[토론회]

# “인권과 이용자 중심의 사이버 보안 전략이 필요하다!”

## - 국내 사이버보안 정책의 재구성 모색 -

■ 사회 : 이호중 (정보인권연구소 이사장)
■ 발제 : 오병일 (정보인권연구소 이사)
■ 토론 :
- 박병욱 (교수, 경찰대학 경찰학과)
- 권석철(큐브피아 대표)
- 심우민 (국회입법조사처 입법조사관)
- 이광철 변호사 (변호사, 민변 디지털정보위원회)

■ 일시 : 2016년 12월 16일(금) 오전 10시-12시
■ 장소 : 민변 대회의실
■ 주최 : 정보인권연구소, 민변 디지털정보위원회
■ 후원 : 49통일평화재단

[정보인권연구소 보고서]

# 국가정보원과
# 국내 사이버 보안 정책 개혁 방안

# 목차

# 1. 서론

8일, 192시간에 걸친 필리버스터 끝에, 결국 2016년 3월 2일 밤, 테러방지법이 국회를 통과했다. 지난 2015년 말 파리에서 발생한 테러 사건 이후, 정부와 새누리당은 테러방지법 및 사이버테러방지법을 핵심 법안으로 올려놓았고, 마치 누군가 뒤에서 조종한 듯 여러 언론들은 테러방지법 제정을 촉구했다.

북한의 해킹 공격에 대한 뉴스도 심심치않게 들려온다. 테러방지법 통과 이후 사이버테러방지법 논란이 불거질 즈음, 정부 안보라인 주요 인사들의 스마트폰이 해킹당했고, 금융기관에 보안 소프트웨어를 납품하는 업체의 전자인증서가 북한의 해킹으로 탈취되었다고 난리가 났다. 2016년 1월부터 6월까지 외교안보 핵심 관계자 90명의 이메일이 해킹당한 것으로 드러났으며, 5월 인터파크 해킹으로 고객정보를 유출한 범인도 북한으로 지목되었다. 물론 그 이전에 북한의 소행으로 규정되었던 해킹 방법과 유사한 방법으로 이루어졌다는 것을 근거로, 이번 사건도 북한의 소행이라는 수사기관의 발표를 어디까지 믿을 수 있는지는 의문이다. 이번 사건은 또 다음 번에 북한의 소행임을 입증하는 근거로 사용될지도 모른다.

국제적으로도 사이버 보안은 핫이슈 중의 하나이다. 지난 2013년 5월, 미국 국가안보국(NSA)의 직원이던 에드워드 스노든이 NSA의 인터넷 대량감청을 폭로한 이후 움츠려들었던 정보기관들은 전 세계에서 빈발하는 테러 사건을 계기로 다시 목소리를 높이기 시작하고 있다. 2015년 12월, 미국 샌 버나디노에서 발생한 총기 테러를 수사하면서 미연방수사국(FBI)이 용의자 아이폰의 암호화 잠금해제를 애플에 요청했으나, 애플이 이를 거부하면서 암호화를 둘러싼 세계적인 논란이 불거졌다. 인터넷 업계와 인권활동가들은 강력한 암호화의 필요성을, 정보수사기관은 암호화된 콘텐츠에 대한 접근 필요성을 주장하면서 미국에서는 90년대 암호 전쟁에 이은 제2의 암호 전쟁(Crypto War)이 벌어지고 있다.

대부분의 사람들이 반인륜적 테러에 동의하지 않는다. 누구나 사이버 보안의 중요성에 대해 동의한다. 그러나 누구를 위한 보안인가, 사이버 공간의 보안을 어떻게 지킬 것인가, 누가 그러한 결정을 할 것인가에 대해서는 답하기가 쉽지 않다.

종종 보안과 인권은 상반된 것으로 여겨진다. 공항에 설치된 알몸수색기처럼, 테러로부터의 안전을 위해 프라이버시쯤은 희생되고는 했다. 그러나 핸드폰 압수수색을 당하고, 국정원이 해킹 프로그램을 사찰 목적으로 이용해왔으며, 카카오톡 대화내용도 감청당할 수 있다는 것이 알려지면서, 내 핸드폰 보안을 지키는 것은 내 인권을 보호하는 것이라는 것이 명확해졌다. 스노든 폭로를 전후해서 전 세계 인권 활동가와 언론인들은 사이버 보안의 중요성을 인식하기 시작했다. 나의 소중한 자료와 개인정보를 위협하는 것은 테러리스트나 사기꾼들만이 아니다. 정부는 때로는 사이버 보안의 수호자이기도 하지만, 때로는 가장 무서운 공격자가 되기도 한다. 이탈리아 보안 업체 해킹팀이 만든 RCS라는 해킹 프로그램 구매자는 전 세계 정보, 수사기관이었다. 그들은 테러 방지와 범죄 수사를 명분으로 개인의 인권뿐만 아니라, 인터넷의 보안을 위험에 빠뜨렸다.

최근 세계 인권 활동가들은 사이버 보안 이슈에 대해 인권적 관점에서 개입하기 위해 노력하고 있다.[1] 2015년 4월, 네덜란드 헤이그에서 개최된, 사이버 보안을 논의하기 위한 국제포럼인 '사이버스페이스 세계회의(Global Conference on Cyberspace)'에는 정부, 업계 관계자들과 함께, 270여 명의 시민사회 인사들이 참가하였다.[2] 그러나 시민사회나 인권 활동가들에게 정부 감시로부터 스스로를 보호하기 위한 맥락에서만 사이버 보안이 중요한 것은 아니다. 그들은 인권적 관점에서의 사이버 보안을 정의하고, 정책 결정 과정에 개입하기 위해 노력하고 있다. 예를 들어, 사이버 공간을 둘러싼 국가간의 긴장이 높아지는 것은 인터넷의 분절화(fragmentation)를 야기하고, 안정성을 해칠 수 있다. 국가간 긴장 완화를 위한 신뢰구축조치(Confidence Building Measure)들이 이제 사이버 공간에서도 필요해지고 있는데, 이러한 논의는 단지 정부 정책결정자들의 몫일까?

국내 시민사회, 인권 활동가들도 국가안보나 범죄 수사를 명분으로 한 감시와 인권침해에 맞서 싸워왔다. 국정원과 사이버테러방지법에 대한 문제제기 역시 그런 활동의 맥락 속에 있다. 그러나 좀 더 나아갈 필요가 있다. 보안 조치의 인권 침해 문제에 대한 비판을 넘어, 사이버 보안 정책에 인권적 관점으로 보다 적극적으로 개입할 필요가 있다. 누구의, 무엇을 위한 사이버 보안인지를 묻고, 사이버 보안 정책의 결정 과정이 비단 정책 결정자나 기술자의 몫이 아니라, 관련된 모두가 참여할 수 있어야 함을 얘기해야 한다. 인권적 관점의 사이버 보안 정책이 구체적으로 무엇인지는 아직 명확하지 않다. 이 보고서는 그러한 답을 찾아가는 하나의 과정이다.

이 보고서는 우선 사이버 보안의 개념이 사용되는 다양한 맥락을 소개하고 있다. 사이버 보안은 가장 많이 사용되는 용어지만, 아직 세계적으로 그 정의가 합의되지 않은 개념이기 때문이다. 이어 사이버 보안과 관련한 국제적인 동향을 살펴보고, 미국, 유럽연합, 영국, 일본 등 주요 국가의 사이버 보안 정책을 검토하였다. 특히, 각 국가의 사이버 보안 전략과 수행체계(거버넌스 체계), 주요 기반시설 보호를 위한 정책을 중심으로 살펴보았다.

3장에서는 국내 사이버 보안 정책을 검토하였다. 국내 사이버 보안 관련 전략(종합대책) 및 주요 법제도를 살펴보고, 특히 국가정보원이 맡고 있는 역할을 중점적으로 검토하였다. 국내 사이버 보안 관련해서 국정원이 실질적 컨트롤타워 역할을 하고 있기 때문이다. 그것이 국내 사이버 보안 정책에 미치는 영향에 대해 분석해보았다. 관련하여 국정원의 권한을 더욱 강화하려고 하는 사이버테러방지법 등 사이버 보안 법안들에 대해서도 살펴보았다.

이상의 분석을 토대로, 마지막 4장에서는 인권적 관점, 이용자 관점에서 국내 사이버 보안 정책을 재구성하기 위한 몇 가지 제안을 다루고 있다.

[1] Anja Kovacs & Dixie Hawtin, "Cyber Security, Cyber Surveillance and Online Human Rights", 2012.6.29
http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
[2] 진보네트워크센터, 2015년 사이버스페이스 세계회의(GCCS 2015) 참가 보고서, 2015.4.22, http://act.jinbo.net/wp/8646/

# 2. 사이버 보안의 개념과 국제 동향

## 가. 사이버 보안의 개념

사이버 보안(cyber security)은 현재 세계 인터넷 거버넌스 영역에서 가장 뜨거운 이슈 중의 하나이다. 해킹과 같은 사이버 범죄, 테러리스트의 사이버 공격으로부터의 방어, 국가간의 사이버 전쟁, 혹은 국가 감시로부터 개인 프라이버시의 보호에 이르기까지 다양한 이슈와 겹쳐져 사이버 보안 이슈가 등장한다.

그런데 사이버 보안이란 무엇일까? 여러 국제기구와 국가의 법령이나 정책에서, 그리고 학술문서에서 사이버 보안 개념을 사용하고 있지만, 아직 세계적으로 합의된 사이버 보안에 대한 정의는 존재하지 않는다.

기술표준을 정하는 '국제표준기구(ISO)'는 사이버 보안을 "사이버공간에서 정보의 기밀성, 무결성, 가용성을 유지하는 것"이라고 정의한다. 여기서 '사이버 공간'이란 "인터넷에서 기술 도구와 그것과 연결된 네트워크를 사용하여 사람, 소프트웨어, 서비스의 상호작용으로부터 나온 복합 환경으로 물리적 형태로 존재하지 않는 것"을 의미한다.[3] 이는 기술 중심적인 정의라고 할 수 있다. 그러나 사이버 보안은 기술적인 맥락을 넘어 다양한 정치적, 이데올로기적 맥락에서 사용되고 있다.

통신정책을 관할하는, UN 산하 국제기구인 국제통신연합(ITU)은 사이버 보안을 "사이버 환경, 기관 및 사용자의 재산을 보호하기 위하여 이용될 수 있는 수단, 정책, 안보개념, 안보조치 및 가이드라인, 위험관리 방법·행위·훈련, 최상의 관행·보장조치·기술의 집합"으로 정의한다.[4] 이 정의는 위협보다는 '위험(risks)'에 초점을 맞춘 것이며, ITU의 역량 강화 사업을 통한, 사전적인 전략이나 장기적인 위험 관리 전략의 구현의 필요성에 따른 것이다.[5]

경제협력개발기구(OECD)는 "정보통신망에 대한 사이버 공격을 사전에 예방하거나 사후에 피해를 복구하는 등 정보통신 시스템이 정상적으로 가동되도록 보장하고, 정보통신 기반시설을 보호하는 것"[6]으로 정의하고 있는데, 이는 정보통신망과 기반시설의 보호에 초점을 맞추고 있다.

---

[3] International Organization for Standardization, ISO/IEC 27032:2012
Officially, ISO/IEC 27032 addresses "Cybersecurity" or "Cyberspace security", defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace". In turn "the Cyberspace" (complete with definite article) is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

[4] "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organization and users assets",
http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[5] Freedom Online Coalition, Cybersecurity: what's the ITU got to do with it?,
https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog7/

[6] http://www.oecd.org/internet/ieconomy/15582260.pdf (한국인터넷진흥원, 2015 p229 재인용)

EU는 사이버보안을 “네트워크 및 인프라의 가용성 및 무결성, 그리고 그 안에 포함된 정보의 기밀성 유지를 목적으로 민간 및 군사 영역에서 독립적 네트워크 및 정보 인프라에 해를 가할 수 있거나 그것과 관련된 위협으로부터 사이버 도메인을 보호하려고 이용될 수 있는 보호조치 및 활동”으로 이해하고 있다.[7]

법에서 ‘사이버시큐리티’라는 용어를 사용하고 있는 일본은 이를 “전자적 방식, 자기적 방식 그 밖에 사람의 지각에 의해 인식될 수 없는 전자적 방식에 의해 기록하고, 발신하며, 전송하고, 또는 수신하는 정보의 누설·멸실·훼손의 방지 및 그 밖에 당해 정보의 안전관리를 위한 조치, 정보시스템 및 정보통신 네트워크의 안전성 및 신뢰성 확보를 위해 필요한 조치가 강구되고 그 상태가 적절하게 유지·관리되는 것을 말한다.”고 정의했다.[8]

보다 인권적 관점에서 사이버 보안 이슈에 접근하고자 하는 온라인자유연합(Freedom Online Coalition)[9]의 ‘자유롭고 안전한 인터넷(An Internet Free and Secure)’ 워킹그룹은 사이버 보안을 다음과 같이 정의하였다.아래 정의는 국가 및 국제 안보적 관점에 치우친 사이버 보안 담론에 인권적 관점의 중요성을 강조하고, 시스템 중심의 접근보다는 개인의 보안을 중심에 놓는 접근을 목적으로 한다. [10]

| |
|---|
| 전문 : 국제 인권법과 국제 인도주의 법률은 오프라인 뿐만 아니라 온라인에도 적용된다. 사이버보안은 기술 혁신과 인권의 향유를 보호해야 한다.<br><br>정의 : 사이버보안은 온라인 및 오프라인에서 개인의 보안을 증진하기 위해, 정책, 기술, 교육을 통해 정보 및 인프라의 가용성, 기밀성, 무결성을 보호하는 것이다.[11] |

[7] European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013.2.7, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS
Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

[8] サイバーセキュリティ基本法 第二条. (한국인터넷진흥원, 2015, p232 재인용)

[9] 온라인자유연합(Freedom Online Coaltion)은 인터넷 자유의 증진을 위해 지난 2011년 27개 정부가 함께 결성한 네트워크이다. 이에 참여한 국가들은 외교적인 노력 및 시민사회, 업계와의 협력을 통해 인터넷 표현의 자유, 집회 결사의 자유 등 인터넷 자유를 증진하고자 한다. 2014년 온라인자유연합은 사이버보안, 디지털 개발과 개방성, 프라이버시와 투명성 등 3개의 워킹그룹을 꾸렸다. 사이버보안 워킹그룹은 사이버 보안 관련 정책에서 핵심적인 고려 요소로서 인권에 대한 관심을 높이는 것을 목적으로 하고 있다. https://www.freedomonlinecoalition.com/about/

[10] Freedom Online Coalition, Why Do We Need a New Definition for Cybersecurity?, https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog8/

[11] PREAMBLE: International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights.
DEFINITION: Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.

대체적으로 보자면, 사이버 보안은 우선 '사이버공간'에서의 문제를 다룬다. 그 대상은 정보, 네트워크, 인프라 등을 포괄하고 있으며, 그 목적은 정보의 '가용성, 기밀성, 무결성'[12]을 보호하는 것이다. 이를 위한 수단은 가이드라인이나 규범을 포함하는 법과 정책, 기술, 교육, 조직 등 다양할 수 있다. 사이버 보안은 그 목적을 달성하기 위한 활동으로 정의되기도 하고, 신뢰성과 안정성이 보장되는 상태를 의미하기도 한다.

현재 국내 법령에서는 사이버 보안이라는 용어를 사용하고 있지 않으며, 대신 '사이버안전', '정보보호', '정보(통신)보안'등이 사용되고 있다.

우선 국가사이버안전관리규정은 '사이버 안전'을 "사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태"로 정의하고 있다. (국가사이버안전관리규정 제2조제3호) 여기서 사이버공격이란 "해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위"를 말한다. 그런데, 이 규정의 적용범위가 국가정보통신망을 대상으로 하고 있기 때문이겠지만, 이 개념은 사이버공격을 국가정보통신망에 대한 공격행위만으로 한정하고 있다는 점에서 사이버 보안 관련 법령에 통일적으로 적용될 수 있는 정의라고 볼 수는 없을 것이다.

여기서 사이버 안전은 사이버 보안과 유사한 개념으로 보이는데, 국내에서 사이버 안전이라는 개념이 사용된 이유는 국가사이버안전관리규정 제정 당시 참여정부가 사이버보안에서 보안이라는 개념이 가진 과거의 부정적인 어감을 고려하여 이를 대체할 새로운 개념을 사용하려고 했기 때문이다.(한국인터넷진흥원, 2015) 그러나 사이버 안전 개념 역시 사이버공격으로부터의 보호만을 규정하고 있는데, 의도적인 공격 외에 사이버 보안을 위협하는 다양한 요인(예를 들어, 관리자의 실수, 시스템 오류, 천재지변과 같은)이 있을 수 있다는 점에서 이러한 개념 정의는 모든 종류의 위협을 포괄하지 못한다.

2016년에 국가정보원이 입법예고한 '국가사이버안보기본법' 제정안은 사이버 안전 대신 '사이버 안보'라는 개념을 사용하고 있다. 여기서 사이버 안보는 "사이버공격과 사이버공격으로 인한 사이버 위기로부터 사이버공간을 보호함으로써 국가의 안전과 이익을 수호하는 활동"으로 정의되어 있는데, 이는 사이버 보안보다는 훨씬 좁은 개념으로 보인다. 즉, 국가 안보(National Security)와 관련된 활동으로 제한되어 있다.

국가정보화기본법 및 정보보호산업의 진흥에 관한 법률은 '정보보호'라는 개념을 사용하고 있다. 그러나 두 법안에서 규정하고 있는 '정보보호'의 정의는 조금 다르다. 또한, 국가정보화기본법은 정보보호시스템으로 '관리적·기술적 수단'만을 포함하고 있는 반면, 정보보호산업의 진흥에 관한 법률은 '물리적 수단'도 포함하고 있다.

[12] 기술적 측면에서 사이버 보안은 정보의 '가용성, 기밀성, 무결성(availability, confidentiality and integrity)'을 보호하는 것이라는 점에는 어느 정도 합의가 있다고 볼 수 있다. Freedom Online Coalition은 사이버 보안에 대한 앞의 정의를 설명하면서, ISO 27000 표준에서 정의하고 있는 바에 따른 '정보의 가용성, 기밀성, 무결성'을 의미한다고 밝히고 있다. 한편, 모질라는 서로 다른 이해관계자 그룹의 사이버 보안 전무가들의 토론 결과를 정리한 보고서(Mozillia, 2015)에서, 사이버 보안에 대한 정의가 맥락에 따라 다양하게 규정될 수 있음에도 불구하고, 사이버 보안의 핵심적 기술 요소로서 '정보의 가용성, 기밀성, 무결성'에 대해서는 일정한 합의가 있었다고 말한다.

"정보보호"란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다. (국가정보화기본법 제2조제6호)

"정보보호"란 다음 각 목의 활동을 위한 관리적·기술적·물리적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다.
가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것
나. 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것
(정보보호산업의 진흥에 관한 법률 제2조 제1호)

‘정보보호’와 거의 같은 개념으로 ‘정보보안’이라는 개념도 사용된다. ‘국민안전처 정보보안 업무 규정’에 따르면 “‘정보보안’ 또는 ‘정보보호’란 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 국가사이버안전관리규정 제2조제3호의 사이버 안전을 포함한다.”고 규정하고 있다(제2조제9호).(한국인터넷진흥원, 2015)

한편, 민간 영역의 사이버 보안을 규율하는 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’(정보통신망법)이나 정보통신기반보호법은 법에서 정보보호나 보안조치에 대한 규정을 포함하고 있음에도 불구하고, 정보보안에 대한 정의 규정을 두고 있지는 않다. 다만, 침해사고에 대한 정의 규정을 두고 이에 대한 예방 및 대응 조치를 규정하고 있다.

"침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다. (정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조1항7호)

2. "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.
3. "침해사고"란 전자적 침해행위로 인하여 발생한 사태를 말한다.
(정보통신기반보호법 제2조)

이처럼 사이버 보안에 대한 개념 정의도 다양하고, 사이버 보안이라는 개념 대신, 사이버 안전, 정보 보안 등 다른 개념이 사용되기도 한다. 그러나 이들 개념은 종종 사이버 보안과 같은 개념으로 사용되기도 하지만, 또 다른 맥락에서는 사이버 보안과 그 의미가 조금 다르게 해석될 수 있다.[13] 예를 들어, ‘정보 보안(information security)’이라고 할 때에는 오프라인 상의

[13] ITU는 사이버 보안과 정보 보안의 차이를 다음과 같이 설명한다. 두 개념 모두 기밀성, 무결성, 가용성의 특성을 유지하고자 한다는 점에서는 같지만, 첫째 정보 보안은 독립적인 시스템으로부터 시작하지만, 사이버 보안은 법적인 불확실성 하에 있는 지구적 위협에 관련된다는 점, 둘째 사이버 보안은 인터넷의 구조 때문에 공격자의 식별을 사실상 불가능하게 만든다는 점, 셋째 정보 보안은 군사적, 외교적인 측면에서 기원했기 때문에 기밀성에 초점을 맞추는 반면, 사이버 보안은 무결성과 가용성에 더 초점을 둔다는 점에서 다르다고 한다. 그래서 사이버 보안은 관할권의 불확실성과 공격자 식별 문제를 가진 정보 보안이라고 본다. (ITU, 2011)

정보에 대한 보안 역시 포괄할 수 있다. 혹은 사이버 보안과 정보 보안이 정치적으로 다른 함의를 갖는 경우도 있는데, UN과 같은 국제 기구에서 러시아나 중국 등이 '정보 보안' 개념의 사용을 선호하는 반면, 미국이나 영국은 이 개념이 '정보' 자체를 위협으로 간주하여 보안 조치가 검열을 야기할 수 있다는 이유로 '사이버 보안' 개념을 사용할 것을 주장하기도 한다.[14] 모질라 재단은 사이버 보안에 대한 최근 보고서(Mozilla, 2015)에서 '컴퓨터 보안' 개념이 주로 (보안 위협에 대한) 전술이나 일상적인 전투에 관련되는 반면, '사이버 보안'은 종종 환경적 요소, 근본적인 비-기술적 규칙들의 조정에 관련되며 전략적이고, 장기적인 권력관계의 변화를 수반한다고 지적하고 있다. 즉, 사이버 보안 개념은 논쟁적이고 광범위한 개념이며, 정치적 맥락에 따라 좌우된다.

이와 같이 사이버 보안은 다양한 맥락에서 사용되고 있고, 세계적으로 합의된 정의도 없다. 이는 사이버 보안에 대한 다양한 이해관계자들(예를 들어, 보안 기술자나 보안 기업, 수사기관, 이용자, 정부 등)의 건설적인 논의를 저해할 수 있다. 인터넷 소사이어티(Internet Society)는 2012년 발간한 보고서에서 사이버 보안 개념이 끔찍하게 부정확하며, 수많은 서로 다른 보안 문제들, 그리고 기술적인 것부터 법적인 것에 이르는 해법을 의미하고 있다며, 사이버 보안이 무엇을 의미하는지에 대한 공통된 이해가 필요하다고 지적한 바 있다. (Internet Society, 2012) 그러한 공통의 이해를 마련하기 위한 기반으로 씽크탱크인 '뉴어메리카'는 사이버 보안 및 정보 보안과 관련하여 국제기구 및 각 국가에서 사용하고 있는 개념들 및 그 의미를 정리하는 작업을 하기도 했다.[15]

사이버 보안을 둘러싼 국가 간의 긴장이 높아지고 있는 상황에서, 사이버 보안에 대한 공유된 정의가 없다는 것은 그러한 긴장을 완화하기 위한 국제적인 논의와 협력을 어렵게 할 수 있다. 일국 내에서도 사이버 보안과 관련한 한 국가의 법률에서 정의가 제대로 되어 있지 않다면, 규제 대상도 모호해지고 관련 법령 간의 일관성이나 체계성도 떨어질 수밖에 없을 것이다. 이런 측면에서 국내 사이버 보안 관련 법령들에서 개념의 정의가 제대로 되어 있지 않다는 점은 심각한 문제이다. 예를 들어, 2016년 국가정보원이 입법예고한 '국가사이버안보기본법' 제정안은 국가안보라는 관점에서 사이버 보안을 바라보고 있다. 그러나 정보통신망법 등은 개인이나 기업의 사이버 보안까지 포괄하는 훨씬 넓은 의미에서 사이버 보안 문제를 다루고 있다.

이 보고서에서는 "온라인 및 오프라인에서 개인의 보안을 증진하기 위해, 정책, 기술, 교육을 통해 정보 및 인프라의 가용성, 기밀성, 무결성을 보호하는 것"이라고 사이버 보안을 정의한 온라인자유연합의 규정에 기반하여 논의하고자 한다.

---

[14] United Kingdom, Submission to the United Nations General Assembly Resolution A/68/156, p. 15
The United Kingdom will use its preferred terminology of "cybersecurity" and related concepts in the present submission, denoting efforts aimed at the preservation of the confidentiality, availability and integrity of information in cyberspace. The term "information security" is often used by business and standards organizations to mean the same thing, and the term is also accepted by the United Kingdom with this specific meaning. There is scope for potential confusion in the use of the term "information security" in that it is used by some countries and organizations as part of a doctrine that regards information itself as a threat against which additional protection is needed. The United Kingdom does not recognize the validity of the term "information security" when used in this context, since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

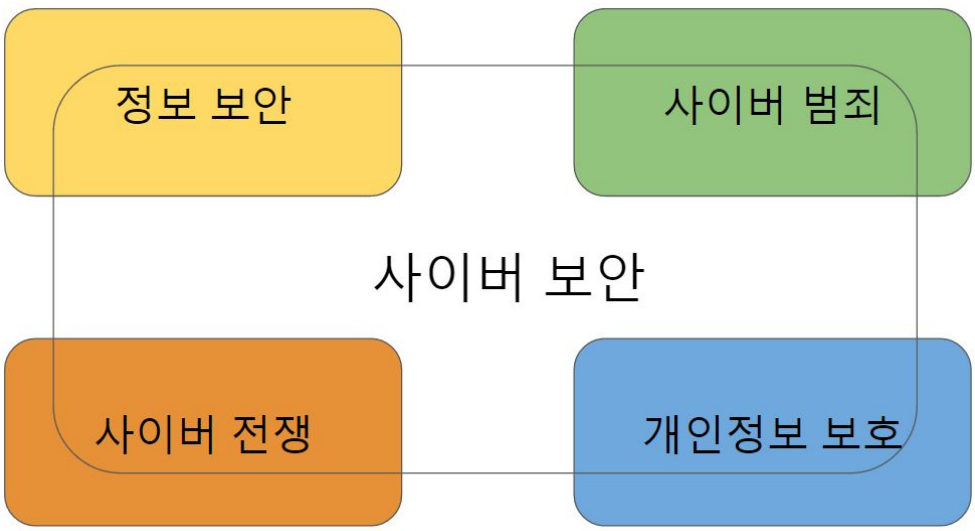
[15] Tim Maurer and Robert Morgus, Compilation of Existing Cybersecurity and Information Security Related Definitions, 2014.11.5,
http://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/

한편, 사이버 보안 문제는 사이버 보안과 관련되지만 독자적인 영역을 갖는 다른 이슈와 연관되어 있다. 첫째, 사이버 범죄 문제이다. 각 국에서 해킹과 같은 특정 행위를 불법화하는 법령을 갖고 있고, 국제적으로는 2011년 체결된 '부다페스트 사이버범죄 조약'이 있지만(한국은 가입국이 아니다), 무엇이 '사이버범죄'에서부터 국제적인 정의나 합의가 되어 있는 것은 아니다. 해킹과 같이 정보화에 따라 새롭게 나타난 범죄에서부터, 온라인을 통한 사기와 같이 전통적인 범죄가 단지 온라인을 통해서 이루어지는 것도 있기 때문이다. 온라인 저작권 침해나 핵티비즘과 같이 불법화 여부에 대해 이견이 존재하는 행위도 존재한다. 사이버 범죄가 세계적으로 이루어질 수 있다는 점에서 사이버 범죄를 단속하기 위한 국가간의 협력을 어떻게 할 것인지, 사이버 범죄 수사 과정에서의 인권 침해를 최소화하기 위한 방안은 무엇인지 등도 쟁점이다.

둘째는 사이버 전쟁의 문제이다. 정보기관이나 군을 중심으로 이루어지는, 적대국을 포함한 해외 국가를 상대로 한 사이버 정보 수집이나 사이버 공격 등을 둘러싼 국가간의 긴장이 높아지고 있다. 혹은 정부와 연결된 민간 해커집단에 의해 상대국에 대한 사이버 공격이 이루어지기도 한다. 이와 관련하여, 한 국가의 다른 국가를 상대로 한 사이버 공격을 어떻게 규정할 것인가(예컨대, 민간 해커의 공격도 국가간의 사이버 공격인가), 어느 정도의 행위를 사이버 전쟁이라고 부를 수 있는가, 공격자에 대한 정확한 파악이 힘들다는 점을 고려할 때 상대국가를 공격자로 규정할 수 있는 근거는 무엇일까, 이와 같은 사이버 공간을 둘러싼 국가간의 긴장을 어떻게 완화할 것인가 등의 문제가 복잡하게 얽혀있다.

셋째는 개인정보 보호 문제이다. 이용자 관점에서 사이버 보안은 개인 정보와 데이터의 보호 문제이기도 하다. 개인정보에 대한 침해자는 해커 뿐만이 아니라, 정부나 기업이 될 수도 있으며, 때로는 '합법적으로' 이루어질 수도 있다. 사이버 보안 사고를 통해 수많은 개인정보 유출이 발생하기도 한다. 따라서 개인정보 보호를 위해서 사이버 보안은 필수적인 전제조건이지만, 개인정보 보호는 그 이상의 문제이기도 하다.

사이버 범죄, 사이버 전쟁, 개인정보 보호 등은 그 자체로 검토되어야 할 중요한 이슈이지만, 이 보고서에서는 정보 보안 측면에서의 사이버 보안, 특히 사이버 보안 관련 법제도와 거버넌스 문제에 집중하여 검토하고자 한다.



# 나. 사이버 보안 관련 국제 동향

사이버 보안은 국제적인 이슈다. 인터넷 자체가 세계적인 네트워크이고 범죄 목적이든 정치적인 목적이든 사이버 위협은 국경을 넘나든다. 이 때문에 테러에 대한 국제적 공조를 위해서, 사이버 전쟁을 둘러싼 국가 간의 긴장 완화를 위해서, 혹은 세계 시민들의 인권 보호를 위해서 사이버 보안을 위한 국제적인 논의가 필요하다. 그리고 이러한 논의에 정부 및 수사기관 뿐만 아니라, 인터넷 서비스 기업, 보안 업체, 기술자 공동체, 인권사회단체, 학계 및 이용자 등 모든 이해관계자들의 참여할 수 있어야 한다.

아직 사이버 보안에 관한 세계적인 조약이나 이를 담당하는 단일한 기구는 없으며, 다양한 공간에서 논의가 이루어지고 있다. '온라인자유연합'은 사이버 보안 관련 국제적인 논의 공간을 다음과 같은 다섯 영역으로 구분하고 있다.[16]

◯ **UN 및 부속 기구** : UN 총회(UNGA), 정부전문가위원회(GGE), 정보사회세계정상회의(WSIS), 국제통신연합(ITU), UN 인권위원회(HRC), 범죄예방및사법정의위원회(CCPCJ), UN 마약범죄사무소(UNODC) 등
◯ **IGF 및 관련 절차들** : 세계 인터넷거버넌스포럼(IGF)과 지역별, 국가별 IGF
◯ **정부 및 정부간 절차들** : 유럽안보협력기구(OSCE), 아프리카연합, 미주기구(OAS), 유럽연합, 나토(NATO), G7, 상하이협력기구(SCO), 아세안지역포럼(ARF), 브릭스(BRICS), 온라인자유연합(FOC), 사이버스페이스세계회의(GCCS) 등
◯ **기술 및 표준수립 기구** : 인터넷 소사이어티(ISOC), 국제인터넷표준화기구(IETF), 인터넷아키텍처위원회(IAB), 월드와이드웹 컨소시엄(W3C), 인터넷주소자원관리기구(ICANN) 등
◯ **기타 절차들** : 국가별, 기업별 침해사고대응팀(CERT 혹은 CSIRT), 사고대응 및 보안팀 포럼(FIRST), 유럽 네트워크 및 정보보안 기구 (ENISA) 등

**유엔 정부전문가그룹(UN GGE)**

UN 차원의 사이버 보안 논의는 '국제안보 관점에서 정보통신기술 발전 방안에 관한 유엔 정부전문가그룹(UN GGE)'[17]을 중심으로 이루어지고 있다. UN 총회 산하에는 3개의 위원회가 있는데, 그 첫번째 위원회가 '군축 및 국제안보(Disarmament and International Security)' 위원회다. 제1 위원회는 UN GGE를 두고 현존하는 사이버 위협 및 잠재적인 위협과 이에 대응한 협력 조치를 논의하고 있다. UN GGE는 세계 사이버 보안 관련 의제를 설정하고, 디지털 공간에 국제법 적용의 원칙을 도입했다는 평가를 받는다.[18]

---

[16] Freedom Online Coalition, Mapping Cybersecurity - A visual overview of relevant global spaces in 2015, 2015.5
https://www.freedomonlinecoalition.com/wp-content/uploads/2015/05/Mapping-Brochure-WEB-1.pdf

[17] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
https://www.un.org/disarmament/topics/informationsecurity/

[18] GIP Digital Watch, "UN GGE", http://digitalwatch.giplatform.org/processes/ungge
GIP Digital Watch는 UN GGE에서 논란이 되고 있는 이슈들을 다음과 같이 소개하고 있다.
- UN GGE의 업무범위에는 포함되지 않으나 사이버 보안 관련한 UN GGE의 활동에 영향을 미치는 이슈들(예를 들어, 인터넷 기반, 콘텐츠 관리, 표현의 자유, 프라이버시 보호, 디지털 경제 등)을 어떻게 다룰 것인가?
- '무력 행사' '무력 공격'에 해당하는 사이버 공격을 어떻게 규정할 것인가?

UN GGE의 구성은 1998년 러시아가 '국제안보 관점에서 정보통신 기술 발전방안(Developments in the Field of Information and Telecommunications In the Context of International Security)' 결의안 초안을 제안한 것이 계기가 되었다. UN GGE는 2004년 첫번째 GGE가 구성된 이후, 2016년-2017년 운영될 5차 GGE까지 5차례에 걸쳐 구성되었다.[19] 2004년 구성된 1차 UN GGE는 미국 등 서방세계와 러시아, 중국 등 상하이협력기구(SCO) 사이의 의견 대립으로 별 성과 없이 종료되었다. 러시아와 중국, 브라질, 벨라루스는 국제사회의 간섭이나 제한 없이 자국의 정보안보와 관련된 행위를 보장하는 것을 강조한 반면, 미국과 EU 국가들은 군축과 관련된 용어들이 포함되는 것을 거부했기 때문이다. 또한, 국경을 넘나드는 콘텐츠 역시 정보 보안의 위협으로 볼 것인지에 대한 국가간 이견이 존재했다. 그러나 2009년 구성된 2차 GGE에서는 논의의 진전이 있었는데, 이는 2007년 에스토니아에서 발생한 국가적 차원의 사이버 공격 등으로 인해 세계적인 차원의 사이버 보안 논의의 필요성에 대한 공감대가 커졌기 때문이다. 2차 GGE는 UN 총회 보고서를 제출하였는데, 현재 상황과 위협 현황, 그리고 이를 해결하기 위한 협력 방안에 대한 아이디어와 함께 향후 해당 과제를 논의하기 위한 권고사항을 포함하였다.

2012년 구성된 3차 GGE는 권고안[20]에 합의하였는데, 이는 국제안보 차원에서 사이버보안 관련 최초의 국제적 합의라는 점에서 의미를 부여할 수 있다. 이 권고안은 국제안보적 차원에서 사이버 보안 이슈를 다루어야 할 필요성에 대한 인식에 동의하였으며, 비국가 행위자 뿐만 아니라 국가 역시 위협이 주체가 될 수 있다는 점을 인정하였다. 또한, 그동안 논란이 되었던 이슈 중 하나는 기존의 국제법이 사이버 공간에 적용될 수 있는지 였는데, 이번 권고안에서 UN 헌장을 포함한 국제법이 사이버 공간에 적용된다는 것을 합의하였다. 또한, 권고안은 "국가의 주권과 국제적인 규범과 원칙이 ICT 관련 국가의 행위 및 국경 내의 ICT 기반에 대한 관할권에 적용된다"는 것과 "국가는 자신들이 원인이 된 국제적인 잘못된 행동에 대해 국제적인 의무를 부담해야 한다"는 것을 확인하였다. 더불어, "ICT 보안 문제 해결을 위한 국가의 노력은 세계인권선언 및 다른 국제기구에 의해 확립된 인권과 기본적 자유에

---

- 중요 인터넷 기반(예를 들어, DNS 시스템)의 보호는 UN GGE의 업무 범위에포함되는가?
- 기존의 국제법 규범을 적용하는 것으로 충분한가, 아니면 새로운 규범이 필요한가?
- 사이버 공간은 국제 문제에 있어서 고유한 영역인가?
- 디지털 이슈에서 정부의 책임을 어떻게 규정할 것인가?
- 다른 국가의 사이버 기반에 대한 비정부 행위자의 행위에 대해 정부가 책임이 있는가?
- UN GGE는 사이버 공간의 군축과 비군사화, 혹은 무력 분쟁 법의 보다 정확한 사용에 초점을 맞추어야 하는가?
- 평화 시기에 중요 기반을 공격하지 않는다는 규범을 어떻게 운용할 것인가?
- 디지털 중요 기반은 세계적 공공재인가?
- 제한된 회원제를 넘어 어떻게 UN GGE의 활동에 더 많은 참여를 보장할 것인가? (특히, 어떻게 개발도상국들을 참여시킬 것인가)
- 어떻게 기술적, 법적, 정책적으로 사이버 공격의 책임자 귀속 문제를 다룰 것인가?
- 사이버 기술의 양면적 성격을 다룰 것인가?
- 기술계, 업계, 시민사회와 어떻게 효과적으로 소통할 것인가?

[19] 1차 GGE (2004-2005) : UN 총회 결의안 A/RES/58/32
2차 GGE (2009-2010) : UN 총회 결의안 A/RES/60/45
3차 GGE (2012-2013) : UN 총회 결의안 A/RES/66/24
4차 GGE (2014-2015) : UN 총회 결의안 A/RES/68/243
5차 GGE (2016-2017) : UN 총회 결의안 A/RES/70/237

[20] UN GA(2013), "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 2013.6.24, A/68/98, https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf

대한 존중과 함께 가야 한다"고 강조하고 있다.[21] 국가의 의무와 책임, 신뢰구축조치(Confidence Building Measurements, CBM) 등 국가간의 분쟁을 예방하고 협력을 증진하기 위한 방안도 포함되었다. 2014년 구성된 4차 GGE는 3차 권고안을 확대하여 국가 책임행위 관련 규범, 주요기반시설 보호, 신뢰구축조치 등에 대한 진전된 합의안[22]을 도출하였다. (장규현, 임종인, 2014; GIP Digital Watch)

UN 총회 제3 위원회인 '사회, 인도주의 및 문화위원회'는 2000년에 범죄 예방 및 사법 정의 관련 사업의 일환으로 '정보기술의 범죄적 이용에 대한 대응'을 논의하였고, 몇 년 후에 사이버 범죄 관련 논의는 '범죄예방 및 사법정의 위원회(CCPCJ)'로 이동하였다. 제2 위원회인 '경제 및 금융위원회'는 '지구적 사이버보안 문화의 형성'에 초점을 둔 결의안들을 채택하였는데, 이는 2002년에 미국 정부가 제안한 것으로 핵심 정보 인프라 보호를 강조하고 있다.[23]

**국제전기통신연합(ITU)과 사이버 보안**

국제전기통신연합(ITU)는 정보통신기술을 담당하는 UN 기구이며, 표준 제정 등 국제적인 전기통신 인프라가 상호 운용가능하도록 조정하는 역할을 맡아왔다. 반면, 인터넷 기술 표준은 주로 IETF와 같은 기술자 커뮤니티 기구를 통해서 이루어져 왔으며, 이는 국가간의 합의에 의한 것이 아니라 사실상의 표준으로 자리잡아 왔다. 그래서 인터넷 공공정책 이슈와 관련된 ITU의 역할은 아직 여전히 논란이 되고 있는 상황이며, 사이버 보안 문제 역시 예외는 아니다. 정부간 기구로서의 ITU의 역할은 전통적으로 통신 인프라와 관련되어 왔는데, 인프라, 프로토콜, 콘텐츠의 구분이 모호하거나 상호 영향을 미칠 수 있기 때문이다.

