이상적인 사이버 안보 거버넌스 모델 구축 논의를 위한 워크숍

목차

EWHA,
THE FUTURE
WE CREATE

01 사이버 안보, 무엇이 문제인가?

1) 국내 법제 변화

2017년 정부가 제출했던 '국가 사이버안보 법안'의 입법 추진 취지

1) "국가사이버안전관리규정"이 있으나, 이는 국가 및 공공기관에만 해당하기에
체계적인 대응의 근거 법령으로서 미흡

2) 국가정보원은 공격에 대한 분석 및 대응에 있어 기술력을 지니고 있으며,
사이버안보 분야에서 국가정보원이 실제 주도적 역할을 수행

3) 북한이라는 변수를 지니고 있기에 다층적인 안전장치 필요

01 사이버 안보, 무엇이 문제인가?

1) 국내 법제 변화

국내 법제 변화와 사이버 안보 체제 정비

국가 전략적 차원에서 보았을 때, 사이버 안보 시스템은 총괄적 통제 기구가 부재한 상태

(공공부문/국가정보원 민간부문/ 한국인터넷진흥원 군/ 사이버작전사령부 관할로 분장)

이에 2021년 '국가사이버안보센터'로 재정비,
1급 조직으로 격상 및 국가와 국제사이버 체계 강화 추진

-> 국가 사이버 안전 정책 총괄, 사이버 위기 예방 활동, 사이버 공격 탐지 활동,
사고 조사와위협 정보 분석 업무를 담당

2) 이슈 정리 _

미국 NSA 기밀자료 폭로 사건

- 2013년, NSA 계약 요원이 미국 국가안보국인 NSA와 영국의 GCHQ등의 정보기관들이 전세계의 민간인들의 통화 기록과
인터넷 사용 정보등의 비밀정보수집 프로그램을 통해 무차별적으로 수집과 사찰을 해온 사실을 폭로하는 사건 발생

- 이와 관련하여 2015년도, 내부 고발자는 한국 어디든 도청과
감청이 가능하다고 언급하며, 실제로 올해 2023년 4월에 불거진
도청 의혹에 대한 문제점 확인 가능

NSA 내부 고발자 에드워드 조지프 스노든

01 사이버 안보, 무엇이 문제인가?

2) 이슈 정리 _

국내 북한 천산망을 노리는 북한의 사이버 공격

- 북한의 정찰총국이 배후인 해커 조직 '라자루스'가 지난 2021년 4월부터 KT 그룹 금융보안 전문 기업 소프트웨어 취약점을 공격할 준비하는 사례 발생

- 2022년 6월부터 워터링홀 수법으로 국내외 61개 주요 기관 PC 207대 해킹 발생
- 이에 한국 정부는 라자루스를 사이버 분야 대북 독자 제재 대상으로 지정

01 사이버 안보, 무엇이 문제인가?

2) 이슈 정리 _ 국내외

우크라이나 전쟁으로 인한 사이버 위협

- 온라인상에 유출된 1급 국가 기밀 문서:
  '한국정부의 우크라이나 전쟁 관련 포탄 지원'에 대한 구체적인 수치가 담긴 문건이 존재

- 사건 발생 후 현정부가 인터뷰를 통해 우크라이나에 대한 군사 지원 가능성을 밝힘
- 러시아는 지원에 대한 반발 발생, 러시아와의 관계 악화 가능성 제기

→ 이는 곧 한국을 겨냥한 사이버 공격 우려로 다가올 수 있는 문제점으로 번질 수 있음

01 사이버 안보, 무엇이 문제인가?

2) 이슈 정리 _

• 중국 반한 감정, 대만 이슈로 이어지는 사이버 위협

- 중국 해커 집단으로 추정되는 '샤오치잉'은
  한국을 상대로 사이버 공격을 벌이겠다고 선전포고,
  이후 국내 연구 소나 학회 웹사이트 등 상대적으로 보안이 약한 기관 사이트 공격
- 현정부는 인터뷰를 통해 양안 관계 긴장 고조에 대해
  대만 문제 언급, 중국은 이에 대한 반발과 함께 반한 감정 고조
- KISA 조사 결과에 따르면 '샤오치잉'은
  취약점을 악용 및 공격을 이어나간 것으로 밝힘

