Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.5, Oct. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.5.1259

주요국 사이버보안 거버넌스 분석과 정책적 시사점

주 문 호,† 권 헌 영, 임 종 인‡
고려대학교 정보보호대학원

Cyber Security Governance Analysis in Major Countries and Policy Implications

Moon-ho Joo,† Hun-Yeong Kwon, Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

최근 전 세계적으로 사이버위협이 일상화되었으며, 그 범위 또한 단순한 개인의 장난과 사이버 범죄 수준을 넘어 대규모 범죄조직과 국가 주체가 개입된 사이버 테러 및 전쟁으로 확대되고 있다. 이러한 흐름 속에서 빠르게 국가 차원의 대응 전략을 세우지 않는다면 우리나라도 정보통신 강국에서 사이버보안 취약국의 지위로 순식간에 전락할 것이며, 우리의 발달한 정보통신망은 세계가 부러워하는 4차 산업혁명의 기반시설이 아니라 국민 생활에 큰 위협을 가져오는 공격의 매개체가 될 것이다. 국가적 차원에서의 사이버 보안은 민·관·군 등 다양한 주체들이 참여하여 다양한 분야의 위협정보를 신속히 공유하고 사고 예방을 위한 대비책을 마련하며 유사 시 유기적으로 대응할 수 있을 때 보장될 수 있다. 이러한 점에서 각 부처, 각 주체들의 역할과 책임, 권한이 명확하게 부여되어야 하며, 이를 관리·조율하며 소통할 수 있는 체제를 구축하기 위한 효과적인 국가 사이버보안 거버넌스의 수립이 요구된다.

이에 본 연구는 실용적이고 효율적인 차세대 국가 사이버보안 거버넌스의 정립을 위해 최근 국가 사이버보안 전략을 발표하여 사이버보안 거버넌스 체계를 신속히 정비해나가고 있는 미국, 독일, 영국, 일본, 중국 그리고 한국의 사이버보안 전략, 법령, 조직 및 추진 부처별 역할에 대한 분석을 실시한다. 특히 실질적인 거버넌스 구성을 파악하기 위해 국가의 주요 사이버보안 기능 분류 기준을 제안하고, 해당 분류 기준에 따라 국가 사이버보안 기능별 담당 기관과 수행 전략을 분석한다. 본 연구는 해당 분석 결과를 바탕으로 국내 사이버보안 거버넌스 개선을 위한 시사점과 개선 방향을 제시하였다.

ABSTRACT

This study analyzes cyber security strategies, laws, organizations, and the roles of the ministries in the US, Germany, UK, Japan, China, and Korea and draws implications for establishing a practical and efficient next generation national cyber security governance. Under this goal, this study analyzes cyber security strategies, laws, organizations, and the roles of the ministries in the US, Germany, UK, Japan, China, and Korea and draws implications for establishing a practical and efficient next generation national cyber security governance. Based on the results of this analysis, this study suggests suggestions and directions for improvement of domestic cyber security governance.

Keywords: Cybersecurity, Governance, Strategy, National Cybersecurity, Laws

Received(06. 04. 2018), Modified(1st: 109. 03. 2018, 2nd: 09. 19. 2018), Accepted(09. 20. 2018)

† 주저자, mhjoo@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr(Corresponding author)

I. 서 론

최근 남북 간 긴장 완화 분위기 가운데서도 북한발 사이버 공격은 계속되고 있다[1]. 남과 북이 판문점에서 정상회담을 진행하고 있는 도중에도 북한 해커그룹의 사이버 간첩활동은 지속된 것으로 확인되었고[2], 2018년 4월 27일 판문점 선언 내에 사이버 공간에 대한 명시적 합의가 없었던 만큼, 북한의 사이버 위협에 대해 안심하기에는 아직 이른 상황이다. 또한 북한이 대표적인 비대칭 전략 자산인 핵무기를 포기하게 된다면, 사이버 간첩활동 및 외화벌이를 목적으로 또 다른 비대칭 전력인 사이버 공격 역량 강화에 더욱 집중할 가능성도 무시할 수 없다.

최근엔 북한의 사이버 위협뿐만 아니라 미국과 중국 그리고 러시아를 비롯한 주요국들을 중심으로 '사이버 신냉전' 체제가 구축되고 있으며[3], 이에 따라 미국, 일본, 독일, 영국은 물론 이스라엘 등의 사이버안보 강국들이 새로운 '국가사이버전략'을 발표하면서 사이버 전략우위를 확보하기 위하여 각축을 벌이고 있는 상황이다[4]. 이러한 흐름 속에서 우리나라도 빠르게 국가 차원의 대응 전략을 마련하지 않는다면, 정보통신 강국에서 사이버보안 취약국의 지위로 순식간에 전락할 수 있다.

우리나라는 아시아태평양 국가 중 가장 사이버 공격에 취약한 국가이며[5], 국가 차원의 사이버 공격과 더불어 개인 차원에서의 정보 유출, 피싱 등 사이버 범죄, 기업의 영업비밀과 국가 주요 기밀 유출 등 피해사례도 꾸준히 증가하고 있는 추세에 있다. 이러한 피해는 실제 정치·경제·군사·사회·문화 등 분야를 막론하고 확산되어 국가 안보를 위협하는 수준에 이르렀으며 정부, 금융, 방송, 통신 등 주요 국가기반시설을 대상으로 하는 사이버 위협도 지속되고 있다. 나아가 기술의 발전으로 사이버 위협의 양과 질은 지금까지와는 다른 수준에 이르렀기에 물리적 공간과 사이버 공간, 국가와 민간, 정치와 경제 등 분야를 구분하는 것은 무의미해졌다. 즉, 민·관·군 등 다양한 주체들이 참여하여 다양한 위협정보를 신속히 공유하고 사고 예방을 위한 대비책을 마련하고, 유사시 유기적으로 대응할 수 있는 국가적 차원에서의 사이버 보안 체계가 간절히 요구되는 시점이 된 것이다. 이를 위해서는 사이버보안과 관련된 주요 부처들의 역할과 책임, 권한 등이 명확히 부여되어야 하며, 이를 관리·조율하며 소통할 수 있는 효과적인 국가 사이버안보 거버넌스의 수립이 필요하다.

우리나라는 2005년부터 범정부 차원의 사이버위기 대응체계와 다양한 대책을 마련해오고 있으며 사이버 안보 체계 수립, 인력 양성, 연구 개발 지원 등의 노력들을 수행하여왔으나, 실질적인 국가 사이버 안보 강화로 이어지지 못하였으며 다양한 사이버 공격에도 효과적으로 대응하지 못하고 있다[6]. 이는 다양한 이유가 있을 것이나 사이버보안 강화와 안전 유지라는 목표를 위해 원칙 기반의 구조를 정립하기보다는 부처 이기주의와 기관별 이해관계에 의한 역할 및 책임 분배에 따른 효율적 대응의 어려움, 국가 사이버보안 컨트롤타워의 부재, 인권 및 프라이버시 침해에 관한 국민들의 우려, 정보 공유 체계 및 민관 협력의 효율성 부재 등이 주요 원인으로 꼽힌다[7][8]. 또한 사이버보안 거버넌스가 역할과 책임, 관계 등을 다룬다는 점에서 명확한 법적 근거를 요함에도 불구하고 사이버보안 관련 주체들의 역할과 책임이 법률에 의해 부여되고 있지 못한 상황이다. 미국, 일본 등 주요 선진국들은 2000년대 초반부터 사이버 위협에 대응하기 위한 국가적 차원의 대응 체계를 수립하여왔으며[4], 관련 법적 권한과 역량 강화를 위해 조직 구조 개편 및 신설과 역할 부여, 다양한 법제와 정책들을 수립, 시행하고 있다. 국가별 역사와 사회, 문화적 배경에 따라 통일된 모델을 갖추고 있는 것은 아니지만, 전반적인 추세는 실질적 조정 및 집행 권한을 갖춘 의사결정 기관에 컨트롤 타워 임무를 부여하고 민간을 포함하여 각 부처 및 기관에 수평적 협력과 정보 공유가 이루어지도록 하고 있다. 이에 반하여 우리나라는 유기적이고 수평적인 협력, 대응체계 부재와 더불어 아직 사이버보안 거버넌스 체계 마련을 위한 기초가 되는 법적 토대조차 갖추고 있지 못한 상황인 것이다.

이처럼 현 국가 사이버보안 대응체계는 새로운 환경에 걸맞게 사이버 보안 강화를 위한 목표와 원칙을 제대로 세우고 실질적이며 효율적인 대응체계 마련을 위한 사이버보안 거버넌스를 구성해야 할 때를 맞이하였다. 이를 위해 본 연구는 실질적인 차세대 국가 사이버보안 거버넌스 정립을 위해 해외 주요국의 사이버보안 거버넌스 체계를 비교분석하여 시사점을 도출하는 것을 목적으로 한다. 또한 본 연구는 국가의 주요 사이버보안 기능 분류 기준을 제안하고, 해당 분류 기준에 따라 주요국의 국가 사이버보안 기능별 담당 기관 및 수행 근거를 분석한다. 대상 국가는 최근 국가 사이버보안 전략을 발표하고 사이버보안 거버넌스를 신속히 정비해나가고 있는 미국, 독일, 영

국, 일본, 중국, 그리고 우리나라를 대상으로 하며, 해당 비교 분석 결과를 바탕으로 국내 사이버보안 거버넌스의 개선 방향과 시사점을 도출하도록 한다.