ITU의 사업은 라디오 통신을 담당하는 ITU-R, 전기통신 표준을 담당하는 ITU-T, 전기통신 개발을 담당하는 ITU-D 부문으로 나뉘어 지는데, 사이버 보안은 주로 ITU-T와 ITU-D의 관할에 속한다. 앞 장에서 보았듯이, ITU는 사이버 보안을 "사이버환경, 기관 및 사용자의 재산을 보호하기 위하여 이용될 수 있는 수단, 정책, 안보개념, 안보조치 및 가이드라인, 위험관리 방법·행위·훈련, 최상의 관행·보장조치·기술의 집합"으로 정의하고 있다. 현재 사이버 보안과 관련된 ITU의 사업은 정보사회세계정상회의(WSIS)[24]의 행동지침(action line) 5 "ICT 사용에 있어서 신뢰와 보안의 구축"에 근거하고 있다. 이에 따라 ITU는 2007년 '지구적 사이버보안 의제(Global Cybersecurity Agenda, GCA)'를 출범시켰는데, 이는 사업영역으로 법적 조치, 기술 및 절차적 조치, 조직 구조, 역량 강화와 국제 협력 등을 규정하고 있다. (ITU, 2011) GCA의 구현을 위한 핵심 사업은 "IMPACT(Multilateral partnership Against Cyber Threat)" 프로젝트[25]인데, 이는 ITU의 193개 회원국과 UN 산하 기구들에게 사이버 보안 지원을 제공하는 역할을 한다.

---

[21] Freedom Online Coalition, "Cybersecurity and the United Nations", 2014. https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/cybersecurity-and-united-nations/

[22] UN GA(2015), "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 2015.7.22, A/70/174, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[23] Freedom Online Coalition, 앞의 글.

[24] WSIS는 2003년 제네바, 2005년 튀니스 등 두 차례에 걸쳐 개최된 정보사회와 관련된 세계 회의로서, ITU는 WSIS를 주관하기도 하였다.

[25] http://www.impact-alliance.org/

이 외에 ITU가 사이버 보안 관련해서 수행하는 사업들[26]은 각 국의 사이버 보안 수준을 측정하는 글로벌 사이버보안 인덱스, 최빈국의 사이버보안 증진, 국가적인 사이버긴급대응팀 설립을 지원하는 CIRTs 프로그램, 온라인 아동보호 사업, 국가 사이버보안 전략[27] 등이 있다.[28]

### 사이버 보안 관련 UN 인권기구의 역할

앞서 살펴본 것이 사이버 보안에 초점을 둔 UN의 활동이었다면, UN 내에는 사이버 보안 관련 논의가 국제인권 규범을 준수하면서 이루어질 수 있도록 역할하는 단위도 존재한다. UN 인권이사회, UN 인권최고대표사무소(Office of the High Commissioner for Human Rights, OHCHR), 인권조약 기구(Human rights treaty bodies), UN 특별보고관 제도 등이 그것이다. UN은 특정 주제나 국가와 관련된 이슈를 조사하고 보고서를 작성하는 특별보고관 제도를 두고 있는데, 여러 특별보고관이 사이버 보안 및 인권 이슈를 직간접적으로 다루고 있다.[29]

2013년 6월 에드워드 스노든이 미 국가안보국(NSA)의 대량감청을 폭로하기 이전, UN 표현의 자유 특별보고관 프랑크 라 루는 2011년 UN 총회에 제출한 보고서에서 인터넷 관련 인권 이슈를 폭넓게 검토했으며[30], 2013년 4월에는 국가의 통신감시 문제를 다룬 보고서를 발표하였다.[31]

스노든의 폭로 이후, 각 국 정부기관에 의한 무차별적 대량 감청과 개인정보 수집으로 인한 프라이버시 침해 문제를 어떻게 해결할 것인지가 전 세계적인 관심사로 떠올랐으며, UN에서도 예외는 아니었다. 2013년 12월 18일, UN 총회는 '디지털 시대의 프라이버시권'[32] 결의안을 만장일치로 채택하였다. 이 결의안은 △ 디지털 통신을 포함하여, 프라이버시권을 존중하고 보호할 것, △ 자국법이 국제인권법을 준수하고 있는지를 포함하여, 권리 침해를 막을 조치를 취할 것, △ 통신감시, 감청, 개인정보 수집과 관련하여 절차와 관행, 법률을 재검토할 것, △ 국가 감시를 감독할 독립적이고 효과적인 감독기구를 설립할 것 등을 권고하였다.

이어 UN 총회는 2014년 11월 18일, 2차 결의안을 채택하였다.[33] 이 결의안에서는 UN 인권이사회로 하여금 프라이버시권에 대한 특별절차(Special Procedures) 수립을 검토하도록 하는 내용이 포함되어 있었는데, 이에 따라 2015년 7월 3일, UN 인권이사회는 첫번째 프라이버시권 특별 보고관으로 조셉 카나타치(Mr. Joseph CANNATACI)를 임명하였다.[34]

---

[26] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
[27] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx
ITU는 현재 각 국가의 사이버 보안전략 수립을 위한 툴킷을 만들고 있는데, 2016년에 공개할 계획이라고 한다.
[28] Freedom Online Coalition, "Cybersecurity: what's the ITU got to do with it?", 2014, https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog7/
[29] Freedom Online Coalition, " Utilizing the UN Human Rights Mechanisms for the Advancement of Digital Rights, by Sarah McKune", 2015. https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog-6/
[30] A/HRC/17/27, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement
[31] A/HRC/23/40
[32] The right to privacy in the digital age. A/RES/68/167. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167
[33] A/RES/69/166. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166
[34] http://www.ohchr.org/EN/HRBodies/SP/Pages/HRC29.aspx

2014년 UN 총회에 요청에 따라 UN OHCHR은 '디지털 시대 프라이버시권' 보고서를 제출하였다.[35] 이 보고서는 정보기관의 대량 감시(mass surveillance)및 전자적 수단을 이용한 국가 감시(state surveillance) 문제에 대한 분석과 권고를 담고 있는데, △ 많은 국가들의 전자감시에서 국제인권법 위반을 발견하였고 △ 전자감시에 효과적으로 대응하기 위해 다양한 이해관계자(multi-stakeholder)의 참여가 필요하다고 결론을 내리며, △ 국내 법, 정책과 관행의 국제인권법 준수 여부에 대한 검토 △ 명확하고 엄밀한 입법체계와 효과적이고 독립적인 감독 제도와 관행을 마련 등을 각국에 권고하였다.

한편, 2014년 9월 23일, 벤 에머슨 유엔 반테러와 인권보장 특별보고관은 제69차 유엔 총회에 제출한 4차 연례보고서에서 반테러 목적으로 대량 전자 감시를 시행하는 문제와 대규모 접근기술이 자유권협약 제17조 프라이버시권에 미치는 함의에 대하여 검토하였다.[36] 특별보고관은 보고서에서, 테러와의 전쟁이 너무나 중요해서 원칙적으로는 인터넷 대량 감시를 그럴듯하게 정당화할 수 있는 여지를 줄 수 있다며, 그러나 "대규모 접근 기술은 온라인 프라이버시를 무차별적으로 좀먹고 프라이버시권의 가장 본질적인 내용을 침해" 한다며, "각국 정부는 자신들의 인터넷 침투 활동의 성격과 범위, 그 방법론 및 정당성에 대해 투명해야 하고, 그 사용으로 축적된 실제 편익에 대해 공개적으로 상세하게 설명해야" 한다고 지적했다.

2015년 5월 22일, 프랑크 라 루 이후 UN 표현의 자유 특별보고관을 맡은 데이비드 케이는 '암호화와 익명성'에 대한 보고서를 발표했다.[37] 이 보고서에서 데이비드 케이는 디지털 시대에 안전한 소통을 위해 암호화와 익명성이 어떤 역할을 하는지, 그것이 표현의 자유 및 프라이버시와 어떠한 관계가 있는지, 암호와와 익명성을 제약하는 현실의 문제는 무엇인지를 검토하고, "암호화와 익명성은 디지털 시대 표현의 자유권 행사를 위해 필요한 프라이버시와 보안을 제공한다"며, 각 국가는 암호화와 익명성을 증진해야 하며, 이를 제한하지 말 것을 권고하였다.

### 멀티스테이크홀더 논의 공간인 인터넷거버넌스포럼

시민사회가 의견을 제출하는 통로가 없는 것은 아니지만, 결국 UN은 정부간 기구이기 때문에 비정부 이해관계자의 참여는 제한적일 수밖에 없다. 이런 점에서 인터넷거버넌스포럼(IGF)은 정부 뿐만 아니라 세계 인권, 사회단체 등 비정부 당사자들이 사이버 보안과 관련된 자신의 견해를 표명할 수 있는 좋은 공간이다. IGF는 2005년 정보사회세계정상회의(World Summit on Information Society, WSIS)의 결과물인 튀니스 어젠더(Tunis Agenda)에 따라, 2006년부터 개최되고 있는 멀티스테이크홀더 국제 포럼이다. IGF는 각 국가에 구속력 있는 결정을 하는 기구는 아니지만, 디지털 권리, 망중립성, 접근권과 개발 등 다양한 이슈들이 정부, 업계, 시민사회, 기술계, 학계 등 관련 이해관계자들의 자유롭고 개방적인 참여에 기반하여 논의되는 공간인데, 사이버 보안은 매해 개최되는 IGF의 주요 의제 중의 하나이다. IGF는 구속력이 없는 반면, 오히려 그렇기 때문에 사이버 보안에 대한 다양한 이슈들이 보다 자유롭게 논의될 수 있다는 장점이 있다.

---

[35] A/HRC/27/37. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[36] A/69/397. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement
[37] A/HRC/29/32. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

세계 IGF는 UN의 주관 하에 개최되지만, 각 지역별, 국가별 IGF는 각 지역 및 국가의 주체들에 의해 자발적으로 운영이 된다. 현재 유럽 지역의 EuroDIG, 아프리카 지역의 AfIGF, 남미와 캐리비안 지역을 포괄하는 LACIGF, 아랍 지역의 ArabIGF, 아태지역을 포괄하는 AprIGF 등이 개최되고 있다. 각 국가별로도 national IGF를 개최하는 나라들이 있는데, 한국 역시 2013년부터 한국 IGF(KrIGF)[38]를 개최하고 있다.

**NATO 공동사이버방위센터(CCD COE)와 탈린매뉴얼**

UN 차원의 논의 외에 지역적 차원의 다양한 정부간 기구에서 사이버 보안 이슈를 다루고 있다. 2008년 5월 14일 설립된 북대서양조약기구(NATO) 산하 공동사이버방위센터(CCD COE)[39]는 국제군사조직으로서 NATO 가입국 및 협력국 사이에 교육, 연구 및 개발, 협의 등을 통해 사이버 방위 영역에서 역량 강화, 협력, 정보 공유를 증진하는 것을 목적으로 한다. 애초에 2003년부터 에스토니아가 설립을 제안하였는데, 2007년에 발생한 에스토니아에서의 대규모 사이버 공격 사태가 이 센터 설립의 계기가 되었다. 2013년, CCD COE는 '사이버 전쟁에의 국제법 적용에 관한 탈린 매뉴얼'[40]을 공식적으로 발표하였다. 탈린매뉴얼은 전쟁선포 및 전쟁행위의 정당성, 관할권, 국가 책임, 자위권, 무력분쟁, 대응조치, 사이버공격 대상의 제외, 사이버공격 시 전쟁포로 보호, 인프라 공격 시 주의, 중립지역에서 공격권 행사금지 등의 내용을 다루고 있는데, NATO의 공식 문서는 아니며 독립적인 전문가들에 의해서 쓰여지기는 했지만, 사이버공간에서 국제법 적용방안을 모색했으며 각 국의 정책 수립과 전략 수립의 기초가 될 수 있다는 점에서 많은 시사점을 제공하고 있다.(장규현, 임종인, 2014;2016국가정보보호백서) 2016년에는 탈린매뉴얼 2.0이 발표되었다. 기존의 탈린매뉴얼이 '무력 공격'에 해당하는 파괴적인 사이버 작전에 대한 것이라면, 탈린매뉴얼 2.0은 그 보다 낮은 수준의 일상적인, 악의적 사이버 작전의 문제를 다루고 있다.[41]

**사이버스페이스 세계회의**

최근 사이버 보안과 관련한 세계 포럼으로서 주목받고 있는 것은 사이버스페이스 세계회의(Global Conference on CyberSpace, GCCS) 혹은 런던 프로세스(London Process)이다. 이 회의는 2011년 영국 외무부장관인 윌리엄 헤이그가 개최한 '사이버스페이스 런던 회의'[42]로 시작되었다. 이 회의는 사이버 보안, 사이버 범죄, 국제평화와 안보, 경제성장과 개발 등의 의제를 다루는 장관급 회의였다.

이 회의에 이어, 2012년에는 부다페스트에서 2차 회의가 열렸고, 2013년에는 서울에서 개최되었다. 서울 회의에서는 처음으로 기존의 다양한 원칙과 가이드라인을 종합한 '사이버스페이스 서울 선언문'이 채택되었다.[43] 런던 프로세스는 사이버 보안 의제에 개발도상국의 참여를 이끌어 냈다는 의미가 있는데, 서울 회의에서는 90개 정부에서 참여했으며 그 중 반 이상이 장관급 이상이었다. 4차 회의는 2015년 4월 16-17일, 네덜란드 헤이그에서 개최되었다.[44] 기존에는 정부 중심의 회의였다면, 4차 회의에서는 비정부 참여자를 적극적으로 참여시켜 보다 포괄적인 회의가 되었다는 의미가 있다. 특히, 시민사회

[38] http://krigf.kr/
[39] Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/about-us.html
[40] Michael N. Schmitt et al.(2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press.
[41] https://ccdcoe.org/research.html
[42] https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement
[43] http://www.korea.net/NewsFocus/Sci-Tech/view?articleId=110835
[44] https://www.gccs2015.com/

자문위원회를 구성하여 시민사회의 참여를 촉진한 결과 250명 정도의 시민사회 인사들이 참여하였으며, 효과적인 참여를 위해 시민사회의 사이버 보안 역량강화를 위한 사전 교육 프로그램을 마련하기도 하였다.[45] 또한, 사이버긴급대응팀(CERTs)와의 연계 강화를 위해 네덜란드 CERT는 ONE conference라는 별도의 행사를 조직하였다.[46]

# 다. 주요 국가의 사이버 보안 정책

이미 세계 각 국은 자신의 인터넷 발전 수준, 사이버 위협의 정도, 자신의 법제도적 맥락에 따라 나름의 사이버 보안 관련 전략을 수립하고, 관련 법제나 정책을 시행하고 있다. 사이버 보안이 개인의 정보통신 기기의 보안에서부터, 사이버 공간에서의 국가간 분쟁에 이르기까지 다양한 영역에 걸쳐있고, 인터넷이 정치, 경제, 문화 등 사회의 모든 부문에 긴밀하게 결합되면서 사이버 보안 정책의 폭도 무척 넓다. 국가안보적 측면에서의 사이버 위협에 대한 대응에서부터, 온라인 사기 등 사이버 범죄, 컴퓨터 시스템의 보안, 국가간의 사법 공조나 분쟁을 막기 위한 신뢰구축조치까지 사이버 보안 정책에 관련된다고 할 수 있다. 또한, 사이버 보안을 위해서는 관련 법제도의 구축 뿐만 아니라, 보안을 위한 투자, 기술 개발 및 연구, 역량있는 관리인력의 양성, 개인들의 보안 인식 등 다양한 수준에서의 대응과 이들간의 협력이 필요하다.

ITU는 각 국가의 사이버 보안 정책 수립에 도움이 될 수 있는 가이드를 만들면서, 세계 사이버 보안 의제를 법적조치(Legal Measure), 기술적, 절차적 조치(Technical and Procedural Measure), 조직 구조(Organizational Structure), 역량강화(Capacity Building), 국제협력(International Cooperation)으로 구분한 바 있다. (ITU, 2011)

본 보고서에서는 미국, 유럽연합, 영국, 일본 등 주요 국가의 사이버 보안 전략의 방향, 주요 법제 및 조직 구조를 중심으로 다루고자 한다. 물론 사이버 보안을 위해서는 기술개발과 연구, 교육 및 인력양성, 국제협력 등도 중요하며, 군사적 측면의 사이버 보안 대응 및 사이버 범죄의 대응도 그 자체로 중요한 영역이기는 하지만, 이 보고서에서 중점적으로 다루지는 않는다.

## 1) 미국

미국은 1980년대 중반부터 컴퓨터 보안과 관련된 법률[47]을 갖고 있었으며, 1998년 5월 대통령 지침(Presidential Decision Directive) 제63호를 통해 주요 기반시설에 대한 범정부적 보호체계를 처음으로 마련하였다.(박영철 등, 2015) 2001년 9.11 테러가 발생한 이후 국가 기반시설의 보안에 대한 중요성이 증대되었는데, 2002년 11월 국토안보법(Homeland

[45] https://www.gccs2015.com/participants/civil-society
[46] Freedom Online Coalition, "Promoting International Norm Development in Cyberspace through the “London Process”", 2015, https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/wg-1-blog-3/
[47] 1980년부터 1990년대에 제정된 미국의 사이버안보 관련 법안은 아래와 같다.「위장접근수단 . 컴퓨터사기 및 컴퓨터남용법」(Counterfeit Access Device and Computer Fraud and Abuse Act)(1984),「전자통신 사생활보호법」(Electronic Communications Privacy Act)(1986),「컴퓨터 보안법」(Computer Security Act)(1987),「문서감축법」(Paperwork Reduction Act)(1995),「정보기술관리 개혁법」(Information Technology Management Reform Act 또는 Clinger-Cohen Act)(1996) (KISA, 주요정보통신기반보호 강화 방안 마련, 2013. 12)

Security Act)이 제정되면서 국토안보부(Department of Homeland Security, DHS)가 신설되었고, 국토안보부는 국토안전 뿐만 아니라 사이버 보안의 주무부처가 되었다.

같은 해인 2002년 전자정부법(E-Government Act of 2002)의 일부분인 연방정보보안관리법(Federal Information Security Management Act, FISMA)이 제정되었는데, 이 법은 미국 정부기관의 사이버 보안 절차를 표준화하기 위해 국가표준기술원(NIST)이 개발한 위험관리 프레임워크를 도입하였다. 이 법은 관리예산처(Office of Management and Budget, OMB) 내에 연방최고정보책임자를 두고 정부의 기술 사용을 감독하였다. 연방 컴퓨터 시스템의 보안 표준에 대한 NIST의 책임을 강화하였고, 관리예산처가 연방 사이버 보안 표준 공표의 책임을 지도록 하였다. (Piret Pernik 등, 2016) 그러나 FISMA는 비효율적이라는 비판을 받았고, 2014년 12월에 연방정보보안현대화법(Federal Information Security Modernization Act of 2014)으로 개정되게 된다.

미국은 2003년에 처음으로 국가 사이버 보안 전략(National Strategy to Secure Cyberspace of 2003)[48]을 수립하였다. 여기서 설정한 전략 목표는 3가지 였는데, 첫째 사이버 공격으로부터 국가 기반시설의 보호, 둘째 사이버 공격으로부터의 국가적 취약점 축소, 셋째 사이버 공격 발생시 피해 및 복구시간 최소화이다. 이러한 목표를 위한 5가지 우선 사업은 연방 컴퓨터 시스템 및 네트워크의 보호, 대응 시스템 개발, 위협 및 취약점 감소 프로그램, 사이버 보안 인식 제고 및 훈련 프로그램, 국제 협력 시스템의 개발 등이다.(Piret Pernik 등, 2016)

2008년 1월, 부시 행정부에서 발표된 '국가보안 대통령지침 54(National Security Presidential Directive 54)와 '국토보안 대통령지침 23(Homeland Security Presidential Directive 23)에 따라 '국가 사이버 보안 종합계획(Comprehensive National Cybersecurity Initiative, CNCI)이 만들어졌다. CNCI의 목적은 법집행, 정보수집, 방첩, 군사력을 포함하는 포괄적 접근을 통해 모든 종류의 사이버 위협에 대해 방어하고 사이버 보안 환경을 강화하는 것이다.

2009년 1월 출범한 오바마 정부는 CNCI를 발전시킨 전략 체계를 마련하기 위해 2009년 5월 <사이버공간 정책 리뷰(Cyberspace Policy Review)>[49]를 발표하였다. 이는 사이버 보안 진행 상황을 전체적으로 점검하여, 정책, 법 구조, 관리, 조정, 연구 등에 있어서 핵심적인 문제점을 파악하기 위한 것이었다. 정책 리뷰는 ▸백악관, 연방정부 등 최상위 리더십에 따른 정책 추진(Leading from the top), ▸보안교육, 전문 인력 양성 등 디지털 국가를 위한 역량 제고(Building Capacity for a Digital Nation), ▸민·관 협력을 위한 파트너십 구축 등 공동 책임(Sharing Responsibility for Cybersecurity), ▸효율적인 정보 공유 및 사고 대응 능력제고(Creating Effective Information Sharing and Incident Response), ▸혁신 촉진 (Encouraging Innovation) 등의 의제를 담고 있으며, 그 이행을 위해 10개의 단기 과제와 14개의 중기 과제를 제시하였다. 사이버공간 정책 리뷰의 발표로 인해 기존에 국토안보부 장관이 맡고 있는 사이버 보안 컨트롤타워의 역할이 백악관 내에 신설된 사이버보안조정관(Cybersecurity Coordinator)으로 이전되었다.

사이버 보안과 관련된 미국의 법률은 필요에 따라 그때그때 만들어져 왔다. 그래서 사이버 보안에 관련된 특정 주제에 초점을 맞춘 법률이 50여 개에 이르지만, 현재의 사이버 보안 전략 전체를 아우르는 포괄적인 법률은 없는 상황이다.(Piret Pernik 등, 2016)

[48] https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
[49] https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

**사이버 보안 정책 추진체계**


그럼 : 미국 사이버보안 정책 추진체계 (출처 : 박영철 등, 2015)

사이버 보안 관련 최고 정책 조정 역할은 백악관 국가안보위원회(National Security Council) 산하 '정보통신기반 기관간 정책위원회(Information and Communications Infrastructure Interagency Policy Committee, ICI-IPC)에 있다. ICI-IPC는 국토안보위원회와 국가안보위원회 사이버보안국(Cyber Security Office)의 사이버보안조정관이 공동 의장을 맡고 있다. 사이버보안조정관은 기관간 국가 사이버 보안 전략 및 정책 개발을 주도하고 그 정책의 이행을 감독하며, 국가안보위원회의 대통령 수석 자문으로 역할한다.(Piret Pernik 등, 2016)

국토안보부(DHS)는 주요 기반시설 보호를 위한 전반적인 연방정부의 활동을 담당한다. 국토안보부 산하  국가보호및프로그램부(National Protection and Programs Directorate, NPPD)는 법집행 외에 국토안보부의 국가적 사이버 보안 사업의 집행을 책임진다.

미국의 외교정책을 책임지는 국무부(DoS)는 사이버 보안 관련해서는 외국 정부와의 협력 등 국제적인 사이버 보안 정책을 조정한다. 법무부(DoJ)는 산하에 연방수사국(FBI)를 두고 있으며, 침해 사고에 대한 조사 및 기소, 공격자에 대한 정보수집, 다른 부처에 대한 법적, 정책적 지원 등 사이버 보안 관련 법집행을 책임진다. 또한, 해외 정보기관, 테러리스트 등 국가적 보안 위협에 대응하는 국내 사이버 보안 작전을 수행한다. 국방부(DoD)는 2010년 5월 사이버 공간에서의 작전 능력 강화를 위해 사이버사령부(USCYBERCOM)를 개설하였다. 상무부는 산하에 국립표준기술원이 있으며, 사이버 보안 기준을 만족하는 제품 및 서비스를 보급한다. (박영철 등, 2015)

미국 국가정보국(Director of National Intelligence, DNI)는 대부분 국토안보부와 국방부 산하에 있는 17개 정보기관을 조정한다. 정보통신 인프라를 통해 흐르는 정보 역시 담당하는

정보기관의 특성상 정보기관 역시 사이버 보안과 연결될 수밖에 없다. DNI 내에 사이버 보안 관련한 주요 정보기관은 국가안보국(NSA)인데, NSA 국장은 DNI에 보고하며, 국방부의 여러 단위에 신호정보를 제공한다. (Piret Pernik 등, 2016)

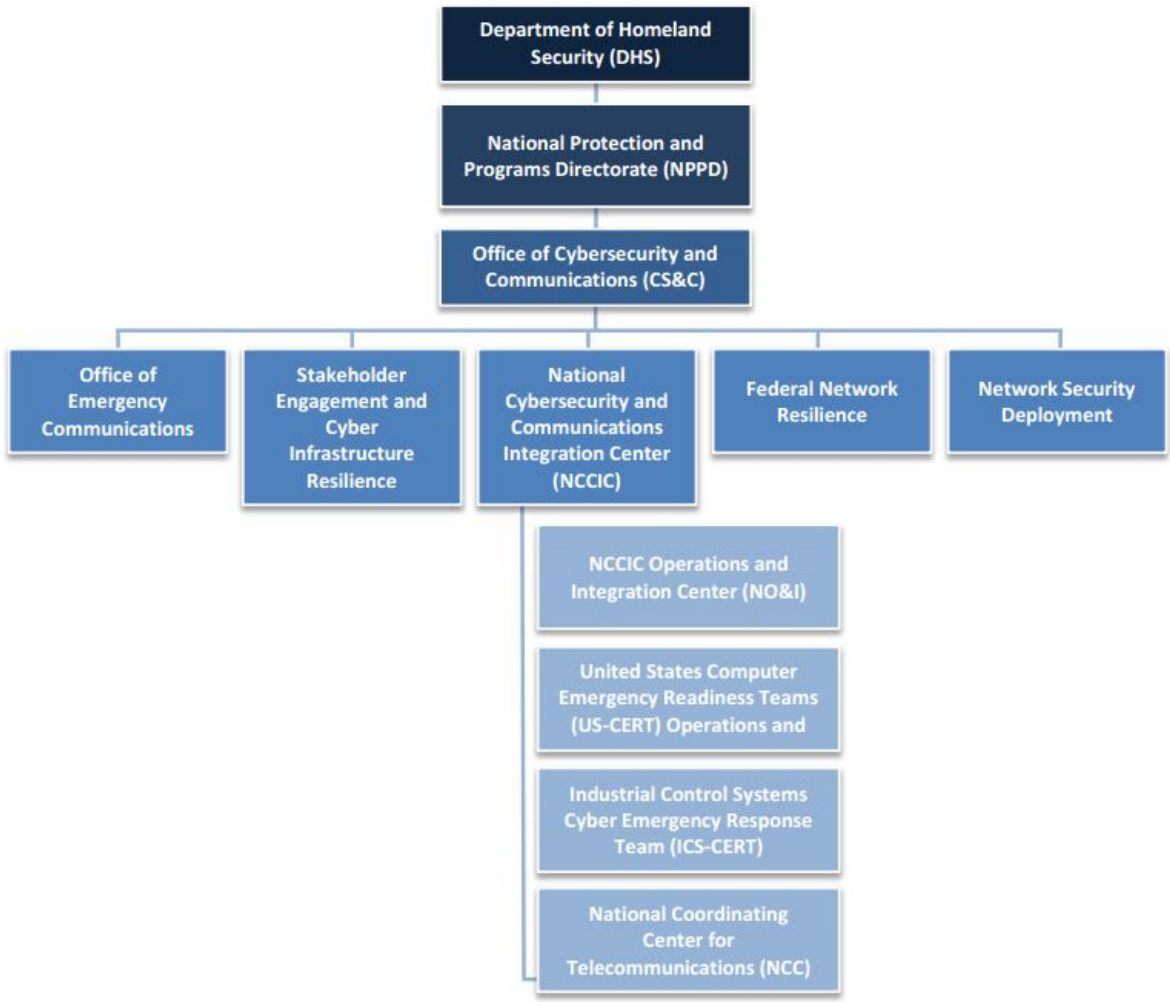



그림 : 사이버보안 및 통신국(CS&C) 조직구조 (출처 : Piret Pernik 등, 2016)

국토안보부의 국가보호및프로그램부(NPPD) 산하의 '사이버보안 및 통신국(Office of Cybersecurity and Communications , CS&C)은 미국 전역의 사이버 통신 기반에 대한 위기 관리, 사고 대응, 방어 능력을 제공한다. 그 산하에 국가 사이버보안 및 통신통합센터(National Cybersecurity & Communications Integration Centre, NCCIC)를 두고 주요 기반시설의 사이버 보안을 조정한다. NCCIC는 연방정부, 정보 기관, 법집행기관의 소통을 통합하는 관리 센터를 제공하며, 모든 수준에서 정부와 민간영역 사이의 협력과 정보 공유를 강조하고 있다. 그러나 민간 기업에 특정 조치를 강제할 권한은 없으며, 취약점, 침입, 사고, 복원 등에 대한 적절한 상황 인식을 제공한다.  NCCIC는 그 산하에 작전 및 통합센터(NO&I), 미국 컴퓨터 긴급준비팀(US-CERT), 산업적 미국컴퓨터긴급준비팀(ICS-CERT), 국가통신조정센터(NCC)를 두고 있다.(Piret Pernik 등, 2016)

**주요 기반시설의 사이버 보안**

주요 기반시설에 대한 미국의 전략적 접근은 정부 기관이 조정 및 우선순위 설정의 책임을 갖지만, 공공-민간 파트너쉽을 강조하고 있다는 점이다. (Piret Pernik 등, 2016) 1998년 5월

대통령 지침(Presidential Decision Directive) 제63호를 통해 주요 기반시설에 대한 범정부적 보호체계를 처음으로 마련하였고, 2002년 국토안보법에 의해 설립된 국토안보부가 주요 기반시설 보호에 관한 조정 역할을 하였다.

오바마 대통령은 주요 기반시설 보호에 대한 국토안보부의 책임을 법률로 뒷받침하고자 사이버 정보공유 및 보호법(Cyber Intelligence Sharing and Protection Act), 사이버보호법(Cyber Security Act of 2012) 등을 추진했지만 의회 통과에 실패하였다. 그 대신 오바마 정부는 행정명령[50] 13636(Executive Order 13636) '주요 기반시설 사이버보안의 증진'[51]과 대통령 정책지침 21(PPD-21) '주요 기반시설 보안 및 복원'(PPD-21)을 발표하였다. 행정명령은 주요 기반시설의 보호체계 구축을 위한 사이버보안 프레임워크의 개발과 보급을 핵심 목적으로 하며, 주요 내용은 사이버보안 관련 정보공유 시스템 구축, 주요 기반시설에 대한 사이버보안 프레임워크 개발 및 보급, 사이버보안 강화 프로그램 추진 등이다. 이러한 행정지침에 따라 일반 행정기관의 하나인 상무부 소속 국립표준기술연구소(NIST)의 주도로 사이버 보안 프레임워크[52]가 개발되어 2014년 2월 최종안이 발표되었다. 이 프레임워크는 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover) 등 각 기능별로 구체적인 사이버 보안 활동을 명시하고, 이를 각 기관(공공기관 및 주요 기반시설을 운영하고 있는 민간기업)에서 어떻게 적용할 것인지에 대한 표준을 제시한다. 또한, 2013년 6월에는 기업들이 이 프레임워크를 자발적으로 도입할 수 있도록 재무, 기술지원, 규제완화 등의 인센티브를 제안하였다. 즉, 연방정부에서 도입을 강력하게 권장하기는 하지만, 기업들을 강제하는 방식은 아니다. 한편, 행정명령은 국토안보부로 하여금 매년 사생활 및 시민의 자유 보호와 관련된 보고서를 발간하도록 하고 있다.

정책지침은 주요 기반시설 보호에 관련되는 중앙 부처들의 역할과 의무를 명확히 하는 것을 주요 내용으로 한다. 예를 들어, 국토안보부가 주요 기반시설에 대한 사이버보안을 총괄하고 있지만, 미국 영토 외의 기반시설은 국무부·대테러 및 수사 관련 업무는 법무부·정부 시설과 국가 기념물은 내무부 등으로 분류된다. (송은지, 강원영, 2014)

2014년에는 주요 기반시설 보호와 관련된 4개의 법안이 입법되었는데 다음과 같다. (Piret Pernik 등, 2016)

• 연방 정보보안 현대화법 (Federal Information Security Modernization Act of 2014): 2002년 연방정보보안관리법(FISMA)을 개정한 것으로, 연방 기관의 디지털 정보 보호에 대한 국토안보부의 역할 명확화, FISMA 요구사항 이행을 위한 관리예산처(OMB)의 책임, 사이버 사고에 대한 보고 요구조건 등을 내용으로 한다.
• 국가 사이버보안 보호법(National Cybersecurity Protection Act of 2014) : 이는 국토안보부 산하 국가 사이버보안 및 통신통합센터(National Cybersecurity & Communications Integration Centre, NCCIC)의 권한을 법률로 뒷받침한 것이다.[53] 국토안보부가 민간기업과

[50] 미국에서 행정명령은 연방입법으로서의 효력을 가지며, 해당 대통령의 임기 내에서는 유효하다.(박영철 등, 2015)
[51] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[52] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[53] Sean B. Hoar, Congress Passes the National Cybersecurity Protection Act: Codifies National Cybersecurity Center & Creates Federal Agency Data Breach Notification Law, 2014.12.18, http://www.privsecblog.com/2014/12/articles/cyber-national-security/congress-passes-the-national-cyber

정보를 공유하고 사이버 사고에 대응하며, 민간업체 및 연방기관을 지원하고, 사이버 보안 조치를 권고하도록 한다. 이 법은 또한, 공공기관에서 정보유출 사고가 발생할 경우 정보주체 및 의회에 통지하도록 하고 있다.
• 국가 사이버보안 및 주요 기반시설 보호법(National Cybersecurity and Critical Infrastructure Protection (NCCIP) Act of 2013) : 사이버 보안 사고를 예방하고 대응하는 국토안보부의 역할을 규정하고, 국토안보부와 기반시설 사업자 사이의 정보공유 파트너쉽을 수립하도록 한다.
• 사이버보안 증진법(Cybersecurity Enhancement Act of 2014) :
국립표준기술연구소(NIST)가 기반시설에 대한 사이버 공격의 위험을 최소화할 수 있는 자율적인 표준을 개발할 권한을 주고 이를 지원한다.

**사이버 위협 정보의 공유**

미국은 공공기관과 민간 사이에서 사이버 위협 정보를 공유하기 위한 노력을 계속 기울여왔다. 앞서 언급했던, 행정명령 13636(Executive Order 13636) '주요 기반시설 사이버보안의 증진'은 주요 기반시설을 운영하는 민간업체와 보안 관련 정보의 공유를 강화하고 협력하는 파트너쉽을 강조하고 있다. 2015년 2월에 내려진 민간 사이버보안 정보 공유 촉진 행정명령(Promoting Private Sector Cybersecurity Information Sharing Executive Order 13691)은 민간 사이의, 혹은 민간과 공공기관 사이의 정보공유와 협력의 거점이 되는 '정보공유분석기관(Information Sharing and Analysis Organizations, ISAO)의 설립을 장려하고 있다. 국토안보부 산하 국가사이버보안 및 통신 통합센터(NCCIC)는 ISAO 사이에서 지속적이고 포괄적인 조정의 역할을 한다.

2015년에는 사이버보안 정보 공유법(Cybersecurity Information Sharing Act of 2015)이 의회를 통과하였다. 이 법은 공공기관 및 민간기업 사이에서 사이버 위협 정보의 공유를 촉진하면서 개인의 프라이버시와 시민권 보호를 목적으로 한다. 민간기업은 자발적으로 사이버 위협 정보를 공유하며, 이들에게는 법적 책임이 면제된다. 국토안보부는 사이버 위협에 대한 정보 수집과 대응방안을 전파하는 일차적인 관문이 된다. 이 법안은 '프라이버시 시민권 감시 위원회(Privacy Civil Liberties Oversight Board, PCLOB)에 의한 프라이버시 영향 및 이행 등에 대한 보고서 제출을 의무화하고 있고, 공유되는 정보에서 개인을 식별할 수 있는 정보를 제거하도록 하고 있다. (박영철 등, 2015) 그러나 IT 기업들[54] 및 EFF나 ACLU와 같은 미국의 정보인권단체들은 이용자 프라이버시 침해를 우려하며 이 법에 반대해왔다. EFF 등은 이 법안이 기업들로 하여금 '위협정보'라는 명분으로 이용자의 사적인 통신을 보관할 수 있도록 하고, 이 정보를 영장도 없이 미 국가안보국(NSA)을 포함한 공공기관에 제공하게 한다고 비판하고 있다.[55]

## 2) 유럽연합(EU)

security-protection-act-codifies-national-cybersecurity-center-creates-federal-agency-data-breach-notification-law/
[54] FOX News, Twitter slams controversial cybersecurity bill, 2015.10.20, http://www.foxnews.com/tech/2015/10/20/twitter-slams-controversial-cybersecurity-bill.html
[55] EFF, Stop the Cybersecurity Information Sharing Act, https://act.eff.org/action/stop-the-cybersecurity-information-sharing-act

유럽연합 사이버 보안 전략[56]과 유럽안보의제(European Security Agenda)[57]는 사이버 보안 및 사이버 범죄에 관한 유럽의 전반적인 전략적 프레임워크를 제공한다. 현재 유럽은 디지털 단일시장(Digital Single Market) 전략을 추진하고 있는데, 디지털 단일시장의 성공을 위해서도 신뢰와 보안은 중요하게 인식되고 있다.

유럽연합 집행위원회(European Commission)는 사이버 보안과 관련된 핵심 목표로 3가지를 제시하고 있다.[58]첫째는 사이버 보안 역량과 협력의 강화로서 이는 '네트워크 및 정보 시스템 보안 지침(Directive on security of network and information systems, NIS Directive)를 통해 지원된다. 둘째는 사이버 보안 시장에서의 유럽연합의 경쟁력을 강화하는 것이고, 셋째는 EU 정책에서 사이버 보안을 일관성있게 추진하는 것이다.