晓骑营

CYBER SECURITY TEAM

01 사이버 안보, 무엇이 문제인가

3) 법과 현실 사이의 괴리

1) 처벌

: 사이버 범죄에 대한 처벌 수위 강화를 지적

2) 규제

: 공공에서 사이버 안보 신규 규제 설치 필요성 설명 필요와 기업의 정보 보안 기술 및정보 지원 병행 필요

3) 거버넌스

: 정보보안 거버넌스 체계 구축과 사이버 관련 사건 발생 시 대응 계획 및 로드맵, 정보보안 전략 도입 등 관련 정책 도입 필요성 강조

4) 커뮤니케이션

: 정부부문에 관한 질문 응답의 전문가 의견이 수렴되고 있지 않는 문제점 발생

01 사이버 안보, 무엇이 문제인가?

4) 쟁점 제시

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 분석

- 국제 동향 비교 분석
- 미국의 사이버 안보 전략과 추진 체계

2000년대	2003. 2.	2008. 9.	2009. 5.
9.11 테러 발생	NSSC 발표	CNCI 발표	CPR 발표
사이버 안보 국가 전략 형성 본격화	• National Strategy to Secure Cyberspace • 부시 행정부	• Comprehensive National Cybersecurity Initiative • 부시 행정부 • 국가안보 차원에서 최초로 문제 인식, 대응책 마련	• Cyberspace Policy Review • 오바마 행정부 • 미국 사이버 안보전략의 근간을 형성한 전략서

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 분석

- 국제 동향 비교 분석
- 미국의 사이버 안보 전략과 추진 체계

사이버안보법 (Cybersecurity Act)