II. 국가 사이버보안 거버넌스의 주요 기능 도출

사이버보안 거버넌스는 사이버공간, 즉, 초국가적 네트워크로서 영역 간, 국가 간 물리적 경계가 발생하지 않는 사이버환경에서 발생 가능한 위험에 대응하기 위한 노력에 중점을 둔다는 점에서, 안정적인 정보시스템의 도입과 활용을 위한 기존의 IT 거버넌스와는 차이가 있다[9]. IoT 기술 발전으로 인한 CPS(Cyber Physical System)의 구현으로 국가가 지켜야 할 대상이 단순히 컴퓨터와 인터넷이 아니라 이를 매개로 하는 모든 국민, 사물, 공간으로 확대되었고, 사이버보안의 관념이 컴퓨터 내의 정보를 보호하는 '정보보호'의 개념에서 인간의 심리, 물리적 시설, 사회적 평판 등과 같은 비정보자산(non-information based assets)까지 포괄적이고 종합적으로 방어하여야 하는 '전 영역 보안'의 개념으로 진화하면서 국가적 차원에서 이러한 사이버위협에 대응할 수 있는 체계적인 국가 사이버보안 거버넌스의 구축이 필요해진 것이다.

사이버보안 거버넌스 구축 전략은 조직의 설립 목적 및 성격, 보호대상과 범위, 정책의 체계와 초점, 정책 추진 과정, 컨트롤타워의 유형 등에 따라 다양한 방향으로 논의될 수 있다[10]. 본 연구에서는 국가차원의 사이버보안 대응능력 강화라는 목표 아래 국가 사이버보안 거버넌스가 수행하여야 하는 주요 기능을 도출하고, 실제 각 기능을 담당하고 있는 국가 부처 및 기관을 분석하는 방법으로 주요국의 사이버보안 거버넌스 형태를 비교함으로써 국내 사이버보안 추진체계의 부족한 부분 및 문제점을 도출하고 관련 개선방안을 제시하고자 한다.

이를 위해 국가 사이버보안 거버넌스 체계를 갖추고 있는 주요국인 미국, 독일, 영국, 일본, 중국과 우리나라를 포함한 6개국이 사이버보안과 관련하여 최근 10년 간 발표한 국가차원의 사이버보안 전략 25개(미국 5개, 독일 4개, 영국 4개, 일본 4개, 중국 2개, 한국 6개)와, 사이버보안 관련 법률 67개(미국 18개, 독일 9개, 영국 9개, 일본 7개, 중국 9개, 한국 15개)에서 국가가 수행하도록 요구하고 있는 사이버보안 관련 기능을 망라적으로 분석하여(부록 참조), 여 국가 사이버보안 거버넌스에 요구되는 주요 기능과 세부 기능을 도출하였다. 분석 결과, 국가 사이버보안 거버넌스의 주요 기능은 ① 국가 사이버보안 정책 수립·조정, ② 국가 사이버위기 대응, ③ 공공 영역 사이버보안, ④ 민간 영역 사이버보안, ⑤ 개인정보보호, ⑥ 사이버보안 산업 부문, ⑦ 사이버보안 역량 강화, ⑧ 사이버보안 국제협력, ⑨ 전자금융보안, ⑩ 의료 보안, ⑪ 산업 보안, ⑫ 사이버보안 감사, ⑬ 정보보증, ⑭ 사이버 범죄 수사, ⑮ 사이버 국방, ⑯ 사이버 위협정보 수집 등 16가지로 분류되었으며, 각 기능별 세부 기능은 Table 1과 같다.

Table 1. Key Functions of National Cyber Security Governance

Key Functions	Detailed Functions
1. Establish and coordinate national cyber security policy	• Establish and coordinate national cyber security policies and strategies
	• Establish and coordinate national cyber security basic plan
	• Operate National Cyber Security Center
	• National Cyber Security Committee Composition
	• Planning and coordination of national cyber security task
	• Establishment and coordination of private information protection policy
	• Establishment and verification of cyber security budget
2. National Cyber Crisis Response	• Establishment and operation of cyber crisis management system
	• Operate Cyber Threat Joint Response Team
3. Public domain cyber security	• Protection of national information network
	• National Infrastructure Cyber Security
	• Development and distribution of security system for public institutions
	• Public sector cyber security control
4. Private domain Cyber Security	• Cyber security diagnosis of major infrastructures in private sector
	• Cyber infringement incident management
	• Private cyber threat information sharing
	• Private sector cyber security control
5. Personal Information Protection	• Coordination of national privacy policy
	• Deliberation and decision of personal information protection policy
	• Deliberation and decision of personal information protection basic/execution

	plan
	• Advising corrective actions for infringement of personal information by public institutions
	• Introduction and operation of certification system for personal information protection management system
	• Operation of Joint Inspection Team for Personal Information Protection
6. Cyber Security Industry	• Establish and coordinate cyber security industry regulation policy
	• Promotion and support policy for cyber security industry
7. Enhancing Cyber Security Capability	• Cyber Security R&D
	• Enhance cyber security awareness
	• Training cyber security personnel
8. Cyber Security International Cooperation	• International cooperation on cyber investigation
	• Global cyber threat information sharing
9. Electronic Financial Security	• Establishment of electronic financial security policy
	• User protection of electronic financial system
	• Securing the safety of electronic financial system
10. Medical information security	• Establishment and promotion of medical security policy
11. Industrial Security	• Establish and promote industrial security policy
12. Cyber Security Audit	• Establish cyber security audit plan
	• Federal agency audit and budget cuts
	• Audit of major national infrastructure
	• Private infrastructure audit
	• Financial institution audit
13. Information Assurance	• Development and certification of public sector information security standards
	• Development and certification of private sector information security standards
14. Cybercrime Investigation	• Cybercrime investigation
15. Cyber Defense	• Response to cyber terrorism…
	• Establish tactics and strategies for cyber warfare
	• Construction of cyber defense system
	• Cyber Weapons Development and Research
16. Cyber Threat Information Collection	• Collect domestic cyber threat information
	• Collect cyber threat information overseas
	• Cyber threat information management, analysis, and provision

나아가, 도출한 국가 사이버보안 거버넌스 주요 기능의 타당성과 포괄성을 담보하기 위하여 국제적으로 사이버 및 사이버보안의 수준 측정을 위해 개발된 국제 지표인 소프트웨어연합(Business Software Alliance, BSA)의 사이버보안 대시보드(Cybersecurity Dashbaord, CSD), 국제전기통신연합(International Telecommunication Union, ITU)의 세계사이버보안지수(Global Cyber Security Index, GCI), 호주전략정책연구소(Australian Strategic Policy Institute, ASPI)의 아·태지역 사이버성숙도(Cybersecurity Maturity in the APAC region, CSM)의 평가항목들에 해당 사이버보안 거버넌스의 주요 기능들이 포함되어 있는지 비교검토를 수행하였다.

Table 2. The Relationships between the key functions of national cybersecurity governance and cybersecurity international index

Category	Cybersecurity International Index		
Key Functions	CSD	GCI	CSM
1. Establish and coordinate national cyber security policy	O	O	O
2. National Cyber Crisis Response	O	O	O
3. Public domain cyber security	O	O	X
4. Private domain Cyber Security	O	O	O
5. Personal Information Protection	O	O	X
6. Cyber Security Industry	X	X	O
7. Enhancing Cyber Security Capability	O	O	O
8. Cyber Security International Cooperation	X	O	O
9. Electronic Financial Security	X	X	O
10. Medical information security	O	X	X
11. Industrial Security	X	X	O
12. Cyber Security Audit	O	O	X
13. Information Assurance	O	O	X
14. Cybercrime Investigation	X	O	X
15. Cyber Defense	X	X	O
16. Cyber Threat Information Collection	O	O	O

* O/X: Presence or absence of item

검토 결과, 주요 선진국의 사이버보안 전략 및 법률에 대한 종합 분석을 통해 도출한 16가지의 국가 사이버보안 거버넌스의 주요 기능들은 모두 국제 사이버보안 지표의 평가항목으로 포함되어 있어, 각 국의 사이버보안 전략 및 법률과 국제 평가지표의 지향점이 같음을 확인할 수 있었다.

이에 본 연구는 위와 같은 국가 사이버보안 거버넌스 주요 기능 분류 기준에 따라 주요국의 사이버보안 거버넌스를 분석하고자 한다.

III. 주요국 사이버보안 거버넌스 분석

3.1 미국의 사이버보안 거버넌스

미국은 2001년 9.11테러의 발생 이후 본격적으로 국가안보를 위한 법제와 정책 추진 체계를 정비하여 왔다. 2006년 미 국무부 해킹, 2007년 F-35 설계도 유출, 2014년 북한에 의한 소니 픽쳐스 해킹, 2015년 인사관리처 해킹, 2016년 러시아의 대선 개입 사건 등 미국은 다양한 사이버 공격의 표적이 되어왔다. 일련의 사고들을 계기로 미국 정부는 사이버 공격이 국가 안정성을 저해하고 사회적 혼란을 야기한다는 점에 깊이 공감하여 사이버 보안을 핵심적인 국정 과제로 추진하고 있다.