유럽연합(EU)은 지난 2010년 3월, 'Europe 2020 전략'을 발표했는데, 그 중 하나인 '디지털 어젠다[59]'는 7개의 추진 전략[60]으로 구성되었다. 7개의 추진 전략 중 하나가 'EU 사이버 보안 전략 및 지침 제안'이다. 이에 따라 최초의 유럽 차원의 포괄적인 사이버 보안 전략인 'EU 사이버보안전략 : 개방적이고, 안심할 수 있는 안전한 인터넷'(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)[61]이 2013년 7월 수립되었다. 이 전략은 사이버 보안의 맥락에서 중앙집중적인 EU의 감독은 답이 아니며, 각 국가가 사이버 보안사고의 예방과 대응을 조직하는 주요한 행위자여야 한다고 강조하고 있다.[62]

이 전략은 5개의 사이버 보안 원칙과 5개의 전략적 우선순위 및 행동을 제시하고 있다. 5개의 원칙은 ① 유럽의 핵심적 가치는 디지털 세계에도 물리적 세계와 마찬가지로 적용되어야 함, ② 기본권, 표현의 자유, 개인정보 및 프라이버시의 보호, ③ 모두를 위한 접근, ④ 민주적이고 효율적인 멀티스테이크홀더 거버넌스, ⑤ 보안을 보장하기 위한 공유된 책임 등이다. 또한, 5개의 우선순위 및 행동은 다음과 같다.

• 사이버 복원력의 달성
• 사이버 범죄의 급격한 감소
• 공통 보안 및 방위 정책(Common Security and Defence Policy, CSDP)과 관련된 사이버방위 정책 및 능력 개발
• 사이버보안을 위한 산업적, 기술적 자원의 개발
• EU를 위한 일관성있는 국제 사이버공간 정책의 수립 및 EU의 핵심적 가치 증진

네트워크 및 정보 시스템 보안 지침(NIS Directive)은 2013년에 유럽연합 집행위원회가 제안하여, 2016년 7월 6일 유럽의회를 통과하였다.[63] 2016년 8월 발효되었으며 이후 21개월

---

[56] https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

[57] http://europa.eu/rapid/press-release_IP-15-4865_en.htm

[58] https://ec.europa.eu/digital-single-market/en/cybersecurity

[59] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Asi0016

[60] 디지털 어젠다는 ① 브로드밴드 신규 규제 환경 조성, ② 유럽의 시설 자금 연계를 통한 공공 디지털 서비스 기반 신규 조성, ③ 디지털 기술습득과 채용 관련 대연합 착수, ④ EU사이버보안전략 및 지침(Directive) 제안, ⑤ EU저작권 프레임워크 개정, ⑥ 공공분야시장을 통한 클라우드 컴퓨팅 활성화, ⑦ 신규 전자산업 전략 추진 등 7개의 추진전략으로 구성되었다. (박영철 등, 2015)

[61] https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[62] https://ccdcoe.org/eu-0.html

[63] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

동안 유럽연합 각 국은 자국의 법으로 제정해야 한다. 이 지침은 유럽연합에서의 전반적인 사이버 보안 향상을 위한 법적 조치를 제공하고 있다. 그 주요 내용은 다음 세 가지이다.
첫째, 회원국은 적절한 컴퓨터보안긴급대응팀(CSIRT)와 국가 NIS 기관을 수립해야 한다.
둘째, 회원국 간의 정보공유와 전략적 협력을 위해 협력 그룹을 수립한다. 또한, 특정한 사이버 보안 사고와 보안 위협 관련 정보공유에 대한 효율적인 운영상 협력을 증진하기 위해 CSIRT 네트워크를 설립할 필요가 있다.
셋째, 특히 주요 기반시설에서의 보안 문화의 형성이다. 각 국이 지정한 주요 기반시설 사업자들은 적절한 보안 조치를 취하고, 중대한 사고에 대해 관련 당국에 통지해야 한다. 또한, 중요한 디지털 서비스 제공자(클라우드 서비스, 검색 서비스 등) 역시 보안 및 통지 요구조건을 충족해야 한다.

**사이버 보안 정책 추진체계**

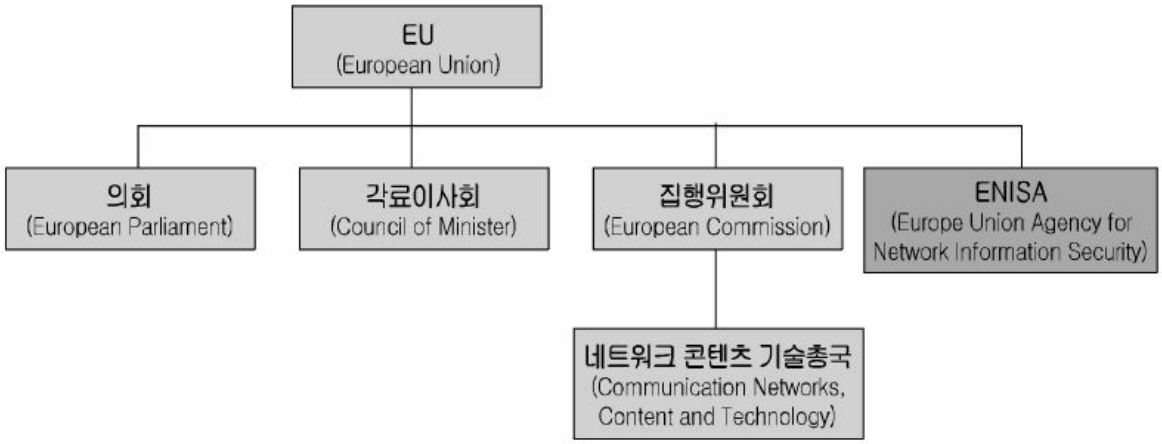



그림 : EU 사이버 보안 추진체계 (출처 : 배병환, 송은지, 2014)

EU는 단일국가가 아닌 연합체이기 때문에 사이버보안 추진 체계도 다소 상이한 구조이다. 유럽연합의 사이버 보안은 집행위원회 산하 네트워크콘텐츠기술총국(Communication Networks, Content and Technology)에서 총괄하고 있으며, 산하기관인 유럽네트워크정보보호기구(ENISA)에서 지원을 받고 있다. ENISA는 EU 회원국 네트워크 및 정보보안을 지원하며, 국가 간 정보교류 증대와 네트워크 보안 기능 조정 등의 역할을 수행하는 기관으로 'ENISA 설립 규정'에 따라 2004년에 설립되었다. 특히, 집행위원회, 회원국, 회원국의 기업체 등의 사이버보안 업무 지원 및 자문·연구를 통해 사이버보안 위협 대응능력을 개선하고 매년 사이버위협평가보고서를 발간하고 있다.(배병환, 송은지, 2014) CERT-EU는 2010년 유럽 디지털 어젠더에 따라 집행위원회가 설립 준비를 시작했으며, 2012년 9월에 EU 기구로서 결정되었다.CERT-EU는 EU 주요 기구의 IT 보안 전문가들로 구성되며, 회원국의 CERT와 긴밀하게 협력한다.[64]

**주요 기반시설의 사이버 보안**

2009년 3월, 집행위원회는 '핵심 정보기반 보호에 관한 통신(Communication on Critical Information Infrastructure protection, CIIP)'[65]을 채택하였다. CIIP는 회원국 및 민간기업을

[64] https://cert.europa.eu/cert/plainedition/en/cert_about.html
[65] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

포함하는 행동계획을 개시하였는데, 준비와 예방, 탐지와 대응, 완화와 복구, 국제 협력, ICT 영역의 유럽 핵심 기반을 위한 표준 등 5개 분야에 기반하고 있다.

2011년 3월, 집행위원회는 이행결과를 평가하면서 CIIP '성과와 다음단계 : 지구적 사이버보안을 향해'[66]를 채택하였는데, 보안 및 복원력을 위한 일국적 접근은 한계가 있으며 유럽연합 전체적으로 일관되고 협력적인 접근이 필요하다고 결론을 내고 있다.

2012년 6월, 유럽의회는 '핵심 정보기반 보호 : 지구적 사이버보안을 향해' 결의안[67]을 채택하였다. 이 결의안은 2011년 CIIP를 폭넓게 승인하면서 집행위원회에 향후 방향에 대한 몇 가지 권고를 하였고, 이 권고들은 2013년 사이버 보안 전략과 NIS 지침 제안서로 수렴되었다.

CIIP 정책은 몇 가지 주요 성과를 가져왔는데, 우선 회원국을 위한 유럽 포럼과 복원력을 위한 민관협력체( European Public-Private Partnership for Resilience)를 설립하였으며, Cyber Europe 2010 과 2012와 같은 유럽 전역의 훈련을 시행하였다. ENISA는 국가적 CERT를 위한 최소한의 기본 역량, 서비스, 관련 정책 권고를 채택하였다.[68]

**사이버 위협 정보의 공유**

EU는 사이버 보안 전략을 통해 국가별 네트워크 및 정보보호 권한 기관, 유럽경찰기구(Europol), 유럽방위청(European Defense Agency) 등 민·관·군의 위협 정보 공유의 중요성을 밝히고 있다. 유럽경찰기구는 유럽검찰기구와 함께 사이버범죄 대응에 관련한 정보를 공유하고 있으며, 유럽경찰기구 내 유럽 전역의 인터넷 범죄자들의 신원, 범죄 행태 등에 대한 정보를 공유하고 있다. EU는 효과적인 사이버위협 정보의 공유를 위해 2013년 1월, 유럽사이버 범죄센터(European Cybercrime Centre)를 설립하였다.(배병환, 송은지, 2014)

## 3) 영국

영국은 EU 국가 내에서도 사이버보안과 관련한 기술과 전문 인력을 보유한 사이버보안 선진국가에 속한다. 특히 기업들의 정보보호 정책 수립비율은 국내에 비해 5배 가량 높으며, 정보보호 투자와 관련해서도 국내에 비해 16배 높다.(배병환 등, 2014)

영국은 2008년 국가안보전략에서 사이버 공격의 위협을 언급한 이후, 2009년 최초로 사이버 보안 전략을 채택하였다. 이 전략은 사이버 공간의 기회를 긍정적으로 활용하기 위한 안전, 보안, 복원력에 초점을 맞추었다. 2010년 영국 국가안보위원회(National Security Council)는 '영국의 사이버 공간에 대한 다른 국가 및 거대 사이버 범죄의 악의적인 공격'을 최고 수준의 국가 안보 위협으로 간주하였다. 국가안보전략과 함께, 영국은 4개년 국가 사이버 보안 프로그램(National Cyber Security Programme, NCSP)을 수립하였다.

---

[66] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[67] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167

[68] European Commission, Policy on Critical Information Infrastructure Protection (CIIP), https://ec.europa.eu/digital-single-market/news/policy-critical-information-infrastructure-protection-ciip

2011년에 새로 발표된 영국의 국가사이버보안전략(The UK Cyber Security Strategy)은 2015년까지 영국 사이버 보안의 전략적 비전과 함께, 구체적인 목표, 필요한 활동, 역할과 책임의 분배, 주요 원칙 등을 제시하였다. 또한, 2012년까지 NCSP 사업의 이행 상황을 보고하도록 하였고, 2013년에도 유사한 평가가 수행되었다. 그 결과 <국가사이버 보안전략의 목표의 진전사항 - 2013년 12월>[69]과 <국가사이버보안전략 : 향후 계획 - 2013년 12월>[70] 두 개의 평가문서가 제출되었다. 영국 국가사이버보안전략은 국가 정보 보증 전략 2007, 국가 사이버 범죄 전략 2010, 정부 ICT 전략 2011 등 다른 국가 전략들과 연계되어 있다. (Anna-Maria Osula, 2015)

2011년 영국 사이버 보안 전략은 사이버 공간에서 정부의 권한은 한계가 있으며, 산업계 및 학계 등과의 밀접한 협력이 필요하다는 것을 강조하고 있다. 그리고 ▸ 사이버 범죄 감소 및 안전한 사이버 공간 구축, ▸ 사이버 공격에 대한 복원력 강화와 사이버 상의 권익 보호, ▸ 열린, 역동적, 안정적인 사이버 공간 구현, ▸ 사이버보안 지식, 기술, 능력 구축  등의 네 가지 목표 하에 세부 실행과제 57개를 제시하였다. 또한 4년간 6억 5천만 파운드 규모의 '국가 사이버보안 프로그램(National Cyber Security Programme, NCSP)'을 통해 정책 수행에 필요한 재원을 마련하였다. (배병환, 송은지, 2014)

2013년 12월의 평가 보고서를 바탕으로, 영국정부는 전략 추진 방향을 제시하는 '국가 사이버 보안 전략 계획(The National Cyber Security Our Forward Plans)'을 발표하였는데, 그 내용은 다음과 같다.(배병환 등, 2014)

① 고도화된 사이버 위협에 대비한 국가 대응 능력 향상
② 인터넷 비즈니스 신뢰성 강화 및 사이버 범죄 해결을 위한 법 집행기관 역할 강화
③ 영국 주요 시스템 및 네트워크 복원력 강화
④ 영국 산업 내 사이버 인식 및 리스크 관리능력 향상
⑤ 대중들의 사이버보안 인식 제고 및 제품, 서비스에 대한 높은 수준의 사이버보안 요구
⑥ 사이버보안 연구 및 교육 강화를 통한 보안 전문 인력 양성
⑦ 사이버 범죄 해결 및 개방적이고 안전한 사이버 공간 구축을 위한 국제 협력 지원

**사이버 보안 정책 추진체계**

2009년 국가사이버보안전략 채택 이후, 영국은 사이버 보안과 관련된 주요 조직 개편이 시행되었다. 그러나 이후 부분적으로 수정이 되었고, 2011년 국가사이버보안전략에서도 추후에 상황에 따라 변경될 수 있다고 했기 때문에 향후에도 유동적일 수 있다.(Anna-Maria Osula, 2015)

69 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/265384/Progress_Against_the_Objectives_of_the_National_Cyber_Security_Strategy_December_2013.pdf

70 http://www.cyberriskinsuranceforum.com/sites/default/files/The_National_Cyber_Security_Strategy_Our_Forward_Plans_December_2013.pdf

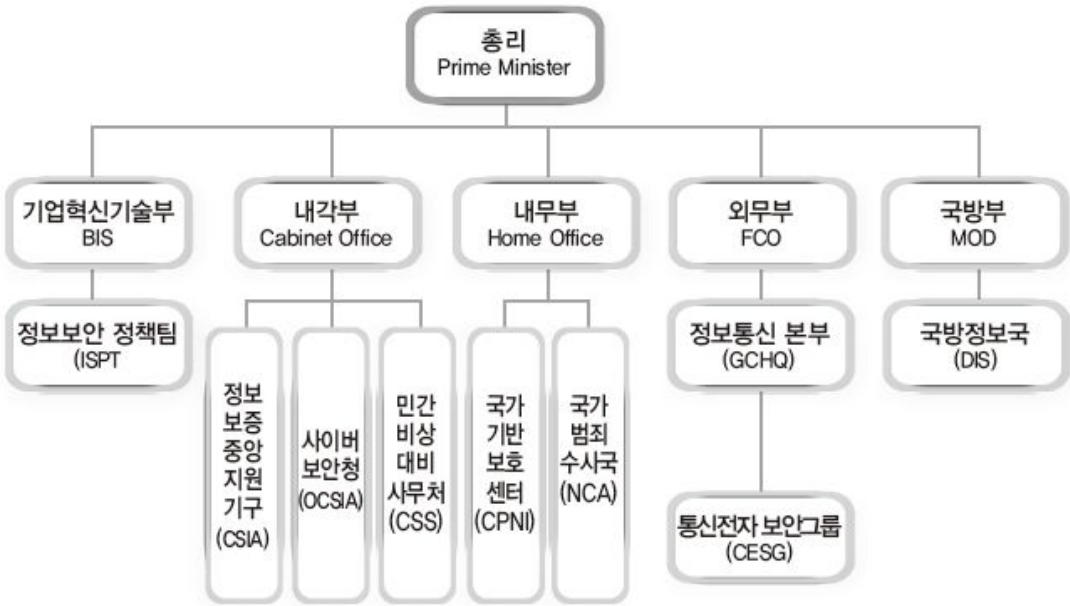



그림 : 영국 사이버보안 체계 (출처 : 배병환 등, 2014)

사이버 보안에 대한 범정부적 조정 및 전략 제시는 전반적으로 내각부(Cabinet Office)의 책임 하에 있다. 사이버 보안은 내각부 내의 국가안보사무국(National Security Secretariat)의 임무이며, 국가안보위원회와 수상을 지원한다. 내각부 아래에는 정보보증중앙지원국(CSIA), 사이버보안청(Office of Cyber Security & Information Assurance, OCSIA), 민간비상대비사무처(CSS) 등을 두고 있다. OCSIA[71]는 내각부 장관과 국가안보위원회가 사이버 보안 관련 우선순위를 결정하는 것을 지원하며, 전략적 방향을 제공하고 범정부적 국가 사이버보안 프로그램(NCSP)[72]를 관장한다. 그 외에 교육, 인식제고, 훈련 등 지원, 민간기업과의 정보교환 및 모범 사례 증진, 기술 역량 및 운영 구조의 개선, 정부의 ICT 기반 보안을 위한 정부최고정보책임자(OGCIO)와의 협력, 국제 협력 등의 업무를 맡고 있다. (Anna-Maria Osula, 2015)

정보보증중앙지원기구는 영국 정부의 정보보증(Information Assurance)[73] 개선을 주로 담당하고 있으며, 이를 위해 정보통신 기술을 활용해 정부의 공공서비스가 원활히 제공될 수 있도록 지원하며, 훼손될 위험이 있는 정보 및 정보시스템을 보호해 국가기반보호센터(CPNI), 중대조직범죄청(SOCA) 등 협력관계에 있는 기관들을 주도해 정보보안 활동을 전개해 나가고 있다. 민간비상대비사무국은 내각부 내의 비상사태에 대응하는 업무를 담당하기 설립된 기관이다.(배병환 등, 2014)

[71] Office of Cyber Security and Information Assurance, https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

[72] NCSP는 2009년에 범정부적으로 처음 도입되어, 2010년 '국가 방위 및 안보 리뷰'에서 수립되었는데, 영국 사이버 보안 및 방위 기관들에 추가 재원을 제공하는 4개년 투자 프로그램이다. 2011년 국가사이버보안전략에서는 이를 확대하고 2011년에서 2015년까지의 투자를 도입하였다. (Anna-Maria Osula, 2015)

[73] 정보보증(Information Assurance)는 데이터의 무결성, 가용성, 비밀성 등의 보호와 데이터의 저장, 처리, 전송 과정의 위험을 관리하는 것으로서 정보 보안과 유사한 개념이다.

내무부는 주요 기반시설의 보호와 출입국관리, 테러대응, 경찰 통솔 등을 담당하고 있는 정부부처로서 산하에 미국의 FBI와 유사한 국가 사이버범죄 대응기구인 국가범죄수사국(NCA)과 주요 기반시설 보호를 담당하고 있는 국가기반보호센터(CPNI)를 두고 있다. 기업혁신기술부(Department for Business Innovation and Skills, BIS)는 산하에 정보보안정책팀(Information Security Policy Team)을 두고 있는데, 기업의 사이버 보안 관련 지원 및 규제를 담당하며, 유럽네트워크정보보안국(ENISA) 운영위원회의 일원으로 업무지원 활동을 수행한다.(배병환 등, 2014)

영국의 신호정보 정보기관인 정보통신본부(GCHQ) 역시 사이버 보안과 관련된 중요한 역할을 하고 있다. GCHQ는 외무부(Foreign&Commonwealth Office) 산하에 있으며, 통신정보(Signals Intelligence)를 수집·제공하고, 관련 기관에 보안 정보를 권고·보고하는 등 크게 2가지 업무를 담당하고 있다.사이버 보안 관련한 GCHQ의 업무는 방어적 사이버 보안, 기기 및 정보 보증 관련 업무, 사이버 위협(사이버 범죄를 포함하여)의 탐지 및 분석, 사이버 공간의 정보 작전, 해외 동맹기관과의 협력 등이다.

GCHQ는 산하에 사이버보안운영센터(CSOC), 국가정보보증기술국(CESG), 컴퓨터긴급대응팀(CERT-UK) 등을 두고 있다. 사이버보안운영센터는 정부 및 민간 관계자로 구성된 기구로서 사이버 공격에 대한 정보와 자문을 업체 및 공중에게 제공한다. 국가정보보증기술국(기존 전자통신보안그룹에서 전환됨)은 GCHQ 내의 정보보증을 담당하는 기구로서, 정부 내의 정보보안의 기술적 측면-컴퓨터 네트워크의 보안, 사이버 공격 예방, 취약점 차단, 네트워크 관제 및 공격자 식별 등-에서 핵심적인 역할을 한다. CESG는 국가기반보호센터(CPNI), 비밀 정보기관인 MI5나 MI6 등과 긴밀하게 협력한다. CESG는 2014년부터 CERT-UK도 운영하고 있다. CERT-UK는 공공 영역에 침해 사고에 대한 경고와 지원의 역할을 하며, 정부, 업계, 학계, 국제조직 등과 협력한다. 또한 CERT-UK는 사이버보안정보공유협력체(Cyber Security Information Sharing partnership, CISP)팀을 운영하고 있다.(Anna-Maria Osula, 2015)

이외에도 국방부 산하 국방정보국(DIS, Defence Intelligence Staff)를 통해 사이버보안 관련 군사 정보 수집과 방첩활동을 지원하고 있으며, 영국 정보기관인 군 정보청 5과(MI5), 군 정보청 6과(MI6)을 통해 보안, 국방 등 영국의 중대한 이익에 영향을 미치는 문제에 관하여 국외 비밀 정보를 수집하고 있다.(배병환 등, 2014)

**주요 기반시설의 사이버 보안**

영국의 주요 기반시설의 80%는 민간에 의해서 운영되고 있다. 주요 기반시설에 대한 단일한 정책이나 법은 없으며, 영역별 법률들이 존재하고 있다. 정부는 주요 기반시설 보안에 대한 주된 규제자이자 정책 결정자이지만, 기반시설 보안을 위한 투자나 실질적인 대책의 선택은 그것을 소유한 기업에 맡겨져 있다. 주요 기반시설의 목록은 비공개이다. (Anna-Maria Osula, 2015)

국가 주요 기반시설의 보호는 내무부 산하의 국가기반보호센터(CPNI)가 담당한다. 국가기반보호센터는 핵심 국가기반 시설의 보호에 초점을 맞추고 기업 및 단체들에게 보안에 관한 통합 정보를 제공한다.(박영철 등, 2015)

**사이버 위협 정보의 공유**

사이버보안정보공유협력체(CISP)는 민간과 공공의 사이버위협 정보를 실시간으로 교류할 수 있는 플랫폼으로서 2013년 3월 발족하였다. CISP 가입조직들 사이에서 위협 정보를 실시간으로 공유하고 정부 및 산업네트워크방어분석가로 구성된 퓨전셀(Fusion Cell)의 조언을 받는다. 2013년에 약 250여 개의 조직이 가입하였으며, 2014년까지 500여 개로 확대할 계획을 가지고 있다. 또한, CISP는 정부의 사이버 보안 훈련 프로그램을 수행하고 있는데, 금융, 법집행, 운송, 식량 등 주요 기반 시설의 복원력과 대응을 실험하기 위해 2012년-2013년에 10번의 훈련 프로그램을 진행하였다. 예를 들어, 'Waking Shark II'는 은행 부문의 사이버 방어 및 사고 대응 훈련 프로그램이다.(Anna-Maria Osula, 2015)

## 4) 일본

일본은 2012년 'Active Japan ICT 전략'을 수립하면서 '사이버 보안'을 포함시킨데 이어, 2013년 6월에는 '사이버보안 전략 2014'를, 2015년 9월에는 '사이버보안 전략 2015'를 수립하였다. 그리고 2014년 11월에는 사이버보안 정책에 대한 법적 근거를 마련하기 위하여 '사이버보안 기본법'을 제정하였다.[74]

2012년 'Active Japan ICT 전략'에서는 2015년까지 '세계 최고수준의 사이버 보안환경 실현'을 목표로 5개의 추진전략을 도출하였는데, 첫째, 사이버공격의 국제적인 정보공유·즉각 대응 기술 확립, 둘째, 사이버공격에 대한 실천적인 방어기술 확립, 셋째, 이용자 프라이버시가 확실히 보호됨과 동시에 적절하게 이용하고 활용할 수 있는 환경 실현, 넷째, ICT서비스 시작으로 인터넷에 관한 글로벌 룰(Global Rule)의 조화, 다섯째, 새로운 기술·서비스를 접하는 청소년부터 고령자에 이르기까지 누구나 안심할 수 있고 안전한 이용환경 정비 등이다.

급증하는 사이버 공격에 대한 대응 뿐만 아니라, 지진·해일·태풍 등 천재지변에 따른 사이버 보안 사고의 급증은 '사이버보안 전략 2014'를 수립하는 배경이 되었다. 또한 2020년 도쿄올림픽 개최에 대비한 사이버 보안 강화도 고려한 것이다. '사이버보안 전략 2014'는 정부기관 대상 정책, 주요 기반시설 사업자 대상 정책, 기업 및 연구기관 대상 정책, 사이버공간 위생, 사이버공간 범죄대책, 사이버공간 방위 등 주요 주체별 사이버 보안 강화를 위한 세부 정책을 제시하고 있다. 그 일환으로 일본 정부 정보시스템의 통합 관리를 추진하는 한편, 내각관방(Cabinet Secretariat) 산하에 정부기관 전반에 걸친 사이버공격 정보 수집 및 분석 권한을 가진 전문기구인 '사이버보안센터'를 설립하였다.

2014년 11월 '사이버보안 기본법'이 제정된 후, 이 법의 규정에 따라 2015년 9월, 새로운 국가전략인 '사이버보안 전략 2015'[75]가 수립되었다. '자유롭고, 안심할 수 있으며, 안전한 사이버 공간의 보장'을 위해 ▸ 사회경제적 활성화와 지속가능한 발전을 증진하고, ▸ 사람들이 안심하고 안전한 삶을 영위할 수 있는 사회를 구축하며, ▸ 국제 공동체와 국가 안보의 평화와 안정성을 보장하는 것을 목표로 하고 있다. 또한, 기본 원칙으로 ① 정보의 자유로운 흐름 보장, ② 법치, ③ 개방성, ④ 자율성, ⑤ 멀티스테이크홀더 사이의 협력을 강조하고 있다.

일본의 법률 체계를 보자면, 기존에는 2001년에 제정된 '고도 정보통신 네트워크 사회형성 기본법'에 따라 사이버보안 관련 정책을 시행해왔다. 그리고 1999년 제정된 '부정악세스 행위의 금지 등에 관한 법률' 등 개별 법률에서 사이버 보안 관련 규정이 반영되어 있었다.

[74] 일본의 사례는 박영철 등(2015)을 참고하였다.
[75] CYBERSECURITY STRATEGY, 2015.9.4, Cabinet Decision, The Government of Japan, http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

2014년에 제정된 '사이버보안 기본법'은 일본의 사이버보안에 관한 기본이념을 정하고, 국가 및 지방공공단체의 책무 등을 정한 기본법이라고 할 수 있다. 또한, 이 법률은 사이버보안 전략의 개발 및 사이버보안에 관한 시책의 기본이 되는 사항을 정하는 동시에, 새로운 조직으로서 '사이버보안 전략본부'를 설치하도록 하고 있는데, 이 조직이 현재 일본의 사이버보안 컨트롤타워의 역할을 하고 있다.

기본법은 우선 제2조에서 사이버시큐리티란 "전자적 방식, 자기적 방식 그 밖에 사람의 지각에 의해 인식될 수 없는 전자적 방식에 의해 기록하고, 발신하며, 전송하고, 또는 수신하는 정보의 누설·멸실·훼손의 방지 및 그 밖에 해당 정보의 안전관리를 위한 조치, 정보시스템 및 정보통신네트워크의 안전성 및 신뢰성 확보를 위해 필요한 조치(정보통신네트워크 또는 전자적 방식으로 만들어진 기록에 관계된 기록매체를 통한 전자계산기에 대한 부정한 활동으로 인한 피해의 방지를 위하여 필요한 조치를 포함한다.)가 강구되고 그 상태가 적절하게 유지·관리되는 것을 말한다"고 정의하고 있다.

그리고 총 6개의 기본이념을 제시하고 있는데, 첫째 사이버보안 주체(국가, 지방공공단체, 주요 기반시설 사업자 등)사이의 연계성, 둘째 대국민 사이버보안 인식제고 및 자발적 대응체계, 피해방지 및 신속복구체제 구축, 셋째 인터넷 및 기타 고도 정보통신 네트워크 정비와 이를 활용한 활력있는 경제사회의 구축, 넷째 사이버보안 관련 국제협력, 다섯째 고도 정보통신 네트워크 사회형성 기본법과의 정합성 확보, 여섯째 국민권리의 부당한 침해방지 등이다.

또한, 국가 행정기관 등의 사이버보안 확보, 주요 사회기반 사업자 등의 사이버 보안 확보, 민간사업자 및 교육연구기관 등의 자발적 활동촉진, 사이버보안 주체들 간의 연계, 산업의 진흥 및 국제 경쟁력 강화, R&D 추진, 인력확보, 교육 및 학습 진흥, 국제협력 등 기본 시책을 규정하고, 사이버보안 정책 추진을 위한 추진체계를 규정하고 있다.

**사이버 보안 정책 추진체계**


그림 : 일본의 사이버보안 추진체계 (출처 : SASAKAWA USA, 2016)

‘사이버보안 기본법’ 제정 이후에는 ‘고도 정보통신 네트워크 사회형성 기본법’에 의해 설치된 ‘고도 정보통신 네트워크 사회 추진전략본부(IT 전략본부)’가 사이버 보안을 포함한 정보화 정책 수립 및 추진을 담당하는 컨트롤타워 역할을 하였다. 그리고 2005년에 설립된 ‘정보보안센터(NISC)’가 사이버 보안 관련 기본전략 입안, 정부 종합대책 촉진 등 핵심적인 역할을 하였다.

‘사이버보안 기본법’이 제정되면서 사이버보안의 컨트롤타워의 역할은 ‘사이버보안 전략본부’로 이전되었다. 사이버보안 전략본부는 사이버보안 전략안 작성 및 실시 추진, 국가 행정기관의 대책기준 작성 및 정책평가, 국가 행정기관에서 발생한 사이버보안 관련 중대사고에 대한 정책평가, 사이버보안 관련 중요정책의 계획에 관한 조사 및 심의, 각 부·성 단위의 횡적 계획 및 관계 행정기관의 경비·견적·방침·정책 실시 관련 지침 작성 등을 하며, 사이버보안 관련 정책들을 종합적으로 조정한다.

내각관방 산하의 정보보안센터는 ‘사이버보안센터(NISC)’로 개편되었다. 사이버보안센터는 사이버보안 전략본부에서 마련한 사회보안 전략을 구체화하고 이를 실행하는 역할을 담당한다. 또한 경찰청, 총무성, 경제산업성, 방위성 및 자위대의 네트워크 허브 역할을 담당한다. 센터의 수장은 방위성 출신의 국가안전보장회의 국가안전보장국 차장이 겸임하고 있다.

각 정부부처 역시 사이버보안 관련 역할이 부여되어 있는데, 경찰청은 사이버 범죄에 대한 대응, 총무성(MIC)은 통신 및 네트워크 정책, 경제산업성은 IT 산업정책, 방위성 및 자위대는 국가 안보 측면의 사이버 보안을 담당한다.

**주요 기반시설의 사이버 보안**

일본의 주요 기반시설의 보호는 각 영역별로 해당 정부기관이 담당한다. 민간기업의 기반시설에 대한 사이버 침해사고가 발생할 경우 영역별 담당 성·청에 신고하고, 사이버보안센터로 공유된다.

‘사이버보안 전략 2014’에서는 ‘주요기반시설 사업자에 대한 사이버보안 전략’으로서 2014년 제정된 주요기반시설 대상의 보안 가이드라인을 지속적으로 검토하고 각 시설에서 이를 수용하도록 함으로써, 해당 가이드라인을 산업표준으로 확립하도록 하고 있으며, 정부기관 및 민간기업 사이의 사이버보안 사고 관련 정보를 실시간으로 공유할 수 있는 체계로서 ‘사이버 정보공유 이니셔티브’의 강화, 사이버사고 대응을 위한 사전 훈련 수행 및 실제 사고 발생 시 기관 및 시설 사이의 수평적 대응 체제 구축을 도모하도록 하고 있다.

**사이버 위협 정보의 공유**

전술했듯이, 주요 기반시설 기업과의 정보공유 강화를 위해 ‘사이버 정보공유 이니셔티브’를 구축하고 있다. 또한 총무성은 2011년 산하에 ‘민관 정보공유 분석센터(Telecom-ISAC)를 두고 있으며, 경찰청은 방위 및 첨단기술 관련 기업 간에 ‘사이버 인텔리전스 공유 네트워크’를 구축하고 있다.

일본 사이버보안 대응체계에서 중요한 역할을 담당하고 있는 ‘일본 침해사고 대응센터(JPCERT/CC)’는 1992년 설립된 민간의 자발적인 조직이다. 국가 및 기업으로부터 독립성을 가지고 있으며, 인터넷 침해사고에 대한 보고 및 접수, 대응지원, 상황파악,

범죄수법분석, 재발방지를 위한 대책 검토 등의 업무를 수행한다. JPCERT는 1998년 국제침해사고대응협의회(FIRST)에 가입하여 국제협력을 진행하고 있다.

# 3. 국내 사이버 보안 정책과 국가정보원

## 가. 국내 사이버보안 정책 현황

### 1) 국내 사이버 보안 전략

국내에서는 사이버보안 전략이라고 할 수 있는 종합대책이 몇 차례 수립되었다. 첫 종합대책은 2009년 수립된 '국가 사이버위기 종합대책'인 것으로 보인다. 물론 종합대책 이전에도 '정보통신망법' '정보통신기반보호법' 등 관련 법령이 제정되었고, 2004년에 국가사이버안전센터가 설립되고 '국가위기관리기본지침'(대통령훈령) 및 국가사이버위기관리 매뉴얼이 제정되었으며, 2005년에 대통령 훈령으로 '국가사이버안전관리규정'이 제정된 바 있다. 2009년 국가 사이버위기 종합대책 이후, 2011년에 국가 사이버안보 마스터플랜, 2013년 국가 사이버안보 종합대책, 2015년 국가 사이버안보 태세강화 종합대책 등이 수립되었다.[76]

- 2009년 : 국가 사이버위기 종합대책
- 2011년 : 국가 사이버안보 마스터플랜
- 2013년 : 국가 사이버안보 종합대책
- 2015년 : 국가 사이버안보 강화방안

**2009년 : 국가 사이버위기 종합대책[77]**

2009년 9월 11일, 정부는 '국가 사이버위기 종합대책'을 '국가 사이버안전 전략회의'에서 최종 확정하여 발표하였다. 이 종합대책의 마련은 같은 해 7월 발생한, 7.7 디도스 대란[78]이 계기가 되었다.

정부는 종합대책을 발표하게 된 배경으로, 첫째 발전한 IT 환경이 오히려 사이버 공격에 대한 취약점이 높기 때문에 사이버 안전 수준을 높일 수 있는 종합적인 대응방안이 요구되었고, 둘째 디도스 대응 과정에서 정부기관간 사전 조율이 없는 것처럼 비춰지고, 민간 분야의 보안이 취약하여 민관을 망라하는 대비책이 필요했으며, 셋째 세계 주요국들의 추세와 같이 21세기 사이버환경의 주도권을 확보하기 위한 대책이 필요한 시점이라고 밝혔다.

[76] 그런데 이러한 종합대책의 원문이 인터넷을 통해서 공개되어 있지 않았다. 다만, 정부가 발표한 보도자료만 올라와 있을 뿐이다. 해외 다른 나라와 같이 기본적인 자료의 보다 충실한 공개가 필요하다.
[77] 방송통신위원회 보도자료, 정부,「국가사이버위기 종합대책」확정 발표 - 사이버위기 대응체계 재정립, 정보보호 인력·예산 대폭 확충키로, 2009.9.14
[78] 2009년 7월 7일, 미국과 국내 주요 정부기관과 포털,은행 등이 DDOS 공격으로 서비스 장애가 발생하였다. 7월 5일에는 백악관 및 27개 사이트가 공격을 받았고, 7월 7일에 국내 주요 언론사와 정당,포털 사이트가 공격을 받았다. 9일에는 국가정보원과 금융기관 일부가 공격으로 서비스 장애가 발생했다.

종합대책은 평시 국가기관 간 역할을 명확히 하여, 국정원이 사이버위기 대응 총괄 역할을 수행하고, 방통위는 좀비PC 제거 및 국민 대상 사이버안전 홍보 및 계도업무를 담당하며, 국방부가 사이버부대를 신편하여 군사 분야를 보강하게 하였다. 또한 민간 분야에서 사이버 보안 교육 확대, 기업 정보보호를 위한 사이버 보안관 양성, 산업별 협회에 보안관제센터(ISAC) 설립 등을 내용으로 하고 있다. 이와 함께, 세부 추진과제를 2010년 및 중장기 과제로 구분하여 제시하였다. [79]

**2011년 : 국가 사이버안보 마스터플랜**[80]

2011년 8월 8일, 정부는 '국가 사이버안보 마스터플랜'을 발표하였다. 이 역시 '국가 사이버안전 전략회의'를 통해 나온 것이다. 마스터플랜은 2011년 3월에 발생한 '3.4 디도스 공격'과 '농협 전산망 장애사건'이 계기가 되었다.

이번 마스터플랜에는 국가차원의 사이버위협 대응체계 정비 및 관련 부처별 역할 정립, 분야별 중점 추진과제 등이 포함되었다. 대응체계 정비 및 부처별 역할 정립에 있어서는 '국가사이버안전센터'를 중심으로 관계부처간 협력·공조와 민간 전문가 참여를 확대해 나가는 한편, 국정원의 컨트롤타워 기능과 부처별 역할을 명확히 하여 그간 제기되었던 기관간의 업무 혼선·중복 및 사각지대 발생의 문제점을 해소하기로 하였다고 밝히고 있다. 이에 따라, 국정원은 평·위기시 총괄, 방통위는 방송통신 등 민간영역 보안, 금융위는 금융 영역, 국방부는 국방 관련 보안, 행안부는 전자정부대민서비스, 정부전산센터 등 행정 영역을 관할하도록 하였다. 그런데, 2009년 종합대책에서 부처간 역할을 명확히 하였다고 했음에도 불구하고, '기관간의 업무 혼선·중복 및 사각지대가 발생'한 이유는 무엇인지에 대해 어떠한 평가가 있었는지 의문이다.