2015년 12월 최종 통과

CISA(Cybersecurity Information Sharing Act)를 중심으로 법안을 통합·조정

민간분야가 소유한 양의 개인정보를 연방정부에 넘기도록 하는 정보 공유 체계 구축

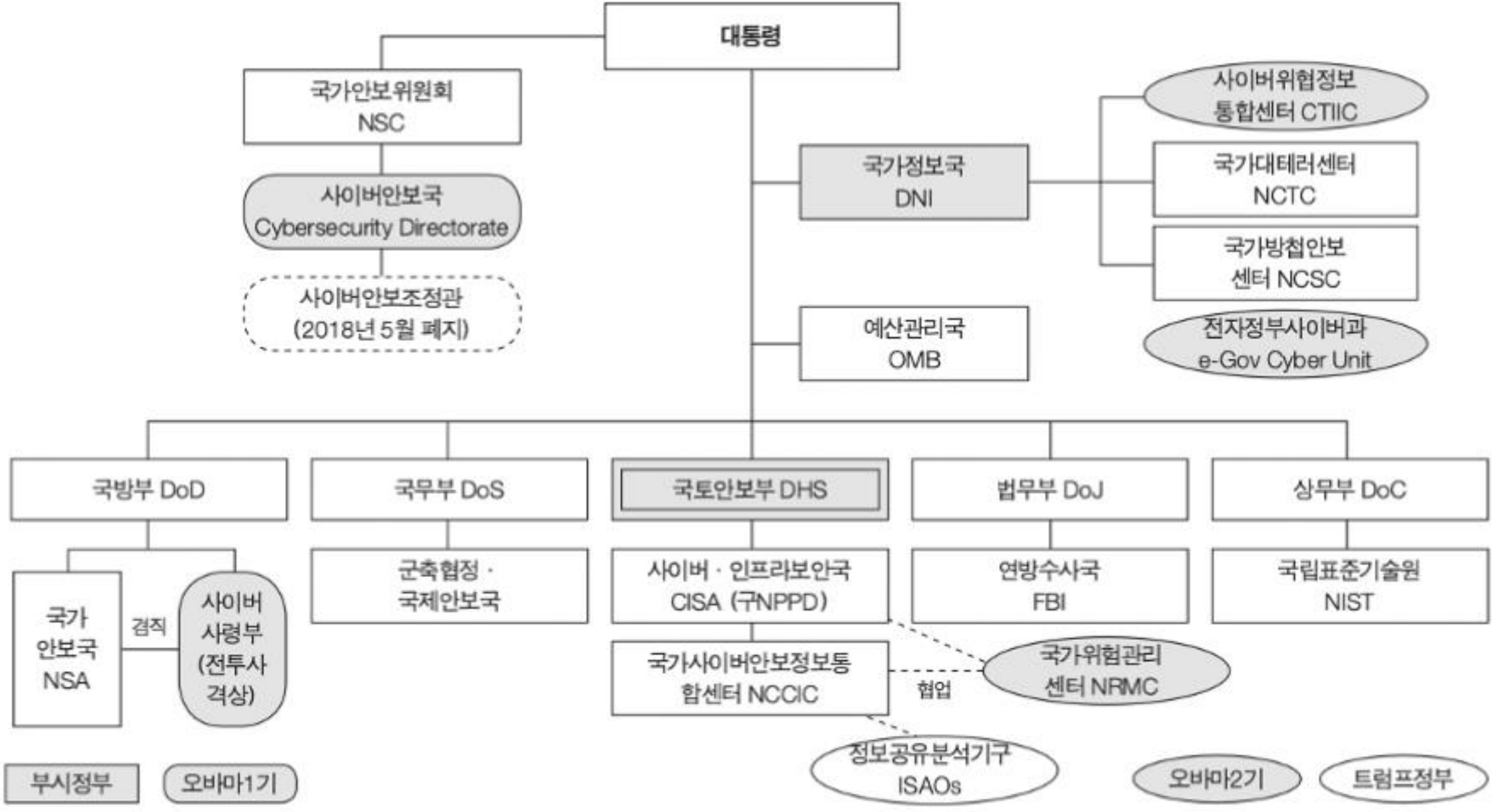


그림 2-1. 미국의 사이버 안보 추진체계

출처: 김상배(2018a), p.155를 보완 · 수정

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 분석

- 국제 동향 비교 분석
- 일본의 사이버 안보 전략과 추진 체계

2000년대 초반

E-JAPAN 전략 발표

2015. 6.

일본연금기구에 대한 대규모 해킹 사건 발생

2015. 9.

