 사이버범죄 국제조약의 동향 - 부다페스트 협약 제2 추가의정서 및 유엔 사이버범죄 조약을 중심으로, 저스티스 185호, 한국법학원, 2021
- 박희영 외, 사이버범죄협약 이행입법연구, 대검찰청, 2015
- 박찬수·박용석, 사이버전의 개념과 대응방안에 관한 연구, 한국정보통신학회 2014 추계종합학술대회 자료집, 2014
- 산업통상자원부, 보도자료 : 스마트그리드 국가로드맵 확정, 2010.1.25.
- 신용우, 「유럽 사이버범죄 방지 협약」 체결 현황과 우리나라의 입법·정책적 대응방향, 국회입법조사처, 2020

- 송영진, 미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호, 2018
- 엄정호, 사이버전을 대비한 사이버 예비군 운영 방안, 보안공학연구논문지 44호, 보안공학연구지원센터, 2015
- 윤해성·라광현, 사이버범죄협약(일명 '부다페스트' 조약) 가입을 위한 선결과제, 가천법학, 제40호, 2019
- 이범룡, 사이버 범죄 조약과 일본의 법안 정비. CLIS Monthly, 2003(4), 정보통신정책연구원, 2003
- 이창수, "초국가적 사이버범죄에 대한 국제공조 활성화방안과 그 선결과제." 형사법의 신동향 21, 대검찰청, 2009
- 이협건 외, 클라우드 기반 스마트 그리드 환경에서의 보안 이슈, 한국정보처리학회: 학술대회논문집, 2010
- 이효영, 경제안보 개념과 최근 동향 평가, 국립외교원 외교안보연구소, 2022
- 외교부 보도자료, 유럽안보협력기구 및 아시아협력동반자국과 새로운 안보 위협 대응 논의(2021.9.22.)
- 유지연, 국가 사이버 안보 전략 패러다임 변화에 대한 주요국 비교분석 연구, 국가정보연구 14(1), 한국국가정보학회, 2021
- 전현욱·이자영, 사이버범죄협약과 형사절차상 적법절차원칙: 저장된 데이터의 보존 및 일부 공개를 중심으로, 형사정책연구 25(2), 한국형사정책연구원, 2014
- 정명현, 유엔 사이버범죄 대응 국제조약의 논의동향과 전망, 국제법 동향과 실무 제62호, 2021
- 정상익, 미국헌법상의 행정협정, 세계헌법연구, 16(1), 2010
- 제20대 대통령직인수위원회, 윤석열 정부 110대 국정과제, 2022
- 청와대 국가안보실, 국가 사이버안보전략, 2019
- 한국인터넷진흥원, 미국 클라우드법(CLOUD ACT)의 주요 내용 및 전망, 2018
- 함승현·박대우, 국가 사이버안보를 위한 정책 연구, 한국정보통신학회논문지 Vol. 21, No. 9, 2017

CyberSecurity Ventures, Special Report: Cyberwarfare In The C-Suite, 2020
FBI, 2020 Internet Crime Report, 2020

INTERPOL report on cyberattacks during COVID-19, 2020

UN General Assembly, Countering the use of information and communications technologies for criminal purposes, UN General Assembly Resolution 74/247 27 December 2019

UN General Assembly, Proposed outline and modalities for the further activities of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/AC.291/2, 15 June 2020

UN Panel of Experts, 2019 final report of the UN Panel of Experts Established Pursuant to Resolution 1874 (2009), investigating North Korean violations of UN sanctions, S/2019/171, 2019

U.S. Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," White Paper, 2019

Abstract



Review of the New Government Action Plans on the National Strategy for Cyber-Security

Kim, Han-Kyun*

The research project on the New Government Action Plans on the National Strategy for Cyber-Security of 2022 aims to review the plan and to propose 10 main tasks for implementing the task No. 101: Strengthening the National Capacity on Cyber-Security.

The task is one of the 110 national tasks to be pursued by the Yoon Suk-yeol administration. The initiatives are designed to promote national interests, pragmatism, fairness and common sense.

The No. 101 task proposes new paradigm of cyber-security; Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. Cyber-security has become the matter of safety for people and security for national economy beyond the traditional notion of national security.

5 core mandates of the task of strengthening the national cyber-security capacities are: ① Reforming cyber-security system; ② Strengthening cyber-security as a matter of economy-security; ③ Strengthening cyber-security for people's safety; ④ Strengthening international cooperation in cyber-security and developing high technology for cyber-security; ⑤ Building up human resources specializing cyber-security.

* Ph.D, Senior Research Fellow, Korean Institute of Criminology & Justice

10 main tasks for implementing the task of strengthening the national cyber-security capacities are : ① Establishment of National Cyber-Security Council and control-tower of national cyber-security system and policy; ② Introduction of National Cyber-Security Act as the legal basis of cooperative system for promoting cyber-security; ③ Strengthening public-private cooperation on cyber-security and contributing to economy security; ④ Implementation of Digital Platform Government secured against cyber-threats; ⑤ Securing of safe IT environment which impacts on people's life; ⑥ Support of research and development on high-technology in the field of cyber-security; ⑦ Positive participation in the process of building international norms on cyber-security; ⑧ Promotion of international cooperative network against cyber-threats; ⑨ Promotion of education and training programs for cyber-security specialists; ⑩ Preparing cyber-warfare including cyber-reserved army.

Above all, the Council of Europe Convention on Cybercrime is a framework that permits practitioners from Parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations. The UN General Assembly voted in December 2019 to begin negotiating a new UN treaty on cybercrime. The treaty is an important step towards helping countries realize national capacity building on cyber-security. Korean Government needs to consider sign the European Convention, and also to participate in the process of drafting new UN norms on cyber-security.



「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법제기반 체계적 정비

발 행 | 2022년 12월

발 행 처 | 한국형사·법무정책연구원

발 행 인 | 하 태 훈

등 록 | 1990. 3. 20. 제21-143호

주 소 | 서울특별시 서초구 태봉로 114

전 화 | (02)575-5282

홈페이지 | www.kicj.re.kr

정 가 | 7,000원

인 쇄 | 고려씨엔피 02-2277-1508/9

I S B N | 979-11-91565-61-4 93360

• 사전 승인없이 보고서 내용의 무단 전재 및 복제를 금함.