---

[79] <당면과제>
1) 사이버위기 관리체계의 강화
① 국가 사이버위기 발생시 위협분석 및 경보발령, 외국과 공조체계 가동 등을 총괄하는 민・관 합동 범정부 대책기구의 구성
② 언론창구는 방송통신위원회로 일원화
③ 악성프로그램 삭제요청권, 침해사고 발생시 시스템 접근요청권 등의 법적 근거의 마련
④ 국가위기관리기본지침 등 정부 규정을 개정하여 대책기구 구성, 경보발령 요건 구체화

2) 사이버안보 리더십의 강화(2010년까지의 추진과제)
① 사이버대응 조직의 보강
② 사이버보안관 3,000명 등의 전문인력 양성 기반의 조성
③ 사이버공격 탐지 사각 지대 해소 등 사이버방어 환경의 개선
④ 중앙정부의 망분리 사업의 추진 및 지방자치단체의 망분리에대한 정부의 지원, 추진

<중장기 과제>
① 관련 법제도 정비
② 정보화 예산 대비 정보보호 예산의 단계적 확대
③ 정보 보호 설비투자 제고를 위해 조세감면의 지속 지원
④ 전력・통신 등 국가기능유지 핵심시설의 보안체계 고도화
⑤ 사이버전 환경변화를 고려한 기존의 정보통신망과 기반시설 보호를 강화하기 위한 사이버공격 대응기술 개발・활용
⑥ 사이버보안 예산 증액 및 관련 교육 강화
(박영철 등, 2015)

[80] 방송통신위원회 보도자료, 정부,「국가 사이버안보 마스터플랜」수립 - 국가 사이버공간 수호를 위한 범정부 차원의 청사진 마련 -, 2011.8.8

한편, 마스터플랜은 사이버공간을 영토·영공·영해에 이어 국가가 수호해야 할 또 하나의 영역으로 보고, 이를 위해 예방, 탐지, 대응, 제도, 기반 등 5대 분야의 중점 전략과제를 선정·추진하기로 하였다.[81]

**2013년 : 국가 사이버안보 종합대책[82]**

2013년 3월에는  방송사 및 금융기관을 대상으로 한 '3.20 사이버테러'가 발생하였다. 이에 정부가 종합대책을 준비하던 와중에, 홈페이지 변조, 언론사 서버 파괴, 디도스 공격 등 '6.25 사이버공격'이 발생하였다. 정부는 7월 4일, 정부부처 합동으로 '국가 사이버안보 종합대책'을 발표하였다.

종합대책은 '선진 사이버안보 강국 실현'을 목표로 4대 전략에 따라 수립되었다. 4대 전략이란, 사이버위협 대응체계 즉응성 강화(Prompt), 스마트 협력체계를 구축(Cooperative), 사이버공간 보호대책 견고성 보강(Robust), 사이버안보 창조적 기반 조성(Creative) 등이다. 이에 따라 사이버보안 컨트롤타워가 국정원에서 청와대로 이관되었고, 국가정보원은 실무

---

[81] <예방>
① 전력, 금융, 의료 등 기반시스템 운영기관 및  기업들의 중요정보 암호화 등 보호조치의 강화
② 주요 핵심시설에 대한 백업센터 및 재해복구시스템 확대 구축
③ 정부 S/W개발 단계에서의 보안취약점 사전 진단 제도의 의무화
④ 국제공조 강화를 통해 사이버도발 억지력의 확보

<탐지>
① 범국가적 사이버공격에 대응하기 위해 3線방어체계(국제관문국·인터넷연동망 ↔ 인터넷서비스 사업자(ISP) ↔기업・개인) 개념의 도입을 통한 공격 트래픽의 단계별 탐지・차단
② 지방자치단체 정보시스템의 사이버공격 탐지 실시
③ 보험・카드사 등 제2금융권 전산망에 대한 보안관제 확대
④ 북한産불법S/W 유통 감시·차단 활동의 강화
⑤ 전문업체를 활용한 년 1회 이상 금융·통신 등 민간 주요시스템에 대한 보안점검 이해 의무화

<대응>
① 조직적인 해커공격에 대응하기 위한 외부전문가가 참여하는 '민·관 합동 대응반'의 운영
② 고도화되는 해킹에 총력 대응하기 위한 주요 국가 및 국제기구와의 협력 강화

<제도>
① 국가.공공기관 대상 정보보안 평가제도 개선
② 민간기업 정보보호관리체계(ISMS) 인증 활성화
③ 금융분야 'IT부문평가' 대상기관 확대
④ 용역사업 및 민간분야 보안 관리 강화
⑤ 범정부 차원의 '사이버 안전의 날' 제정・시행과 '클린 인터넷 운동' 활성화 등을 통한 사이버안보에 대한 마인드 확산
⑥ 사이버위협에 대한 효율적 대응을 위한 관련 법령의 정비

<기반>
① 각 정부기관의 정보보안 인력 증원 및 금융위 보안업무 전담조직 신설
② 한국인터넷진흥원의 정보보호 정규직 비율 상향
③ 원전 등 국가 핵심 기반시설 운영기관의 보안 전담인력 확보
④ 정보보호학과 증설 및 계약형 석사과정 확대
⑤ S/W 분리발주 정착
⑥ 국내 정보보호제품의 해외수출 지원 및 정보보호 R&D 확대 등 관련 산업 및 연구 활성화 지원 강화
(박영철 등, 2015)

[82] 미래창조과학부 보도자료, 정부,「국가 사이버안보 종합대책」수립 - 사이버안보 강화를 위한 4대 전략(PCRC) 마련 -, 2013.7.4

총괄 부처로 역할하게 되었다. 또한, 국가차원의 '사이버 위협정보 공유시스템'을 2014년까지 구축하고, 이를 토대로 민간 부문과의 정보제공, 협력도 강화해 나갈 방침이라고 밝혔다.[83]

정부는 약 1년여 후인 2014년 11월 17일, 국가 사이버안보 종합대책의 이행성과를 발표하였다.[84] 정부는 청와대를 컨트롤타워로 민(미래부), 관(국정원), 군(국방부) 등 분야별 책임기관 체제를 확립하였고, 주요 정보통신기반시설 지정도 2013년 209개에서 2014년 292개로 확대하였다고 밝혔다. 또한, '사이버위협 정보분석·공유시스템(C-TAS)'를 2014년 8월 본격 가동하여, 주요 통신사 및 포털, 백신업체, 보안업체 등과 사이버위협 정보의 공유·연계를 강화하고, 사이버 위협정보 분석시간을 6시간에서 30분으로 단축하는 등 대응 시스템을 고도화했다.[85]

---

[83] <사이버위협 대응 체계 즉응성 강화(Prompt)>
① 사이버컨트롤타워는 청와대
② 실무총괄은 국가정보원
③ 미래창조과학부, 국방부 등 관계 중앙행정기관은 소관분야 담당

<유관기관 스마트 협력체계의 구축 (Cooperative)>
① 국가 차원의 '사이버위협정보공유시스템'의 구축
② 민간부문과의 정보제공・협력 강화

<사이버공간 보호대책 견고성 보강(Robust)>
① 2017년까지 IDC(집적정보통신시설)・의료기관 등을 포함한 주요정보통신기반시설의 확대
② 국가기반시설에 대한 인터넷망과 분리・운영
③ 전력・교통 등 테마별로 특화된 위기대응훈련의 실시
④ 정보보호관리체계(ISMS) 인증 대상의 확대
⑤ 중소기업 대상 보안취약점 점검 및 교육지원 등을 통한보안수준의 향상

<사이버안보 창조적 기반 조성(Creative)>
① 최정예 정보보호 전문가 양성사업 확대 및 영재교육원 설립 등 다양한 인력양성프로그램의 추진을 통하여 2017년까지 사이버전문인력 5,000명 양성
② 미래시장 선점을 위한 10대 정보보호 핵심기술 선정 및 연구개발의 집중적 추진을 통한 기술 경쟁력 강화
* 10대 정보보호 핵심기술 개발 분야 : 5대 기반 분야(암호・인증・인식・감시・탐지), 5대 신성장 분야(스마트폰・IoT/M2M・클라우드・ITS・사회기반)
(박영철 등, 2015)

[84] 미래창조과학부 보도자료,「국가 사이버안보 종합대책」으로 사이버 안심국가 초석 다져, 2014.11.17

[85] <범정부 차원의 사이버위기 대응 체계의 정립>
① 청와대를 컨트롤타워로 민(미래부)・관(국정원)・군(국방부) 등 분야별 책임기관 체제의 확립
② 관계 기관 간 사이버위협 정보공유의 강화
③ 사이버공격 발생시 유기적인 협력이 가능한 확고한 대응체계의 구축
④ 2014년 8월 이후 'C-TAS'18) 가동을 통한 사이버위협 정보의 공유・연계의 강화 및 사이버 위협정보의 분석시간 단축(6시간→30분)
⑤ 범정부로그분석(nSIMS) 구축을 통한 사이버공격 사전 예방 및 해킹방어능력 제고

<침해사고 예방 조치 및 사이버 공격에 대한 보안인프라 보강>
① 주요 정보통신기반시설 지정 확대('13년 : 209개→'14년 292개)
② C-TAS 구축 등 국가 보안인프라 확충
③ 보안취약점 사전 제거를 통한 대응력 강화를 목적으로 Secure Coding 기법을 모바일 전자정부 서비스에도 확대 적용('14.9.)
④ '사이버안전 훈련센터' 개소('14.10)
⑤ 민간 기업에 대한 DDoS 공격 방어를 위한 '디도스 대피소'의방어용량 확대(40기가⇒100기가)
⑥ 공무원 '정보보호' 직류 신설('14.6), 민간영역에서 정보보호최고책임자 지정・신고제도 시행('14.11) 등 정보보호 전문인력보강
⑦ 금융권 사이버안전을 강화하기 위하여 침해사고 대응 전담반운영('14.1), 정보보호최고책임자(CISO) 전임제도(겸직 금지) 도입('14.9), 금융보안 전담기구의 신설('15년초)

**2015년 : 국가 사이버안보 강화방안[86]**

2014년 말 한국수력원자력 해킹되어 설계도면까지 유출되는 사고가 발생하였고, 원전을 중단하지 않으면 유출한 자료를 공개하겠다는 협박도 있었다. 이 사고를 계기로 정부는 2015년 3월, 범정부 차원의 사이버안보 역량 강화, 핵심기술 개발 및 인력양성, 국제공조 확대, 업무수행체계 정비, 컨트롤타워 강화 등의 핵심과제를 담은 '국가 사이버안보 강화방안'을 발표하였다. 또한, 국가안보실 중심의 전반적인 사이버안보 컨트롤타워 기능을 보다 강화하기로 했다고 밝혔다.[87]

---

<정보보호 인력의 캐리어패스(Career-Path)체계 확립>
① '정보보호영재교육원'(4개대) 지정 및 마이스터고 신설(대덕전자기계고)
② '한국형 탈피오트'를 양성하기 위한 민・군 연계 프로그램을 추진('14.2)
③ '비케이(BK)21 플러스 사업'에 정보보호 사업(4개대) 선정, 고용계약형 정보보호 석사과정도 확대(8개)
④ 차세대 보안리더(BOB(Best-of-Best)) 과정과 재직자 중심의 최정예 사이버보안인력 양성(K-Shield) 과정을 통해 화이트해커를 매년 240명 양성
⑤ 화이트햇콘테스트(해킹방어대회, '14.11) 및 'Codegate' 개최('14.5)

<스미싱 대응시스템 구축 및 전자금융사기 피해의 최소화>
① 신규 출시 스마트폰에「모바일 백신앱('13.9)」과「스미싱 차단앱('14.9)」기본 탑재
② 「번호도용 문자차단서비스」19)의 확대

<정보보호 투자 활성화 대책의 수립>
① 조세감면 확대('14년 : 7%→ '15년 : 10%)
② 정보보호 서비스(연구・기술자문) 투자비용에 대한 조세감면(25%) 적용
③ 중소기업의 정보보호 신규인력 채용시 인건비(월 최대90만원/1인) 보조 등 인센티브 강화 방안의 마련・추진
④ 10대 일류 정보보호 제품 기술개발(사이버블랙박스 등) 추진 계획

<정보보호 캠페인 전개>
① "지키GO, 누리GO" 캠페인 전개
② 제3회 정보보호의 날 개최('14.7)
③ 초중고 교육과정에 정보보안 윤리교육 반영
(박영철 등, 2015)

[86] 국무조정실 보도자료, 국가 사이버안보 태세 역량'대폭 강화한다., 2015.3.17

[87] <범정부 차원의 사이버안보 역량 강화>
① 중앙행정기관, 지방자치단체와 주요기반시설 관리기관의 보안능력 확충을 위한 사이버보안 전담조직의 신설・확대의 추진
② 각급기관의 정보보호예산을 별도 항목으로 분리하고 취약점 분석・평가 지원, 사이버징후 탐지・대응기구 운영, 업무망과 인터넷 분리 등 관련 예산의 확대
③ 민・관・군 합동 사이버위기 대응 실전훈련을 강화
④ 사이버위협 정보 종합 수집・분석・공유 시스템의 보강

<사이버안보 핵심기술 개발 및 정예요원 육성을 적극 추진>
① 사이버 능력이 우수한 특기자 전형의 사이버특화 고교・대학의 확대
② 軍에서 전문인력을 효과적으로 활용할 수 있도록 하기 위한 '한국식 탈피오트' 체계의 구축
③ 軍 전역 후 사회 각 분야에서 활용되도록 사이버인력 생태계 조성
④ 전문기관의 사이버안보 핵심기술 개발 투자 확대
⑤ 벤처기업 펀딩 및 정부지원사업 확대

<사이버 대응작전 조직・인력 확충 및 산업 증진>
① 국가 사이버 대응작전 수행 조직・인력의 확충
② 관련 연구개발 예산의 확대
③ 주요 정보통신망에 대한 해킹 방지기술 등 보안기술 및 부품 개발 등 관련 산업 육성

위 방안은 3월 17일 발표되었는데, 4월 30일 '국가 사이버안보 태세 강화 종합대책'이 수립된 것으로 보인다.[88] 그러나 이 종합대책은 공개되어 있지 않아, '국가 사이버안보 강화방안'과 같은 것인지, 아니면 또 다른 대책인지 알 수 없다. 또한, 2016 국가정보보호백서에 따르면, 국가정보원은 2015년 초에 청와대 국가안보실과 공동으로 국가 사이버안보 정책에 대한 중·장기 추진 방향을 제시하는 거시적 개념의 기본전략인 '국가사이버안보전략'을 마련하였다고 한다. 동 전략은 '선진 사이버안보강국 실현(Advanced Cyber-Security Power)'을 비전으로 설정하고, 미래지향적 사이버안보 태세 확립, 국가 핵심 자산의 보호, 창조적 보안기술 중심의 산업생태계 조성, 보안인식 제고 및 제도 개선 등 4대 목표를 달성하기 위한 국가차원의 추진전략을 담고 있다.(2016 국가정보보호백서) 그러나 동 전략 역시 공개되어있지 않아 상세한 내용을 알 수 없다.

지금까지 한국의 사이버 보안 관련 전략의 흐름을 살펴보았는데, 이를 통해 볼 수 있는 몇 가지 시사점은 다음과 같다. 첫째, 2009년부터 2년 간격으로 대책이 발표되었는데, 장기적인 관점의 '사이버 보안 전략'이라기 보다는 항상 대형 사이버 보안 사고가 터진 것을 계기로 급조된 측면이 있다. 그래서 '강화, 확대'를 외치고 있지만 기존 보안 대책의 재탕인 경우가 많다.

둘째, 대책의 제목들이 '사이버안보'라는 용어를 사용하고 있는 것에서 볼 수 있다시피, 국가안보적 관점에서 접근하고 있다. 물론 일부 사이버공격은 국가안보와 연결될 수 있지만, 사이버 보안과 관련한 정책을 국가안보적 시각에서만 보는 것은 지나치게 협소한 시각이 될 수 있다. 사이버 보안은 사이버 공간에서의 국가간의 분쟁, 사이버 범죄의 단속, 기업의 정보보안, 개인의 보안과 인권의 보호 등 여러 차원에 관련되어 있는데, 국내 사이버 보안 대책은 이런 다양한 차원들을 포괄하고 있지 못하고 있다.

셋째, 국내 사이버 보안 정책을 관통하는 비전이나 원칙의 제시가 약하다. 특히, 사이버 보안 정책이 인권이나 인터넷 개방성과 같은 가치에 기반하여 수립되어야 하는데, 국내 대책에서는 이러한 점들이 빠져있다. 즉, 말 그대로 실무적인 차원의 '대책'일 뿐, 사실상 '전략'이라고 할 수 없는 것이다.

예를 들어, 2013년 7월 수립된 EU의 사이버보안 전략은 ① 유럽의 핵심적 가치는 디지털 세계에도 물리적 세계와 마찬가지로 적용되어야 함, ② 기본권, 표현의 자유, 개인정보 및 프라이버시의 보호, ③ 모두를 위한 접근, ④ 민주적이고 효율적인 멀티스테이크홀더 거버넌스, ⑤ 보안을 보장하기 위한 공유된 책임 등 5가지 원칙을 내세우고 있다.
2011년 수립된 영국 사이버 보안 전략의 경우에는 ▸사이버 범죄 감소 및 안전한 사이버 공간 구축, ▸사이버 공격에 대한 복원력 강화와 사이버 상의 권익 보호, ▸열린, 역동적, 안정적인

---

<국제공조확대>
① 사이버공격에 대해 국제 사회와 공조 대응하기 위해 주요국과 사이버안보 관련 정책 및 정보공유 확대
② 국제기구와의 긴밀한 협력을 통하여 사이버공격에 대한 억지력 강화 및 국제규범 마련 노력에 적극 동참

<사이버안보 관련 법령 정비 추진>
국가 사이버안보 정책 의사결정의 일원화 등을 위해 사이버안보 관련 법령을 보완하여 업무수행체계 기반을 지속 정비
(박영철 등, 2015)

[88] 예를 들어, 행정자치부 보도자료 '중앙행정기관, 사이버보안 전문가 보강한다' (2015.11.24)를 보면, 2015년 4월 30일, '국가 사이버안보 태세 강화 종합대책'을 수립하였음을 언급하고 있다.

사이버 공간 구현, ▸ 사이버보안 지식, 기술, 능력 구축 등의 네 가지 목표를 설정하고 있으며, 사이버 공간에서 정부의 권한은 한계가 있기 때문에 산업계 및 학계 등과의 밀접한 협력이 필요하다는 것을 강조하고 있다.
일본 역시 2015년 9월 수립한 '사이버보안 전략 2015'에서, '자유롭고, 안심할 수 있으며, 안전한 사이버 공간의 보장'을 위해 ▸ 사회경제적 활성화와 지속가능한 발전을 증진하고, ▸ 사람들이 안심하고 안전한 삶을 영위할 수 있는 사회를 구축하며, ▸ 국제 공동체와 국가 안보의 평화와 안정성을 보장하는 것을 목표로 제시하고, ① 정보의 자유로운 흐름 보장, ② 법치, ③ 개방성, ④ 자율성, ⑤ 멀티스테이크홀더 사이의 협력 등의 기본원칙을 강조하고 있다.

넷째, 보도자료를 통해 대책의 개요만 공개하고 있을 뿐, 대책의 상세한 내용에 대해서는 공개하고 있지 않다. 사이버 보안 정책 역시 국민 모두의 이해와 공감 속에서 추진되어야 한다고 했을 때, 정보를 비공개한다면 국민들의 이해와 협력을 얻기 힘들 것이다. 또한, 민간의 주체들이 정부의 대책을 비판적으로 검토하고 토론하여 발전적인 대안을 제시하기도 힘들다.

## 2) 국내 사이버 보안 관련 법제

국내 사이버 보안을 규율하는 일반법은 없으며, 각 부문별, 목적별로 개별법이 존재할 뿐이다. 우선 각 부문별로 보면, '국가사이버안전관리규정'과 '전자정부법'이 공공부문, '정보통신망법', '전자금융거래법'이 민간부문의 사이버 보안 관련 규정을 담고 있다. '정보통신기반보호법' 및 '국가정보화기본법'은 공공과 민간부문을 포괄하고 있다.

2001년에 공공 및 민간영역의 사이버 보안을 위한 법체계가 정비되었다고 볼 수 있는데, 주요정보통신기반을 보호하기 위한 정보통신기반보호법이 제정되었고, 기존의 '정보통신망 이용촉진 등에 관한 법률'도 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(정보통신망법)로 변경되면서 정보보호에 관한 내용이 강화되었다. 국가정보통신망의 사이버 보안을 위한 '국가사이버안전관리규정'은 2005년에 대통령 훈령으로 발령되었다.

정보통신기반보호법은 '전자적 침해행위'로부터 공공 및 민간영역의 주요 정보통신기반시설의 보호를 위한 법률이다. 정보통신기반보호위원회의 설립, 보호대책의 수립, 정보통신기반시설의 지정, 침해사고의 대응 등의 내용을 담고 있으며, 공공과 민간영역을 국정원과 미래창조과학부가, 그리고 국방분야는 국방부가 각각 관할하고 있다.

정보통신망법은 정보통신망에서의 개인정보 보호와 정보통신망의 안정성을 확보하기 위한 보안 조치를 규율하고 있다. 정보보호 사전점검, 정보보호최고책임자의 지정, 집적정보통신시설의 보호, 정보보호 관리체계 인증, 침해사고 대응 등의 내용을 담고 있다.

국가사이버안전관리규정은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 있으며, 국가사이버안전과 관련된 정책 및 관리의 총괄·조정을 국정원이 맡고 있다. 그러나 이 규정은 대통령 훈령으로서 체계 정합성이나 법적 구속력에 있어 문제가 지적되어 있다.(박영철 등, 2015)

전자정부법은 행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정하고 있다. 행정전자서명에 대한 규정, 정보통신망 보안대책의 수립 등의 내용을 포함하고 있다. 국가정보화보호법은 기존 '정보화촉진기본법'이 2009년에 전면 개정된 것으로, 국가정보화의

기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정하고 있는데, 정보보호 시책의 마련, 정보보호시스템에 관한 기준 고시 등의 내용을 포함하고 있다. 전자금융거래법은 전자금융거래의 안정성 확보 조치 등의 내용을 규정하고 있다.

주요 법령들의 사이버 보안 대응 체계를 비교해보면 다음과 같다.

표 : 사이버 보안 대응체계의 비교 (출처 : 박영철 등, 2015)

| | 정보통신기반보호법 | 정보통신망법 | 국가정보화기본법 | 전자정부법 | 전자금융거래법 | 국가사이버안전관리규정 |
|---|---|---|---|---|---|---|
| 대상 | 정보통신기반시설 | 개인정보, 정보통신망 | 국가기관이나 지방자치단체가 처리하는 정보의 보호 | 공공기관의 행정정보 및 정보시스템 | 모든 전자금융거래 | 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대한 사이버공격 |
| 침해행위유형 | 해킹, 컴퓨터바이러스, 논리・메일폭탄, 서비스거부 또는 고출력 전자기파 | 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 훼손・멸실・변경・위조 | 정보의 훼손, 변조, 유출 | 위조・변경・훼손, 말소 공개・유포, 누설, 권한 범위를 넘어선 처리 | 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 조작・파괴・은닉, 유출, 파괴 | 해킹・컴퓨터바이러스・논리폭탄・메일폭탄・서비스방해 |
| 대응체계 | 정보통신기반보호위원회, 대책본부 구성, 정보공유・분석센터 운영 | | | | | 국가사이버안전전략회의, 국가사이버안전대책회의, 국가사이버안전센터 |
| 사전예방조치 | 주요정보통신기반시설보호대책의 수립, 주요정보통신기반시설보호계획의 수립, 주요정보통신기반시설의 지정, 취약점의 분석・평가, 보호지침 | 개인정보의 보호조치, 정보통신망의 안전성 확보, 집적된 정보통신시설의 보호, 정보보호 관리체계의 인증, 이용자에 대한 보호조치 | 정보보호 시책의 마련, 정보보호시스템에 관한 기준 마련 | 전자적 대민서비스 보안대책, 정보통신망 등의 보안대책 수립・시행, 정보시스템 장애 예방・대응 | 안전성의 확보의무, 전자금융기반시설의 취약점 분석・평가 | 사이버안전대책의 수립・시행, 사이버위기대응 훈련, 사이버공격과 관련한 정보의 협력, 보안관제센터의 설치・운영 |
| 사후대응조 | 침해사고 | 침해사고의 | | | 침해사고의 | 경보 발령, |

| | | | | | | |
|---|---|---|---|---|---|---|
| 치 | 발생시 통지, 복구조치 | 대응, 침해사고의 신고, 침해사고의 원인 분석 | | | 통지, 침해사고의 대응 | 사고통보 및 복구, 사고조사 및 처리 |

그 외에 특정 목적이나 기능별로 사이버 보안과 관련된 법률이 존재하는데, 주요 법령을 목적, 기능별로 분류해보면 아래 표와 같다.

표 : 정보보호 관련 주요 법령 (출처 : 2016 국가정보보호백서)

| 구분 | 법령명 |
|---|---|
| 정보통신망 및 정보시스템의 안전한 이용 | 국가정보화기본법, 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법, 전자서명법, 국가사이버안전관리규정 등 |
| 침해행위의 처벌 | 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자무역촉진에 관한 법률, 형법 등 |
| 국가기밀보호 및 중요 정보 국외유출 방지 | 군사기밀보호법, 보안업무규정, 군형법, 산업기술의 유출방지 및 보호에 관한 법률, 기술의 이전 및 사업화 촉진에 관한 법률, 민·군겸용기술사업 촉진법 등 |
| 정보보호 여건 구축 | 정보보호산업의 진흥에 관한 법률, 정보통신기반보호법, 국가사이버안전관리규정 등 |
| 개인정보보호 | 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용 정보의 이용 및 보호에 관한 법률 등 |

국내 사이버 보안 관련 법령을 보면, 법령들이 전체적으로 체계적이고 통일적인 체계를 가지고 있다고 보기 힘들다. 관련 정의도 조금씩 다를 뿐더러, 대응 체계도 다양하며, 법령 사이의 중복도 나타나고 있다. 이는 실제 현장에서 사이버 보안 사고에 대응하는데 있어서 혼란을 야기하거나 사이버 보안을 담당하는 업체나 기관에게 불필요한 부담을 줄 수 있다.(박영철 등, 2015)

## 3) 국내 사이버 보안 수행체계

현재 국내 사이버 보안 체제는 2015년 4월, 사이버 안보 태세 강화 종합대책 이후 변화하게 되었다. 2015년 4월 이전의 사이버 보안 체계는 아래 그림과 같다.

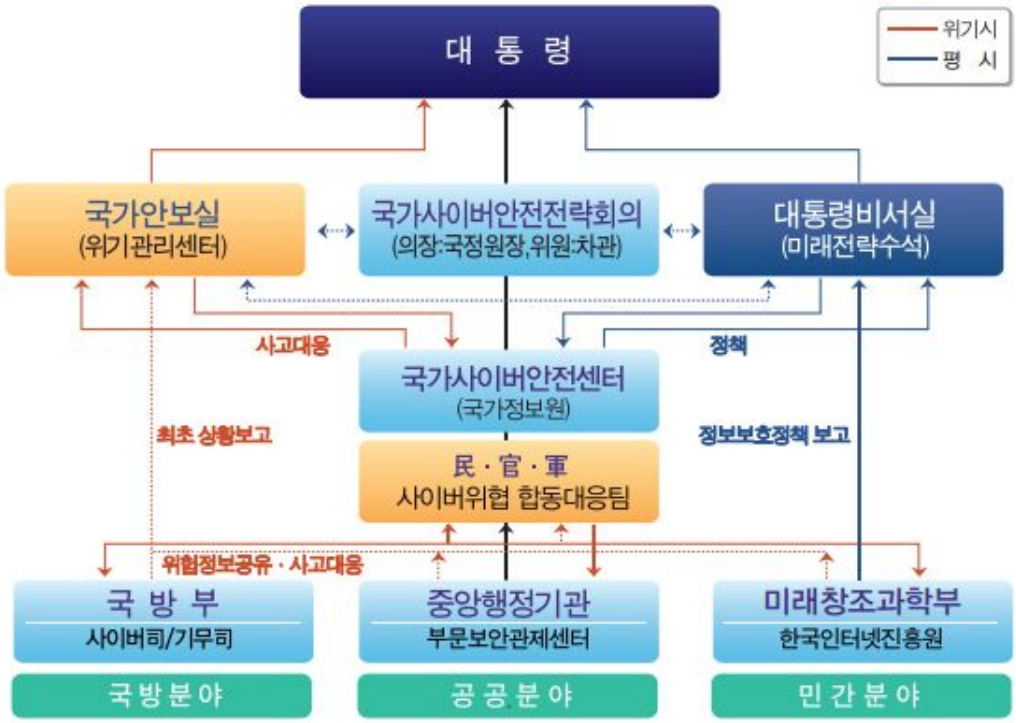



그림 : 2015년 4월 이전, 국가 사이버안보 수행체계 (출처 : 2015 국가정보보호백서)

사이버안보[89] 컨트롤타워를 청와대에 두고, 국가정보원이 실무총괄을 각각 담당하며, 민(民)·관(官)·군(軍) 분야별로 책임기관을 두었다. 청와대의 컨트롤타워 역할은 위기시와 평시로 나뉘어 지는데, 위기시에는 국가안보실이 컨트롤타워로서 사이버위기 상황 보고·전파 및 대응활동을 총괄하며, 평시에는 미래전략수석실이 정보보호 관련 법·제도 정비, 정책 수립 등의 역할을 담당 한다.

국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 '국가사이버안전전략회의'를 두고,국가사이버안전체계 수립 및 개선, 국가사이버안전 관련 정책의 기관 간 역할조정에 관한 사항, 국가사이버안전 관련 대통령 지시사항에 대한 조치방안 등을 심의한다. (국가사이버안전관리규정 제6조 제4항) 전략회의의 의결사항은 국가안보실·미래전략수석실과 협의를 거쳐 최종적으로 대통령에게 보고된다.

국가정보원은 사이버안보 실무총괄 역할을 맡아 '국가사이버안전센터'에서 국가·공공부문 사이버공격 예방 및 침해사고 조사, 사이버위협정보 수집·분석·배포, 국가사이버안전전략회의 운영, 사이버안전기본계획 수립 등의 업무를 수행한다. 또한 사이버위협에 대한 범국가 차원의 체계적인 대응체계를 위해 국가사이버안전센터에 '민·관·군 사이버위협 합동 대응팀'을 운영한다.(국가사이버안전관리규정 제8조)[90]

---

[89] 2015년 국가정보보호백서를 비롯하여, 정부의 종합대책 자료는 '사이버안보'라는 개념을 사용하고 있다. 이는 한 측면에서는 사이버 보안을 국가안보적 측면에서 바라본 것이기도 하지만, 별도의 사이버 보안 정책을 두고 있지 않기 때문에 일정 정도 사이버 보안과 유사한 개념으로도 사용된 것으로 보인다.

[90] 제8조(국가사이버안전센터) ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 "사이버안전센터"라 한다)를 둔다.
②사이버안전센터는 다음 각호의 업무를 수행한다.
1. 국가사이버안전정책의 수립
2. 전략회의 및 대책회의의 운영에 대한 지원

국방부는 국군기무사령부·국군사이버사령부를 통해 국방분야의 사이버안보 업무를 담당하는데, 국방분야 사이버위협 예방 및 침해사고 대응, 전시 사이버전 수행 및 관련 기술 개발 등 임무를 수행한다. 민간분야의 사이버안보 활동은 미래창조과학부가 담당하며, 민간분야 사이버공격 예방 및 침해 사고 대응, 사이버안보 대국민 홍보, 정보보안 산업·인력 육성 및 정보보안 기술개발 등 업무를 수행한다. 사이버공격 등 위기상황 발생 즉시 각급기관은 국가안보실(위기관리센터)과 국가정보원 (국가사이버안전센터)에 동시 최초 상황보고를 하며, 국가정보원은 사이버공격에 의한 피해 및 대응상황을 국가안보실을 통해 대통령에게 보고한다. (2015 국가정보보호백서)

2014년 말 소위 '한수원 해킹' 사고 이후, 2015년 4월, 정부는 국가 사이버 안보 태세 강화 종합대책을 마련하였다. 이에 따라 정부는 국가안보실 중심의 전반적인 사이버안보 컨트롤타워 기능을 보다 강화하기 위해 국가안보실 산하에 사이버안보비서관을 신설하고 국가안보실과 국가사이버안전센터를 통해 국가적인 사이버보안 정책의 수립·시행·평가를 일원화하는 방식으로 사이버안보 수행체계를 변화시켰다.

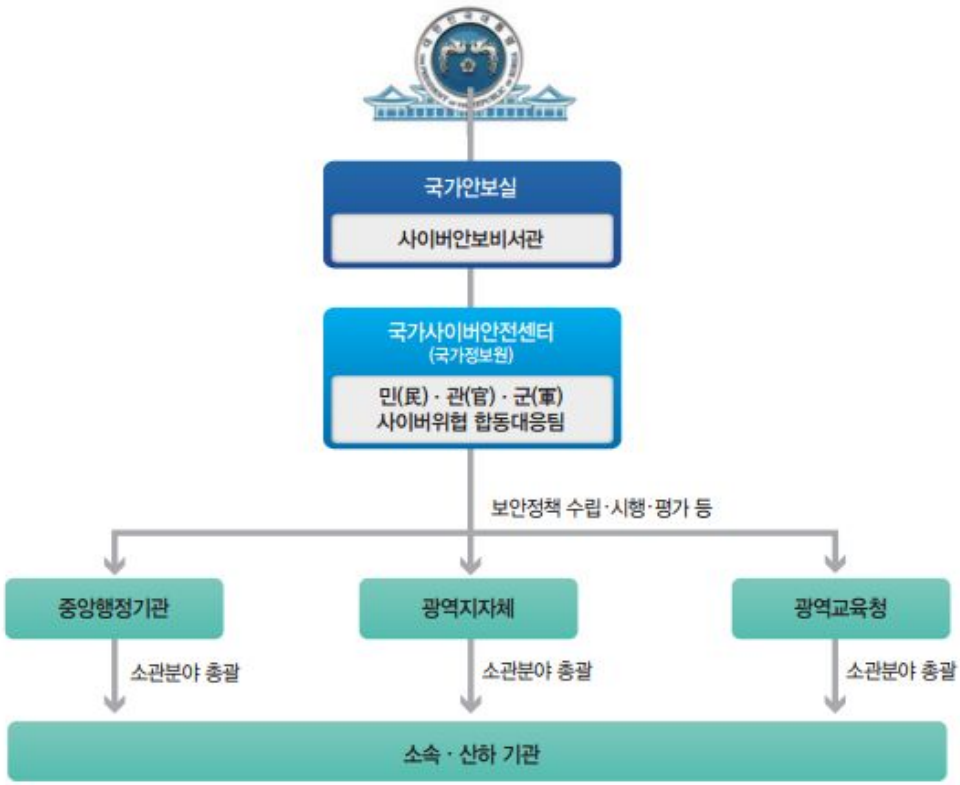



그림 : 2015년 4월 이후 국가 사이버안보 수행체계의 변화 (출처 : 2015 국가정보보호백서)

3. 사이버위협 관련 정보의 수집·분석·전파
4. 국가정보통신망의 안전성 확인
5. 국가사이버안전매뉴얼의 작성·배표
6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원
7. 외국과의 사이버위협 관련 정보의 협력

③ 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반(이하 "합동대응반"이라 한다)을 설치·운영할 수 있다.

④국가정보원장은 합동대응반을 설치·운영하기 위하여 필요한 경우에는 관계 중앙행정기관, 지방자치단체 및 공공기관의 장에게 소속 공무원 및 직원의 파견을 요청할 수 있다.

이를 위해 사이버안보비서관을 국가안보실에 두고, 유관 부처 차관급이 참석하는 사이버안보정책조정회를 두어 법·제도 개선, 인력양성 추진 등 사이버안보 분야의 주요 정책을 수립·조정하고 있다. (2016 국가정보보호백서) 이러한 체계 개편에도 불구하고, (명확하게 설명되어 있지는 않지만) 군과 민간 영역의 사이버 보안을 관할하는 국방부와 미래창조과학부의 역할은 계속 유지되고 있는 것으로 보인다.

### 4) 국가정보통신망의 보호

국가사이버안전관리규정은 제1조에서 "국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함"을 목적으로 한다고 밝히고 있지만, 국가정보통신망이 무엇인지 정의하고 있지는 않다. 다만, 제2조 1호에서 '정보통신망'을 "「전기통신기본법」 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제"로 정의하고 있다. 그리고, 제3조에서 훈령의 적용범위를 '중앙행정기관(대통령 소속 기관, 국무총리 소속 기관 및 국가인권위원회를 포함한다.), 지방자치단체 및 공공기관의 정보통신망'으로 정하고 있기에, 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 국가정보통신망으로 이해할 수 있다.

현재 국가정보통신망을 보호하기 위해 다음과 같은 5개의 제도가 운영되고 있다.[91]

- 정보보안 관리실태 평가
- 보안관제센터 설치 운영
- 보안적합성 검증
- 암호모듈 검증
- 정보보호 제품 평가.인증

정보보안 관리실태 평가는 국가 정보보안 정책의 이행실태를 확인하고 각급 기관의 보안관리 체계를 강화하기 위한 제도이다. 2007년부터 국가·공공기관을 대상으로 실시하고 있으며, 국가정보원은 매년 평가대상 및 일정을 확정하여 대상기관에 통보하는데 2015년에는 121개 기관을 평가하였다고 한다.

보안관제는 정보통신시스템을 24시간 모니터링하고 사이버 위협을 실시간으로 탐지·분석·대응하는 활동을 의미한다. 현재 국가안보실을 중심으로 중앙행정부처 단위에서 39개의 보안관제센터가 운영되고 있는데, 행정자치부의 정부통합전산센터, 국방부의 사이버사령부, 한국인터넷진흥원(KISA) 인터넷침해대응센터, 금융보안원, 검찰 사이버안전센터, 경찰 사이버보안관제센터, 국가보안기술연구소의 보안관제 기술지원센터 등을 포함한다. 보안관제센터는 보안관제 업무 외에도 보안 취약점의 분석·평가 등도 수행하며, 보안관제센터 간에 위협 정보를 실시간으로 공유하고 있다.

보안적합성 검증은 국가·공공기관이 도입하는 정보보호시스템의 보안기능에 대한 안전성을 검증하는 제도이다. 국가·공공기관은 보안기능이 포함된 IT제품, 정보보호시스템, 암호기능이 포함된 제품, 네트워크 장비 등의 도입시에 국가정보원의 보안적합성 검증을 받아야 한다.

[91] 이하 국가정보통신망의 보호 제도 관련 내용은 2016 국가정보보호백서를 참고한 것이다.

암호모듈 검증제도는 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않는 중요 정보를 보호하기 위해 사용되는 암호모듈의 안전성과 구현적합성을 검증하는 제도이다. 2005년부터 시행되었는데, 2009년부터 국가·공공기관에서 사용되는 정보보호제품에 중요 자료를 저장·소통하기 위한 암호 기능이 포함될 경우는 반드시 검증필 암호모듈을 탑재하도록 하고 있다. 국가정보원이 검증기관, 국가보안기술연구소가 시험기관을 맡고 있다.

정보보호제품 평가·인증 제도는 민간업체가 개발한 정보보호시스템에 구현된 보안기능의 안전성과 신뢰성을 보증하여 사용자들이 안심하고 제품을 사용할 수 있도록 지원하는 제도이다. 2005년에는 평가기준을 CC(Common Criteria)로 일원화하고, 모든 정보보호제품으로 평가 대상을 확대하였다. 또한, 2006년 CC에 따른 평가·인증결과를 회원국 간 상호 인정하는 국제상호인정협정(CCRA, Common Criteria Recognition Arrangement)에의 가입과 동시에 인증서발행국 지위를 획득하였다. 1998년 2월부터 IT보안인증사무국[92]이 이를 시행하고 있으며, 미래창조과학부가 정책기관 역할을 하고 있다.