'사이버시큐리티전략' 발표

- 내각사이버시큐리티센터의 기능 강화
- 조사 및 감시대상 확대

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 분석

- 국제 동향 비교 분석
- 일본의 사이버 안보 전략과 추진 체계

사이버시큐리티기본법

2014년 11월 제정, 2015년 2월부터 시행

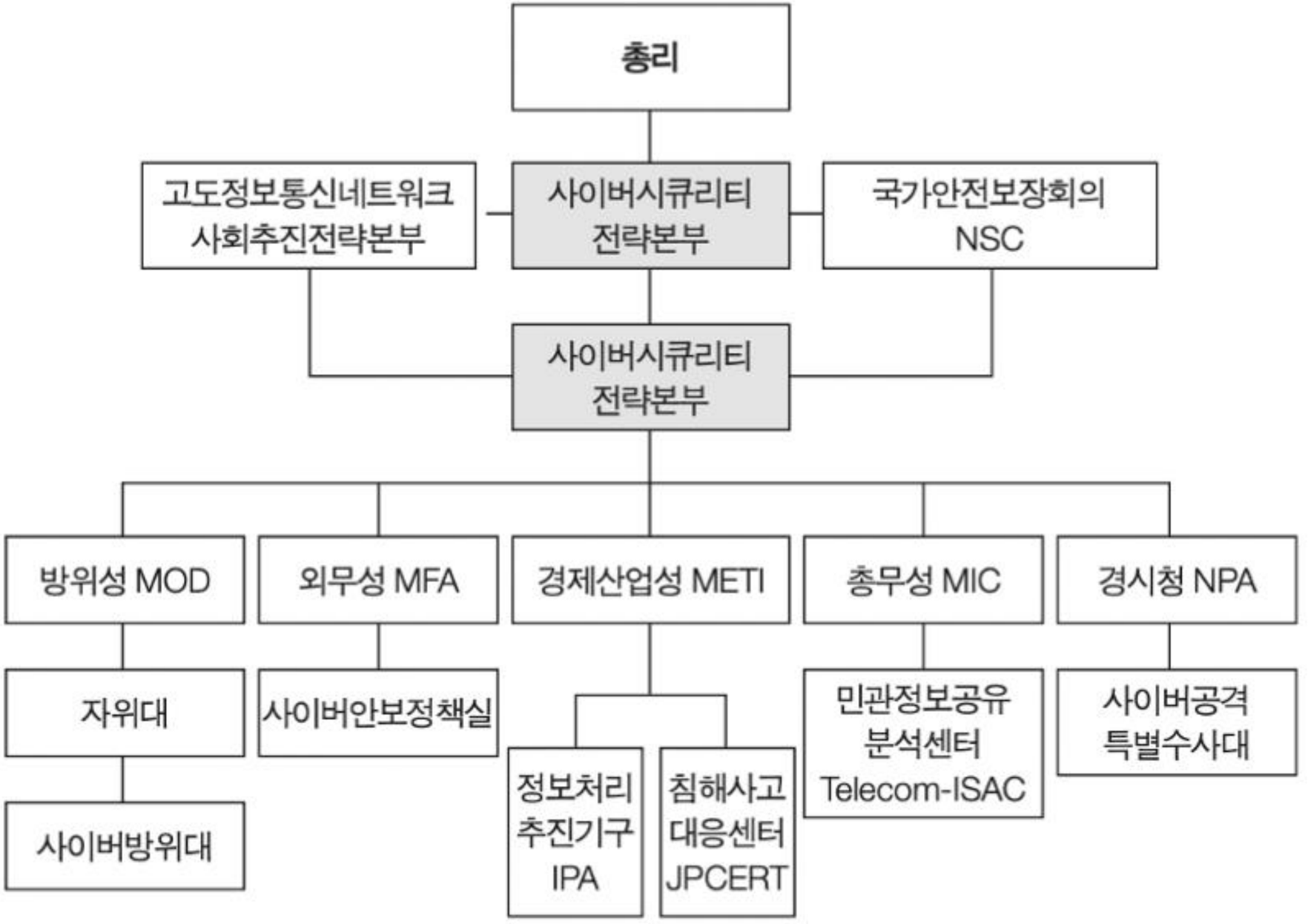


그림 2-2. 일본의 사이버 안보 추진체계

출처: 김희연(2015), p.52를 기반으로 보완하여 작성

02 현실과 이상 사이의 괴리는 무엇인가

1) 쟁점 분석 ?

- 국제 동향 비교 분석
- 중국의 사이버 안보 전략과 추진 체계

시진핑 체제	2014. 2.	2016. 12.
공격적인 사이버 안보전략 추구	시진핑 주석, '안전한 네트워크 구축이 향후 중국 국가이익의 핵심이 될 것'이라 전망	국가사이버공간안전전략 발표 • 사이버 안보 이념/정책 • 최초의 전략서

02 현실과 이상 사이의 괴리는 무엇인가

1) 쟁점 분석 ?