미국의 사이버보안 추진체계는 최고 의사결정 기구의 추진력을 기반으로 개별 부처 간의 이해관계를 조율하고, 변화하는 환경에 따라 주요 분야를 중심으로 유연하게 관련 조직의 구성과 업무 등을 통합, 조정, 신설하며 유기적이고 효율적인 구성 현황을 보이고 있다.

또한 미국은 백악관 차원에서 국가 전체의 사이버보안 정책을 수립, 관리하고 있다. 이를 바탕으로 국토안보부가 실무적인 차원에서 정책을 시행하고 있으며 국방부 사이버사령부와 법 집행기관 또한 막강한 권한을 보유하고 있다. 특히 범부처 차원의 사이버 위협 정보 공유 및 위기 시 대응 체계 마련을 위해 국토안보부 내에 국가사이버안보통신통합센터(NCCIC)를 두고 있으며, 각종 위협정보를 수집, 통합 관리하고 개별 부처와 활발히 공유하며, 종합적인 보고를 통해 국가 전체의 사이버보안 정책 추진 상황 등을 점검할 수 있도록 국가정보국 내에 사이버 위협정보통합센터(CTIIC)를 운영하고 있다. 뿐만 아니라 미국은 분야별 사이버보안 전문 조직을 개별적으로 두어 정부부처조정위원회(GCCs) 및 분야별 전문기관(SSAs)를 통해 연방 기관들 간의 협업을 장려하고 있다. 민간 분야는 주요 기반시설 운영자들을 중심으로 각종 협회 및 기관들이 분야별협력위원회(SCC)를 구성하고 정보공유분석센터(ISACs)를 설립하여 공동체 차원에서 사이버보안 위협에 대응하고 있다. 국가는 이를 지원하기 위해 국토안보부에 정보공유분석기관(ISAOs)를 두고 공공, 민간 등 다양한 구성원간의 협력을 증진시키기 위해 노력하고 있다. 나아가 예산관리처(OMB)는 사이버보안 업무 감사 업무를 맡고 관련 예산을 관리하여 각 부처의 사이버보안 정책 수용 여부를 평가, 판단하여 예산의 낭비를 줄이는 등 효율성을 제고하도록 하고 있다.

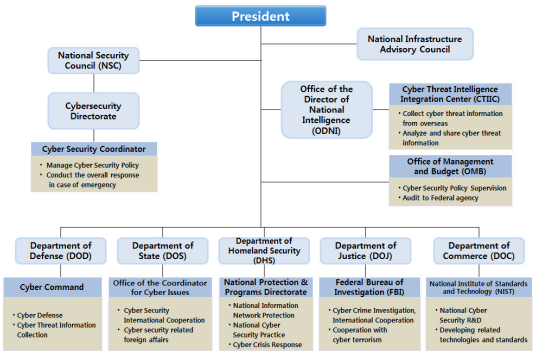

Fig. 1. US Cyber Security Implementation System

이처럼 미국의 사이버보안 추진체계는 정보 공유 및 사고 대응 등 협력 체계가 견고히 구성되어있다는 점과 함께 예산관리처에 막강한 권한을 부여하여 개별적으로 이루어지고 있는 사이버보안 업무가 충실히 수행될 수 있도록 함으로써 분야별 사이버보안 역량을 강화하고 조직 간의 긴밀한 협력, 공유 체계를 갖추고 있다는 것이 특징이다. 이러한 미국의 추진체계는 크게 정보 공유, 협업 체계, 관리 감독, 역량 강화, 인식 제고의 5가지 특성을 보이고 있다. 세부 추진 동력은 정보 공유 및 협업 관련 원칙과 조직들을 정하고 있는 명확한 법적 근거인 사이버안보법(Cybersecurity Act of 2015)을 바탕으로 얻고 있고, 조직들 간의 협업 체계는 타 법령 및 대통령령, 각종 기본 계획 등을 통해 구축하고 있다. 나아가 백악관 차원에서 국가 사이버안보 정책을 추진함에 따라 국가적 인식이 제고되고 개별 부처의 역량이 증진되며 각종 정책의 효율성이 높다는 장점을 가지고 있다. 실무적인 면은 국토안보부에 집중시켜 연방정보보호현대화법(FISMA)을 통해 권한을 강화하되 개별 부처에 각각의 전문 분야에 걸맞은 조직을 두도

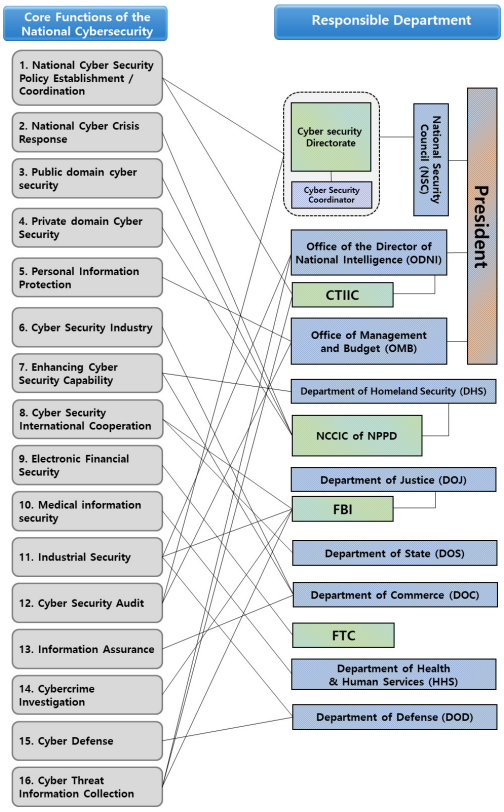

Fig. 2. Implementing agency by cyber security function in US [11][12][13][14][15]

록 하고 있다. 이외에도 본 연구에서 분류한 미국의 국가 사이버보안 기능 별 수행 기관은 Fig.2와 같다.

3.2 독일의 사이버보안 거버넌스

연방제 국가인 독일의 사이버보안 체계는 기본적으로 『연방정보기술보안청 설치에 관한 법』(BSIG : BSI-Erri-chtungsgesetz)에 의해 설립된 연방내무부(BMI) 산하의 연방정보기술보안청(BSI)과 연방통신망청법에 근거한 연방경제기술부(BMIW) 산하의 연방 통신망관리청(BnetzA)이 주로 담당하고 있다. 이 중 현재 사이버보안과 관련하여 가장 많은 기능을 담당하고 있는 연방정보기술보안청(BSI)은 독일이 사이버보안에 대한 위험성과 중요성을 미리 예측하고 1991년에 설립한 기관이다. 독일의 경우 사이버보안을 위해 국가적 차원에서 상당한 지원을 하고 있고 사경제 분야에 있는 기업도 점차 사이버보안과 관련한 책임의 중대성을 인식하고 대비책을 마련하는 과정에 있다.

독일은 연방정부를 중심으로 다양한 분야에 산재해 있는 보호 필요 대상에 대한 사이버보안을 보장하기 위하여 여러 부처가 자신의 소관 분야에서 사이버보안과 관련한 역할을 분담하고 있다. 독일 총리실을 중심으로 하여 연방정보부(BND), 연방내무부(BMI), 연방교육연구부(BMBF), 연방국방부(BM), 연방경제기술부(BMWi)와 같은 부처들이 사이버보안과 관련한 주요 기능을 책임지고 있으며, 그 중에서도 연방내무부(BMI)가 사이버보안 정책을 총괄하는 핵심 역할을 하고 있다. 또한 연방내무부 산하의 연방정보기술보안청(BSI)이 사이버보안 정책의 집행, 다른 부처·기관 및 민간에 대한 지원, 사이버 보안 관련 인증 등 광범위한 사이버보안 업무를 담당하고 있으며, 2015년 정보기술 강화법의 입법으로 인해 더욱 강화된 역할을 부여받게 되었다.

유럽은 최근 EU 집행위원회와 관련된 사이버 공격의 증가, 사이버 범죄로 인한 EU 국가들의 피해액 증가 등의 이슈로 인하여 EU는 2016년 '네트워크 및 정보보호 지침'을 발표하고 2018년 5월까지 각 회원국들이 동 지침의 이행을 위한 국내법을 마련하도록 하였다. 동 지침에 따라 독일은 사이버 보안에 대한 국가 전략인 '독일 국가 사이버보안전략(2016)'을 발표하였고, 각 지침의 이행을 감독하는 담당 기관을 분명히 명시하고 있으며, 각 분야의 사이버 위협에 대비한 전문성 있는 사이버 보안사고 대응팀도 구성하였다. 이처럼 독일은 EU 회원국으로서 EU의 각종 지침 혹은 규정들을 국내에 전환하여 입법하여야하기에, 사이버보안과 관련된 부문들에 대해 다양한 전략과 관련 입법이 복합적이면서도 체계

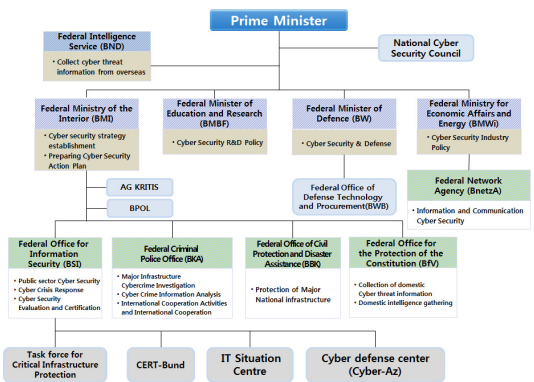

Fig. 3. Germany's Cyber Security Implementation System

적으로 구성되어 있는 상황이다.