## 5) 주요 정보통신 기반시설의 사이버 보안

앞서 해외 주요 국가의 사례에서 보았듯이, 공공 및 민간 영역의 주요 기반시설에 대한 사이버 보안은 어느 나라나 강조하고 있다. 교통, 금융, 통신, 에너지 등 기반시설의 특성상 사회 전반에 미치는 파급력이 크기 때문이다. 국내에서는 주요 기반시설의 보호를 위해 2001년 '정보통신기반보호법'이 제정되어, 이에 따라 보호가 이루어지고 있다.

동 법에서는 정보통신 기반시설을 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망으로 정의하고 있다.
(정보통신기반보호법 제2조 1호) 이에는 공공 및 민간의 기반시설이 모두 포함된다. 주요 정보통신 기반시설 보호를 위한 추진체계는 아래 그림과 같다.

[92] http://itscc.kr/

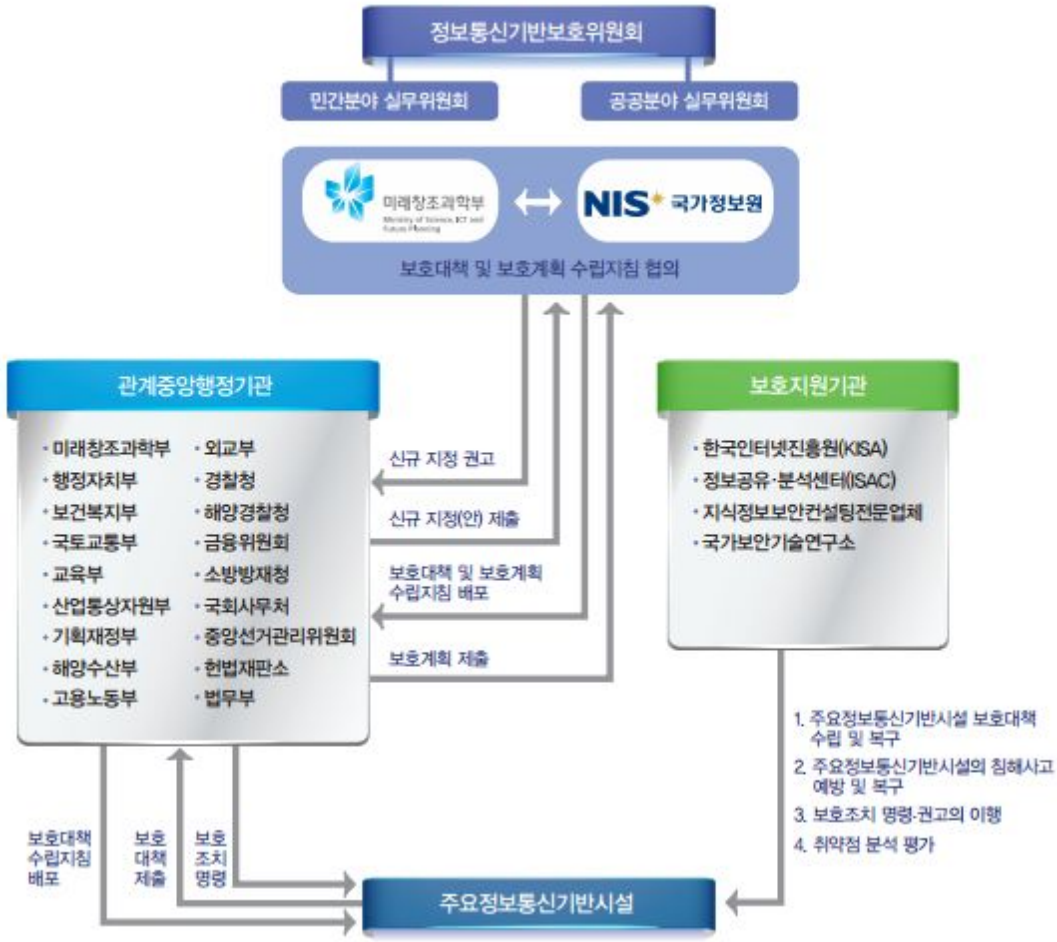



그림 : 주요정보통신기반시설 보호 추진체계 (출처 : 2016 국가정보보호백서)

동 법은 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 '정보통신기반보호위원회'를 두도록 하고 있다.(제3조 1항) 이 위원회의 주요 임무는 주요정보통신기반시설의 1) 보호정책의 조정에 관한 사항, 2) 보호계획의 종합·조정에 관한 사항, 3) 보호계획의 추진 실적에 관한 사항, 4) 관련된 제도 개선에 관한 사항 등의 심의이다.(제4조) 위원회의 위원장은 국무조정실장이 맡고, 위원은 주요 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 구성된다.

위원회를 효율적으로 운영, 지원하기 위해 공공분야와 민간분야를 담당하는 '정보통신기반보호 실무위원회'를 두고 있다. (제3조 4항) 공공분야는 국가정보원이, 민간분야는 미래창조과학부가 맡고 있다.(시행령 제5조)

주요정보통신기반시설의 지정은 중앙행정기관의 장이 지정하는데, 1) 수행하는 업무의 국가사회적 중요성, 2) 수행하는 업무의 정보통신기반시설에 대한 의존도, 3) 다른 정보통신기반시설과의 상호연계성, 4) 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위, 5) 침해사고의 발생가능성 또는 그 복구의 용이성 등을 고려하여 지정한다.(제8조 1항) 중앙행정기관의 장은 소관분야에 대한 주요정보통신기반시설에 관한 보호계획을 수립·시행하며(제6조 1항), 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다.(제6조 2항)

주요 정보통신기반시설을 관리하는 기관을 '관리기관'이라고 한다. 즉, 관리기관은 기반시설을 운영하는 업체나 공공기관이라고 할 수 있다. 관리기관은 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하고(제9조 1항), 그 결과에 따라 소관 기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책(이를 "주요정보통신기반시설보호대책"이라 한다)을 수립·시행해야 한다.(제5조 1항) 관리기관은 침해사고가 발생하여 기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원에 그 사실을 통지해야야 한다.(제13조 1항)

미래창조과학부장관, 국가정보원장, 국방부장관은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다.(제5조의2 1항) 또한 이들은 특정한 주요정보통신기반시설을 관리기관으로 지정하도록 해당 중앙행정기관의 장에게 권고할 수 있는 권한이 있다. 이를 위해 필요한 경우 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청할 수 있다. (제8조의2) 또한, 이들은 필요한 경우 주요정보통신기반시설의 보호를 지원할 수 있다. 특히, 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설의 경우에는 관리기관의 장이 국가정보원장에게 우선적으로 그 지원을 요청해야 하고, 급박한 경우는 요청이 없더라도 국가정보원장이 지원할 수 있도록 하고 있다. 다만, 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에는 지원할 수 없다.(제7조)

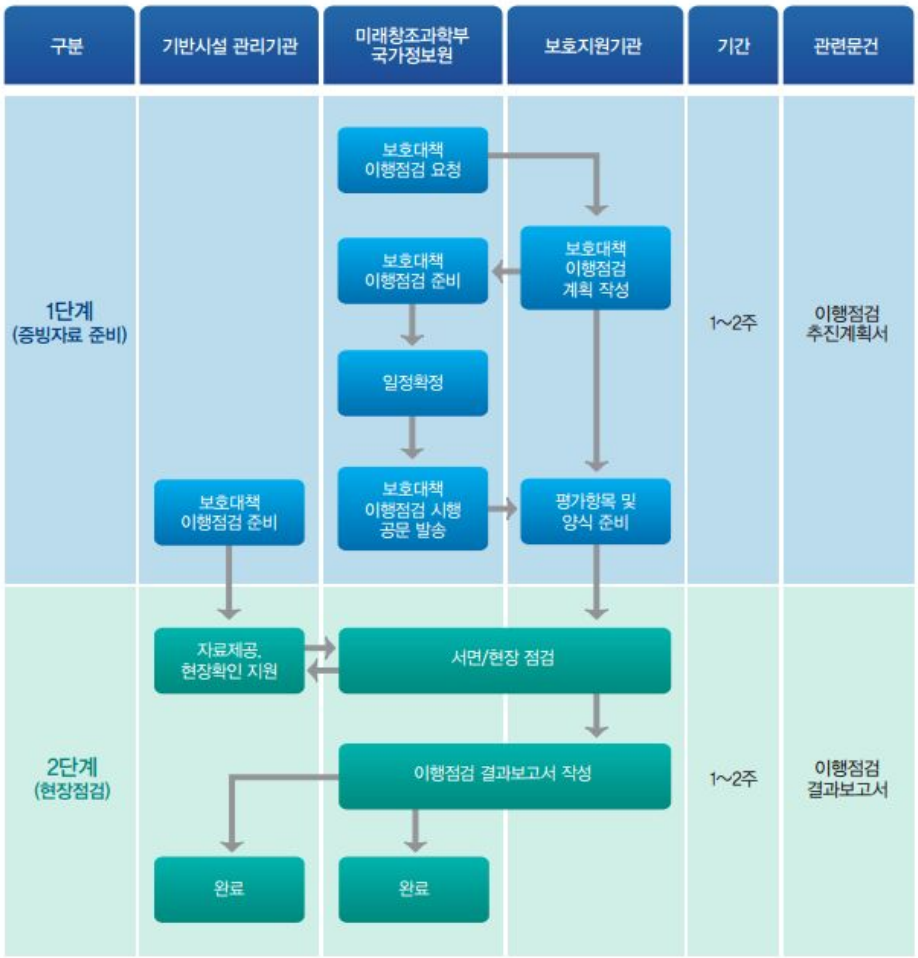



그림 : 주요정보통신기반시설 보호대책 이행점검 절차 (출처 : 2016 국가정보보호백서)

관리기관의 취약점 분석 및 평가를 지원하기 위해, 한국인터넷진흥원, 국가보안기술연구소, 정보공유·분석센터, 정보보호 전문서비스 기업 등 지원기관의 도움을 받을 수 있도록 하고 있다.(제9조) 한편, 금융, 통신 등 각 분야별로 취약점 및 침해요인과 그 대응방안에 관한 정보 제공, 침해사고가 발생하는 경우 실시간 경보·분석체계 운영 등을 위한 '정보공유·분석센터'를 운영할 수 있다.(제16조)

2016년 1월 현재 정보통신 및 미디어, 금융기관, 교통수송, 에너지, 원자력, 식·용수, 식품의약품 관리, 보건복지, 정부기관, 사회안전시설, 건설·환경, 지리정보, 기타 등의 분야에서 19개 관계중앙행정기관, 232개 관리기관, 385개 기반시설이 지정·관리되고 있다. (2016 국가정보보호백서)

표 : 정보통신기반시설 지정 현황 (출처 : 미래부)[93]

| 년도 | 2012년 | 2013년 | 2014년 | 2015년 | 2016년 |
|---|---|---|---|---|---|
| 민간 | 80 | 82 | 99 | 127 | 142 |
| 공공 | 106 | 127 | 193 | 227 | 243 |
| 합계 | 186 | 209 | 292 | 354 | 385 |

정보통신기반보호법 제8조 6항은 중앙행정기관의 장이 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하도록 하고 있다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 않을 수 있는데, 현재 정부는 주요정보통신기반시설 전체 목록을 국가안보를 이유로 공개하지 않고 있다.

## 6) 민간 영역의 사이버 보안

민간영역의 사이버 보안은 주로 정보통신망법, 특히 '6장 정보통신망의 안정성 확보 등'에 의해 규율되고 있으며, 미래창조과학부가 관할하고 있다. 정보통신기반시설의 경우에는 정보통신기반보호법의 적용을 받는다.

정보통신망법에 따르면, 정보통신서비스 제공자는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 해야 하고, 미래창조과학부 장관은 정보보호지침을 정해 고시하고 권고할 수 있다.(제45조) 제45조의2는 정보보호 사전점검 제도를 규정하고 있는데, 이는 서비스 계획이나 설계단계부터 보안대책을 수립하도록 하기 위한 것으로 2013년 2월 18일부터 시행되었다. 또한, 데이터센터와 같은 '집적정보통신시설'을 위한 보호조치를 특별히 규정하고 있다.(제46조, 제46조의2)

제47조에서 규정하고 있는 정보보호 관리체계(Information Security Management System,ISMS)는 정보보호가 기업의 비즈니스 경영방침과 연계될 수 있도록 정보보호최고책임자를 지정하고, 위험분석을 통한 정보보호정책을 수립하여 그에 대한 정보보호 활동을 전개할 수 있도록 하는 체계이다. 정보보호 관리체계는 정보보호 정책에 따라 수행된 정보보호 활동을 모니터링 및 검토하여 지속적으로 개선할 것을 요구한다.

[93] 박홍근 의원실, 주요정보통신기반시설 비공개 결정… 국정원 빅브라더 첫걸음?, 2016.10.14, http://blog.naver.com/bakhonggeun/220836219562

정보보호 관리체계 인증제도는 기업 또는 조직의 정보보호 관리체계가 인증기준에 적합한지를 제3의 인증기관이 평가하여 인증을 부여하며, 이를 위해 정보보호 관리체계에 대한 표준적 모델 및 기준을 제시한다. 한국인터넷진흥원이 인증기관으로서의 역할을 수행해 왔으며, 한국정보통신진흥협회(2014.5), 한국정보통신기술협회(2015.2), 금융보안원(2015.7)이 추가 지정되었다.(2016 국가정보보호백서) 현재 일정 기준이상의 정보통신서비스 제공자들은 의무적으로 인증을 받도록 하고 있다.[94]

인터넷 침해사고의 예방 및 대응을 위해 미래창조과학부 및 한국인터넷진흥원은 '인터넷침해대응센터(KrCERT/CC, Korea Computer Emergency Response Team Coordination Center)'를 운영하고 있다. 인터넷침해대응센터는 종합상황실을 통해 국내 주요 통신사업자 및 보안관제업체와 연계하여 24시간 365일 인터넷트래픽의 이상 징후를 모니터링하고, 보안 취약점 및 악성코드 등 보안위협에 대한 정보를 수집·분석한다. 또한, 2014년 8월부터 C-TAS(Cyber Threats Analysis System)라는 사이버위협 정보분석·공유시스템을 운영하며, 악성코드 정보, 취약점 및 침해사고 분석정보 등 사이버위협 정보를 관계기관 간에 공유하고 있다.

한편, 정보통신망법 제48조의4는 중대한 침해사고가 발생할 경우 민·관합동조사단을 구성할 수 있도록 하고 있다. 이에 따라 인터넷침해대응센터는 2014년부터 '사이버 보안전문단'이라는 민·관 합동조사단 전문가 풀(pool)을 운영하고 있다.(2016 국가정보보호백서)

# 나. 사이버보안 관련 국가정보원의 역할

국가정보원은 국가사이버안전정책 및 관리의 총괄·조정, 국가사이버안전센터의 운영, 공공영역의 주요정보통신기반시설의 보호, 정보보안 관리실태 평가, 보안적합성 검증, 암호모듈 검증 등 국내 사이버 보안과 관련한 핵심적인 역할을 맡고 있다.

## 1) 국가사이버안전 정책·관리 총괄·조정

국가정보원은 국가사이버안보 수행 체계에서 실질적인 컨트롤타워 역할을 맡고 있다. 2013년 7월 수립된 '국가 사이버안보 종합대책'에서 사이버안보 컨트롤타워가 국정원에서 청와대로 이관되었고, 2015년 4월 '국가 사이버 안보 태세 강화 종합대책'에 따라 국가안보실 산하에 사이버안보비서관을 신설하고 국가안보실 중심의 컨트롤타워 기능을 보다 강화했다고 하지만, 실무총괄 기능은 여전히 국정원에 있다.

대통령 훈령인 국가사이버안전관리규정에 따르면 여전히 국정원이 사이버안보 컨트롤타워를 맡고 있는 것으로 나온다.[95] 동 훈령 제5조는 국정원이 관계 중앙행정기관의 장과 협의하여

[94] 정보통신망법 제47조의2는 다음의 사업자를 의무 인증 대상 사업자로 규정하고 있다.
1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

[95] 공개된 국가사이버안전관리규정은 2013년 9월 2일에 최종 개정되었다.

국가사이버안전과 관련된 정책 및 관리를 총괄·조정하도록 하고, 이를 위해 국가사이버안전기본계획을 수립·시행하도록 하고 있다.

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

국가사이버안전에 관한 중요사항을 심의하기 위해 국정원장 소속하에 '국가사이버안전전략회의'를 둔다. 전략회의의 의장은 국정원장이며, 관계 중앙행정기관의 차관급 공무원이 전략회의의 위원을 구성한다. 전략회의는 1) 국가사이버안전체계의 수립 및 개선에 관한 사항, 2) 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, 3) 국가사이버안전 관련 대통령 지시사항에 대한 조치방안, 4) 그 밖에 전략회의 의장이 부의하는 사항을 심의한다.(제6조) 또한, 전략회의의 효율적인 운영을 위하여 국가사이버안전대책회의를 두고 있다.(제7조)

그런데 2016년 국가정보보호백서에 따르면, 2015년 4월 '국가 사이버 안보 태세 강화 종합대책'에 따라 사이버안보비서관을 국가안보실에 두고, 유관 부처 차관급이 참석하는 사이버안보정책조정회를 두어 법·제도 개선, 인력양성 추진 등 사이버안보 분야의 주요 정책을 수립·조정하는 것으로 체계 개편이 이루어졌다고 하는데, 이러한 체계 개편이 훈령에는 반영되어 있지 않다. 한편, 국정원 홈페이지에는 2016년 3월 8일자로 '국가사이버안전 대책회의 결과' 보도자료가 올라온 것으로 보아, 훈령에 따른 전략회의 및 대책회의가  여전히 운영되고 있는 것으로 보인다.[96] 그러나 전략회의 및 대책회의와 '사이버안보정책조정회'는 어떤 관계인지 명확하지 않다. 한편, 2016년 9월 1일, 국정원이 입법예고한 '국가사이버안보기본법 제정안'에서는 사이버안보에 관한 중요사항을 심의하기 위하여 대통령 소속 하에 '국가사이버안보위원회'를 두고, 국가안보실장을 위원장으로, 유관 부처 차관급을 위원으로 하고 있다. 사이버안보정책조정회를 국가사이버안보위원회라는 이름으로 하고, 국가사이버안보기본법 제정을 통해 수행 체계의 변화를 입법으로 반영하려한 것으로 추측된다. 그러나 아직 국가사이버안보기본법이 제정되지 않았음에도 불구하고 체계 개편이 이루어졌다면, 사실상 법적 근거도 없이 운영되고 있는 셈이다.

국가사이버안전관리규정과 정보통신기반보호법의 관계도 모순적이다. 정보통신기반보호법은 국무조정실장이 위원장인 정보통신기반보호위원회에서 주요정보통신기반시설 보호정책의 조정, 보호계획의 종합·조정, 관련 제도의 개선 등을 심의하도록 하고 있다. 그런데, 훈령인 국가사이버안전관리규정에서 국정원장으로 하여금 국가사이버안전과 관련된 정책 및 관리를 총괄·조정하는 권한을 부여하고 있는 것은 상위법에 위배될 수 있다. 물론 국가사이버안전관리규정 제3조(적용범위)에서 정보통신기반시설에 대해서는 정보통신기반보호법을 우선 적용한다고 하고 있으나, 정보통신기반시설에 대한 보호를 포함한 전반적인 사이버 보안 정책 총괄 권한을 훈령에서

96 http://www.nis.go.kr/CM/1_4/view.do?seq=142&currentPage=1&selectBox=&searchKeyword=&fromDate=&toDate=

국정원에 부여하고, 법률에서 규정된 정보통신기반보호위원회는 주요정보통신기반시설의 보호정책만을 다룬다는 것은 체계가 맞지 않다.

한편 국정원은 실무차원의 컨트롤타워라고 할 수 있는 '국가사이버안전센터'도 운영하고 있다.(8조) 국가사이버안전센터는 1) 국가사이버안전정책의 수립, 2) 전략회의 및 대책회의의 운영에 대한 지원, 3) 사이버위협 관련 정보의 수집·분석·전파, 4) 국가정보통신망의 안전성 확인, 5) 국가사이버안전매뉴얼의 작성·배표, 6) 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, 7) 외국과의 사이버위협 관련 정보의 협력 등의 업무를 수행한다. 또한, 국정원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반을 설치·운영할 수 있다.

국가사이버안전관리규정에서 국정원에 부여하고 있는 권한은 다음과 같다.

- 국가사이버안전과 관련된 정책 및 관리를 총괄·조정 (제5조 1항)
- 국가사이버안전기본계획의 수립·시행 (제5조 2항)
- 국가사이버안전기본계획 추진을 위해 관계 기관에 예산 반영 등에 관한 협조 요청(제5조 3항)
- 국가사이버안전전략회의 운영 (제6조)
- 국가사이버안전대책회의 운영 (제7조)
- 국가사이버안전센터 운영 (제8조 1항)
- 민·관·군 합동대응반 설치·운영 (제8조 3항)
- 합동대응반 설치·운영에 필요한 경우 관계 중앙행정기관, 지방자치단체 및 공공기관의 장에게 소속 공무원 및 직원 파견 요청 권한 (제8조 4항)
- 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼 및 관련 지침 작성 배포 (제9조 3항)
- 사이버안전대책의 이행여부 진단·평가 등 정보통신망에 대한 안전성을 확인할 수 있으며 필요하다고 인정하는 경우에는 해당 중앙행정기관의 장에게 시정 등 필요한 조치 권고 권한(제9조 4항)
- 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 대상으로 사이버위기 대응 통합훈련을 실시 (제9조의2 2항)
- 훈련 결과 필요하다고 판단하는 경우에는 중앙행정기관, 지방자치단체 및 공공기관의 장에게 필요한 시정조치 요청 권한 (제9조의 2 3항)
- 사이버공격 관련 정보의 수집 (국가안보의 위협을 초래한다고 판단되는 경우, 수사정보도 포함) (제10조 1항)
- 사이버공격 관련 정보를 제공받은 경우, 대응에 필요한 조치를 강구하고 그 결과를 해당기관의 장에게 통지 (제10조 2항)
- 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장이 독자적으로 보안관제센터를 설치·운영하지 못하는 경우, 보안관제센터 업무 제공 (제10조의2 1항)
- 보안관제센터에서 수집·탐지한 사이버공격 정보의 수집 (제10조의2 2항)
- 보안관제전문업체의 지정·관리 등에 필요한 사항에 대해 미래부 장관과 협의(제10조의2 4항)
- 보안관제센터의 설치·운영 및 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항 결정(제10조의2 5항)
- 사이버공격 경보 발령 (제11조 1항)
- 경보 발령에 필요한 정보를 관계 중앙행정기관의 장에게 요청 권한 (제11조 4항)

- 사이버공격으로 인한 사고의 발생 또는 징후에 대한 통보 수령 (제12조 1항, 2항)
- 사고복구 및 피해의 확산방지에 필요한 조치 요청 (제12조 3항)
- 사고 원인 분석을 위한 조사 권한 (제13조 1항)
- 조사한 결과 범죄혐의가 있다고 판단되는 경우 수사기관의 장에게 그 내용 통보 (제13조 2항)
- 사이버위기 대책본부 구성·운영 (제13조 3항)
- 대책본부 내에 합동조사팀 등 필요한 하부기구를 두고, 그 구성·운영 등에 필요한 사항의 결정 (제13조 4항)
- 사고조사 및 피해복구 등의 조치를 위하여 관계 중앙행정기관의 장에게 필요한 인력·장비 및 관련 자료의 지원 요청 권한 (제13조 5항)
- 사이버공격에 의한 피해 및 대책본부의 대응 상황을 국가안보실장에게 통보 (제13조 6항)
- 사이버안전업무를 전담하는 전문기구를 운영하는 기관 간 원활한 협력을 위한 관계전문가 회의 소집 (제14조 2항)
- 국가사이버안전에 필요한 기술개발과 기술수준의 향상을 위하여 필요한 시책 추진 (제15조 1)
- 국가보안기술연구소에 의한 사이버안전에 필요한 기술의 연구개발에 관한 세부사항 결정 (제15조 3항)
- 사이버안전과 관련한 전문인력의 양성, 교육 및 홍보에 필요한 지원 (제16조 2항)
- 국방부장관으로부터 국가안보에 필요하다고 판단되는 경우에는 관련 내용의 통보 수령 (제18조 2항)

## 2) 주요정보통신기반시설의 보호

국가정보원은 미래창조과학부 및 국방부와 함께 주요정보통신기반시설의 보호를 책임지고 있다. 특히 국가정보원은 공공영역의 주요정보통신기반시설을 관할하지만, 경우에 따라 민간영역의 주요정보통신기반시설의 사이버 보안에도 관여할 수 있도록 되어 있다. 정보통신기반보호법에 따른 국가정보원의 권한은 다음과 같다.

- 국가정보원 차장이 정보통신기반보호위원회 위원으로 참여(제3조 3항, 시행령 제2조)
- 국가정보원 차장이  공공분야 실무위원회 위원장 담당 (제3조 4항, 시행령 제5조)
- (공공분야) 관리기관에 대하여 주요정보통신기반시설 보호대책의 이행 여부 확인 권한 (제5조의2 1항)
- 주요정보통신기반시설 보호대책의 이행 여부 확인을 위하여 필요한 경우, 관계중앙행정기관의 장에게 주요정보통신기반시설보호대책 등의 자료 제출 요청 권한(제5조의2 2항), 보호조치의 세부적인 내용을 확인·점검 권한(시행령 제9조의2 3항)
- 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보(제5조의2 3항)
- (미래창조과학부 장관과 협의하여) 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보(제6조 4항)

- 관리기관에 대한 기술적 지원[97] (제7조 1항)
- 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설[98]에 대한 관리기관의 장이 기술적 지원을 요청하는 경우에 국가정보원이 우선적으로 지원. 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 요청이 없더라도 관계중앙행정기관의 장과 협의하여 지원할 수 있음. (제7조 2항) 다만, 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행해서는 안됨.(제7조 3항)
- 필요하다고 판단할 경우, 중앙행정기관의 장에게 특정 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있는 권한(제8조의2 1항)
- 이러한 권고를 위해 필요한 경우, 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료 요청 권한(제8조의2 2항), 주요정보통신기반시설지정 조사반을 통해 주요정보통신기반시설 지정 필요성을 검토 권한(시행령 제16조의2 1항)
- 미래창조과학부가 취약점 분석·평가에 관한 기준을 정할 때 협의 (제9조 4항)

이와 같이 국가정보원은 공공영역[99] 정보통신기반시설에 대하여 보호대책 및 수립지침 수립, 기반시설의 사전조사 및 지정권고, 보호대책의 이행 여부 확인 및 개선권고, 관리기관에 대한 기술적 지원 등 대책의 수립부터 피해 조사까지 광범한 권한을 가지고 있다.

한편, 정보통신기반보호법 제8조 6항은 중앙행정기관의 장이 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하도록 하고 있고, 이에 따라 2015년까지 공개되어 왔다. 그러나 2016년에 갑자기 비공개로 전환되었다. 박홍근 의원이 미래창조과학부를 통해 받은 국무조정실의 자료 <제21차 정보통신기반보호위원회 개최결과 알림> 문서에 따르면, 정부는 지난 2016년 1월 4일부터 8일까지 서면심의를 통해 비공개하기로 결정했다고 한다. 이 문서는 “정보통신기반보호위원회에서 심의한 지정시설 지정 또는 지정 취소에 대해 고시하지 않기로 의결하였으니, 이를 참조하여 후속절차를 간사기관(공공분야: 국가정보원, 민간분야:미래창조과학부)과 협의하여 조치”하라고 통보하고 있다.[100] 또한, 2015년 12월 말에도 서울신용평가, KT스카이라이프를 비롯하여 이동통신 3사의 본인확인서비스와 클라우드 시스템, 집적정보통신서비스망 등 개인정보와 관련된 핵심적인 시설들이 새롭게 지정되었다고 한다.

박홍근 의원의 지적처럼, 목록 자체가 비공개 되었을 경우 정보통신기반시설로 지정된 기관이 별다른 사회적 통제없이 확대될 수 있는데, 특히 방송사나 포털의 지정 여부가 사회적

[97] 여기서 기술적 지원은 다음과 같은 업무를 의미한다. (제7조1항)
- 주요정보통신기반시설보호대책의 수립
- 주요정보통신기반시설의 침해사고 예방 및 복구
- 제11조에 따른 보호조치 명령·권고의 이행

[98] 다음의 주요정보통신기반시설을 의미한다. (제7조 2항)
- 도로·철도·지하철·공항·항만 등 주요 교통시설
- 전력, 가스, 석유 등 에너지·수자원 시설
- 방송중계·국가지도통신망 시설
- 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

[99] 시행령 제5조 4항은 공공분야 실무위원회가 담당하는 정보통신기반시설을 다음과 같이 규정하고 있다.
가. 중앙행정기관·지방자치단체 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설
나. 국회·법원·헌법재판소·중앙선거관리위원회 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설
다. 「전자정부법」 제2조제3호에 따른 공공기관이 관리하는 주요정보통신기반시설

[100] 박홍근 의원실, 주요정보통신기반시설 비공개 결정… 국정원 빅브라더 첫걸음?, 2016.10.14, http://blog.naver.com/bakhonggeun/220836219562

논란이 될 수 있다. 정보통신기반보호법에 따라 관리기관은 기반시설의 취약점 정보 등 민감한 정보를 정부에 제출해야 한다는 점에서, 정부의 민간 통제 우려를 불러올 가능성이 있다. 또한, 비록 민간영역의 정보통신기반시설 관할 부처는 미래창조과학부이지만, 민간 정보통신기반시설의 취약점 정보나 업체의 기밀이 국가정보원과도 공유될 가능성을 배제할 수 없고, 특정한 경우 국가정보원은 관리기관의 요청이 없이도 기술적 지원을 하겠다고 나설 수 있다. 지난 2014년 미래창조과학부는 KBS 등 방송사들을 주요정보통신기반시설로 지정하고자 했으나, 한국방송협회를 비롯한 각 지상파 방송사에서 지정 권고를 완강히 거부하여 관할 부처인 방송통신위원회가 권고를 전면 보류한 바 있다. 방송사들은 언론사가 정보통신기반시설로 지정되면 취재를 통해 획득한 정부, 정치인, 기업 등의 비공개 정보나 내부 고발자 정보 등 취재 내용을 국가에서 감시할 수 있다며 우려를 표한 바 있다.[101]

## 3) 정보보안 관리실태 평가

정보보안 관리실태 평가는 국가 정보보안 정책의 이행실태를 확인하고 각급 기관의 보안관리 체계를 강화하기 위한 제도로서, 국가정보원이 이 과정을 주도하고 있다. 이 제도는 국가정보원법 제3조 제2항[102], 전자정부법 제56조 제3항[103], 정부업무평가기본법 제14조·제21조·제22조, 국가사이버안전관리규정 제9조 제4항[104], 국가정보보안기본지침[105]

---

[101] 디지털데일리, 방송사 주요정보통신기반시설 지정 어렵다, 2014.2.14, http://www.ddaily.co.kr/news/article.html?no=114911

[102] 제3조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.
1. 국외 정보 및 국내 보안정보[대공(對共), 대정부전복(對政府顚覆), 방첩(防諜), 대테러 및 국제범죄조직]의 수집·작성 및 배포
2. 국가 기밀에 속하는 문서·자재·시설 및 지역에 대한 보안 업무. 다만, 각급 기관에 대한 보안감사는 제외한다.
3. 「형법」 중 내란(內亂)의 죄, 외환(外患)의 죄, 「군형법」 중 반란의 죄, 암호 부정사용의 죄, 「군사기밀 보호법」에 규정된 죄, 「국가보안법」에 규정된 죄에 대한 수사
4. 국정원 직원의 직무와 관련된 범죄에 대한 수사
5. 정보 및 보안 업무의 기획·조정
② 제1항제1호 및 제2호의 직무 수행을 위하여 필요한 사항과 같은 항 제5호에 따른 기획·조정의 범위와 대상 기관 및 절차 등에 관한 사항은 대통령령으로 정한다.

[103] 제56조(정보통신망 등의 보안대책 수립ㆍ시행)
③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.

[104] 제9조(사이버안전대책의 수립ㆍ시행 등) ① 중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 한다.
②관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 사이버안전대책을 수립·시행하도록 할 수 있다.
③국가정보원장은 제1항 및 제2항에 따른 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼 및 관련 지침을 작성 배포할 수 있다. 이 경우 국가정보원장은 미리 관계 중앙행정기관의 장과 협의하여야 한다. <개정 2012.1.2>
④국가정보원장은 제1항 및 제2항에 따른 사이버안전대책의 이행여부 진단·평가 등 정보통신망에 대한 안전성을 확인할 수 있으며 필요하다고 인정하는 경우에는 해당 중앙행정기관의 장에게 시정 등 필요한 조치를 권고할 수 있다. 다만, 지방자치단체 및 공공기관의 정보통신망에 대한 안전성 확인은 관계 중앙행정기관의 장과 협의하여 수행한다.

[105] 국가 정보보안 기본지침은 국가정보원이 작성, 배포, 관리하는 비공개(외부공개제한) 규정이다. 국가정보원법, 보안업무규정 및 보안업무기획, 조정규정, 국가사이버안전관리규정 및 전자정부법, 정보통신기반보호법, 공공기록물관리에 관한 법률 시행령 등에 따라, 국가 정보보안을 위하여 각급 기관이 수행하여야 할 기본활동을 규정한다. 중앙행정기관(대통령 소속기관 및 국무총리 소속 기관 포함), 그 소속기관, 지방자치단체와 그 소속기관 및 공공기관에 적용된다. 이 지침이 비공개로 관리되는 이유는 정보통신업무의 특성 상 해당 업무 내용이 정보통신망을 통하여 노출될 수 있기 때문이라고 하며,

제121조 등에 의거하여 실시되고 있다. 국가정보원이 매년 평가대상 및 일정을 확정하여 대상기관에 통보하고 각급 기관이 기관별 자체평가를 하지만, 국가정보원이 현장실사, 결과분석 및 점수산출, 평가결과의 통보 등 거의 전 과정을 관장하고 있다.[106]


그림 : 정보보안 관리실태 평가 단계 (출처 : 2016 국가정보보호백서)

## 4) 보안적합성 검증

보안적합성 검증은 국가·공공기관이 도입하는 정보보호시스템의 보안기능에 대한 안전성을 검증하는 제도이다. 「전자정부법」 제56조[107] 및 「공공기록물 관리에 관한 법률 시행령」 제5조[108]에 근거하여 실행되고 있는데, 국가정보원이 2001년 9월부터 보안적합성 검증업무를, 국가보안기술연구소가 보안적합성 시험업무를 수행하고 있다.

국가·공공기관은 보안기능이 포함된 IT제품 도입 시 국가정보원에 보안적합성 검증을 신청해야 하며 검증결과 발견된 취약점을 제거한 후에 운용해야 한다. 또한, 국가정보원이 필요성을 인정하는 정보보호시스템( 2016년 7월 현재 24종)의 경우는 반드시 안전성이 확인된 CC 인증 제품 등 도입요건을 만족한 제품을 도입해야 한다. 또한, IT제품에 중요자료 저장·소통을 위한 암호기능이 포함될 경우 국가정보원장이 안전성을 확인한 검증필 암호

---

이 때문에 지침의 수량과 배포대상을 제한하고 있다고 한다.
http://www.securitya.kr/eduwiz/bb/bbs/board.php?bo_table=c402&wr_id=5

[106] 2016정보보호백서

[107] 제56조(정보통신망 등의 보안대책 수립 · 시행) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다.
② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다.
③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.
④ 제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 보안조치를 마련하여야 한다.

[108] 제5조(기록물관리의 원칙) 공공기관 및 기록물관리기관의 장은 기록물의 생산부터 활용까지의 모든 과정에 걸쳐 진본성(眞本性), 무결성(無缺性), 신뢰성 및 이용가능성이 보장될 수 있도록 관리하여야 한다.

모듈을 탑재해야 한다. 중앙행정기관의 장 및 주요정보통신기반시설 관리기관의 장은 네트워크장비[109] 도입시 국가정보원에 보안적합성 검증을 신청하여야 하며 검증결과 발견된 취약점을 제거한 후에 운용해야 한다. 2016년 7월 1일부 정보보호시스템의 경우에도 중앙행정기관 및 광역시·도, 광역시·도 교육청, 주요정보통신 기반시설 관리기관 등 중요기관을 대상으로 적용한다.[110]

국가·공공기관의 정보보호시스템 도입절차는 아래 그림과 같다.

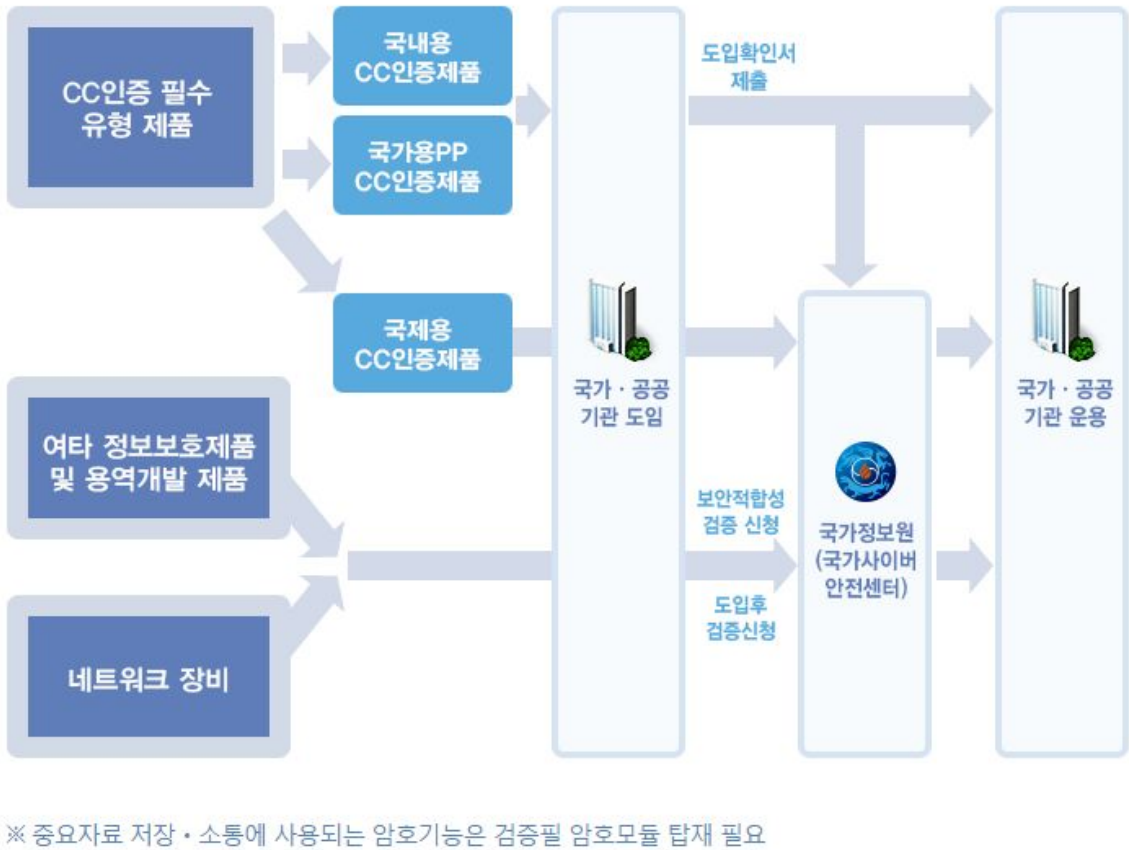



그림 : 정보보호시스템 국가·공공기관 도입절차 (출처 : 국가정보원)

국가정보원은 검증기관으로서 1) 정보보호시스템 보안적합성 시험기준·방법수립, 2) 국가·공공기관의 보안적합성 검증신청서 접수, 3) 시험기관에 시험의뢰 및 시험결과 검토, 4) 검증결과 통보 및 보완조치 이행여부 확인 등을 수행한다. 시험기관인 국가보안기술연구소는 1) 정보보호시스템 보안적합성 시험기준·방법 연구, 2) 정보보호시스템에 대한 시험실시 및 시험결과 작성, 3) 필요 시 보완사항에 대한 추가시험 실시 등의 역할을 수행한다.