- 국제 동향 비교 분석
- 중국의 사이버 안보 전략과 추진 체계

신국가 안전법

2015년 7월, 중국 전국인민대표회의

사이버 공간의 테러와 해킹에 대응하는 핵심 기반시설의 보안 심사 및 안전평가, 중국의 주권수호 활동 명분 마련

인터넷 안전법

2016년 12월

온라인 실명제 도입 등

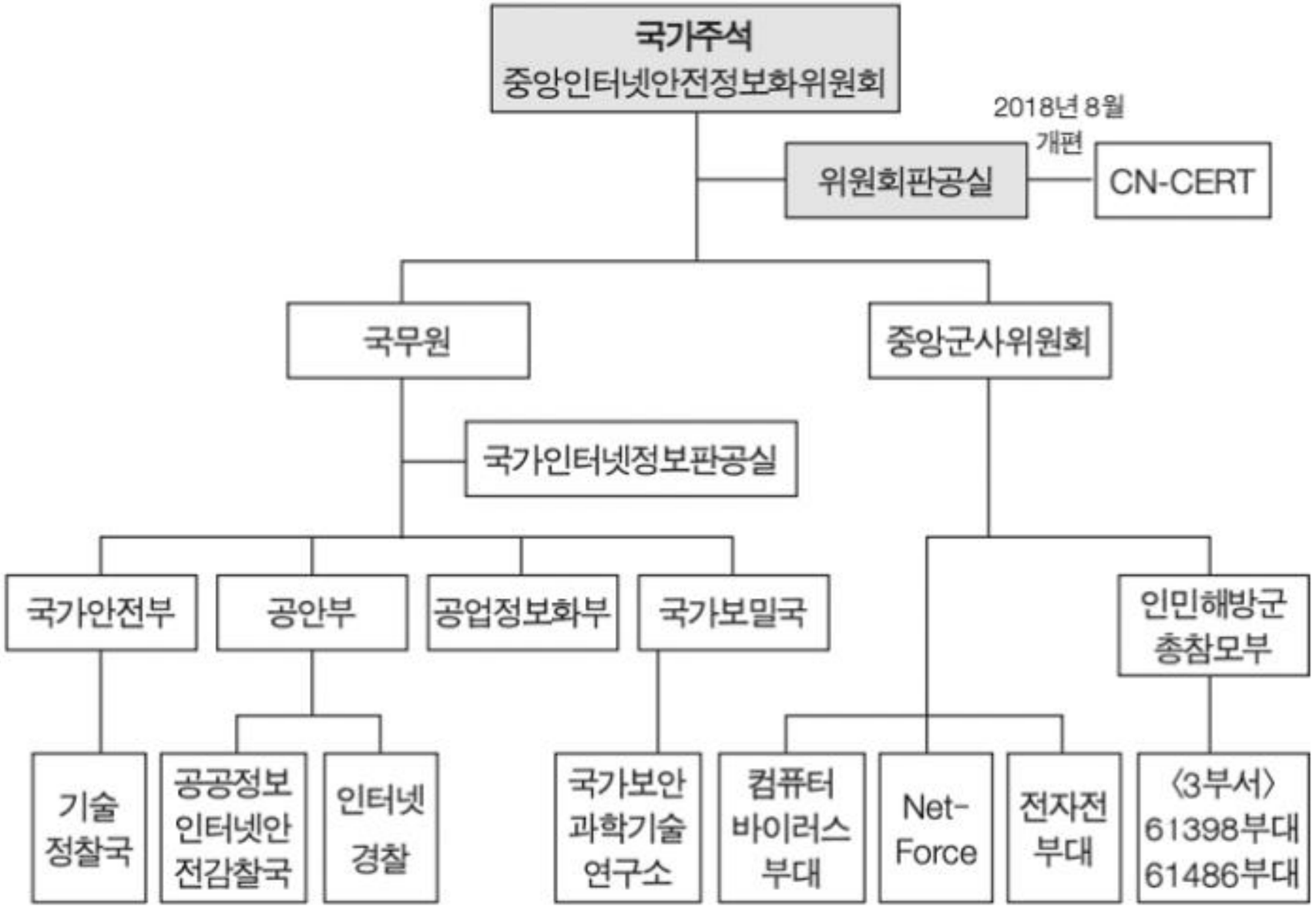


그림 2-3. 중국의 사이버 안보 추진체계

출처: 김희연(2015), p.49를 수정 · 보완