독일은 연방내무부(BMI)가 사이버보안 전략을 총괄하고 내무부 산하의 연방정보기술보안청(BSI)이 공공부문 사이버보안, 사이버 위기 대응, 사이버 보안 관련 평가·인증 업무 등 광범위한 범위에 대해 실질적인 정책 집행 업무를 추진하고 있다. 연방정보기술보안청(BSI)은 2015년 정보기술 강화법의 입법을 통해 주요기반시설에 대한 보안 관련 감독 및 관리 권한, IT제품, 시스템, 서비스에 대한 보안 조사 및 심사 역할과 권한을 부여받았으며, 이는 독일이 사이버보안 추진체계를 더욱 실질적이고 핵심적인 기관으로 격상시키고자 하는 의지라고 볼 수 있다.

독일의 사이버보안 거버넌스 추진의 방향은 2016년 발표한 국가 사이버보안전략을 통해 살펴볼 수 있다. 전략은 기존에 체계적으로 구성되어 있던 사이버보안 체계를 더욱 실효성 있고 지속 가능한 형태로 보완 및 강화할 것을 선언하고 있다. 이는 국가 사이버방위센터 강화, 연방정보기술보안청 내 모바일 사고 대응팀 창설, 연방범죄수사청 내 신속 대응팀(QRF) 창설, 연방헌법수호청 내 모바일 사이버팀 창설, 연방정보부의 사이버 조기 경보 시스템 구축, 보안 영역 정보 기술 중앙 센터 설치, 독일 CERT 역할 강화, 연방 정부와 주정부간 협력 강화 등의 정책으로 나타나고 있다. 또한 사이버보안 관련 역할을 수행함에 있어 각 기관별로 필요한 실질적 권한이나 조직 구성에 대해 고려하고 해당 기능을 더욱 효율적이고 지속 가능한 형태로 실현시킬 수 있게끔 국가 차원에서 법적 차원, 구조적 차원에서 힘을 실어주고 있는 것으로 보인다. 본 연구에서 분류한 독일의 국가 사이버보안 기능 별 수행 기관은 Fig.4와 같다.

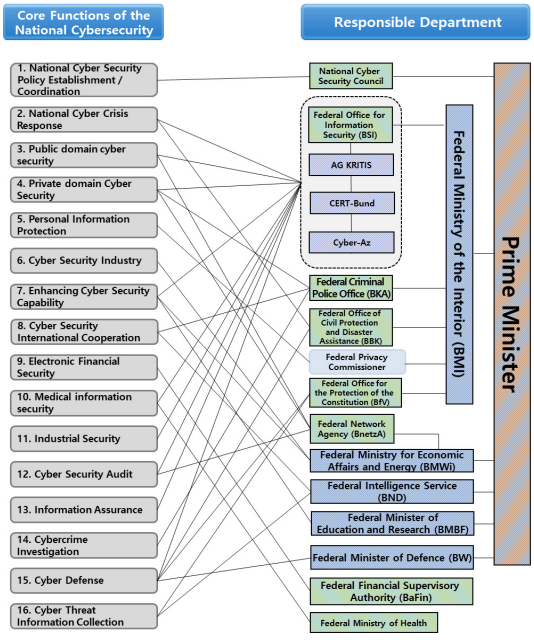

Fig. 4. Implementing agency by cyber security function in Germany [16][17][18][19]

3.3 영국의 사이버보안 거버넌스

영국은 유럽 내에서만이 아닌 세계적으로도 사이버보안을 선도하고 있는 국가에 속한다. 매년 사이버보안 전략의 발표와 더불어 추진 사항 및 진행 현황에 대한 검토를 진행하고 있고 검토한 내용을 사이버보안 전략 실행 계획에 반영하는 등 전략 실효성 제고를 위해 노력하고 있다. 또한 철저한 사이버보안 체계를 통한 관련 개발 등으로 사이버보안 분야에서 모범 국가로 꼽히고 있다.

영국의 사이버보안은 전략, 정책적으로는 내각부(Cabinet Office)를 중심으로 하여 운영되고 있고, 실무적으로는 정보통신본부(GCHQ)의 국가사이버보안센터(NCSC)에 의해 운영되고 있다. 영국은 기존에 정보보호법(Data Protection Act 1998)에 따라 정보보호와 관련된 법규를 마련하고 사이버보안과 관련된 전략을 펼쳐왔고, 사이버범죄의 인식 확대와 민간의 대응능력 제고 등을 위해 2009년 6월 최초로 범정부 차원의 사이버보안 전략을 수립하여 발표하였다. 이후 사이버보안전략 2011, 사이버보안전략 2016등을 통해 국가 전반의 사이버안전을 위해, 또한 세계에서 사이버보안을 선도적으로 이끌기 위해 많은 노력을 기울이고 있다. 사이버보안전략 2016에서는 사이버보안의 효율성을 높이기 위해 정부의 정책, 조직 및 구조를 단순화시킨다는 내용을 언급했으

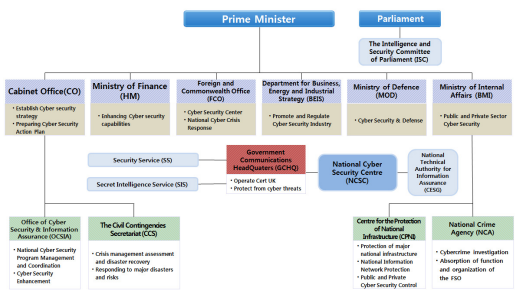

Fig. 5. UK Cyber Security Implementation System

며, 해당 전략에 따라 국가사이버보안센터(NCSC)를 설립하고 기존에 다른 부처가 갖고 있던 사이버보안 기능들을 다수 해당 기관으로 옮겨왔다. 현재 국가사이버보안센터(NCSC)는 각 정부에 사이버보안과 관련하여 조언을 하는 역할 뿐만 아니라 위험에 대응하고 사건사고를 관리하며 연구를 진행하는 등의 역할을 맡고 있다.

영국은 사이버보안전략에 의거하여 내각부(Cabinet Office)가 중심이 되어 사이버보안 관련 전략 수립의 중추적인 역할을 담당하고 있다. 영국 내각부(CO)는 국가사이버보안전략을 발표하고, 사이버공간에서의 위험요소 감소를 통한 범죄대응 기회 포착, 보안지식 및 대응력제고, 의사결정체계 강화 등 사이버보안과 관련된 기본계획을 수립·조정한다. 내각부(CO)의 사이버보안청(OCSIA)은 사이버 범죄를 포함한 영국의 사이버 보안 및 정보보증에 관한 전략적 방향을 제공한다. 또한 사이버 공간 확보와 관련하여 내각부와 국가 안보위원회를 지원하는 역할을 한다.

사이버 위기관리에 대해서는 주로 내각부(CO)와 내무부(HO)가 소관하고 있다. 내각부의 사이버보안청(OCSIA)은 정보보호 관련 활동에 대해 정부 전체를 조정하는 역할을 맡고 있으며, 내무부(HO)는 테러·범죄 및 반사회적 위험으로부터 사회를 지키며, 주요 기반시설의 보호와 입국관리, 테러대응, 경찰 통솔 등을 담당하고 있다.

영국정부는 국가사이버보안센터(NCSC)가 공공·민간 영역의 사이버보안을 종합적으로 관장하고 있다. 국가사이버보안센터(NCSC)은 사이버보안 사고를 식별하고 대응하며, 완화조치를 지원하고, 사이버보안 위협에 대한 이해를 구축하는 역할을 하며, 공공·민간의 사이버보안 관제 역할도 수행하고 있다. 그 외에도 본 연구에서 분류한 영국의 국가 사이버보안의 주요 기능 별 수행 기관은 Fig.6과 같다.

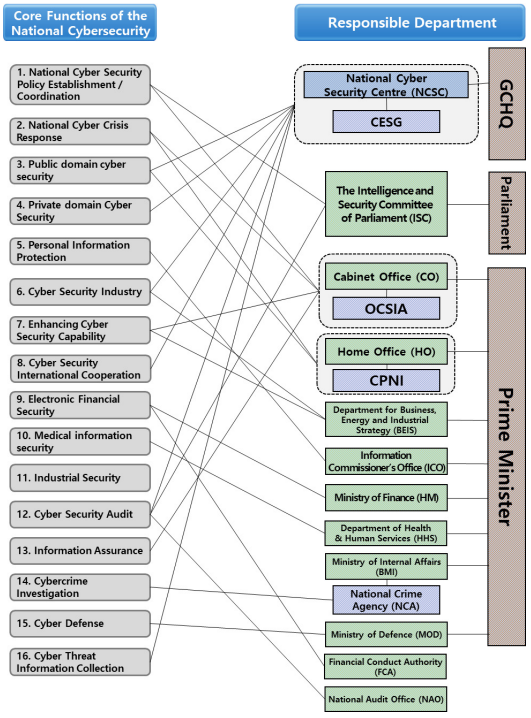

Fig. 6. Implementing agency by cyber security function in UK [20][21][22][23]

3.4 일본의 사이버보안 거버넌스

일본은 IT기술의 발전으로 국민 생활, 사회, 경제, 행정, 안보 등 국가의 모든 요소가 사이버 공간에 귀속되자 이로 인한 위협이 국가 및 사회의 기반을 흔드는 수준으로 확대되었다고 인식하고, 2020년 하계올림픽 개최에 초점을 맞추어 국가적으로 대대적인 사이버보안 강화 정책을 추진하고 있다.