[109] 2014년 10월 1일 부로 시행한 네트워크장비의 경우 중앙행정기관 및 광역시 · 도, 광역시 · 도 교육청, 주요 정보통신 기반시설을 대상으로 적용한다.
[110] 국가정보원, 보안적합성 검증 개요, http://www.nis.go.kr/AF/1_7_2_1.do

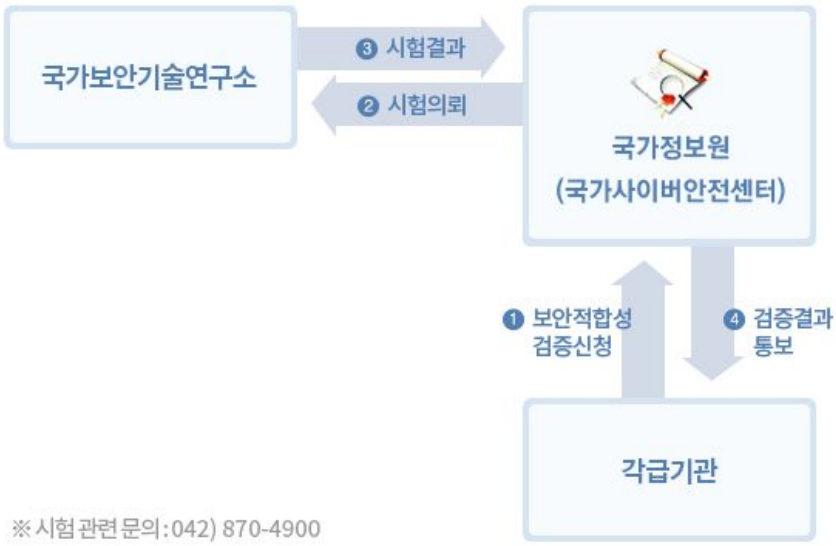



그림 : 국가·공공기관 정보보호시스템 검증절차 (출처 : 국가정보원)

## 5) 암호모듈 검증

국가정보원은 암호모듈을 검증하는 역할도 맡고 있다. 암호모듈 검증제도는 전자정부법 시행령 제69조[111]와 '암호모듈 시험 및 검증지침'에 근거하여 시행되고 있는데, 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않는 중요 정보를 보호하기 위해 사용되는 암호모듈의 안전성과 구현적합성을 검증하는 제도이다. 국가·공공기관에서 사용되는 정보보호제품에 중요 자료를 저장·소통하기 위한 암호 기능이 포함될 경우는 반드시 검증필 암호모듈을 탑재해야 한다.

국가정보원은 검증기관으로서 암호모듈 검증 관련 정책 수립 및 시행, 검증 기준 개발 및 시험 관련 기술 승인, 시험기관 지정·관리·감독 및 시험결과 검증, 검증위원회 개최, 검증필 암호모듈 목록 관리 등의 역할을 수행한다. 시험기관은 국가보안기술연구소에서 맡고 있는데, 암호모듈 검증계약 체결 및 시험 업무 수행, 암호모듈 시험 관련 기준 및 기술 연구·개발 등의 역할을 수행 한다.(2016 국가정보보호백서)

암호모듈 검증을 신청하기 위해서는 신청서와 함께, 기본 및 상세 설계서, 형상관리문서, 개발과정 각 단계별 수행해야 하는 시험항목, 각 시험항목별 시험목적, 시험절차 및 결과서, 제품 및 소스코드를 제출해야 한다.

---

[111] 제69조(전자문서의 보관 · 유통 관련 보안조치) ① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.
1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용
2. 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행
② 행정기관의 장이 제1항의 보안조치를 이행하는 경우에는 미리 국가정보원장에게 보안성 검토를 요청하여야 한다.
③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치에 관하여 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.

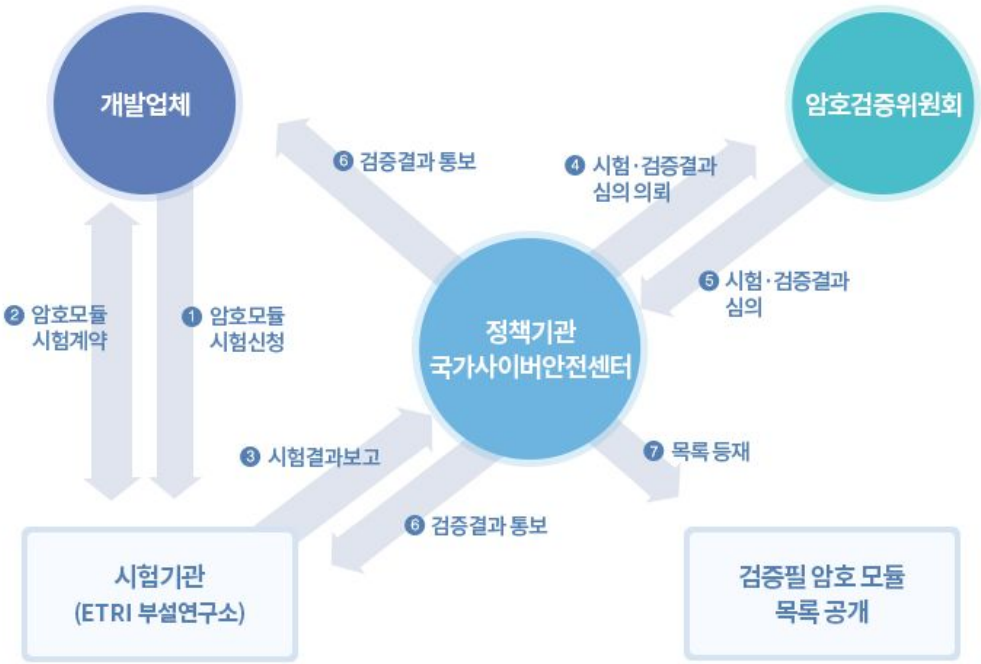



그림 : 암호모듈 검증체계 (출처 : 국가정보원)

국가정보원은 과거 중앙정보부 시절부터 '보안업무규정'에 따라 공공기관의 '비밀'과 '암호자재'의 관리 업무를 해왔다.[112] 과거 암호가 군사 및 국가안보 목적으로 주요 사용되어 왔기 때문이다. 그러나 인터넷이 보편화된 환경에서 이제 암호는 일반 개인 이용자의 통신 보안을 위해서도 중요한 수단이 되고 있다. 암호모듈 검증은 국가·공공기관에서 사용되는 정보보호제품에 포함된 암호기능에 대한 것이지만, 암호개발 업체들이 공공기관 납품에 크게 의존하고 있는 현실을 고려하면, 암호모듈 검증은 공공 및 민간영역에서 사용되는 암호 기술의 개발 및 이용에 영향을 미칠 수 있다. 이 때문에 공공기관에서 사용되는 암호모듈에 대한 검증이 필요하다고 할지라도, 이를 국가정보원이 검증·정책기관으로서 역할하는 것이 적정한지는 재검토될 필요가 있다.

## 6) 보안관제 및 사이버공격 정보 수집

국가보안기술연구소는 산하에 보안관제 기술지원센터를 운영하고 있다. 보안관제 기술지원센터는 국가·공공기관의 보안관제 사각지대 해소와 보안관제기술 연구개발을 위해 국가사이버안전관리규정 제10조의2에 따라 2010년 설립되었다.(2016 국가정보보호백서)

> 제10조의2(보안관제센터의 설치 · 운영) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 설치·운영하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 다른 중앙행정기관(국가정보원을 포함한다)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다.
> ② 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를

[112] 보안업무규정은 중앙정보부법 제2조제2항의 규정에 따라, 대통령령 제1664호로 1964년 3월 10일 처음 제정되었다.
http://www.law.go.kr/lsInfoP.do?lsiSeq=19077&ancYd=19640310&ancNo=01664&efYd=19640310&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000

국가정보원장 및 관계 기관의 장에게 제공하여야 한다.
③ 보안관제센터를 설치·운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다.
④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 미래창조과학부장관이 지정하는 보안관제전문업체의 인원을 파견받아 보안관제업무를 수행하도록 할 수 있다. 이 경우 보안관제전문업체의 지정·관리 등에 필요한 사항은 미래창조과학부장관이 국가정보원장과 협의하여 정한다.
⑤ 제1항의 보안관제센터의 설치·운영 및 제2항의 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.

국가·공공기관이 직접 보안관제센터를 설치·운영하지 못하는 경우에는 국정원 등 다른 중앙행정기관의 장에게 업무를 위탁할 수 있는데, 국정원이 운영하는 보안관제센터가 '보안관제 기술지원센터'라고 할 수 있다.

한편, 국정원은 이 규정에 따라 각 보안관제센터에서 수집·탐지한 사이버공격 정보를 제공받으며, 보안관제센터의 설치·운영 및 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항을 (관계 중앙행정기관의 장과 협의하여) 정한다.

## 7) 정보보호제품 평가·인증

정보보호제품 평가·인증 제도는 민간업체가 개발한 정보보호시스템에 구현된 보안기능의 안전성과 신뢰성을 보증하여 사용자들이 안심하고 제품을 사용할 수 있도록 지원하는 제도이다. 이 제도는 국가정보화기본법 제38조[113] 및 동법 시행령 제35조[114], 정보보호시스템 평가·인증지침(미래창조과학부고시 제2016-73호, 2016.6.27., 일부개정)에 근거하여 운영되고 있다. 국가정보화기본법은 미래창조과학부 소관 법률이고, 미래창조과학부가 CC 평가인증정책의 정책기관으로 되어 있다.[115]

[113] 제38조(정보보호시스템에 관한 기준 고시 등) ① 미래창조과학부장관은 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다. <개정 2013.3.23.>
② 미래창조과학부장관은 유통 중인 정보보호시스템이 제1항에 따른 기준에 미치지 못할 경우에 정보보호시스템의 보완 및 그 밖에 필요한 사항을 권고할 수 있다. <개정 2013.3.23.>
③ 제1항에 따른 기준을 정하기 위한 절차와 제2항에 따른 권고에 관한 사항 및 그 밖에 필요한 사항은 대통령령으로 정한다.

[114] 제35조(정보보호시스템의 보완 등) ① 미래창조과학부장관은 법 제38조제1항에 따라 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하거나, 그 기준에 맞는지의 여부를 평가 또는 인증하는 업무에 관한 세부 사항을 정할 때에는 관계기관의 장과 미리 협의하여야 한다. <개정 2013.3.23., 2015.12.22.>
② 미래창조과학부장관은 정보보호시스템을 제조하거나 수입하는 자가 그 시스템이 법 제38조제1항에 따른 기준에 합치되는지의 확인을 요청한 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원의 장 또는 관계 국제협약에서 정한 기준에 맞는 기관의 장에게 그 시스템을 조사 또는 시험·평가하게 할 수 있다. <개정 2013.3.23.>
③ 제2항에 따른 조사 또는 시험·평가를 요청하는 자는 미래창조과학부장관이 정하여 고시하는 기준에 따라 한국인터넷진흥원의 장 또는 관계 국제협약에서 정한 기준에 맞는 기관의 장이 정한 수수료를 내야 한다.

[115] 국가정보화기본법은 애초에 행정안전부가 관장하였으나 2013년 정부조직법 개정으로 미래창조과학부로 변경되었다.

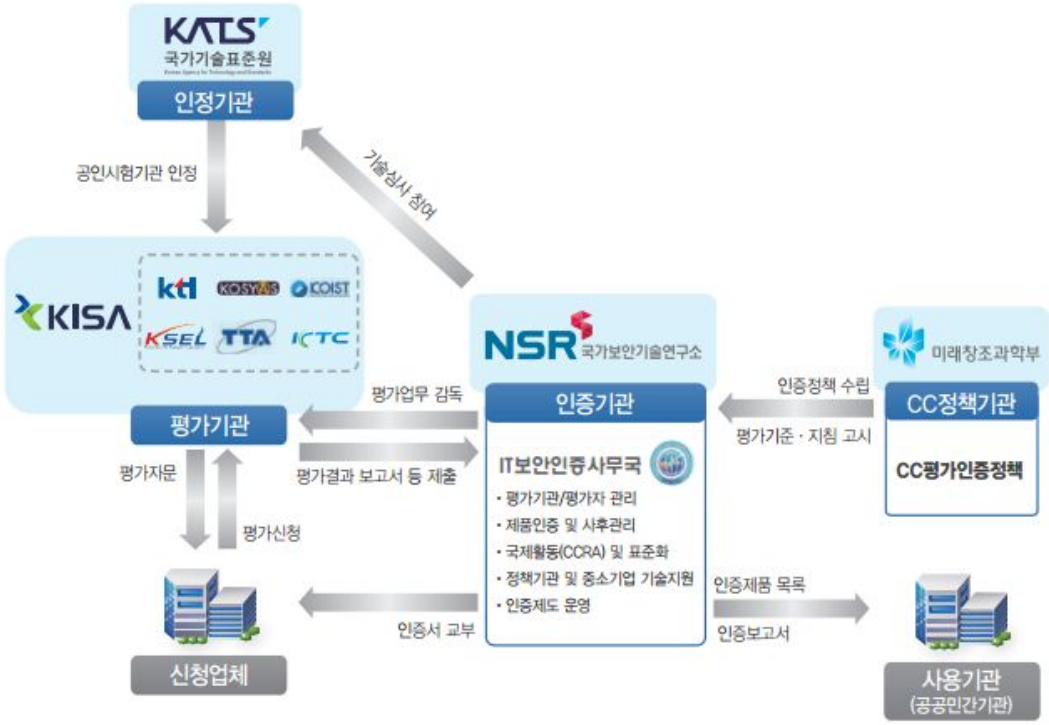



그림 : 정보보호제품 평가·인증체계 (출처 : 2016 국가정보보호백서)

그러나 이 제도 역시 국가정보원이 일정하게 관여해 온 것으로 보인다. 정보보호시스템 평가·인증지침 2.2.1에서 인증기관을 한국전자통신연구원 부설 국가보안기술연구소로 지정하고 있다. 이는 2016년 6월 27일 개정된 고시에 따라, 국가정보원에서 국가보안기술연구소로 개정된 것이다. 개정이유를 보면, CC인증 업무가 2014년 10월 국정원에서 미래부로 이관되었고, 2012년 11월에 인증기관 또한 변경이 되었는데, 이러한 사항이 고시에 반영되지 않아 뒤늦게 변경을 한 것이다. 2016 국가정보보호백서에 따르면, 2012년 11월에 IT보안인증사무국이 국가사이버안전센터 산하 기관에서 국가보안기술연구소로 이관된 바 있다.

국가보안기술연구소(NSR, National Security Research Institute)는 「과학기술 분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조 제1항의 규정에 의해 2000년에 설립된 정보보호 전문연구기관으로, 산하에 보안관제기술지원센터, 사이버안전훈련센터, IT보안인증사무국 등을 운영하고 있다. (2016 국가정보보호백서) 그런데, 국가보안기술연구소는 '국가정보보안에 관련된 임무를 수행하는 연구기관'으로 조직이나 운영과 관련한 자세한 사항이 공개되어 있지 않고[116], 국정원 출신이 연구소장 및 연구원으로 재취업하는 등, 공식적으로는 한국전자통신연구원 부설 기관으로 되어 있지만, 사실상 국가정보원 산하 연구소로 역할하고 있는 것으로 보인다.[117]

[116] 국가보안기술연구소 소개 홈페이지 http://www.nst.re.kr/nst/about/03_12.jsp
[117] 뉴시스, "과학기술 정부출연硏도 관피아…5년간 24명 재취업", 2014.10.11, http://www.newsis.com/ar_detail/view.html?ar_id=NISX20141011_0013224190&cID=10301&pID=10300
전자신문, [시큐리티톱뷰]<73>김광호 국가보안기술연구소 소장, 2014.4.13, http://www.etnews.com/20140411000102

한편, 2014년 7월 국제상호인정협정(CCRA)는 CC인증 결과를 상호인정하는 협정서를 공동보호프로파일(cPP, collaborative Protection Profile) 기반으로 개정하고, 9월에 26개 전체 회원국이 재서명하였는데, 한국은 국정원과 국가보안기술연구소가 서명기관으로 공동 서명하였다고 한다. 또한, 2015년에 국정원, 미래창조과학부, 국가보안기술연구소 IT 보안인증사무국은 국내·외 정보보호제품 기술 동향을 반영하여 국가·공공기관용 평가·인증대상을 정비하였으며, 2016년 1월 1일부로 일부 대상을 통폐합하여 24종으로 개편하였다고 한다.(2016 국가정보보호백서) 이를 보아도 정보보호제품 평가·인증에 국가정보원이 깊게 관여하고 있는 것으로 보인다.

## 8) 사이버보안 관련 국정원의 역할에 대한 검토

2016 국가정보보호백서는 "국가정보원은 「국가정보원법」, 「정보통신기반보호법」, 「전자정부법」, 「국가정보화기본법」 등 관계법령에 근거하여 국가 정보보안 업무의 기획·조정 및 보안정책 수립·시행 등 국가·공공기관에 대한 정보보안 업무를 총괄하고 있다. 특히 2005년 1월에 제정한 「국가사이버안전관리규정」(대통령훈령 316호, 2013.9.2 개정)에서 국가의 사이버안전과 관련된 정책 및 관리에 대해 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정하도록 규정하였다."고 설명하고 있다. 국정원법은 제3조에서 국정원의 직무를 다음과 같이 규정하고 있다.

> 제3조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.
> 1. 국외 정보 및 국내 보안정보[대공(對共), 대정부전복(對政府顚覆), 방첩(防諜), 대테러 및 국제범죄조직]의 수집·작성 및 배포
> 2. 국가 기밀에 속하는 문서·자재·시설 및 지역에 대한 보안 업무. 다만, 각급 기관에 대한 보안감사는 제외한다.
> 3. 「형법」 중 내란(內亂)의 죄, 외환(外患)의 죄, 「군형법」 중 반란의 죄, 암호 부정사용의 죄, 「군사기밀 보호법」에 규정된 죄, 「국가보안법」에 규정된 죄에 대한 수사
> 4. 국정원 직원의 직무와 관련된 범죄에 대한 수사
> 5. 정보 및 보안 업무의 기획·조정

이 중 사이버 보안과 관련된 직무는 1항 2호의 보안 업무와 5호 정보 및 보안 업무의 기획·조정 업무일 것이다. 그러나 사이버 보안 정책의 총괄·조정의 역할은 이를 지나치게 확대한 것이라는 비판이 제기될 수 있다. 국정원법 1조 목적에서 규정하고 있듯이 국정원의 핵심역할은 '국가안전보장'에 관련된 것이다. 비록 특정한 사이버 공격이 국가안보에 큰 영향을 미칠 수 있으나, 사이버 보안 정책 전반을 국가안보적 시각에서 바라보는 것은 협소할 뿐만 아니라, 사이버 보안 정책에 부정적인 영향을 미칠 수 있다. '국가안보'의 특성상 사이버 보안 정책이 통제위주로 추진될 수 있으며 기본권과 자율성을 제약할 가능성이 크기 때문이다.

1항 2호의 업무의 경우 구체적으로는 '보안업무규정'에 따라 이루어지고 있는데, 앞서 '암호모듈 검증' 업무와 관련해서 지적하였듯이, 인터넷이 보편화되어 일반 개인 이용자의 통신 보안을 위해 암호 사용이 일반화된 상황에서 여전히 국정원이 과거의 관행대로 '암호자재'의 관리 업무를 담당하는 것은 적절하지 않다. 기술환경의 변화에 따라 동일한 행위라도 맥락이 달라지게 되는데, 국정원이 암호 업무를 담당하는 것은 국가안보를 넘어 민간의 통신 보안에 관여하게 되는 것이기 때문이다.

1항 5호에서 규정한 기획·조정의 업무는 사이버 보안 이슈와 무관하게 국정원의 권한에서 배제되어야 한다는 비판을 받아왔다. 국정원이 각 행정부처,기타 정보 및 보안업무 관련기관의 업무에 대하여 기획 및 조정권한을 가짐으로써 정보기관이 다른 행정부처의 상급 감독기관처럼 군림해 왔기 때문이다.[118]

김도승(2016)은 "(국정원이) 사이버안보와 관련된 업무를 사실상 총괄하여 집행하는 모습을 보이는데, 이러한 총괄기능이 과연 현재 국가정보원법상의 국가정보원의 직무권한에 비추어 볼 때 과도한 직무와 권한의 창설은 아닌지에 대한 문제"를 지적하고 있는데, 이는 국가사이버안보기본법 제정안에 대한 비판적 맥락에서 지적한 것이기는 하지만, 제정안에 준하는 수준의 권한을 국가사이버안전관리규정에 의해 이미 국정원이 수행하고 있다는 점에서 동일한 비판이 가능할 것이다.

박영철 등(2015) 역시 "국가정보원장에게 사이버보안을 위한 광범한 권한을 부여하는 것은 국가정보원의 직무의 범위를 벗어난 것"이라며, "현실적으로 정보기관에 대한 입법·사법·행정 및 제4부로서의 언론에 의한 감시 및 통제가 매우 어렵다는 점에서 이를 받아들이기는 매우 어렵다"고 지적하고 있다.[119] 또한, 국민의 기본권은 법률에 명확한 근거가 있고 필요한 경우에 한하여 제한되어야 함(헌법 제37조제2항)에도 불구하고, 국정원의 사이버 보안에 관한 권한이 대통령 훈령인 국가사이버안전관리규정에 근거하고 있는 것은 헌법상 법치주의의 원칙을 위반하고 있음에 틀림없다고 비판한다.

국정원이 사이버 보안 정책의 총괄·조정 역할을 맡음으로써 사이버 보안 정책의 투명성과 사회적 감독 기능이 약화되는 것에 대한 우려도 제기된다. 비밀정보기관으로서 국정원은 여타 정부부처에 비해 언론이나 국회에 의한 감독과 견제 기능이 약할 수밖에 없다. 조직, 인력, 예산, 사업 등 모든 측면에서 투명하게 공개되지 않기 때문이다. 앞서 지적했듯이, 국내 사이버 보안 종합대책과 관련해서도 보도자료로만 알려질 뿐, 원 자료가 투명하게 공개되어 있지 않다. 심지어 한국전자통신연구원 부설로 되어 있는 국가보안기술연구소조차 조직이나 운영과 관련한 자세한 사항이 공개되어 있지 않다. 이러한 불투명성은 사이버 보안과 관련해서도 국정원의 권한 남용에 대한 우려를 불러일으킬 수밖에 없다. 한 국가의 사이버 보안 정책이 민간 기업이나 국민들의 신뢰와 협력 속에서 가능하다고 할 때, 그리고 비판과 토론을 통해 합리적인 정책 수립이 가능하다고 할 때, 이러한 불투명성은 국가적 사이버 보안에 해로울 수밖에 없다.

앞서 사이버 보안 관련 국제동향과 다른 나라의 사례에서 보았듯이, 사이버 보안 정책의 수립과 집행 과정에서 다양한 이해관계자의 참여와 민간의 자율성이 강조되고 있다. 그러나 비밀정보기관인 국정원이 컨트롤타워를 맡고 있는 상황에서 이해관계자와의 협력이나 민간의 자율성을 기대할 수 있을지 의문이다. 2014년 국정감사에서 김재경 의원은 '국가 사이버안보 전담기구' 사이버보안청 설립의 필요성을 제기하면서, "우리나라 국가 사이버 안보의 총괄 책임은 국가정보원에 있음. 그러나 국가 최고 정보기관으로서 업무 특성상 폐쇄성, 기밀성, 비공개성 원칙에 따라 움직이기에 국제적 대응과 국내 민·관·학·연·산 등의 사이버보안 (외교, 기술, 정책, 서비스, 교육 등) 관련 기관들에 대한 통합적 리더쉽은 매우 제한적일 수 밖에 없음"이라고 지적하고 있다.[120]

---

[118] 국회의원 진성준 등, 정책자료집 <국가정보원 개혁을 위한 제안서>, 2013.2

[119] 이 역시 사이버테러방지 관련 법안에 대한 지적이지만, 현재 국가사이버안전관리규정에 의한 국정원의 권한에 대한 지적으로 받아들여도 무방하다고 본다.

[120] 국회의원 김재경, '국가 사이버안보 전담기구' 『사이버보안청』 설립 필요, 2014년도 국정감사

마지막으로 국정원에 의한 감시와 사찰, 인권 침해의 우려가 제기된다. 사이버테러방지법안이 수차례 국회 통과에 실패한 이유도 이 때문이다. 보안관제나 침해사고 분석 등의 과정에서 기업비밀이나 이용자 개인정보 등이 유출되거나 악용될 위험성이 크다.(이은우, 2016) 국제전기통신연합(ITU) 역시 2011년에 발간한 <ITU 국가 사이버보안 전략 가이드>에서 “정보기관의 참여는 종종 논란이 있을 수 있다. 사이버 보안 계획에 정보기관을 참여시키는 것은 민/군의 구분을 흐릿하게 하고 시민 자유 문제를 야기할 수 있다”고 지적한 바 있다.(ITU, 2011)

보안관제는 이용자가 발생시키는 모든 데이터의 수집이 가능하고 수집한 정보를 실시간으로 분석할 수 있어 프라이버시 침해 위협이 크다. 기술적으로는 특정인에 대한 추적·감시나 온라인 활동에 대한 실시간 도청(서비스 접속, 일체의 활동, 이메일, 메신저, 통화 내역, 화상전화 도청 등)이 가능하다. 따라서 보안관제  정책의 설정, 수집된 데이터의 분석·관리 과정에서 개인정보 보호원칙이 지켜질 필요가 있으며, 보안관제 수행기관에 대한 엄격한 감독이 필요하다. 침해사고의 원인을 분석하는 과정에서 기관이나 업체의 민감한 정보가 드러날 수도 있다. 일종의 수사 과정으로서 영장주의의 잠탈 위험성이 있다.(이은우, 2016)

정보통신망법에서 침해사고의 대응이나 원인 분석 과정에서 ‘제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용’하도록 하고(제48조의2 5항), ‘제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기’하도록(제48조의4 5항) 하고 있는 것도 이 때문이다. 또한, 정보통신기반보호법에서도 국정원이 ‘금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니’하도록 규정(제7조 3항)하고 있으며, 제27조에서 비밀유지의무를 두고 있는 것 역시 이러한 이유이다.

이 때문에 국정원이 사이버 보안 정책 수립에서부터 사이버위협 정보의 수집, 침해사고에 대한 조사에 이르기까지 총괄·조정의 역할을 하고 있는 것에 대해 우려가 높아질 수밖에 없다. 국정원은 광범한 정보수집 권한과 수사권을 매개로 국내 정치에 개입하고 민간인을 사찰해 온 역사가 있기 때문이다. 2015년에는 국정원이 RCS라는 해킹 프로그램을 사용해왔다는 사실이 드러나기도 했다. 국정원은 민간인 사찰이 없었다고 주장하지만, 문제는 해킹팀의 서버가 해킹되어 정보가 공개되기 전까지 이러한 사실이 알려지지 않았고, 그 후에도 국회에 의한 사후검증마저 실패했다는 점이다. 즉, 민간인 사찰이 없었거나 앞으로도 없을 것이라는 것을 보증할 수 있는 감독체계가 부재하다는 것이다. 국정원의 막강한 권한에 비해 이를 감독할 수 있는 사법적, 입법적, 혹은 사회적 감독 체계가 부실한 상황에서 국정원에 대한 신뢰가 형성되기는 힘들다.

## 다. 사이버테러방지법안 등 사이버안보 법제 검토

앞서 보았듯이, 국내에서 국가 사이버 보안에 대한 기본법은 존재하지 않으며, 국가정보통신망의 사이버 보안을 규율하는 것은 대통령 훈령에 불과한 국가사이버안전관리법안이 있을 뿐이다. 그래서 이를 법제화하고자 하는 시도가 이미 18대 국회에서부터 계속되어 왔다.

18대 국회에서는 2008년 10월 28일, 공성진 의원이 '국가 사이버위기 관리법안'을 대표발의한 바 있으며, 19대 국회에서는 2013년 3월 26일 하태경 의원이 대표발의한 '국가 사이버안전 관리에 관한 법률안', 2013년 4월 9일 서상기 의원이 대표발의한 '국가 사이버테러 방지에 관한 법률안', 2015년 6월 24일 이노근 의원이 대표발의한 '사이버테러 방지 및 대응에 관한 법률안' 등이 있다. 한편, 사이버위협 정보의 공유에 초점을 맞춘 '사이버위협정보 공유에 관한 법률안'을 이철우 의원이 대표발의하기도 했다. 또한, 19대 국회 말미인 2016년 초, 테러방지법(국민보호와 공공안전을 위한 테러방지법안)이 국회에 직권상정되어 논란이 되었을 때, 서상기 의원이 대표발의한 '국가 사이버테러 방지 등에 관한 법률안'도 다시 발의가 되었다. 그러나 지금까지 발의된 사이버테러방지법안들은 민간 정보통신망에 대한 국정원의 권한 확대를 둘러싼 사회적인 논란을 불러일으켰으며, 결국 모두 임기만료로 폐기되었다.

20대 국회 들어와서, 이철우 의원이 다시 '국가 사이버안보에 관한 법률안'을 발의하여 2016년 12월 현재 국회에 계류 중이며, 2016년 9월 1일에는 국정원에서 '국가 사이버안보 기본법 제정(안)'을 입법예고하였다.

- 2008.10.28 국가 사이버위기 관리법안 (공성진 의원 대표발의), 18대, 임기만료 폐기[121]
- 2013.3.26 국가 사이버안전 관리에 관한 법률안 (하태경 의원 대표발의), 19대, 임기만료 폐기[122]
- 2013.4.9 국가 사이버테러 방지에 관한 법률안 (서상기 의원 대표발의), 19대, 임기만료 폐기[123]
- 2015.5.19 사이버위협정보 공유에 관한 법률안 (이철우 의원 대표발의), 19대, 임기만료 폐기[124]
- 2015.6.24 사이버테러방지 및 대응에 관한 법률안 (이노근 의원 대표발의), 19대, 임기만료 폐기[125]
- 2016.2.22 국가 사이버테러 방지 등에 관한 법률안 (서상기 의원 대표발의), 19대, 임기만료 폐기[126]
- 2016.5.30 국가 사이버안보에 관한 법률안 (이철우 의원 대표발의), 20대, 계류 중[127]
- 2016.9.1 국가 사이버안보 기본법 제정(안) (국가정보원 입법예고)[128]

[121] 의안번호 1801619
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_I0S8T1G0H2K8E1L7D5H8O4U9D4W8S5
[122] 의안번호 1904286
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_P1D3O0N3T2Y6A1K7D5A5E5J8Q2M5Q3
[123] 의안번호 1904459
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_N1Q3G0N4A0A9R1X7S3M6L0L6N4M0U2
[124] 의안번호 191518
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_V1F5Z0J5U1L9T1X3E4S1B4T2L1F7W7
[125] 의안번호 1915777
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_C1Z5Z0N6B2A4T1L6C5S3G1N7X4S8U6
[126] 의안번호 1918583
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_W1J6T0P2L2F2G2Y2E5Y0K5P4U9O3C8
[127] 의안번호 2000032
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_L1Z6M0L5M3W0U1W4T2M8K4L3S5I0Y2
[128] 법제처 홈페이지 입법예고 게시판,
http://www.moleg.go.kr/lawinfo/lawNotice;jsessionid=dz9nl4XrzWPks7Egk5tzVppzSw6xmoFU3ncApBTAawca62NZQVnSrgQ2ZmB9YTA7.moleg_a1_servlet_engine2?ogLmPpSeq=34625&mappingLbicId=0&announceType=TYPE5&pageIndex=&rowIdx=7

지금까지 발의된 법안들은 현재 대통령 훈령인 국가사이버안전관리규정을 기본 틀로해서 그 적용범위를 정보통신기반시설과 주요 민간 사업자의 정보통신망으로 확대하고, 사이버보안 수행체계 등 일부 조항을 수정한 것이다.

국가사이버안전관리규정과 2016년 서상기 의원이 대표발의한 국가 사이버테러 방지 등에 관한 법률안(이하 사이버테러방지법안), 그리고 국가정보원이 입법예고한 국가 사이버안보 기본법 제정(안)의 조항들을 비교해보면 아래 표와 같다.

표 : 국가사이버안전관리규정, 서상기의원안, 국가사이버안보기본법(안) 비교

| 국가사이버안전관리규정 | 국가 사이버테러 방지 등에 관한 법률안 (서상기 의원 대표발의) | 국가사이버안보기본법 제정(안) |
|---|---|---|
| 제1조(목적) 이 훈령은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다. | 제1조(목적) 이 법은 국가 사이버테러 방지에 관한 기본적인 사항을 규정하여 국가안보를 위협하는 사이버테러를 예방하고 사이버위기 발생 시 국가 역량을 결집하여 신속하게 대처함으로써 국가의 안전 보장과 이익보호에 이바지함을 목적으로 한다. | 제1조(목적) 이 법은 사이버안보에 관한 기본적인 사항을 규정하여 국가의 사이버공간에 대한 사이버공격을 예방하고 사이버위기 발생시 역량을 결집하여 신속하게 대처함으로써 국가의 안전보장과 이익보호에 이바지함을 목적으로 한다. |
| 제2조(정의) 이 훈령에서 사용하는 용어의 정의는 다음과 같다.<br>1. "정보통신망"이라 함은 「전기통신기본법」 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.<br>2. "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.<br>3. "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.<br>4. "사이버위기"란 사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 말한다.<br>5. "공공기관"이라 함은 다음 각목의 기관을 말한다.<br>가. 「공공기관의 운영에 관한 법률」 제5조에 따라 지정된 공기업 또는 준정부기관인 공공기관<br>나. 「공공기관의 운영에 관한 법률」 제5조에 따라 지정된 기타공공기관 중 「정부출연연구기 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따른 연구기관 | 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.<br>1. “사이버테러”란 외국이나 대한민국의 통치권이 사실상 미치지 아 니하는 한반도내의 집단, 해킹·범죄조직 및 이들과 연계되거나 후원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단 에 의하여 정보통신망을 공격하는 행위를 말한다.<br>2. “사이버안전”이란 사이버테러로부터 정보통신시설과 정보를 보호 하기 위하여 수행하는 관리적. 물리적. 기술적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함한다.<br>3. “사이버위기”란 사이버테러로 인하여 국가 기반시설의 핵심기능 이 훼손·정지·무력화 또는 국가기밀과 중요정보가 대량 유출되어 국가안보에 영향을 미치거나 사회·경제적 혼란을 유발하는 상황을 말한다.<br>4. “사이버테러정보”란 정보시스템 및 정보보호시스템(소프트웨어를 포함한다) 등에 의해 사이버테러 행위로 판단되는 정보로서 사이 버테러 근원지를 파악하기 위한 인터넷프로토콜주소(IP)와 네트워크카드주소(MAC)를 포함한다.<br>5. “사이버테러 방지 및 위기관리 책임기관(이하 “책임기관”이라 한다)”이란 사이버테러 방지 및 위기관리에 관한 업무를 수행하고 있는 다음 각 목의 기관을 말한다.<br>가. 「대한민국헌법」, 「정부조직법」, 그 밖의 법령에 따라 설치 된 국가기관(그 소속·산하기관을 포함한다)과 지방자치단체(그 소속·산하기관을 포함한다) 및 「국가정보화 기본법」 제3조제 10호에 따른 공공기관 | 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.<br>1. “사이버공간”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1호의 규정에 따른 정보통신망과 정보의 수집·가공·저장·검색·송신 또는 수신에 활용되는 기기(이하 "정보통신기기"라 한다)가 상호 연결되어 정보를 생성·전송·수신·저장·처리하는 영역을 말한다.<br>2. “사이버공격”이란 해킹 · 컴퓨터바이러스 · 서비스방해 등의 전자적 수단에 의하여 사이버공간을 불법침입 · 교란 · 마비 · 파괴하거나 정보를 절취 · 훼손하는 등의 공격행위를 말한다.<br>3.“국가안보를 위협하는 사이버공격”이란 다음 각 목에 해당하는 행위를 말한다.<br>가. 대한민국의 통치권이 사실상 미치지 아니하는 한반도 내의 집단이 자행하는 사이버공격<br>나. 전자정부와 국가기반시설 등 국가적으로 중요한 사이버공간을 교란 · 마비 · 파괴하는 사이버공격<br>다. 국가 기밀이나 핵심 산업기술 등 국가적으로 중요한 정보를 절취 · 훼손하는 사이버공격<br>4. “사이버위기”란 사이버공격으로 인하여 다수의 국가기반시설의 핵심기능이 훼손 · 정지 · 무력화되거나 국가기밀 등 중요정보가 대량으로 유출되어 국가의 안전과 이익에 위해로운 결과를 초래하는 상황을 말한다.<br>5. “사이버안보”란 사이버공격과 사이버공격으로 인한 사이버위기로부터 사이버공간을 보호함으로써 국가의 안전과 이익을 수호하는 활동을 말한다. |

| | | |
|---|---|---|
| 다. 「초·중등교육법」 및 「고등교육법」에 따른 국·공립학교<br>라. 그 밖에 다른 법령의 규정에 의하여 설립된 공공기관 중 제6조의 규정에 의한 국가사이버안전전략회의에서 정보통신망의 안전성 확보가 필요하다고 지정한 기관 | 나. 「정보통신기반 보호법」 제5조제1항에 따른 주요정보통신기반시설을 관리하는 기관<br>다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조 제1항에 따른 집적정보통신시설사업자 및 같은 법 제47조의4제 2항에 따른 주요정보통신서비스 제공자<br>라. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관<br>마. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 법 제 3조제10호에 따른 전문연구기관<br>6. “사이버테러 방지 및 위기관리 지원기관(이하 “지원기관”이라 한다)”이란 사이버테러에 대한 신속한 탐지·대응 및 사고조사·복구 등을 지원하는 다음 각 목의 기관 또는 업체를 말한다.<br>가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원<br>나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조 에 따른 한국인터넷진흥원<br>다. 「소프트웨어산업 진흥법」 제24조에 따라 소프트웨어사업자로 신고한 자 중 컴퓨터바이러스 백신소프트웨어를 제작 또는 판 매하는 자<br>라. 「국가정보화 기본법」 제3조제6호의 정보보호시스템을 제작하거나 수입하는 자<br>마. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업 바. 관계 행정기관의 장이 지정한 보안관제전문업체 | 6. “책임기관”이란 사이버안보에 관한 업무를 수행하는 다음 각 목의 기관을 말한다.<br>가. 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다) 및 그 소속 기관, 특별시, 광역시, 특별자치시, 도, 특별자치도(이하 “시·도”라 한다)와 시·군·구 및 그 소속 기관, 시·도 교육청과 교육지원청 및 그 소속기관(다만, 국·공립학교는 제외한다)<br>나. 「국군조직법」에 따른 합동참모본부, 각 군 및 국방부 직할 부대·기관<br>다. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관과 「지방공기업법」 제49조에 따른 지방공사 및 같은 법 제76조에 따른 지방공단<br>라. 「정보통신기반 보호법」 제5조에 따른 주요정보통신기반시설을 관리하는 기관<br>마. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관<br>바. 「방위사업법」 제3조에 따른 방위산업체 및 전문연구기관<br>사. 「방위산업기술 보호법」 제7조에 따른 방위산업기술 보유기관<br>아. 기타 제5조의 국가사이버안보위원회의 의결을 거쳐 “책임기관”으로 지정한 기관<br>7. “지원기관”이란 책임기관 등의 사이버공간 보호 업무를 지원하는 다음 각 목의 기관 또는 업체를 말한다.<br>가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소(이하 “국가보안기술연구소”라 한다)<br>나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원<br>다. 「전자정부법」 제72조에 따른 한국지역정보개발원<br>라. 「한국교육학술정보원법」에 따른 한국교육학술정보원<br>마. 「한국재정정보원법」에 따른 한국재정정보원<br>바. 「전자금융거래법」 제21조의6 제1항 제4호에 따라 금융위원회가 지정한 기관<br>사. 「산업기술의 유출 방지 및 보호에 관한 법률」 제16조에 따른 산업기술보호협회<br>아. 제16조에 따라 지정한 사이버안보 전문업체<br>자. 기타 제5조의 국가사이버안보위원회의 의결을 거쳐 “지원기관”으로 지정한 기관 |
| 제3조(적용범위) 이 훈령은 중앙행정기관(대통령 소속 기관, 국무총리 소속 기관 및 | | 제3조(사이버안보의 기본이념) ① 정부는 사이버공간의 보호와 함께 사이버공간에서 정보의 자유로운 |