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 분석

- 국제 동향 비교 분석
- 러시아의 사이버 안보 전략과 추진 체계

2002

- 세계 첫 해커부대 창설
- 사이버 전문 인력의 양성 및 기술 개발 적극 추진
- 물리적 전쟁을 위한 지원역량으로 활용

2010

- 미국과 이스라엘이 스턱스넷으로 이란의 핵 시설 공격

-〉 러시아의 사이버 안보에 대한 관심 본격화

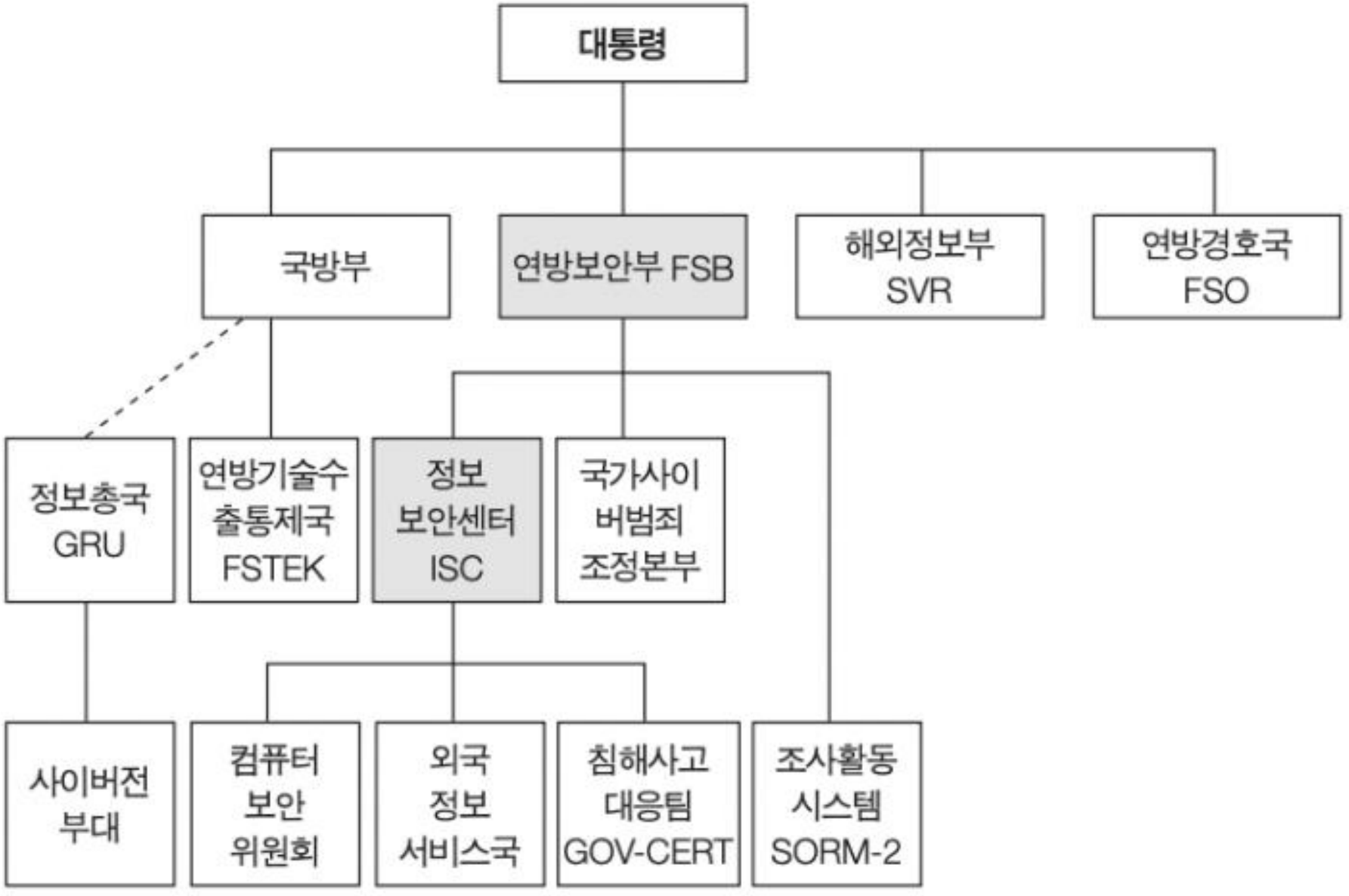
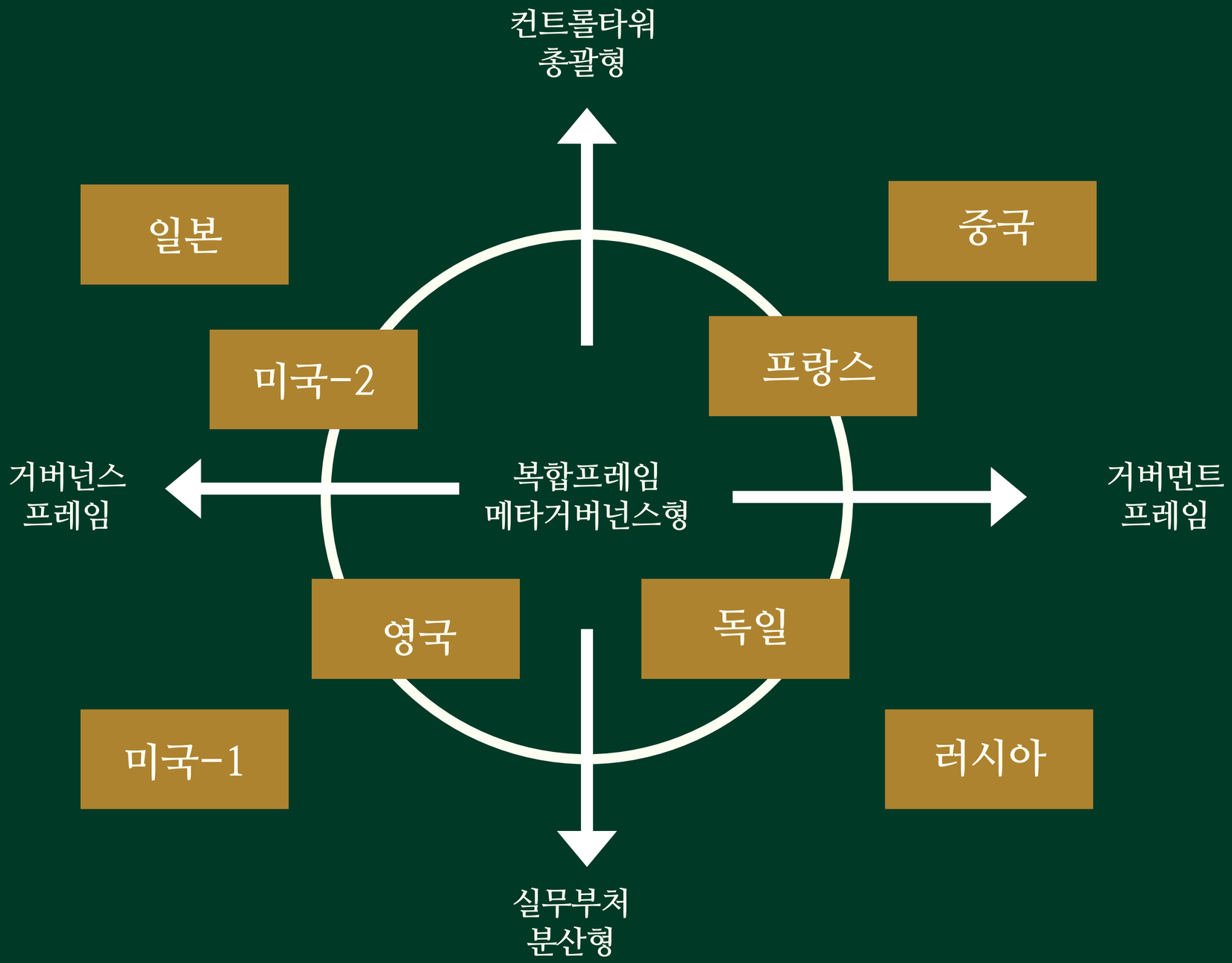