일본의 사이버보안 추진체계는 내각의 사이버보안 전략본부와 내각관방의 사이버보안센터를 중심으로 모든 기관이 각 분야에 따른 역할을 수행하고 있다. 『고도 정보통신네트워크 사회형성 기본법』에 따라 설치된 고도정보통신네트워크 사회형성 추진 전략본부(이하 IT 종합 전략 본부)는 IT분야 전반에 대한 정책 및 전략을 총괄하고 정보통신 전략의 심의 및 조정을 담당하고, ICT R&D 지원 정책 추진 등 국가 ICT 산업과 관련된 사안을 모두 다루고 있었으나, 2014년 11월 『사이버보안 기본법』이 제정된 이후, IT 종합 전략본부의 기능 중 사이버보안에 관한 기능을 대부분 흡수하여 사이버보안 전략본부가 설립되었다.

사이버보안 전략본부는 국가 전체의 사이버보안 전략을 수립하고 정부부처 및 지방공공단체와 협력하여 정책을 조정하는 역할을 한다. 또한 사이버보안 전략본부는 기존의 IT전략본부, 국가안보회의와 중요한 현안에 대해 함께 연계하고 협력하여 사이버보안 세부 전략을 수립한다. 전략본부는 사이버보안 기본법에 법적 근거를 두고 있고, 법에 명시된 권한을 부여받고 있기 때문에 실질적으로 민관 전체를 이끄는 사이버보안 컨트롤타워 역할을 하고 있다.

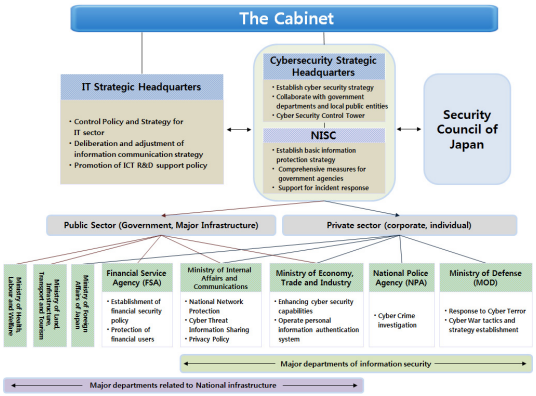

Fig. 7. Japan's Cyber Security Implementation System

이처럼 일본의 사이버보안은 국가 사이버보안 컨트롤타워 역할을 하는 사이버보안 전략본부와 사이버보안센터(NISC)가 주도하여 추진하고 있지만, 『사이버보안 기본법』은 이뿐만 아니라 모든 정부 기관에게 사이버보안 관련 세부 책임과 역할들을 부여하고 있다. 정부기관, 주요 인프라의 사이버보안 등 공공 부문의 사이버보안과 관련되는 부처들은 의료·수도를 담당하는 후생성, 철도·항공·물류 등의 교통을 담당하는 국토교통성, 전력·가스·화학·석유 등을 담당하는 경제산업성, 건전한 금융 질서 확립을 담당하는 금융청, 국가 통신망을 관장하는 총무성 등이 있다. 이들은 사이버 위협을 받을 시 국가 기반이 무너질 수도 있는 주요 인프라들을 소관하는 부처들이라는 공통점이 있으며, 해당 부처들은 '2014 사이버보안 전략'에서 언급한 횡적 사이버보안 대응체제 구축으로 인한 자기 주도적 사이버보안 역량 강화라는 목표에 부합할 수 있도록 각 소관 분야별 사이버보안 대응에 힘쓰고 있다.

한편 기업, 개인이 속해 있는 민간 부문을 소관하는 부처들로는 외교·안전 보장을 담당하는 외무성, 사이버 범죄 수사를 담당하는 경찰청, 사이버 테러 대응 및 사이버전 전술·전략 수립을 담당하는 방위성, 그리고 총무성과 경제산업성 등이 포함된다고 볼 수 있다. 이 중 총무성, 경제산업성, 경찰청, 방위성은 정보보호 4대 주무부처라 불리는 주요 부처로써, 국가 사이버보안에 있어 각 분야별로 상당히 중요한 역할들을 부여받고 있다. 그 외에도 본 연구에서 분류한 일본의 국가 사이버보안 기능 별 수행 기관은 Fig.8과 같다.

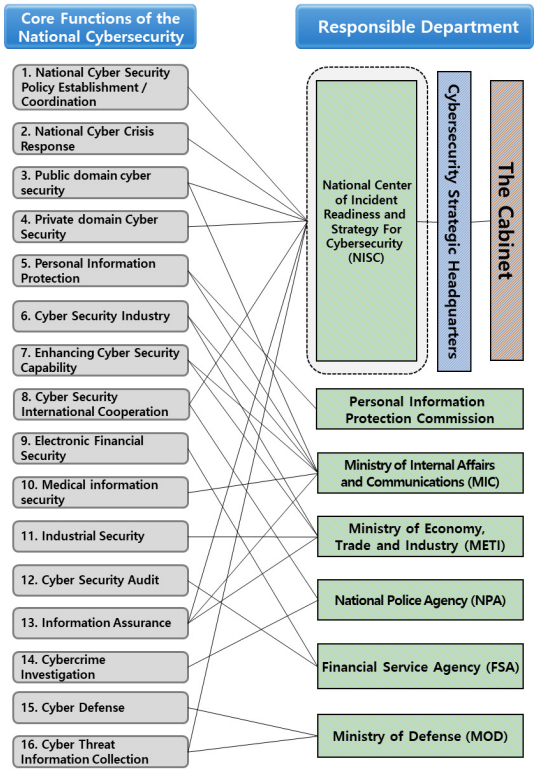

Fig. 8. Implementing agency by cyber security function in Japan [24][25][26][27]

3.5 중국의 사이버보안 거버넌스

2011년 중국은 UN 총회에서 상하이 협력기구를 통해 국제 인터넷주소관리기구(ICANN)에 대한 체제 변화를 주장하며 사이버공간에서의 주권 개념을 공개적으로 주장하였다[28]. 당시 중국은 사이버 공간에서 제3국의 간섭은 배제되어야 하며 국가 주권의 개념이 확립되어야 한다고 주장하였으며, 이러한 중국의 사이버 주권 개념은 자국 내 인터넷 사용 통제 강화 및 사이버 안보 개념 확립으로 이어졌다[29]. 이에 따라 중국은 Chinanet을 통한 일괄접속을 통해 사이버 공간을 형성하고 있으며 반정부적 내용에 대하여 엄격한 통제를 가하고 있다. 2016년 11월 중국은 온라인 통제 강화를 주 내용으로 하고 있는 사이버보안법(網絡安全法)을 제정하여 2017년 6월부터 시행하였고, 2016년 12월에 '국가 사이버공간 안전전략'을 마련, 발표하였다.

중국의 사이버 거버넌스의 최고 담당 기관은 중국공산당 정치국 상무위원회(Politburo Standing

Committee), 국무원(State Council), 중앙 군사위원회(Central Military Commission)로 구성된다[28]. 특히 2014년 설립된 '중앙인터넷안전정보화영도소조'는 기존 국가정보화영도소조와 국가 네트워크 및 정보안전 협력소조를 흡수하여 중국 공산당 정치국 상무위원회 아래 최고의사결정기관으로 작용하고 있다[30]. 나아가 국가 안보와 사이버 공간에서의 국가적 이익, 경제 발전 등을 위해 여러 분야에서의 사이버 보안 및 정보화 문제들을 총괄 담당하고 있으며, 이로써 중국의 사이버 관련 정책의 지도적 역할을 수행하고 있다.

중국의 사이버보안 추진체계 관련 조직으로는 국가안전부(MSS, Ministry of State Security), 공안부(MPS, Ministry of Public Security), 국가보밀국, 인터넷경찰 및 중국 침해사고 대응센터 등이 있다. 국가안전부 산하 기술정찰국은 국가암호 및 사이버 보안정책을 수립하여 사이버안전업무를 총괄하고 있다. 공안부에서는 국가기밀에 관한 업무를 중심으로 중국 정부 기관에 납품하는 보안 제품 등에 대한 검사와 정보통신망 보안정책 및 관련 제품 개발에 관여한다. 국무원 국가보밀국은 공공 분야의 국가보안업무를 담당하여 보안 감사, 관련 정책 수립 및 통제, 감독 등의 업무를 수행한다. 인터넷 경찰은 사이버 범죄 수사와 불온 사상의 전파 방지, 정보통신망 취약성 발굴 및 경고 등을 수행한다. 신식산업부(MIIT, Ministry of Industry and Information Technology) 산하에 비영리기관으로 설치되어있는 중국 침해사고대응센터는 민간 분야의 사이버 침해사고 대응 및 조사 등을 수행한다.