| | | |
|---|---|---|
| 국가인권위원회를 포함한다. 이하 같다), 지방자치단체 및 공공기관의 정보통신망에 적용한다. 다만, 「정보통신기반보호법」에 따른 주요정보통신기반시설에 대해서는 「정보통신기반보호법」을 우선 적용한다. | | 소통과 표현의 자유 등 국민의 기본권을 보장하는 정책을 균형 있게 시행한다.<br>② 정부와 기업은 사이버안보를 국가안보의 중요한 요소로 인식하고 상호간의 긴밀한 협력을 통해 국가의 사이버공간을 보호한다.<br>③ 정부는 국제기구 · 단체 및 외국과의 적극적인 협력관계를 구축하여 국제 사이버공간의 안전성과 신뢰성 확보를 위해 노력한다.<br><br>제4조(다른 법률과의 관계) ① 사이버안보에 관하여 다른 법률을 제정하거나 개정할 때에는 이 법의 목적과 기본이념에 맞도록 하여야 한다.<br>② 사이버안보에 관하여 다른 법률의 규정에도 불구하고 제10조에서 제17조까지는 이 법을 우선 적용한다. 다만, 전시 및 계엄 시에는 계엄법의 규정에 따른다. |
| 제4조(사이버안전 확보의 책무) ① 중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임이 있으며 이를 위하여 사이버안전업무를 전담하는 전문인력을 확보하는 등 필요한 조치를 강구하여야 한다.<br>②관계 중앙행정기관의 장은 소관 공공기관 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 전문인력의 확보 등 필요한 조치를 강구하도록 하여야 한다. | 제3조(사이버안전관리의 책임) ① 책임기관의 장 및 이를 지휘·감독할 의무가 있는 기관의 장은 사이버안전관리에 대한 책임을 진다.<br>② 책임기관의 장은 소관 정보통신망에 대한 보안대책을 마련하는 등 사이버안전관리를 위해 자율보안관리 체계를 구축·운영하여야 한다. | 제9조(책임기관의 책무) ①책임기관의 장은 사이버공격으로부터 소관 사이버공간을 안전하게 보호하는 책임을 진다.<br>② 상급 책임기관의 장은 사이버공격으로부터 소관 영역의 사이버공간을 보호하기 위한 전담 조직을 설치하고 관련 예산을 확보하는 등 자체적인 사이버안보 역량을 확보한다.<br>③ 정부는 책임기관의 장이 이 법에 따른 사이버안보 업무를 수행하는데 필요한 행정적 · 재정적 · 기술적 지원을 할 수 있다.<br>④ 제3항에 따른 지원 대상의 선정과 관리 및 지원 요건 등에 관하여 필요한 사항은 대통령령으로 정한다. |
| 제5조(국가사이버안전정책 및 관리) ① 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다.<br>② 국가정보원장은 제1항에 따른 총괄·조정 업무를 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관의 장과 협의하여 국가사이버안전기본계획을 수립·시행한다.<br>③ 국가정보원장은 제2항에 따른 국가사이버안전기본계획을 원활하게 추진하기 위하여 관계 기관에 예산 반영 등에 관한 협조를 요청할 수 있다. | 제4조(국가사이버테러 방지 및 위기관리 기본계획 수립 등) ① 정부는 사이버테러 방지 및 위기관리 대책의 효율적이고 체계적인 추진을위하여 국가사이버테러 방지 및 위기관리 기본계획(이하 “기본계획” 이라한다)을 수립. 시행하여야 한다.<br>② 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장(국회사무총장, 법원행정처장, 헌법재판소 사무처장, 중앙선거관리위원회 사무총장 을 말한다. 이하 같다) 및 중앙행정기관의 장은 제1항의 기본계획에 따라 소관 책임기관의 장이 활용할 수 있도록 국가사이버테러 방지 및 위기관리 시행계획(이하 “시행계획”이라고 한다)을 작성하여 소 관 책임기관의 장에게 배포하여야 한다.<br><br>제5조(시행계획의 이행여부 확인) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 소관 책임기관에 대하 여 매년 시행계획의 이행여부를 확인하여야 한다.<br>② 정부는 제1항의 확인결과를 종합하여 국가사이버테러 방지 및 위기관리 실태를 점검. 평가하여야 | 제7조(사이버안보 기본계획 수립 등) ① 국가정보원장은 사이버안보 업무를 효율적이고 체계적으로 추진하기 위하여 매 3년마다 위원회의 심의를 거쳐 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립 · 시행하여야 한다.<br>② 중앙행정기관의 장, 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 시. 도 및 시. 도교육청(이하 “상급 책임기관”이라 한다)의 장은 제1항의 기본계획에 따라 사이버안보 시행계획(이하 “시행계획”이라 한다)을 작성하여 소관 업무범위 내의 책임기관의 장에게 배포하여야 한다.<br>③ 기본계획 및 시행계획의 작성 방법 · 절차 및 내용 등에 관하여 필요한 사항은 대통령령으로 정한다.<br><br>제8조(사이버안보 실태의 평가) ① 국가정보원장은 제2조제6호 가목 내지 다목의 책임기관 중에서 대통령령으로 정하는 책임기관을 대상으로 사이버안보 업무수행체계의 구축과 사이버안보 활동 및 사이버안보 기반 조성 등에 관한 실태를 평가(이하 “실태평가”라 한다)할 수 있다. |

| | | |
|---|---|---|
| | 한다. 다만, 국회, 법원, 헌법재 판소, 중앙선거관리위원회에 대한 점검. 평가는 해당기관의 장이 요 청한 경우에 한정한다.<br>③ 제1항 및 제2항의 절차와 방법 등에 관하여 필요한 사항은 대통 령령으로 정한다. | ② 국가정보원장은 제1항에 따른 실태평가의 표율적 수행과 실태평가에 관한 전문적·기술적인 연구 또는 자문을 위하여 사이버안보실태합동평가단(이하 “합동평가단”이라 한다)을 구성·운영할 수 있다.<br>③ 실태평가의 방법과 절차, 결과의 처리 및 합동평가단의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다. |
| 제6조(국가사이버안전전략회의) ① 국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의(이하 "전략회의"라 한다)를 둔다.<br>②전략회의의 의장은 국가정보원장이 된다.<br>③ 전략회의의 위원은 다음 각 호의 사람과 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원이 된다. 이 경우 차관 또는 차관급 공무원이 2명 이상인 기관은 사이버 안전 업무를 담당하는 차관 또는 차관급 공무원이 위원이 된다.<br>1. 기획재정부차관<br>2. 미래창조과학부차관<br>3. 교육부차관<br>4. 외교부차관<br>5. 통일부차관<br>6. 법무부차관<br>7. 국방부차관<br>8. 안전행정부차관<br>9. 산업통상자원부차관<br>10. 보건복지부차관<br>11. 국토교통부차관<br>12. 금융위원회 부위원장<br>13. 대통령비서실 사이버안전 담당 수석비서관<br>14. 국가안보실 사이버안전 담당 비서관<br>15. 국무조정실 국무차장<br>④전략회의는 다음 각호의 사항을 심의한다.<br>1. 국가사이버안전체계의 수립 및 개선에 관한 사항<br>2. 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항<br>3. 국가사이버안전 관련 대통령 지시사항에 대한 조치방안<br>4. 그 밖에 전략회의 의장이 부의하는 사항<br>⑤ 제4항에 따라 전략회의의 심의를 거친 사항 중 중요 사항은 대통령 및 국무총리에게 보고한다.<br>⑥전략회의의 구성·운영 등에 관하여 필요한 사항은 전략회의의 의장이 따로 정한다. | | 제5조(국가사이버안보위원회) ① 사이버안보에 관한 중요 사항을 심의하기 위하여 대통령 소속하에 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다.<br>② 위원회의 위원장은 국가안보실장이 되고 위원은 국회 · 법원 · 헌법재판소 · 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다.<br>③ 위원회의 효율적 운영과 지원을 위하여 위원회에 국가안보실장과 국가정보원장이 공동으로 운영하는 국가사이버안보실무위원회(이하 “실무위원회”라 한다)를 둔다.<br>④ 위원회 및 실무위원회의 구성 · 운영 등에 관하여 필요한 구체적인 사항은 대통령령으로 정한다.<br><br>제6조(위원회의 기능) ① 위원회는 다음 각 호의 사항을 심의 · 의결한다.<br>1. 사이버안보에 관한 전략 · 정책 및 법령에 관한 사항<br>2. 사이버안보 기본계획 및 시행계획에 관한 사항<br>3. 사이버안보 실태평가에 관한 사항<br>4. 사이버위협정보 공유에 관한 사항<br>5. 책임기관과 지원기관의 지정 및 지원에 관한 사항<br>6. 그 밖에 위원회의 위원장이 부의하거나 위원이 제출한 사항<br>② 위원회의 위원장은 제1항 각 호의 사항을 심의 · 의결하기 위하여 필요한 경우 책임기관의 장 및 지원기관의 장에게 필요한 자료의 제출을 요청할 수 있다. 이 경우 요청을 받은 기관은 그에 성실히 응하여야 한다. |
| 제7조(국가사이버안전대책회의) ① 전략회의의 효율적인 운영을 위하여 전략회의에 국가사이버안전대책회의(이하 "대책회의"라 한다)를 둔다.<br>②대책회의의 의장은 국가정보원의 사이버안전업무를 담당하는 차장이 되며, 위원은 전략회의의 위원이 | | |

| | | |
|---|---|---|
| 속하는 기관의 실·국장급 공무원으로 한다.<br>③대책회의는 다음 각호의 사항을 심의한다.<br>1. 국가사이버안전 관리 및 대책방안<br>2. 전략회의의 결정사항에 대한 시행방안<br>3. 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항<br>4. 그 밖에 대책회의의 의장이 부의하는 사항<br>④대책회의의 구성·운영 등에 관하여 필요한 사항은 대책회의의 의장이 따로 정한다. | | |
| 제8조(국가사이버안전센터) ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 "사이버안전센터"라 한다)를 둔다.<br>②사이버안전센터는 다음 각호의 업무를 수행한다.<br>1. 국가사이버안전정책의 수립<br>2. 전략회의 및 대책회의의 운영에 대한 지원<br>3. 사이버위협 관련 정보의 수집·분석·전파<br>4. 국가정보통신망의 안전성 확인<br>5. 국가사이버안전매뉴얼의 작성·배표<br>6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원<br>7. 외국과의 사이버위협 관련 정보의 협력<br>③ 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반(이하 "합동대응반"이라 한다)을 설치·운영할 수 있다.<br>④국가정보원장은 합동대응반을 설치·운영하기 위하여 필요한 경우에는 관계 중앙행정기관, 지방자치단체 및 공공기관의 장에게 소속 공무원 및 직원의 파견을 요청할 수 있다. | 제6조(국가사이버안전센터의 설치) ① 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방. 대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터(이하 “안전센터”라 한다)를 둔다.<br>② 안전센터는 다음 각 호의 업무를 수행한다.<br>1. 국가사이버테러 방지 및 위기관리 정책의 수립<br>2. 사이버테러 관련 정보의 수집. 분석. 전파<br>3. 사이버테러로 인하여 발생한 사고의 조사 및 복구 지원<br>③ 국가정보원장은 제1항의 안전센터를 운영함에 있어 국가차원의 종합판단, 상황관제, 위협요인 분석, 사고 조사 등을 위해 민. 관. 군 합동대응팀(이하 “합동대응팀”이라 한다)을 설치. 운영할 수 있 다.<br>④ 국가정보원장은 합동대응팀을 설치. 운영하기 위하여 필요한 경우에는 책임기관 및 지원기관의 장에게 인력의 파견과 장비의 지원 을 요청할 수 있다 | |
| 제9조(사이버안전대책의 수립 · 시행 등) ① 중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 한다.<br>②관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 사이버안전대책을 수립·시행하도록 할 수 있다.<br>③국가정보원장은 제1항 및 제2항에 따른 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼 및 관련 지침을 작성 배포할 수 있다. 이 경우 국가정보원장은 미리 관계 중앙행정기관의 장과 협의하여야 한다.<br>④국가정보원장은 제1항 및 제2항에 따른 사이버안전대책의 이행여부 진단·평가 등 정보통신망에 대한 안전성을 확인할 수 있으며 필요하다고 인정하는 경우에는 해당 중앙행정기관의 장에게 시정 등 필요한 조치를 권고할 수 있다. 다만, | 제7조(사이버테러 방지대책의 수립. 시행) ① 책임기관의 장은 소관 정보통신망과 정보 등의 안전성 및 신뢰성 확보를 위한 사이버테러 방지대책을 강구하여야 한다.<br>② 국가정보원장은 관계 중앙행정기관의 장과 협의하여 제1항에 따 른 사이버테러 방지대책의 수립에 필요한 지침을 작성 배포할 수 있다. 다만, 국회, 법원, 헌법재판소 및 중앙선거관리위원회의 경우 에는 해당 기관의 장이 필요하다고 인정하는 경우에 적용한다. | |

| | | |
|---|---|---|
| 지방자치단체 및 공공기관의 정보통신망에 대한 안전성 확인은 관계 중앙행정기관의 장과 협의하여 수행한다. | | |
| 제9조의2(사이버위기 대응 훈련) ① 중앙행정기관, 지방자치단체 및 공공기관의 장은 소관 정보통신망을 대상으로 매년 정기적으로 사이버위기 대응 훈련을 실시하여야 한다.<br>② 국가정보원장은 국가 차원의 사이버위기 발생에 대비하여 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 대상으로 사이버위기 대응 통합훈련을 실시할 수 있다. 이 경우 국가정보원장은 특별한 사유가 없으면 사전에 훈련 일정 등을 해당 기관의 장에게 통보하여야 한다.<br>③ 국가정보원장은 제2항의 훈련 결과 필요하다고 판단하는 경우에는 중앙행정기관, 지방자치단체 및 공공기관의 장에게 필요한 시정조치를 요청할 수 있다. 이 경우 해당 기관의 장은 특별한 사유가 없는 한 그 요청에 따라야 한다. | | 제13조(대응훈련) ① 정부는 사이버위기에 체계적이고 효율적으로 대응하기 위하여 훈련을 실시하여야 한다.<br>② 제1항의 훈련은 매년 정기 또는 수시로 구분하여 실시할 수 있으며, 정기 훈련은 「비상대비자원 관리법」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.<br>③ 제1항의 훈련 대상 · 실시방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다. |
| 제10조(사이버공격과 관련한 정보의 협력) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을 국가안보실장 및 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가안보실장 및 국가정보원장에게 통보하여야 한다.<br>②국가정보원장은 제1항의 규정에 의하여 관련 정보를 제공받은 경우에는 대응에 필요한 조치를 강구하고 그 결과를 정보를 제공한 해당기관의 장에게 통지한다. | | 제11조(사이버위협정보의 공유) ① 국무조정실장은 다음 각 호의 사항에 해당하는 정보(이하 “사이버위협정보”라 한다)의 공유를 위하여 책임기관으로부터 파견된 인력으로 구성된 사이버위협정보공유센터(이하 “공유센터”라 한다)를 둔다.<br>가. 사이버공격에 관한 정보<br>나. 악성 프로그램 및 이와 관련된 정보<br>다. 정보통신망, 정보통신기기 및 소프트웨어 보안취약점에 관한 정보<br>라. 그 밖에 사이버공격의 징후나 사이버공격에 활용될 수 있는 사항에 관한 정보<br>② 책임기관의 장은 필요하다고 인정하는 경우 대통령령이 정하는 바에 따라 소관 사이버위협정보를 공유센터의 장에게 제공할 수 있으며, 공유센터의 장은 책임기관으로부터 제공받은 사이버위협정보를 다른 책임기관에게 제공하여야 한다.<br>③ 공유센터의 장은 책임기관 및 민간의 전문가 등이 참여하는 협의회를 구성하여 사이버위협정보의 공유 과정에서 발생할 수 있는 권리 침해를 방지하기 위한 관리적 · 물리적 · 기술적 대책을 수립 · 시행하여야 한다.<br>④ 누구든지 제3항에 따라 제공받은 사이버위협정보를 사이버안보에 필요한 업무범위에 한하여 정당하게 사용 · 관리하여야 한다.<br>⑤ 그 밖에 공유센터의 구축 · 운영에 관하여 필요한 사항은 대통령령으로 정한다. |
| 제10조의2(보안관제센터의 설치 · 운영) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 | 제8조(보안관제센터 등의 설치) ① 책임기관의 장은 사이버테러 정보 를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축·운영하거나 다음 각 호의 기관이 구축·운영하는 보안관제센터에 | 제10조(사이버공격의 탐지 · 대응) ① 정부는 국가 사이버공간에 대한 사이버공격에 신속하고 효율적으로 대응하기 위하여 국가 차원의 사이버공격 탐지 · 대응체계를 구축 · 운영하여야 한다. |

| | | |
|---|---|---|
| 설치·운영하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 다른 중앙행정기관(국가정보원을 포함한다)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다.<br>② 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다.<br>③ 보안관제센터를 설치·운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다.<br>④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 미래창조과학부장관이 지정하는 보안관제전문업체의 인원을 파견받아 보안관제업무를 수행하도록 할 수 있다. 이 경우 보안관제전문업체의 지정·관리 등에 필요한 사항은 미래창조과학부장관이 국가정보원장과 협의하여 정한다.<br>⑤ 제1항의 보안관제센터의 설치·운영 및 제2항의 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다. | 그 업무를 위탁하여야 한다. 다만, 「정보통신 기반 보호법」 제16조에 따른 정보공유·분석센터는 보안관제센터로 본다.<br>1. 제2조제5호가목의 기관<br>2. 제2조제6호바목의 보안관제전문업체<br>② 책임기관의 장은 제1항에 따른 사이버테러 정보와 정보통신망. 소프트웨어의 취약점 등의 정보(이하 “사이버위협정보”라 한다)를 관계 중앙행정기관의 장 및 국가정보원장과 공유하여야 한다.<br>③ 정부는 제2항의 사이버위협정보의 효율적인 관리 및 활용을 위 하여 관계기관의 장과 공동으로 사이버위협정보통합공유체계를 구축·운영할 수 있다.<br>④ 누구든지 제2항에 따라 공유하는 정보에 대하여는 사이버위기관리를 위하여 필요한 업무범위에 한하여 정당하게 사용 관리하여야 한다.<br>⑤ 제1항에 따른 보안관제센터와 제3항에 따른 사이버위협정보통합 공유체계 구축·운영 및 정보 관리에 관한 사항과 제2항에 따른 사이버위협정보의 공유에 관한 범위. 절차. 방법 등에 관한 사항은 대통령령으로 정한다. | ② 책임기관의 장은 제1항에 따른 사이버공격 탐지 · 대응체계의 구축을 위하여 대통령령이 정하는 바에 따라 소관 사이버공간에 대한 사이버공격을 탐지 · 분석하여 즉시 대응조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축 · 운영하거나 다른 책임기관의 장 또는 지원기관 등이 구축 · 운영하는 보안관제센터에 그 업무를 위탁하는 등의 조치를 취하여야 한다. |
| 제11조(경보 발령) ① 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를 발령할 수 있다. 다만, 민간분야에 대하여는 미래창조과학부장관이 경보를 발령하고, 국방분야에 대하여는 국방부장관이 경보를 발령하며, 국가정보원장, 미래창조과학부장관 및 국방부장관은 국가차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 발령 전에 상호 교환하여야 한다.<br>②제1항의 규정에 의하여 경보를 발령하였을 때에는 관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장에게 이를 신속히 전파하고 적절한 조치를 취하여야 한다.<br>③국가정보원장은 사이버공격이 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우에는 국가안보실장과 협의하여 심각 수준의 경보를 발령할 수 있다.<br>④국가정보원장은 제1항의 규정에 의한 경보 발령에 필요한 정보를 관계 중앙행정기관의 장에게 요청할 수 있다. 이 경우 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다. | 제10조(사이버위기경보의 발령) ① 정부는 사이버테러에 대한 체계적 인 대비와 대응을 위하여 책임기관의 장의 요청과 제8조제2항에 따 라 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있다. 이 경우 국가안보실장과 미리 협의하여야 한다.<br>② 정부는 제1항의 사이버위기경보를 발령할 경우 관계기관의 장과 경보 수준을 사전 협의하여야 한다.<br>③ 책임기관의 장은 제1항에 따른 사이버위기경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 취하여야 한다.<br>④ 사이버위기경보 발령의 주체·절차·기준 및 책임기관의 장의 조치 등에 관하여 필요한 사항은 대통령령으로 정한다. | 제14조(사이버위기경보의 발령) ① 정부는 사이버공격에 대한 체계적인 대응을 위하여 단계별 사이버위기경보(이하 “경보”라 한다)를 발령할 수 있다. 이 경우 경보의 발령 시점과 단계 등에 관하여 위원회의 위원장과 미리 협의 하여야 한다.<br>② 책임기관의 장은 제1항에 따른 경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 취하여야 한다.<br>③ 경보 발령의 주체 · 기준 · 절차 및 책임기관의 장의 조치 등에 관하여 필요한 사항은 대통령령으로 정한다. |
| 제12조(사고통보 및 복구) ① 중앙행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체없이 그 사실을 국가안보실장 및 국가정보원장에게 통보하여야 한다. | | |

| | | |
|---|---|---|
| ② 지방자치단체의 장 및 공공기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 지체 없이 국가안보실장, 국가정보원장 및 관계 중앙행정기관의 장에게 통보하여야 한다.<br>③국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 제1항 및 제2항의 규정에 의한 통보를 받은 때에는 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있으며, 요청받은 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다. | | |
| 제13조(사고조사 및 처리) ①<br>국가정보원장은 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 해당 기관의 장이 자체적으로 조사하게 할 수 있으며, 이 경우 해당 기관의 장은 사고개요 및 조치내용 등 관련 사항을 국가정보원장에게 통보하여야 한다.<br>②국가정보원장은 제1항의 규정에 의하여 조사한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다.<br>③국가정보원장은 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우에는 관계 중앙행정기관의 장과 협의하여 범정부적 사이버위기 대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다.<br>④ 사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위하여 대책본부 내에 합동조사팀 등 필요한 하부기구를 둘 수 있다. 이 경우 하부기구의 구성·운영 등에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.<br>⑤ 국가정보원장은 제4항에 따른 사고조사 및 피해복구 등의 조치를 위하여 관계 중앙행정기관의 장에게 필요한 인력·장비 및 관련 자료의 지원을 요청할 수 있다.<br>⑥ 국가정보원장은 사이버공격에 의한 피해 및 대책본부의 대응 상황을 국가안보실장에게 통보하고, 국가안보실장은 이를 종합하여 대통령에게 보고한다. | 제9조(사고조사) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인하여 소관분야에 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하여야 한다. 또한, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기 관의 장에게 통보하여야 한다.<br>② 제1항의 경우 피해가 중대하거나 확산될 우려가 있는 경우 중앙 행정기관의 장은 즉시 미래창조과학부장관, 국가정보원장 및 금융위 원장 등 대통령령으로 정하는 전문기관의 장에게 사고조사 등 기술 적 지원을 요청할 수 있다. 다만, 국회, 법원, 헌법재판소, 중앙선거 관리위원회는 해당기관의 장이 필요하다고 인정하는 경우에 한한다.<br>③ 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙 행정기관의 장은 제1항에 따라 사고조사 결과를 통보받거나 제2항 에 따라 기술적 지원을 한 결과, 피해의 복구 및 확산방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요 한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.<br>④ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사 이버테러와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.<br><br>제11조(사이버위기대책본부의 구성) ① 정부는 경계단계 이상의 사이 버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민. 관. 군 전문가가 참여하는 사이버위기대책본부(이하 “대책본부”라 한다)를 구성·운영할 수 있다.<br>② 대책본부의 장(이하 “대책본부장”이라 한다)은 관계 중앙행정기 관의 장이 국가안보실장과 협의하여 정하고, 대책본부의 구성·운영 등에 관하여 필요한 사항은 대책본부장이 관계 중앙행정기관의 장과 협의하여 정한다. | 제12조(사이버공격 사고의 신고 · 조사) ① 국가정보원장은 책임기관의 사이버공격으로 인한 사고가 발생하는 경우 피해를 최소화하고 피해의 확산을 차단하기 위하여 국가 차원의 일원화된 신고 및 조사 체계를 운영하여야 한다.<br>② 책임기관의 장은 소관 사이버공간에서 사이버공격으로 인한 사고가 발생한 때에는 피해를 최소화하는 조치를 취하고 신속하게 그 사실을 상급 책임기관의 장에게 신고하여야 한다. 이 경우 시 · 도지사는 행정자치부 장관, 교육감은 교육부장관에게도 각각 신고하여야 하며, 국가안보를 위협하는 사이버공격으로 인한 사고이거나 상급 책임기관의 장이 운영하는 사이버공간에서 발생한 사고의 경우에는 국가정보원장에게도 신고하여야 한다.<br>③ 상급 책임기관의 장은 제2항에 의한 신고를 받은 경우 신속히 사고조사를 실시하여야 하고, 필요한 경우 지원기관의 장에게 기술적 지원을 요청할 수 있다. 다만, 국가안보를 위협하는 사이버공격의 경우에는 그러하지 아니한다.<br>④ 국가정보원장은 국가안보를 위협하는 사이버공격이 발생하거나, 제2항에 따른 신고를 받은 경우 지체 없이 사고조사를 실시하여야 한다. 다만, 민간 영역의 책임기관을 대상으로 하는 경우에는 대통령령으로 정하는 바에 따라 관계 중앙행정기관, 수사기관 및 지원기관 등으로 구성된 합동조사팀을 운영하여야 한다.<br>⑤ 누구든지 제3항과 제3항에 따른 사고조사에 협조하여야 하며 사고조사를 완료하기 전에 사이버공격과 관련된 자료를 임의로 삭제 · 훼손 · 변조하여서는 아니 된다.<br>⑥ 상급 책임기관의 장 및 국가정보원장은 제3항과 제4항에 따라 사고조사를 수행하는 과정에서 사이버공격과 관련된 악성프로그램 또는 악성프로그램의 감염을 유인하는 전자적 정보(이하 “악성프로그램 등”이라 한다)가 포함된 컴퓨터, 웹사이트 또는 소프트웨어 등을 발견한 경우에는 그 관리자에게 관련 악성프로그램의 제공을 요청하거나 백신프로그램의 제공 등을 통하여 |

| | | |
|---|---|---|
| | ③ 대책본부장은 제1항에 따른 대책본부를 구성·운영하기 위하여 책임기관 및 지원기관의 장에게 필요한 인력의 파견 및 장비의 제공 을 요청할 수 있다. | 악성프로그램 등을 삭제 또는 차단을 요청할 수 있다.<br><br>제15조(사이버위기대책본부의 구성) ① 정부는 경계단계 이상의 사이버 위기경보가 발령된 경우 또는 위원회의 위원장이 필요하다고 판단하는 경우 국가역량을 결집하여 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 책임기관, 수사기관 및 지원기관 등이 참여하는 사이버위기대책본부(이하 “대책본부”라 한다)를 구성 · 운영할 수 있다.<br>② 대책본부의 장은 사이버위기가 발생한 사이버공간을 관할하는 상급 책임기관의 장 또는 국가정보원장이 위원회의 위원장과 협의하여 정하고, 대책본부의 구성 · 운영 등에 관하여 필요한 구체적인 사항은 대통령령으로 정한다.<br>③ 대책본부의 장은 제1항에 따른 대책본부를 구성 · 운영하기 위하여 책임기관 및 지원기관의 장에게 필요한 인력의 파견 및 장비의 제공을 요청할 수 있다. |
| 제14조(전문기관간 협력) ① 사이버안전업무를 전담하는 전문기구를 운영하는 기관은 국가사이버안전업무를 효율적으로 수행하기 위하여 다음 각호의 사항을 상호 긴밀히 협력하여야 한다.<br>1. 사이버위협 관련 정보의 탐지 및 정보공유체계의 구축·운영<br>2. 사이버안전 관련 정보의 분석·전파<br>3. 사이버안전 위해 요소에 대한 조치방안<br>4. 공격기법 분석 및 공격차단 등 대응방안<br>5. 그 밖에 경보의 수준별 세부 대응조치 등 필요한 사항<br>②사이버안전센터장은 제1항의 규정에 의한 전문기구를 운영하는 기관간 협력을 원활하게 하기 위하여 관계전문가 회의를 소집할 수 있다. | | 제16조(사이버안보 전문업체의 지정 · 관리) ① 미래창조과학부장관은 이 법에서 규정한 업무를 지원할 수 있는 능력이 있다고 인정되는 자를 사이버안보 전문업체(이하 “전문업체”라 한다)로 지정 · 관리할 수 있다. 다만, 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호전문서비스기업은 전문업체로 지정을 받은 것으로 본다.<br>② 미래창조과학부장관은 전문업체가 다음 각 호의 어느 하나에 해당하는 경우에는 청문을 거쳐 전문업체의 지정을 취소하거나 그 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호의 경우에는 지정을 취소하여야 한다.<br>1. 속임수나 그 밖의 부정한 방법으로 지정을 받은 경우<br>2. 업무에 관한 기록 및 자료를 안전하게 보존하지 아니한 경우<br>3. 제1항에 따른 지정기준에 미달한 경우<br>③ 전문업체의 지정 · 관리에 필요한 구체적인 사항은 대통령령으로 정한다.<br><br>제17조(사이버안보 활동의 지원) ① 지원기관의 장은 책임기관의 장이 요청할 경우 대통령령이 정하는 바에 따라 다음 각 호의 사이버안보 활동의 수행에 필요한 기술적 지원을 할 수 있다.<br>1. 제10조에 따른 사이버공격의 탐지 · 대응<br>2. 제12조에 따른 사이버공격 사고의 조사<br>3. 제14조에 따른 피해발생의 최소화 및 피해복구를 위한 조치<br>4. 제15조에 따른 대책본부의 운영<br>② 정부는 대통령령이 정하는 바에 따라 제1항에 따른 지원기관의 기술지원 실태를 점검할 수 있으며 기술적 지원에 소요되는 비용의 전부 |

| | | |
|---|---|---|
| | | 또는 일부를 지원기관에게 지원할 수 있다. |
| 제15조(연구개발) ① 국가정보원장은 국가사이버안전에 필요한 기술개발과 기술수준의 향상을 위하여 필요한 시책을 추진할 수 있다.<br>②중앙행정기관의 장은 공공분야의 사이버안전 관련 기술의 확보를 위하여 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항의 규정에 의하여 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소로 하여금 관련 연구개발을 수행(연구개발을 위하여 보안관제업무를 수행하는 것을 포함한다)하게 할 수 있다.<br>③제2항의 규정에 의한 사이버안전에 필요한 기술의 연구개발에 관한 세부사항은 국가정보원장이 따로 정한다. | | 제18조(연구개발) ① 정부는 사이버안보에 필요한 정책ㆍ기술의 개발과 수준 향상을 위하여 다음 각 호의 시책을 추진할 수 있다.<br>1. 사이버안보에 관한 국가 연구개발 계획의 수립ㆍ시행<br>2. 사이버안보 관련 기술 수요조사 및 관련 동향분석 등에 관한 사업<br>3. 사이버안보에 관한 정책ㆍ기술의 개발ㆍ보급ㆍ확산 사업<br>4. 그 밖에 사이버안보 관련 정책ㆍ기술 개발 및 수준 향상 등에 관하여 필요한 사항<br>② 정부는 제1항의 시책을 추진하기 위하여 전문연구기관을 설립하거나, 다른 법령에 의하여 설립된 기관 및 기관부설연구소를 전문 연구기관으로 지정하여 사이버안보에 필요한 연구개발을 수행하게 할 수 있다.<br>③ 사이버안보 정책ㆍ기술의 연구개발에 관한 절차ㆍ방법 등 세부사항은 대통령령으로 정한다.<br><br>제19조(산업육성) ① 미래창조과학부장관은 관계중앙행정기관의 장과 협의하여 사이버안보에 필요한 산업의 육성을 지원하기 위하여 다음 각 호의 시책을 수립ㆍ시행하고 이에 필요한 재원 확보 방안 등을 마련하여야 한다.<br>1. 사이버안보 산업 진흥정책 수립 지원<br>2. 사이버안보 산업 발전을 위한 유통시장 활성화 지원<br>3. 사이버안보 산업 육성을 위한 산ㆍ학ㆍ연 협력체계 구축<br>4. 사이버안보 산업 관련 국제교류ㆍ협력 및 해외진출의 지원<br>② 제1항에 따른 시책은 「정보보호산업진흥에 관한법률」 제5조에 따른 정보보호산업 진흥계획과 조화를 이루도록 수립하여야 한다. |
| 제16조(인력양성 및 교육홍보) ① 관계중앙행정기관의 장은 사이버안전의 기반 조성에 필요한 기술인력을 양성하고 국민의 인식제고를 위하여 다음 각호의 시책을 강구하여야 한다.<br>1. 사이버안전 관련 전문기술인력의 확보 및 양성<br>2. 사이버안전 교육프로그램의 개발 및 투자<br>3. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항<br>②국가정보원장은 관계중앙행정기관의 장이 사이버안전과 관련한 전문인력의 양성, 교육 및 홍보를 위하여 필요한 지원을 요청하는 경우 이에 대하여 지원할 수 있다. | | 제20조(인력양성 및 교육홍보) ① 미래창조과학부장관과 교육부장관은 관계중앙행정기관의 장과 협의하여 사이버안보 기반을 조성하고 국민적 인식을 제고하기 위하여 다음 각 호의 시책을 강구하여야 한다.<br>1. 사이버안보 관련 전문인력의 양성<br>2. 사이버안보에 관한 대국민 홍보활동 및 교육<br>3. 그 밖에 사이버안보 관련 전문인력 양성 및 교육홍보 등에 관하여 필요한 사항<br>② 책임기관의 장은 전문연구기관의 장에게 소속 직원들을 대상으로 사이버안보에 관한 교육훈련 지원 등을 요청할 수 있다.<br><br>제21조(국제협력) ① 외교부장관은 관계중앙행정기관의 장과 협의하여 국가 사이버공간의 보호를 위해 국제기구ㆍ단체 및 외국과 적극적인 협력 활동을 수행하여야 한다.<br>② 제1항에 따른 국제협력 활동은 다음 각 호의 업무를 포함한다. |

| | | |
|---|---|---|
| | | 1. 사이버안보를 위한 상호간 협력체계 및 신뢰구축<br>2. 사이버안보 기술, 위협, 수사 등에 관한 정보의 교류와 공동대응<br>3. 사이버안보 분야의 인사교류 및 역량강화<br>③ 정부는 국제 사이버공간의 안전성과 신뢰성 확보를 위해 국제 사회가 공감하는 보편타당한 국제규범 수립에 적극 참여하여야 한다. |
| 제17조(예산) 중앙행정기관의 장은 소관분야와 관련된 사이버안전대책의 수립·시행에 필요한 재정상의 조치를 강구하여야 한다. | 제12조(비밀 엄수의 의무) 이 법에 따라 사이버테러 방지 및 위기관리 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.<br><br>제13조(포상 등) ① 정부는 사이버테러 방지 및 위기관리와 관련하여 다음 각 호의 어느 하나에 해당하는 자에 대하여 포상하고, 예산의 범위에서 포상금을 지급할 수 있다. 1. 사이버테러 기도에 관한 정보를 제공한 자 2. 사이버테러를 가한 자를 신고한 자 3. 사이버테러의 탐지 및 대응·복구에 공이 많은 자 ② 제1항에 따른 포상과 포상금 지급의 기준·방법과 절차, 구체적인 지급액 등 필요한 사항은 대통령령으로 정한다 | 제22조(비밀 엄수의 의무) 이 법에 따라 사이버안보 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.<br><br>제23조(포상 등) ① 정부는 다음 각 호의 어느 하나에 해당하는 자에 대하여 포상하고, 예산의 범위에서 포상금을 지급할 수 있다.<br>1. 사이버공격 기도에 관한 정보를 제공한 자<br>2. 사이버공격을 가한 자를 신고한 자<br>3. 사이버공격의 탐지 및 대응·복구에 공이 많은 자<br>4. 사이버공격의 예방 및 탐지·대응에 필요한 신기술을 개발한 자<br>5. 사이버위협정보 제공에 공이 많은 자<br>② 제1항에 따른 포상과 포상금 지급의 기준 · 방법과 절차, 구체적인 지급액 등 필요한 사항은 대통령령으로 정한다. |
| 제18조(안전성 확인 등에 대한 특례) ① 제9조, 제12조 및 제13조에도 불구하고 국방분야의 사이버안전과 관련한 다음 각호에 대하여는 국방부장관이 그 업무를 수행한다.<br>1. 제9조제4항의 규정에 의한 안전성 확인<br>2. 삭제 <2013.9.2><br>3. 제12조제1항의 규정에 의한 사고통보<br>4. 제13조제1항의 규정에 의한 사고조사<br>②국방부장관은 제1항의 규정에 의한 업무를 수행함에 있어 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다. | 제14조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.<br>1. 제8조제2항 및 제4항을 위반한 자<br>2. 제9조제4항을 위반한 자<br>3. 제12조를 위반한 자<br>② 업무상 과실로 인하여 제1항의 죄를 범한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.<br><br>제15조(과태료) ① 제9조제3항을 위반한 자는 1천만원 이하의 과태료 에 처한다.<br>② 제1항에 따른 과태료는 대통령령이 정하는 바에 따라 관계 중앙 행정기관의 장이 부과. 징수한다. | 제24조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.<br>1. 제11조제4항을 위반하여 사이버위협정보를 사이버안보에 필요한 업무 이외에 영리 또는 부정한 목적으로 사용 · 관리한 자<br>2. 제12조제5항을 위반하여 사고조사를 방해할 목적으로 사이버공격과 관련된 자료를 삭제 · 훼손 · 변조한 자<br>3. 제22조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이용한 자<br><br>제25조(과태료) ① 제12조제2항을 위반하여 사이버공격 사고를 신고하지 아니한 자는 1천만원 이하의 과태료에 처한다.<br>② 제1항에 따른 과태료는 대통령령이 정하는 바에 따라 관계 중앙 행정기관의 장이 부과 · 징수한다.<br><br>제26조(공무원에 대한 징계) 제2조제6호가목에 해당하는 기관에 종사하는 자로서 제24조 각호의 어느 하나에 해당하는 자는 「국가공무원법」, 「지방공무원법」, 「외무공무원법」, 그 밖의 법령에 따라 정해진 공무원의 징계사유에 해당하는 것으로 본다.<br><br>제27조(국방 분야에 대한 특례) 국방부 본부를 제외한 합동참모본부, 각 군 및 국방부 직할 부대 · 기관은 다음 각 |

| | | |
|---|---|---|
| | | 호에 대해 국방부장관이 그 업무를 수행한다.<br>1. 제8조에 따른 사이버안보 실태평가<br>2. 제12조에 따른 사이버공격 사고의 조사<br>3. 제14조에 따른 사이버위기경보의 발령<br>4. 제21조에 따른 국제협력 |

사이버테러방지법안을 비롯한 사이버 보안 관련 법안들의 문제점들을 검토해보면 다음과 같다.