그림 2-4. 러시아의 사이버 안보 추진체계

출처: 조성렬(2016), p.405를 수정 · 보완


컨트롤타워
총괄형
일본
중국
미국-2
프랑스
거버넌스
프레임
복합프레임
메타거버넌스형
거버먼트
프레임
영국
독일
미국-1
러시아
실무부처
분산형

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 분석

2. 사이버 안보 기본법의 한계

공공/민간 부문의 분리

공공 부문: 국가정보원
국가사이버안전관리규정
및
사이버안보업무규정 기반
민간 부문: 과학기술정보통신부
정보통신망법 등 근거로
사이버공격 예방 및 대응
업무 담당

한계

통합법/거버넌스 필요

한국의 사이버안보 관련 법은 다양한 법령 및 훈령에 흩어져 있음

법정 대응체계 분산으로 처리와 수습 과정의 혼선

-> 일원화된 업무 수행의 필요성

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 1 컨트롤타워

사이버범죄 발생 증가와 검거율 저하

팬데믹 장기화로 인한 사이버안보 위험 심화

북한의 국가기반시설 사이버공격 위협 증가

사이버안보 침해와 피해의 국제적 동향

사이버범죄의 국가안보 문제화

'국가 사이버안보 대응역량 강화', 국정과제 제시

- 최초로 사이버안보가 독립된 국정과제로 선정
- 사이버안보 분야의 국제 질서 정립 차원까지 시야 확장

02 현실과 이상 사이의 괴리는 무엇인가?

1) 쟁점 컨트롤타워

공공 부문	민간 부문	군사 부문
국가정보원	한국인터넷진흥원	사이버작전사령부

다수 부처에 책임 및 역할 분산

- 사이버 공간에 대한 국가적 책무를 다하기 위해 민관협력과 시민참여 적극 수용 필요
- 컨트롤 타워를 정하는 문제, 역할 배분 문제에 대해 적극적 협의 필요

2. 통제기구의 부재: 북한의 사이버 위협

사이버 위협으로 '북한'이 지목되는 경우 빈발

- 사이버보안이 취약해진 상황을 북한이 악용
- 해커 양성 및 관리를 통해 외국 진출 -> '사이버 외화벌이'