중국의 사이버보안 추진체계는 정보기관과 공안을 중심으로 이루어지고 있다는 점이 가장 큰 특징이다. 공산당 중앙위원회와 국무원이 최고 정책 기관으로서 사이버보안 전략 및 전술에 대하여 관여하고 있으며, 국가 사이버 위기 대응, 공공 및 민간 사이버 보안, 개인정보보호, 사이버보안 산업, 보안 역량 강화, 각종 표준 개발, 사이버 범죄 수사와 사이버 안보 실무, 위협정보 수집 등을 대부분 국무원 산하 공안부 및 인민해방군에서 담당하고 있다. 2014년 중국 최고 의사결정기구인 정치국 상무위원회에 중앙인터넷안전정보화영도소조를 설치하여 시진핑 주석이 조장을 맡았다. 이를 통해 인터넷 통제 강화 또는 사이버 보안 강화를 위한 중국의 국가적 분위기가 형성되었다. 국가안전부는 사실상 국내외에서 모든 정보활동을 수행하고 있으며 공안부는 국내 안정을 위한 활동을 수행하고 있다. 공안부는 국내에서의 사이버 범죄 수사 및 체제 유지를 위한 활동을 진행 중이다.

이처럼 중국은 국가 체제의 특성상 엄격한 통제와 국가안전부, 인민해방군 등 정보기관 중심의 사이버 보안 추진체계를 가지고 있다. 특히 인터넷 활성화에 따른 개방성과 해외와의 교류 활성화, 국민들의 정보 접근권 강화 등을 견제하며 체제의 유지와 안정을 위한 사이버 공간을 형성하고자 하고 있다. 이러한 점에서 중국은 국가 안보 및 사이버 보안 관련 민감한 사항에 대한 대외 공개를 최소화함으로써 사실상 폐

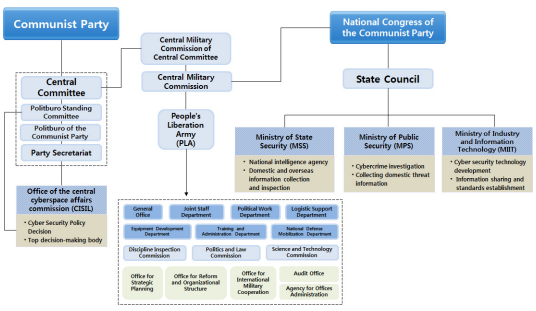

Fig. 9. China's Cyber Security Implementation System

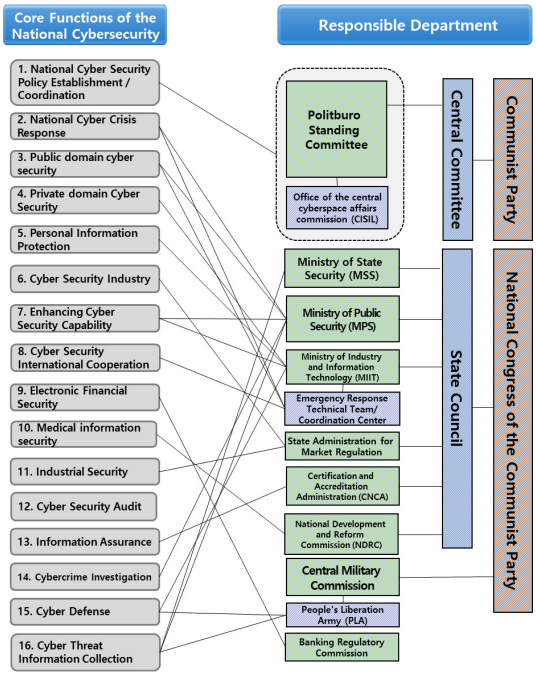

Fig. 10. Implementing agency by cyber security function in China [31][32]

쇄적인 사이버 정책을 펼치고 있다. 이외에도 본 연구에서 분류한 중국의 국가 사이버보안 기능 별 수행 기관은 Fig.10과 같다.

3.6 한국의 사이버보안 거버넌스

우리나라는 청와대 국가안보실이 국가 전반적인 사이버보안 컨트롤 타워 기능을 수행하고 유관 부처 차관급이 참석하는 국가사이버안전전략회의와, 국가 사이버 보안 관련 대책을 심의하는 국가사이버안전대책회의를 통해 사이버보안 관련 주요 정책이 추진된다. 또한 『국가사이버안전관리규정』에 의해 국가정보원장 소속하에 설립된 국가사이버안전센터가 국가 사이버보안 정책 수립·조정 기능, 국가 사이버 위기 대응, 공공 영역 사이버 보안, 사이버 위협정보 수집 등 사이버보안을 위한 실질적인 기능을 대부분 수행하고 있다. 각 분야별·기능별·대상별로도 전문성을 가진 국가 기관들이 분야에 맞는 사이버보안 기능을 수행하고 있다. 예를 들어, 과학기술정보통신부는 민간영역 사이버보안, 사이버보안 산업 진흥, 사이버보안 역량 강화 등의 역할을 수행하고 있고, 국방부는 사이버 안보와 관련된 기능을 담당하고 있다. 이 밖에도 행정안전부는 전자정부 및 개인정보보호, 방송통신위원회는 정보통신망법 적용 대상에 대한 사이버보안 업무, 경찰청은 사이버범죄 예방 및 수사 기능, 금융위원회는 전자금융보안 정책 수립·이용자 보호·안전성 보호 기능, 보건복지부는 의료 보안, 산업통상자원부는 산업 보안 기능, 국가보안기술연구소는 정보보증 기능을 수행한다.

우리나라의 사이버보안 거버넌스의 중심체계는『국가사이버안전관리규정』에 의거하여 구성되어 있다. 사이버안보비서관을 청와대 직속 국가안보실에 두고 있으며, 국가정보원 내 사이버안전센터를 설치하여 청와대 중심의 전반적인 사이버보안 컨트롤타워 기능을 보다 강화하였다. 또한 국가정보원이 국가사이버안전과 관련된 정책 및 관리에 대해 관계중앙행정기관의 장과 협의하여 이를 총괄·조정하도록 되어 있다. 국가정보원은 총괄·조정 업무를 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관의 장과 협의하여 국가 사이버안전기본계획을 수립·수행하여야 하며, 국가사이버안전기본계획을 원활하게 추진하기 위하여 관계 기관에 예산 반영 등에 관한 협조를 요청할 수 있다.

국가 사이버 위기 시에는 국가사이버안전센터가 사이버 공격으로 인하여 발생한 사고의 조사 및 복구 지원을 하여야 하며, 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등은 국가사이버안전센터 내의 민·관·군 합동대응반이 맡고 있다.

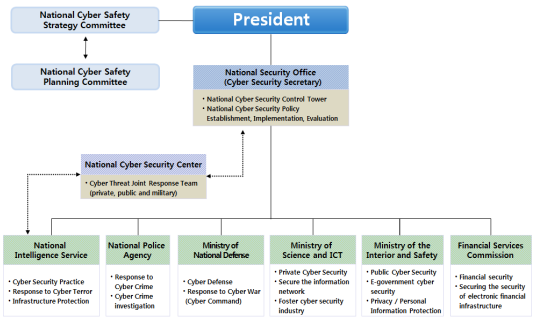

Fig. 11. Korea's Cyber Security Implementation System

공공영역의 사이버보안에 대해서는 국가사이버안전센터가 국가정보통신망의 안전성을 확인하고, 국가사이버안전매뉴얼을 작성·배포하는 등 주도적인 역할을 맡고 있으며, 민간 영역의 사이버보안에 대해서는 과학기술정보통신부와 한국인터넷진흥원이 인터넷침해대응센터를 운영하는 등 국내 인터넷 상의 다양한 사이버 위협에 대한 예방·대비·대응·복구 역할을 분담하고 있다.

사이버 보안 관련한 국제 협력에 대해서는 총괄하여 담당하는 전담기관이 존재하지 않으며, 각 분야별 기관들이 국제 협력과 관련하여 필요에 맞는 조직과 기능을 분담하여 수행하고 있다. 국가정보원장 소속하에 설치된 국가사이버안전센터가 국가 안보 및 보안에 필요한 외국과의 사이버 위협 관련 정보 관련 협력 기능을 수행하고 있으며, 외교부의 외교정보 보안담당관실은 외교정보보호·정보보안 유관기관과의 정보공유 및 협력 기능 등을 수행하고 있다. 한국인터넷진흥원도 글로벌 사이버보안 협력네트워크(CAMP)를 기반으로 주요 전략 국가와 우호 네트워크를 구축하고 협력과제를 발굴하여 사이버보안 분야의 국제협력 기반을 조성하고 있으며, 경찰청 사이버안전국은 사이버국제협력팀을 두어 사이버범죄에 관한 국제공조 활동을 수행하고 있다.