첫째, 법안의 성격이 모호하다. 사이버테러방지법은 국가 사이버 보안을 위한 일반법인가, 아니면 '사이버 테러에 대한 대응'이라는 제한된 목적을 가진 개별법인가.
사이버테러방지법은 '사이버테러'라는 개념을 사용하여, 일반적인 사이버 공격에 대한 대응이나 사이버 보안보다는 국가 위급상황과 같은 특수한 상황에 대응하려는 법안으로 보인다. 그러나 '사이버테러'의 정의가 모호해서 훨씬 광범하게 해석될 수 있고, 책임기관의 사이버안전관리 책임, 국가사이버안전센터 설치 등 기본적인 사이버 보안 수행체계에 대한 내용도 포함하고 있다.

만일 '사이버 테러'에 대한 대응이라는 제한된 목적을 가진 개별법 제정이 목적이라면, 관련 법령이 이미 존재하는 상황에서 별개의 개별법을 제정할 필요성이 있는지 의문이 제기된다.[129] 이미 국내에는 정보통신망법, 정보통신기반보호법 등 사이버 테러를 비롯한 사이버 침해사고를 예방하고, 이에 대응하기 위한 법제가 마련되어 있으며, 비록 훈령이기는 하지만 국가사이버안전관리규정에 기반하여 국가사이버안전전략회의나 국가사이버안전센터 등 국가적 차원의 사이버 보안 수행체계도 마련되어 있다. 물론 국정원 중심의 사이버 보안 수행체계에 대한 재검토나 사이버 보안 관련 법령의 체계적인 검토는 필요할지 몰라도, 사이버테러방지법과 같이 단지 국가사이버안전관리규정의 일부 내용을 수용하고 기존 법제와 중복적인 내용을 가진 새로운 개별법을 제정하는 것은 오히려 규제의 중복과 권한의 혼선을 야기할 수 있다.

국가사이버안보기본법은 사이버 보안을 위한 '기본법'을 표방하고 있지만, '국가안보' 관점에서의 사이버 보안만을 의미하는 것인지, 일반적인 사이버 보안, 정보 보안을 위한 일반법 제정을 목적으로 하고 있는지 모호하다. 이는 한국의 사이버 보안 정책의 관점이 사이버 보안에 대한 총체적인 관점이 아니라, '국가안보'적 측면에 중점을 두고 있는 문제와 연결된다.

둘째, 오히려 기존 법안과의 충돌과 혼란을 야기하고 있다. 사이버테러방지법안과 국가사이버안보기본법 제정안 모두 주요 정보통신기반시설을 책임기관으로 포함하고 있는데, 이는 정보통신기반보호법에 기반한 규제와 중복된다. 지원기관 역시

[129] 정보통신기반보호법의 제정이유를 보면 "정보화의 진전에 따라 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹·컴퓨터바이러스 등을 이용한 전자적 침해 행위가 21세기 지식기반국가의 건설을 저해하고 국가 안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설을 보호하기 위한 체계적이고 종합적인 대응체계를 구축하기 위해 정보통신기반보호법 제정됨."이라고 되어 있다. 이런 이유로 정보통신기반보호법을 제정했고, 그 법이 현재 시행되고 있다면, 그 법이 있음에도 불구하고 법령의 미비로 사이버 침해를 막기가 어려운 것이 무엇인지를 구체적으로 제시할 수 있어야 한다. 만약 현재의 정보통신기반보호법으로도 충분하다면 별도로 사이버테러법을 제정할 이유는 없다. (이은우, 2016)

정보통신기반보호법에서 규정하고 있는 내용이다. 앞서 지적했다시피, 여러 개별법들에서 유사한 규정을 중복해서 규정하는 것은 오히려 혼란을 야기하여 사이버 보안을 약화시킬 수 있다.

셋째, 개념 정의가 모호하고, 기존 법령과의 일관성도 부족하다.
이미 현재 사이버 보안과 관련된 법령에서 사이버안전, 정보보호, 정보보안, 혹은 사이버 공격, 전자적 침해사고 등과 같이 유사한 개념의 서로 다른 용어를 사용하고 있어, 법령간의 체계성과 일관성이 없다는 점을 지적한 바 있다. 그런데 제안 법률안은 이러한 혼란을 해소하기보다는 오히려 부추길 수 있다. 사이버테러방지법안은 '사이버테러'라는 새로운 용어를 도입하여, '사이버공격'과의 혼란을 부추기고 있다. 국가사이버안보기본법 제정안은 '사이버안보'라는 개념을 사용하고 있는데, 이것이 기존의 '사이버안전'과 어떻게 다른지 의문이다.

이러한 혼란과 함께 용어의 정의도 모호하다. 예를 들어, '사이버테러'는 "외국이나 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단, 해킹·범죄조직 및 이들과 연계되거나 후원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단 에 의하여 정보통신망을 공격하는 행위"로 정의되고 있는데, 개인이 독자적으로 수행하는 해킹은 이에 해당하는 것인가? 또한 '국가안보 또는 공공의 안전을 위태롭게 할 목적'은 어떻게 판단할 것인가?

'국가안보를 위협하는 사이버공격'이나 '사이버위기' 등의 정의도 자의적으로 판단될 수 있는 여지가 많다. 이럴 경우 규제 주체인 국정원 등의 자의적인 판단에 따라 권력의 남용 가능성이 존재할 수밖에 없다.[130]

넷째, 사이버테러방지법안이나 국가사이버안보기본법 제정안 모두 사이버 보안 수행체계가 어떻게 변화되는지 모호하다. 사이버테러방지법의 경우 현재 국가사이버안전규정에 포함되어 있는 '국가사이버안전센터'의 설치 근거를 법에 두고 있지만, 기존의 국가사이버안전전략회의나 대책회의는 어떻게 되는지에 대한 설명이 없다. '국가사이버테러방지 및 위기관리 기본계획'의 수립 주최도 '정부'로만 되어 있어 명확하지 않다.

국가사이버안보기본법 제정안의 경우에는 '국가사이버안보위원회'를 두고 있으며, 이 위원회의 위원장을 '국가안보실장'이 맡는 등 2015년 4월 이후 국가 사이버안보 수행체계의 변화를 반영하고 있는 것으로 보인다. 이 위원회는 훈령의 전략회의를 대체한 것이다. 국가사이버안보실무위원회는 훈령의 대책회의를 대체한 것으로 볼 수 있다. 그러나 제정안은 현재 국정원이 맡고 있는 국가사이버안전센터에 대한 규정을 포함하고 있지 않다. 현재 국정원이 국가사이버안전센터를 운영하면서 실질적인 컨트롤타워 역할을 하고 있음을 고려할 때, 만일 국가사이버안전센터가 계속 유지된다면 이를 법이 아니라 시행령을 통해 규정하려고 하는 것은 타당하지 않다.

다섯째, 두 법안 모두 여전히 국정원을 중심으로 한 사이버 보안 수행 체계를 유지하고 있는데, 이는 국정원의 사이버 공간에 대한 권한을 확대할 우려가 크다.
사이버테러방지법안은 국정원장 소속으로 국가사이버안전센터를 두고, 현재와 같이 민·관·군

[130] 관련하여, 김도승(2016)은 "국가를 위협하는 사이버 공격", "사이버위기", "사이버안보" 등 개념에 따라 규율의 온도차가 크게 달라짐에도 그 개념의 구체성을 담보하기 어려워 사실상 규율주체의 의지에 사이버공격의 구조적 특성이 더하여 국가정보원 주도의 강화된 규율 일변도로 흐를 가능성이 상존하는 문제가 있음을 지적하고 있다.

합동대응팀을 설치·운영할 수 있도록 하고 있다. 또한, 사이버테러 방지대책의 수립에 필요한 지침을 작성 배포할 수 있다. 국가사이버안보기본법 제정안의 경우에도, 비록 국가사이버안보위원회의 위원장은 국가안보실장이 맡는다고 하지만, 국가안보실장과 국가정보원장이 공동으로 운영하는 국가사이버안보실무위원회를 두도록 하고 있고, 사이버안보 기본계획을 수립·시행하는 주체가 국정원으로 되어 있다.

이와 같은 국정원의 역할은 국가사이버안전관리규정에서 규정하고 있는 역할, 혹은 현재 국정원이 수행하고 있는 역할과 크게 다르지 않지만, 두 법안이 규율하는 대상이 기존의 정보통신기반시설을 제외한 국가정보통신망에서, 국회 등 헌법기관, 민간까지 포함한 정보통신기반시설 및 주요 정보통신서비스 제공자 등 민간업체로 확대되기 때문에, 결국 국정원의 권한이 확대되는 것과 마찬가지다. 예를 들어, 국가사이버안보기본법 제정안에 따르면, 국정원은 책임기관으로 지정된 민간업체에 대해 실태평가를 할 수 있으며(제8조), 자료제출을 요구할 수도 있고(제5조 2항), 국가안보를 위협하는 사이버 공격이 발생한 경우 사고조사를 실시할 수 있다.(제12조 4항)  이 때문에 시민사회와 야당은 국정원이 사이버 보안을 명분으로 민간의 정보통신망까지 개입하여 민간 사업자나 이용자를 감시·사찰할 수 있다는 우려를 표해왔으며, 이는 사이버테러방지법안이 지금까지 국회에서 통과되지 못한 이유가 되었다.

특히, 사이버테러방지법안은 책임기관에 집적정보통신시설 사업자 및 주요정보통신서비스 제공자까지 포함하고 있기 때문에(제2조 5호) 주요 포털 등에 대한 감시 우려를 불러왔다. 이러한 비판을 의식해서인지 국가사이버안보기본법 제정안은 책임기관에서 주요 정보통신서비스 제공자를 명시적으로 포함하지는 않고 있다. 그러나 국가사이버안보위원회의 의결을 거쳐 책임기관을 추가로 지정할 수 있도록 하고 있기 때문에, 포털이나 언론사 등이 책임기관에 포함될 가능성을 배제할 수는 없다. 이와 관련하여 김도승(2016)은 “국가사이버안보위원회 의결로 책임기관을 추가로 지정할 수 있는데, 국가사이버안보위원회의 구성과 운영 그리고 책임기관 지정 기준이 사실상 법률에서 정하는 바가 없이 대통령령에 모두 위임되어 있어 법률유보의 원칙을 충족하지 못하는 문제”를 지적하고 있다. 또한, 국정원의 사이버 보안 총괄 권한이 국정원의 직무권한에 비추어 볼 때 과도한 직무와 권한의 창설은 아닌지와 국가정보원의 강화된 기능에도 불구하고  이를 견제하는 절차(예를 들어, 관련 사항에 대한 정례적인 국회 보고 등) 등에 대해 법률에서 전혀 다루고 있지 않은 문제를 비판하고 있다.(김도승, 2016)

물론 앞서 살펴보았다시피, 국정원은 이미 국가 사이버 보안의 컨트롤타워 역할을 하고 있고, 민간의 정보통신망에 개입할 수 있는 권한도 어느 정도 보유하고 있다. 그런데, 오히려 국정원이 이미 보유하고 있는 사이버 보안 관련 권한에 대한 재검토가 필요한 상황에서, 사이버테러방지법을 제정하는 것은 기존의 문제를 심화시키는 결과를 초래할 것이다.

# 4. 정책 제안

지금까지 사이버 보안과 관련한 국제동향 및 해외 주요 국가의 현황, 그리고 국내 동향과 국정원이 사이버 보안 컨트롤타워의 역할을 하고 있는 것의 문제점에 대해 살펴보았다. 이를 토대로 국내 사이버 보안 정책을 재구성하기 위한 몇 가지 아이디어를 제안하고자 한다.

첫째, 기존 사이버 보안 정책에 대한 평가를 바탕으로 종합적인 사이버 보안 전략을 수립할 필요가 있다.

국내에서 지금까지 수립되었던 사이버 보안을 위한 종합대책은 '전략'이라기 보다는 말 그대로 '종합대책' 수준이었고, 사이버 보안과 관련된 이슈를 전체적으로 다루기보다는 주로 사이버 공격에 대응하기 위한 대책에 초점을 맞추었다. 또한, '사이버안보'라는 용어에서 알 수 있듯이, 사이버 보안을 국가안보적 관점에서 바라보고 있다. 그러나 사이버 보안 전략은 우리가 지향하는 정보사회의 가치와 운영 원칙을 포함하여, 그러한 가치와 원칙을 지키기 위한 제반 이슈들 - 사이버 범죄, 정보 보안, 국가안보적 측면을 포함한-을 종합적으로 다룰 필요가 있다.

둘째, 사이버 보안 전략은 다음과 같은 가치와 원칙을 반영해야 한다.[131]

• 인권 보장 : 사이버 보안의 궁극적인 가치는 오프라인과 마찬가지로 온라인에서도 인간으로서의 기본권을 향유할 수 있는 것이다. 모든 사이버 보안 정책은 표현의 자유, 프라이버시 등 기본권 보장의 가치에 기반해야 한다.
• 인터넷의 개방성과 혁신[132] : 사이버 보안 정책은 인터넷의 자유 및 개방성과 조화를 이룰 필요가 있다. 예를 들어, 국가가 특정한 기술을 강요하기 보다는 보다 나은 보안 기술의 발전을 위한 경쟁 환경을 조성할 필요가 있다. 보안을 명분으로 국가적인 인트라넷을 구축한 중국의 사례는 또 다른 반면교사일 것이다.
• 공공과 민간의 협력[133] : 대부분의 네트워크는 민간에 의해서 운영, 관리되고 있다. 그래서 세계 대부분의 국가들은 민간 주도 혹은 공공과 민간의 협력에 기반한 정책을 사이버 보안 정책의 기조로 삼고 있다. 경직된 규제보다는 책임성과 함께 자율성을 부여할 필요가 있다.

---

[131] 2013년 수립된 EU 사이버 보안 전략은 다음과 같은 5개의 원칙을 포함하고 있다. ① 유럽의 핵심적 가치는 디지털 세계에도 물리적 세계와 마찬가지로 적용되어야 함, ② 기본권, 표현의 자유, 개인정보 및 프라이버시의 보호, ③ 모두를 위한 접근, ④ 민주적이고 효율적인 멀티스테이크홀더 거버넌스, ⑤ 보안을 보장하기 위한 공유된 책임
또한, 일본의 사이버보안 전략 2015는 기본 원칙으로 ① 정보의 자유로운 흐름 보장, ② 법치, ③ 개방성, ④ 자율성, ⑤ 멀티스테이크홀더 사이의 협력을 강조하고 있다.
사이버 보안 정책의 나아갈 방향에 대한 모질라 보고서(Mozilla, 2015)도 '사이버보안의 궁극적인 목표는 사람의 보안(안전)'임을 강조하고 있다.

[132] EU의 사이버 보안 전략 명칭도 "An Open, Safe and Secure Cyberspace"이다.

[133] "기존에 기여가 이루어진 노력과 자원을 바탕으로 공공과 민간의 파트너쉽이라는 균형을 맞추면서 이를 증진시키는 방향으로 이루어져야 한다는 원칙이다. 과거 10여년 이상 민간 부문에서 공공부문과 발맞추어 사이버 보안과 관련하여 공공부문에 기여한 리더십과 자원, 기술혁신과 책임의식이 있으므로, 이러한 노력과, 투자, 파트너십을 최대한 활용해야만 효과적인 사이버 보안을 달성할 수 있다."
사이버보안을 위한 기술과 전문성은 기본적으로 민간부문에서 창출되기 때문에 공공과 민간의 협력을 이끌어 낼 수 있는 사이버보안이 되어야 한다. (The UK Cyber Security Strategy Protecting and promoting the UK in a digital world , 2011; 이은우, 2016에서 재인용)

• 민주적인 거버넌스 : 사이버 보안 정책의 수립부터 집행에 이르기까지, 관련 이해관계자들-정부, 기업, 기술자, 시민사회, 이용자 등-이 동등하고 자유롭게 참여할 수 있어야 한다.
• 국제협력과 신뢰: 인터넷은 세계적인 네트워크이기 때문에 국제적인 협력없이 사이버 보안의 목적을 달성할 수 없다. 또한, 다른 나라에 대한 선제적 공격을 통해 긴장을 유발해서는 안되며, 국가간 신뢰와 평화에 기반할 필요가 있다.

셋째, 사이버 보안 전략에 있어서 이용자 중심적 관점이 도입되어야 한다.

사이버 보안의 궁극적인 목적은 정보통신 기기나 인터넷을 이용하는 사람의 보안(human security)이다. 즉, 이용자들이 정보통신 기기와 인터넷을 통해 자신이 원하는 것을 자유롭게 안심하고, 안전하게 사용할 수 있도록 보장되어야 한다. 이용자 관점에서 보안을 고려할 때, 해커나 인터넷 범죄자로부터의 보안 뿐만이 아니라, 기기 제조업체, 서비스 제공자, 혹은 정부의 위협으로부터의 보안도 고려될 수 있다. 한편, 보안의 가장 큰 취약점은 '사람'이라고 하듯이, 이용자 자체가 커다란 보안위협이 될 수 있다. 대부분의 일상적 이용자는 기술을 잘 아는 사람이 아니며, 이를 고려한 보안 설계가 되어야 한다. 이용자에 대한 보안 교육도 물론 중요하지만, 이용자들이 보다 쉽게 보안을 위한 선택을 할 수 있도록 기술적 환경(Security by default)이 구축되어야 한다. 예를 들면, 중요한 보안 취약점 패치가 자동 업데이트 되도록 기본 설정화 할 수 있다.(Mozilla, 2015)

반면, 사이버 보안에 대한 국가안보적 시각은 편협할 뿐만 아니라, 때로는 '국가안보'를 명분으로 인터넷 전체의 보안을 약화시킬 위험도 있다. 시티즌랩의 론 디버트 소장은 미국, 영국, 캐나다 등 각 국의 정보기관들이 '국가안보'를 명분으로 소프트웨어 취약점을 고치도록 하는 것이 아니라 은밀히 이용하거나, IT 업체들과 공모 혹은 협박하여 이용자를 감시할 수 있는 백도어를 만들도록 하거나, 이용자의 기기에 스파이웨어를 설치하는 등 특정 이용자뿐만 아니라 인터넷 전체의 보안을 위험에 빠뜨리고 있다고 비판하고 있다. 또한, 정보기관간, 국가간의 경쟁은 인터넷의 보안을 더욱 약화시키는 악순환에 빠지게 할 것이라고 경고한다. (Ron Deibert, 2014) 지난 2015년, 이탈리아 보안 업체인 해킹팀의 서버가 해킹당하면서 이들이 만든 RCS라는 해킹 프로그램을 국정원 역시 구입, 이용해왔다는 사실이 드러난 바 있다. 국정원 역시 한편으로는 사이버 보안의 컨트롤타워 역할을 하면서, 또 한편으로는 보안을 약화시키는 활동을 하고 있던 셈이다.

넷째, 국내 사이버 보안 관련 법령이 체계성과 일관성을 갖도록 정비 될 필요가 있다.

현재 사이버 보안 관련 법령들은 용어의 정의도 통일되어 있지 않고, 중복적인 내용도 다수 있다. 또한, 사용되는 용어의 의미에 대한 합의가 없다면 사회적으로 다양한 이해관계자 그룹 사이에 건설적인 토론이 힘들어질 것이다. '사이버테러방지법'이나 '사이버안보기본법'만 보아도, 이 법의 지향이나 포괄범위(예를 들어, 국가안보적 측면만을 다루는 법안인지, 사이버보안에 대한 일반법을 목표로 하는지 등)가 모호하여 합리적인 토론이 힘들다. 이런 상황에서 사이버테러방지법안과 같은 또 하나의 유사 법령을 제정하는 것은 이러한 혼란을 가중시킬 뿐이다. 합의된 사이버 보안 전략에 기반하여 관련 법령이 체계성과 상호 일관성을 갖도록 정비되어야 하며, 사이버 보안 관련 기본법이 필요하다면 이러한 정비 과정 속에서 입법이 될 필요가 있다.[134]

[134] 박영철 등(2015)은 '사이버보안기본법'을 제안하며, 이 기본법에 포함되어야 할 내용들을 다음과 같이 제안하고 있다.
1. 사이버보안 법제의 기본이념

다섯째, 국정원 개혁과 사이버 보안 관련 국정원 역할의 이전이 필요하다.

비단 현 박근혜 정부에서 뿐만이 아니라, 지금까지 국정원은 국내 정치에 개입하고 민간인을 사찰해 온 어두운 역사를 갖고 있다. 중앙정보부, 국가안전기획부, 국가정보원 등 여러 명칭으로 정보기관의 이름이 변화되어 왔지만, 그 본질적인 속성에 있어서 달라진 것은 없다. 기획·조정의 이름으로 타부처 고유의 정책 영역까지 관장하고, 대법원 등 독립적 사법기관의 판결에 대해 개입하거나, 민간의 민주적 활동영역에 대한 상시적인 사찰 등을 자행해왔다. '중앙정보'라는 이름으로 모든 정보를 탈법적 중앙집권적 방법으로 수집하고, '국가안전기획'이라는 이름으로 재난, 국방, 경찰 등 모든 안전 영역을 기획·관장하던 시대의 이미지를 탈피하고자 김대중 정부 시절 국가정보원이라는 이름으로 변경했지만 달라진 것은 없었다. 오히려 이번에는 '정보'나 '보안'이라는 단어만 들어가면, 정보기반시설의 보호, 보안적합성 검증 등 민주성, 투명성, 책임성이 반드시 요구되는 영역의 업무까지 국정원이 자기 영역으로 확대해가고 있다.

그 동안 국정원의 정치개입이나 민간인 사찰 논란이 불거질 때마다 수차례 국정원 개혁이 논의되었지만, 국정원의 권한 남용은 중단되지 않았다. 국정원에 대한 신뢰는 '앞으로 잘 하겠다'는 다짐만으로 회복되지 않으며, 권한 남용을 방지할 수 있는 구조적인 개혁이 수반되어야 한다. 국정원의 권한 남용을 방지할 수 있는 방향으로 국정원 개혁이 필요하며, 이는 비단 사이버 보안만의 문제는 아니다. 국정원의 수사권과 기획·조정의 권한을 폐지하고, 국정원은 전문해외정보 수집기관으로 개편해야 한다. 국정원을 비롯한 정보기관에 대한 국회의 감독 권한도 강화될 필요가 있다.

자연스럽게 사이버 보안과 관련하여 국정원이 맡고 있던 역할은 미래창조과학부 혹은 국민안전처 등 다른 부처로 이관되어야 한다. 사이버 보안은 법에서 규정하고 있는 국정원의 업무 범위에 포함된다고 하기 힘들다. 더구나 은밀한 감시와 사찰이 가능한 사이버 공간의 특성 상 국정원이 사이버 보안 업무를 담당하게 된다면, 권한 남용에 대한 우려는 더욱 커질 수 밖에 없다. 표현의 자유와 프라이버시 등 기본권의 보장, 인터넷의 개방과 혁신, 민주적인 거버넌스 등 사이버 보안의 핵심적 가치들이 밀행성, 은밀성이라는 본질적 속성을 가진 정보기관을 통해서 달성될 수 있을까? 애초에 불가능한 영역이라고 해야 한다.

세계 어느 나라에서도 비밀정보기관이 사이버 보안의 실질적인 컨트롤타워 역할을 맡고 있는 나라는 없다. 앞서 해외 사례에서 살펴보았다시피, 해외 대부분의 나라에서는 비밀정보기관이 아닌 일반 정부부처에서 사이버 보안의 정책 수립과 집행 총괄의 역할을 맡고 있다. 미국의 국토안보부, 영국의 내각부 산하 사이버보안청(OCSIA), 일본의 내각관방 산하 사이버보안센터(NISC) 등이 그렇다. 정보기관의 역할은 자신들이 수집한 사이버 위협 등과 관련한 정보들을 타 정부부처 및 관련 민간 기관과 공유하고 기술적으로 지원하는 것에 제한하고 있다. 국정원 역시 해외정보수집기관으로서 이러한 역할에 머물러야 할 것이다.

---

2. 사이버보안 관련 법적 정의 명확화
3. 사이버보안 컨트롤타워의 설정
4. 사이버보안 기본계획 및 시행계획의 구체화
5. 컨트롤타워, 실무추진기구, 정부부처 사이의 협업적 집행체계 명확화
6. 민·관 협력체계의 구축에 관한 사항
7. 민간 및 공공부문의 컨트롤타워를 분리·운영하되 상호 유기적 협력관계를 통한 거버넌스 구축
8. 사이버침해사고의 예장 및 침해대응, 복구 등 대응절차 완비

그런데, 민간 및 공공부문의 컨트롤타워를 분리하자는 일곱번째 제안은 다른 제안들과 모순적인 듯 하며, 좀 더 논의가 필요할 듯 하다.

여섯째, 국정원 개혁과 함께, 사이버 보안 수행 체계도 변화가 필요하다.

현재 주요 기반시설의 경우 정보통신기반보호법에 따른 국무총리 소속의 정보통신기반보호위원회가 컨트롤타워 역할을 하고 있으며, 공공, 민간, 국방 영역을 국정원, 미래창조과학부, 국방부가 각각 관할하고 있다. 국가사이버안전관리규정에 따르면 사실상 국정원이 실질적인 컨트롤타워 역할을 하고 있고, 최고 협의기구로 국가사이버안전전략회의를 두고 있다. 그리고 법령에 반영되어 있지 않지만, 2015년 4월 국가사이버안보 태세강화 종합대책 마련 이후, 청와대(국가안보실 사이버안보비서관)가 컨트롤타워 역할을 하고 있다. 이처럼 현재 국내 사이버 보안 수행 체계는 조직과 법제 측면에서 제대로 정비가 되어 있지 않은 상황이다.

역할이 명확하게 부여된다면, 서로 다른 부처에서 서로 다른 영역을 관장하는 것은 큰 문제가 아니라고 본다. 컨트롤타워는 정치적인 최종 책임단위이기는 하지만, 정책부터 실무까지 모든 것을 담당한다기 보다는 사이버 보안 전략의 방향성을 제시하고, 서로 다른 부처의 활동이 일관성을 갖도록 하며, 부처간 역할을 조정하는 등의 임무를 맡으면 된다. 실무적이고 일상적인 차원의 사이버 보안은 어차피 해당 민간 업체나 기관이 맡을 수 밖에 없다. 또한, 민간 기업의 사이버 보안에 정부가 지나치게 개입하는 것은 민간의 자율성을 침해할 수 있고, 국가 감시의 우려를 불러올 수 있다. 현재 사이버 보안 수행 체계의 문제는 정보통신기반보호위원회와 국정원(혹은 청와대) 등으로 컨트롤타워가 분리되어 있다는 점, 이에 따라 긴급 상황에 대한 대처에서 대응 절차에 혼선이 있을 수 있다는 점, 사이버 보안 관련 국정원의 역할이 지나치게 과도하다는 점 등이다.

컨트롤타워를 반드시 대통령 산하에 두어야 하는 것은 아니지만, 정치적 리더쉽을 확보하는데는 용이할 것이다. 그리고 코디네이터와 별개로 각 부처간 협의체를 둘 수 있다.(현재의 사이버보안전략회의 위상)[135] 공공부문의 사이버 보안은 국정원이 아닌 미래부,

---

[135] ITU는 2011년 발간한 <ITU 국가 사이버보안 전략 가이드>에서 국가 사이버보안 프로그램의 요소로 다음과 같은 10가지를 들고 있다.
1. Top Government Cybersecurity Accountability
2. National Cybersecurity Coordinator
3. National Cybersecurity Focal Point
4. Legal Measures
5. National Cybersecurity Framework
6. Computer Incident Response Team (CIRT)
7. Cybersecurity Awareness and Education
8. Public-Private Sector Cybersecurity partnership
9. Cybersecurity Skills and Training Programme
10. International Cooperation
여기서 National Cybersecurity Coordinator 와 별개로 기관간 기구로서 National Cybersecurity Focal Point를 상정하고 있다.
미국의 경우 사이버 보안 코디네이터 역할을 백악관 산하의 사이버보안조정관이 맡고 있으며, 국토안보부(DHS)는 주요 기반시설 보호를 위한 전반적인 연방정부의 활동을 담당한다.
영국은 사이버 보안에 대한 범정부적 조정 및 전략 제시를 담당하는 내각부(Cabinet Office)가 코디네이터 역할을 하고 있다.
일본은 사이버보안 전략본부가 컨트롤타워 역할을 하며, 내각관방산하 사이버보안센터(NISC)가 사이버보안 전략본부에서 마련한 사회보안 전략을 구체화하고 이를 실행하는 역할을 담당하며, 각 부처간 허브 역할을 한다.
독일의 경우에는 '연방정보기술보안청'이라는 행정기관이 국가의 사이버 보안을 총괄하며, 정부와 주요기반시설의 사이버 보안을 통합적으로 추진하고 있다.(박영철 등, 2015)

국민안전처 등 다른 공공기관으로 이관되어야 한다.[136] 민간부문의 경우 정부는 적절한 가이드라인을 제시하고, 이를 준수하도록 유도하는 방식이 바람직할 것이다. 민간에 자율성을 주는 동시에 사이버 보안 사고에 대한 책임 또한 부여하는 것이다. 또한, 사이버 보안과 관련된 집행 과정이 언론, 국회, 시민들의 감독을 받을 수 있도록 해야 한다.

일곱째, 사이버 보안 정책의 수립과 집행은 공개적이고, 관련 이해관계자들의 자유로운 참여와 협력에 기반하여 이루어져야 한다.

국제기구 및 세계 주요 국가들은 모두 민간 주도의 사이버 보안, 이해관계자들의 협력을 강조하고 있다. 국내 사이버 보안도 국가주도의 사이버 보안 체제에서 벗어나야 한다. 사이버 보안 관련 정보들은 투명하게 공개되어, 다양한 이해관계자가 의견을 표명할 수 있도록 해야 한다.

여덟째, 이 보고서에서 자세히 다루지는 않았지만, 이용자 보안에서 핵심적 중요성을 가지는 것 중의 하나가 안전한 암호의 사용이다. 여전히 일반 이용자들에게 암호의 사용은 불편하거나 어렵게 느껴지는데, 이용자들이 쉽게 암호를 이용할 수 있는 환경-예를 들어, 이메일 암호화, 보안웹접속(HTTPs)의 보편화, 스마트폰 암호화 등-이 만들어져야 한다. (Mozilla, 2015) 암호화와 관련한 국제적인 논란이 되고 있는 것은 암호기술의 사용과 암호화된 콘텐츠에 대한 법집행기관의 요구 사이의 긴장이다. 그러나 90년대 미국의 암호 전쟁(Crypto War)에서 교훈을 얻을 수 있듯이[137], 법집행 기관의 필요에 의해 암호 시스템에 백도어를 만들어 놓는 것은 해당 이용자 뿐만 아니라, 인터넷 전체의 사이버 보안을 위협할 수 있다. 국내 사례를 보자면, 지난 2014년 카카오톡 감청 논란이 있은 이후, 카카오톡에서 종단간 암호화를 적용한 '비밀채팅' 기능을 도입한 것을 들 수 있다. 그런데 현재 정부와 여당인 새누리당은 통신사 및 인터넷 서비스 사업자로 하여금 감청 설비 구비를 의무화하고자 하는 통신비밀보호법 개정안을 추진 중이다.[138] 이 법안은 암호화라는 용어를 쓰고 있지는 않지만, 이 법이 통과된다면 카카오톡의 비밀채팅 기능이 위법화될 위험이 있다는 점에서 이 법안은 세계적인 암호화 논쟁과 연결된다. 모든 통신 사업자로 하여금 감청 설비를 도입하도록 의무화하는 것은 자신들도 볼 수 없는 안전한 통신 서비스의 개발을 금지하는 것이며, 통신 서비스에 백도어를 만들어 놓는 것이나 다름없다.

아홉째, 사이버 보안을 위한 위협정보 공유는 필요하지만, 이용자의 프라이버시를 침해하지 않도록 보장해야 한다.

'위협 정보'에는 개인의 민감한 통신 내용이 포함될 수 있으며, 실제 사이버 위협과 관련이 없는 이용자들의 정보나 통신 역시 포함될 수 있다. 프라이버시 보호를 위한 엄격한 조치없이 이 정보를 민간과 공공기관이, 심지어 수사기관이나 정보기관이 공유할 수 있도록 하는 것은,

---

[136] 미국의 경우에는 911 테러 직후에는 국토안보부가 사이버 보안의 컨트롤타워 역할을 하고 있었으며, 오바마 정부 출범 이후 2009년 <사이버공간 정책 리뷰(Cyberspace Policy Review)>를 통해 백악관 내 사이버조정관이 컨트롤타워 역할을 맡는 체제로 변화하였다. 그러나 여전히 사이버조정관은 부처간 역할 조정 등 코디네이터의 역할을 하고, 사이버 보안 집행에 있어서의 중심적인 역할은 국토안보부가 하고 있다고 볼 수 있다. 우리 역시 청와대가 컨트롤타워 역할을 하더라도, 국정원이 아닌 별도의 부처가 현재 '국가사이버안전센터'와 같은 사이버 보안 집행 총괄을 담당할 수 있을 것이다.

[137] Andi Wilson, Danielle Kehl and Kevin Bankston, Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s, 2015.6.17, http://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/

[138] 18, 19대 국회에 '감청설비 구비 의무화'를 내용으로 하는 통신비밀보호법 개정안이 발의되었으나 임기만료로 폐기된 바 있다.

미국에서 사이버보안 정보 공유법을 둘러싸고 논란이 되었듯이 영장주의를 잠탈할 위험성이 있다. 사이버 위협 정보의 공유뿐만 아니라, 사이버 보안 정책 전반적으로 이용자 프라이버시 보호를 보장하기 위하여, 사이버 보안 정책 논의 기구에 개인정보 감독기구인 개인정보보호위원회도 참여해야 한다.[139]

[139] 독일의 경우, 사이버 보안에 의해 침해 또는 위협받을 수 있는 개인의 권익 보호를 위해 보호조치 기준의 마련에서부터 개인정보보호감독기관의 관여를 인정하고 있다고 한다. (박영철 등, 2015)

# 참고문헌


- 국가정보원.미래창조과학부.방송통신위원회.행정자치부, 2016 국가정보보호백서, 2016.4
- 국가정보원.미래창조과학부.방송통신위원회.행정자치부, 2015 국가정보보호백서, 2015.4
- 국회의원 김재경, '국가 사이버안보 전담기구'『사이버보안청』설립 필요, 2014년도 국정감사
- 국회의원 진성준 등, 정책자료집 <국가정보원 개혁을 위한 제안서>, 2013.2
- 김도승(2016), 사이버안보의 복합적 특성과 국가사이버안보기본법(안), 2016.10, 2016년 공동학술대회 <국가사이버안보법제의 제정필요성과 법적 쟁점>
- 김은혜, 이재일, 미 오바마 정부의 사이버보안 주요정책 및 법안, 2011.8, 인터넷 & 시큐리티 이슈
- 박영철 등(2015), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 2015.12. 한국인터넷진흥원 위탁연구.
- 배병환 등(2014), 영국의 사이버보안 추진체계 및 전략 분석, 2014.8, INTERNET & SECURITY FOCUS
- 배병환, 송은지(2014), 주요국 사이버보안 전략 비교. 분석 및 시사점 - 미국, EU, 영국의 사이버보안 전략을 중심으로-, 2014.11, 정보통신방송정책 제26권 21호
- 송은지, 강원영(2014), 미국 오바마 정부 2기의 사이버보안 강화 정책, 2014.9, INTERNET & SECURITY FOCUS
- 이연수 등(2009), 주요국의사이버안전관련법·조직체계비교및발전방안연구, 2009
- 이은우, 사이버테러방지법, 무엇을 노리는가? - 국가권력에 의한 사이버보안관제의 위험성, 2016.3.22, 테러방지법과 사이버테러방지법의 문제점 진단 토론회 <국정원의 국민사찰 고삐 풀리다>
- 임종인(2016), 국가사이버보안 정책과 Think Tank의 역할, 2016.7
- 장규현. 임종인(2014), 국제 사이버보안 협력 현황과 함의 : 국제안보와 UN GGE 권고안을 중심으로, 2014.3.17, 정보통신정책연구원, 정보통신방송정책 제26 권 5호
- 진보네트워크센터, 2015년 사이버스페이스 세계회의(GCCS 2015) 참가 보고서, 2015.4.22, http://act.jinbo.net/wp/8646/
- 한국인터넷진흥원, 주요 국가별 사이버방어 체제 및 대응 동향, 2014.11, KISA Bimonthly 4호
- Andi Wilson, Danielle Kehl and Kevin Bankston, Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s, 2015.6.17, http://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/
- Anja Kovacs & Dixie Hawtin, Cyber Security, Cyber Surveillance and Online Human Rights, 2012.6.29 http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf
- Anna-Maria Osula(2015), National Cyber Security Organisation: UNITED KINGDOM, 2015, CCDCOE
- Internet Society(2012), Some Perspectives on Cybersecurity 2012, 2012.11.16, http://www.internetsociety.org/doc/some-perspectives-cybersecurity-2012
- HM Government, NATIONAL CYBER SECURITY STRATEGY 2016-2021, 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- ITU(2011), ITU National Cybersecurity Strategy Guide, 2011.9
- Mozilla, Mozilla Cybersecurity Delphi 1.0 : Towards a user-centric policy framework, 2015.7
- Piret Pernik 등(2016), National Cyber Security Organisation: UNITED STATES, 2016, CCDCOE
- Ron Deibert(2014), The Cyber Security Syndrome, 2014.11.25, https://www.opencanada.org/features/the-cyber-security-syndrome/
- SASAKAWA USA(2016), Cyber Security in Japan, A Real Quick Overview, 2016, http://spfusa.org/wp-content/uploads/2016/03/20160322-Cyber-Security-in-Japan-Overview.pdf
- Sean B. Hoar, Congress Passes the National Cybersecurity Protection Act: Codifies National Cybersecurity Center & Creates Federal Agency Data Breach Notification Law, 2014.12.18, http://www.privsecblog.com/2014/12/articles/cyber-national-security/congress-passes-the-national-cybersecurity-protection-act-codifies-national-cybersecurity-center-creates-federal-agency-data-breach-notification-law/
- Tim Maurer and Robert Morgus(2014), Compilation of Existing Cybersecurity and Information Security Related Definitions, 2014.11.5, http://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/