한국의 경우: 사이버 안보 분야 기본 법제가 미비

범정부 차원의 컨트롤 타워 구성이나 민간 사이버 안보 협력에 한계

3. 국정원의 역할 규정

기관별로 분리된
국가 사이버 위협 업무 및 대응 체계를
하나로 모아
통합적인 대응 강화 필요성

중심 역할을 수행할 '국정원'의 역할 규정

문제

- 민간인 감시/사찰
- 막강한 권한과 영향력 행사 우려

1. 민관협력

(1) 법안이 제시하는 민관 합동 사이버협력체계의 중요성

2017년 정부법안 제3조 제2항

: 국가·지방자치단체 및 기업은 사이버안보가 국가 안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하여 사이버공간을 보호하도록 노력하여야 한다

• 민관협력

(1) 법안이 제시하는 민관 합동 사이버협력체계의 중요성

-제 6조(정보공유시스템 구축):

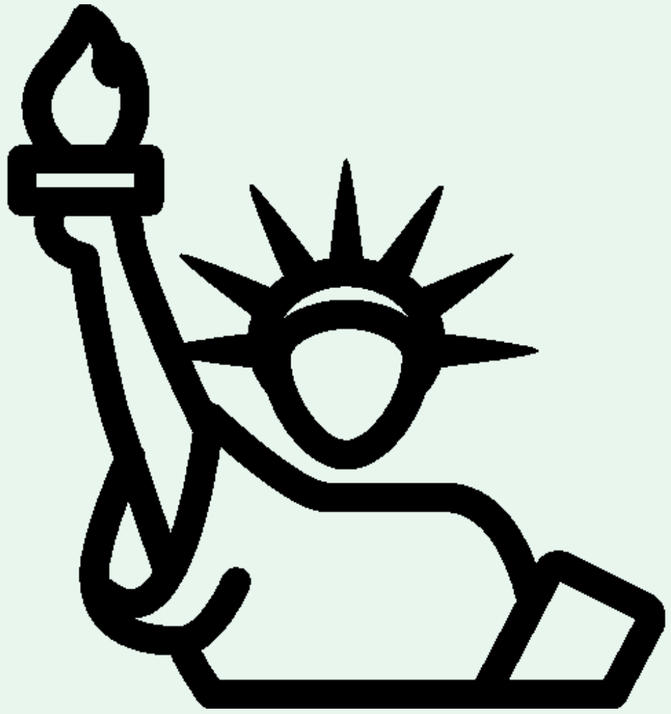
① 국가정보원장은 사이버안보 관련 정보를 중앙행정기관등에 배포·공유하기 위하여 정보공유시스템을 구축·운영할 수 있다.

② 제1항에 따른 정보공유시스템의 활용 대상 및 범위 등 운영에 필요한 사항은 국가정보원장이 관계 중앙행정기관등과 협의하여 정한다.

→ **법적으로 개인정보에 대한 권한이 정확히 명시되어 있지 않음**

- 민관협력

(2) 사이버 협력 체계의 개선점 – 국민의 자유와 인권보장



• 민관협력

(2) 사이버 협력 체계의 개선점 – 개인정보 침해 관련 우려점

• 민관협력

(2) 사이버 협력 체계의 개선점 – 미국 CISA

- 미국 CISA 벤치마킹을 통한 구체적인 가이드라인 구축

자율성 정보공동체

• 민관협력

(2) 사이버 협력 체계의 개선점 – 민간 협력을 위한 기구 창설

- 사이버 안보 총괄 지휘 및 민간 협력 관련 기구 창설

• 주요쟁점 정리

(1) 타국의 사이버 안보 대처법은 일원화된 공조체계를 통해 이루어짐

(2) 한국 사이버 안보 대처기관의 문제점

- 컨트롤 타워의 대표성 부실
- 통제기구의 부재
- 민관의 모호한 역할 규정

민간협력이 가능한 공조기관의 개설

국내:

한 기관으로서 국내 사이버 안보에 대처

국외:

사이버 안보 담당 기관으로서 사이버 안보와 관련된 외교정책에 관여,

입장정리에 참여하도록 함

공조기관을 통한 외교 정책 구성

기존 미국 중심적인 체제 지지

VS

유럽국의 새로운 안보 체제 지지

사이버 안보 공조기관의 입장을 거쳐가는 절차가 필요함