사이버 범죄 수사와 관련한 업무는 경찰청의 사이버안전국이 맡고 있다. 사이버안전국은 사이버범죄를 예방하고 사이버공간의 치안을 확보하여 국민이 안심하고 이용할 수 있도록 하고 기업이 활동하기에 안전한 환경을 조성하는 것을 비전으로 하고 있으며, 민

간, 유관기관, 외국과의 긴밀한 협력을 바탕으로 선제적 사이버범죄 예방 정책을 발굴·시행하여 국민·기업· 국가의 피해를 최소화하며 지속적인 연구개발로 인적· 물적 자원과 기술의 전문성을 높이고, 선택과 집중을 통해 효율적으로 주요 범죄를 제압하여 사이버치안을 확보하는 기능을 수행하고 있다.

사이버안보에 대한 역할은 『국가사이버안전관리규정』, 『국군사이버사령부령』에 근거하여 국방부가 수행하고 있다. 『국가사이버안전관리규정』에 따라 국가정보원이 사이버안전대책의 수립·시행 등의 기능을 맡고 있음에도 불구하고 국방 분야의 사이버안전과 관련하여서는 국방부가 그 업무를 수행하도록 명시하고 있다. 또한 국방부는 『국군사이버사령부령』을 근거로 국방 사이버전(戰)의 기획, 계획, 시행, 연구·개발 및 부대 훈련에 관한 사항을 관장하기 위하여 국방부장관 소속으로 국군사이버사령부를 운영하고 있으며, 사이버사령부는 국방 사이버전의 기획 및 계획 수립, 국방 사이버전의 시행, 국방 사이버전 전문 인력의 육성과 기술 개발, 국방 사이버전을 Homeland Security 대비한 부대 훈련, 국방 사이버전 유관기관 사이의 정보 공유 및 협조체계 구축 등의 기능을 수행하고 있다.

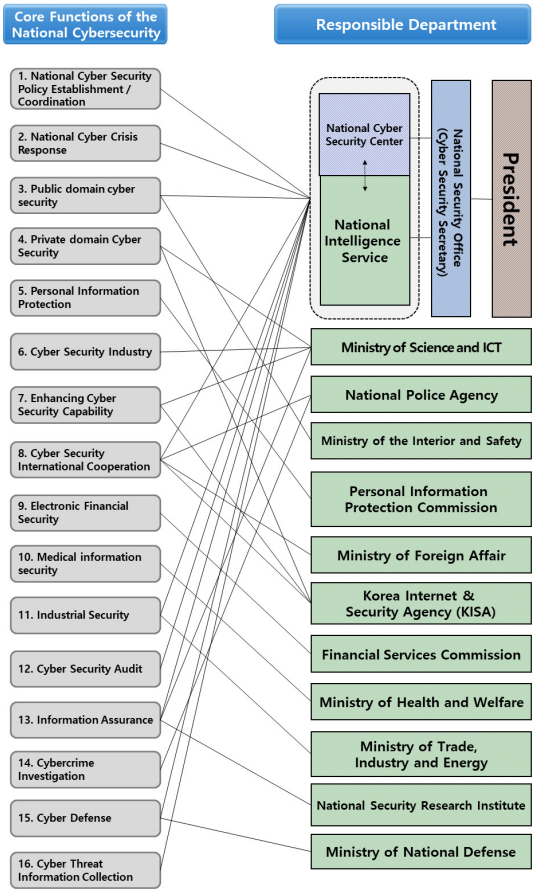

Fig. 12. Implementing agency by cyber security function in Korea[38]

사이버 위협정보 수집과 관련한 기능은 『국가정보원법』을 근거로 국가정보원이 국외 정보 및 국내 보안정보의 수집·작성 및 배포 업무를 맡고 있으며, 국가정보원장 소속하에 설치된 국가사이버안전센터도 사이버위협 관련 정보의 수집·분석·전파와 관련한 업무를 수행하고 있다. 이외에도 본 연구에서 분류한 우리나라의 국가 사이버보안 기능 별 수행 기관은 Fig.12과 같다.

IV. 국가별 사이버보안 거버넌스 특징과 한국에의 정책적 시사점

국가별로 사이버보안 거버넌스의 지향점이 상이하며, 각 국이 가지고 있는 법제도 환경과 문화 또한 다르기 때문에 여러 국가의 사이버보안 거버넌스를 동일한 기준으로 단순 비교 분석을 수행하는 방법으로는 유의미한 결과를 도출하기 어렵다. 따라서 본 논문에서는 각 국 사이버보안 거버넌스의 특징에 주목하여 국가별로 유독 강조하고 있는 주요 사이버보안의 기능이 무엇인지 분석하고 그 특징을 식별하며, 우리나라 사이버보안 거버넌스 개선에 참고할 수 있는 정책적 시사점을 도출하여 제시하고자 한다.

우선 미국은 다 수의 사이버 테러 대응 경험에 입각하여 사이버 공간을 새로 부상하는 전장으로 인식하고, 국가 사이버 위기관리 기능을 강화하는데 초점을 맞추고 있고, 2015년 사이버안보법 제정을 통해 명확한 법적 근거를 기반으로 해당 기능을 더욱 강화하였다는 점에서 정책적 시사점이 있다. 미국은 사이버 위기 발생 시 관리 및 대응을 위한 체계를 국토안보부 국가보호프로그램실(NPPD)의 국가사이버안보통신통합센터로 집중시켰으며, 국가사이버안보통신통합센터(NCCIC) 산하 센터통합운영국이 센터의 활동 전반에서 분석, 정보 공유 및 사고 대응력을 동기화하기 위해 계획, 조정 및 통합 기능을 수행하고 있다[33]. NCCIC의 설립 근거와 역할은 사이버안보법에 근거함으로써 미국의 통합적 사이버안보 거버넌스의 핵심 역할을 할 수 있도록 하였다[34]. 이에 따라 연방 정부와 민간을 포함한 비 연방주체가 서로

정보를 공유하고, 원활한 협력·조정이 이루어지고 있으며, 기존 국가 사이버보안 실무를 총괄하던 국토안보부와 민간과의 관계에서도 NCCIC가 연결점의 역할을 수행하고 있다. 나아가 2015년 2월 민간 사이버보안 정보공유 촉진 행정명령[1]을 통해 민간 조직 사이, 혹은 민간과 공공기관 사이의 정보공유와 협력 대응을 담당하는 정보공유분석기관(ISAO)을 설립하도록 하였다. 이에 따라 국토안보부의 NCCIC는 민간과의 정보 공유를 위해 정보공유분석기관(ISAO)과 지속적이고 포괄적인 조정의 역할을 수행하고 있다. 반면 우리나라의 경우, 국가 사이버보안에 대한 총괄 입법체계가 부재하여, 국가차원에서 사이버테러 방지 및 위기관리 업무를 체계적으로 수행할 수 있는 제도와 거버넌스가 명확히 정립되어 있지 않고[35], 사이버보안 대응체계가 공공과 민간으로 분리되어 있어 체계적인 대응도 어려운 상황이다. 현재의 사이버보안 대응체계의 근거법인 「국가사이버안전관리규정」은 행정기관만을 대상으로 하고 민간과 입법·사법기관은 적용되지 않고 있어 민간부문의 사이버공격을 실시간으로 탐지·차단하거나 신속하게 대응하기엔 법률적 한계가 존재한다. 때문에 우리나라도 미국의 사이버안보법을 참고하여 사이버보안 업무를 총괄 집행할 수 있는 부처를 신설하거나 관련 권한을 적정 조직에 명확히 부여할 필요가 있다. 또한 미국은 9.11 테러부터 각종 위협 및 사이버 공격 등의 경험을 바탕으로 국가 안보에 관한 국가적 공감대가 갖춰진 국가지만 우리나라는 이러한 인식이 미국만큼 높지는 않기 때문에, 대통령 수준에서의 사이버보안에 대한 관심과 정책 추진 의지가 뒷받침되어야 할 것이다.

독일은 2017년 연방정보기술보안청 법(BSI Act) 개정을 통하여 BSI의 사이버보안과 관련된 국내 활동 여건을 강화하고 BSI와 정보기관 간 효율적인 정보공유를 할 수 있도록 하는 제도적 기반을 만들었다는 점에서 시사점이 있다. 독일은 일찍이 BSI가 지휘 하에 공공과 민간이 신속한 정보공유를 하도록 하는 국가사이버대응센터를 운영하고 있으며, 나아가 최근 BSI법 개정을 통해 BSI에 연방정부 및 주요 인프라에 대한 복구권한을 부여하고, 다수의 대외정보기관 및 군사정보기관과 필요한 정보를 공유할 수 있도록 하였다. '2016 독일 사이버전략'에서는 연방 정부와 주정부 간 협력을 강화하기 위해 BSI의 사이버 보안사고 대응과 관련한 국가 당국의 지원을 새로운 과제로 설정하였다. 사이버보안에 있어 BSI 및 관계기관의 국내 활동이 강화되면서 국가안보에 관련된 사이버공간의 문제를 관계기관들이 보다 유기적으로 해결할 수 있는 체계를 지속 발전시키고 있는 것이다[36]. 반면, 우리나라는 각 기관별, 부문별 사이버 위협정보 공유가 원활히 되지 못하고 있으며, 특히 국가정보원을 중심의 정보공유체계는 민간부문에 대해서는 구속력이 없는 상황이다. 따라서 정보기관을 포함하는 정보공유 체계, 민·관 협력 사이버위기 대응 체계 마련에 있어 최근 독일의 법제도 개선 사례를 참고할 필요가 있다.

영국은 정보기관의 성격을 가진 국가사이버보안센터(NCSC)에 막강한 권한을 주고, 다른 부처의 권한까지 집중시키어 실질적이고 효과적인 사이버보안의 중추 역할을 맡기고 있다는 점에서 앞으로의 국내 사이버보안 거버넌스 개선을 위한 참고사례가 될 수 있다. 본 연구의 분석 결과 NCSC는 16가지의 국가 사이버보안 기능 중 무려 6가지의 기능을 수행하고 있었으며, 타 기관들과 협력하여 관여할 수 있는 기능까지 포함한다면 거의 대부분의 국가 사이버보안 기능을 수행하고 있었다. NCSC는 정보공유와 관련해서도 보안부(SS), 비밀정보부(SIS), 정보통신본부(GCHQ)와 긴밀히 협력하며, 보안부 부령에 의해 경찰관서의 특수활동국과도 공조가 가능하다. 또한 2016년 말 통과된 수사권한법(Investigatory Act)은 인터넷서비스 업체가 1년 동안 인터넷 이용자의 기록을 보관하도록 강제하고 있으며, 정보기관의 요청 시 이에 대한 접근이 가능하도록 하고 있다. 만일 현재 논의되고 있는 우리나라의 「국가사이버보안기본법(가칭)」이 국가정보원을 컨트롤타워로 하게 될 시, 사이버공간에 실존적인 위협에 대처할 수 있는 확실한 권한과 적법성을 부여한 영국의 사례를 참고할 만하다. 또한 국민의 프라이버시 침해 우려 등에 대비하여 영국이 사법 및 보안법(Justice and Security Act 2013)에 마련해 둔 제도적 견제 수단과, 영국이 앞으로 내놓을 법·제도적 보완책들도 주의 깊게 지켜볼 필요가 있다.

일본은 2014년 사이버보안 전략에서 언급한 '횡적 사이버보안 대응체제 구축'을 목표로 자기 주도적 사이버보안 역량 강화 전략을 택하고 있었다. 국가 사이버보안의 주도적 역할은 사이버보안 전략 본부와 사이버보안센터(NISC)가 하되, 2015년 제정한 사이버보안기본법이 모든 정부 기관에게 사이버보안 관련 책무를 명확히 명시함에 따라 기관 간 관할 문제

1) Promoting Private Sector Cybersecurity Information Sharing Executive Order 13691

및 업무상 중복·마찰 문제를 최소화하였다. 또한 사이버보안기본법은 단순히 정부부처 뿐만 아니라 국가의 구성원인 지방공공단체, 연구기관, 기업체, 국민 등의 사이버보안 관련 활동에 대한 사항까지 명확히 지정함으로써, 사이버 위협에 대한 사회적 혼선을 최소화하고 위기상황에 체계적으로 대응할 수 있는 발판을 마련하였다. 일본의 사례는 특히 정부부처 사이의 이해상충의 문제와 권한 집중 및 오남용의 우려 등으로 인해 사이버보안기본법의 입법이 지연되고 있는 우리나라의 현 상황에 있어 해결의 실마리를 제공해줄 수 있을 것으로 보인다.

중국은 국가안전부, 인민해방군 등 정보기관이 사이버보안을 주도하고 있으며, 특히 2016년 11월 제정된 「네트워크보안법」은 정부가 영장 청구 등의 절차 없이 네트워크 사업자에 대해 정부가 특정 기술 및 데이터 검열을 요청할 수 있도록 하고 있다. 이처럼 중국은 사이버 공간을 국가 주권 수호의 개념에서 접근 중이며, 이러한 국가 전략과 제정된 법률들을 볼 때 과도하게 인터넷 통제를 강화하고 있고 국민의 기본권인 표현의 자유, 프라이버시 등을 저해할 수 있는 요소도 상당히 많다. 따라서 우리나라도 앞으로 중국 사이버보안 정책 추진 과정과 그에 따라 나타나는 정책 효과 또는 부작용들에 대해 면밀히 관찰하여 향후 정책 방향 수립에 참고할 필요가 있다.

V. 결 론

주요국들은 미국 국가 안보 전략(2015년), EU 사이버보안 전략(2013년), 독일 사이버보안전략(2016년), 영국 국가사이버보안전략(2016년), 일본 사이버보안전략(2015년), 중국 국가 사이버공간 안보 전략(2016년), 한국 국가사이버안보 강화방안(2015년) 등 최근 공통적으로 국가 사이버안보전략을 앞다투어 발표하고 있다. 해당 전략들과 관련 법, 그리고 거버넌스 구성과 사이버보안 기능 별 수행 기관 등을 비교 분석해본 결과 다음 몇 가지로 최근 거버넌스 추진의 공통적 특징을 정리할 수 있었다.

첫째, 국가 거버넌스 추진의 목표가 포괄적인 관점으로 확장되고 있다. 국가 정책이 포괄하여야 할 부분이 기존 정보보호나 사이버 위협에 대비한 국가 방위의 범위에서 산업 보안, 금융 보안, 의료 보안, 개인정보보호 등 다양한 분야의 관련 산업 전반으로 확장됨에 따라, 국가 내에서 운용되는 모든 사이버 공간의 안전과 신뢰를 목표로 두는 관점으로 전환되고 있는 것이다. 예를 들어 과거의 국가 사이버보안 전략에서는 '국가 정보기반시설보호', '국가 중요 인프라 보호', '사이버 안보 및 국방'등이 주요 키워드로 명시되었던 반면, 최근 발표되는 국가 사이버보안 전략들에서는 '안전한 디지털 환경 구축', '신뢰할 수 있는 사이버 공간'등의 키워드들이 주로 사용되어 국가 정책으로 포괄하고 있는 영역으로 보다 넓어진 것을 볼 수 있었다. 이에 따라 각 국은 금융 보안, 산업 보안, 의료 보안 등 각 분야를 관장하는 기관에 사이버보안을 전담하는 조직을 신설하고, 필요시 사이버 위협을 관제할 수 있는 분야 별 사이버보안 관제센터를 설치하도록 하고 있었으며 도움이 필요할 시 정부의 사이버위협 합동대응팀에 협력을 요청할 수 있도록 체계를 정비해가고 있었다.

둘째, 주요국들은 각 국이 구축한 국가 사이버보안 통합 대응 체계의 효율성을 극대화하기 위한 전략을 택하고 있다. 주요국들은 2010년도 전후로 사이버보안 전략, 계획을 발표하고 법률을 제·개정하여 각 국이 처한 환경에 적합한 사이버보안 거버넌스를 구축하였으며, 최근에는 해당 체계에서 법적·제도적으로 발견되는 문제점들이나 비효율적인 부분을 수정·보완하고, 주요 역할을 수행하는 기관 중 법적 권한이 없거나 미비했던 기관에는 법의 제·개정을 통해 법적 권한을 더욱 강화하는 등의 움직임을 보이면서 사이버보안 정책의 실효성과 지속가능성을 높이고 있었다. 예를 들어 영국은 사이버보안의 효율성을 높이기 위해 정부의 정책, 조직 및 구조를 단순화시키고자 노력하고 있으며, 이를 위해 국가사이버보안센터(NCSC)를 설립하고 전략, 법률 등을 통해 기존에 다른 부처가 가지고 있던 사이버보안 기능 다수를 해당 기관으로 이동시키고 있다. 반면 일본은 횡적 사이버보안 대응체계 구축을 목표로 자기 주도적 사이버보안 역량 강화를 위해 노력하고 있으며, 이를 위해 각 소관 분야별 정부 기관에게 사이버보안 관련 책무와 권한을 분담시키고 연계부처에서 내각의 사이버보안센터와 협력 업무를 추진할 수 있도록 개별 조직을 신설하였다.

셋째, 주요국들은 4차 산업혁명 시대가 도래함에 따라 사이버보안 정책을 국가 방위의 관점만이 아닌 국가 경제 발전을 위한 핵심 과제로 인식하고 있다. 각 국이 최근 발표한 국가 사이버보안 전략에는 공통적으로 국가 사이버보안 강화를 통한 경제의 활력, 지속가능한 발전, 사이버 공간의 안전과 신뢰의 확보를 강조하고 있으며 사이버보안 연구 촉진 및 투자

확대, 사이버보안 인식 제고, 사이버보안 인력 양성 등을 통해 사이버보안 산업 자체의 기반을 강화하고 사이버보안 산업을 국가 주요 핵심 분야로 키우고자 하는 움직임을 보이고 있다. 이를 위해 각 국은 사이버보안 산업 강화, 사이버보안 역량 강화 등을 위한 담당 기관을 지정하여 운영하고 있으며, 관련 정책 수행을 위한 예산 투자도 매 년 빠른 속도로 늘리고 있다.

넷째, 정보 공유 및 사이버 위협 공동 대응을 위한 협력 체계가 강화되고 있다. 갈수록 사이버위협의 수준이 고도화됨에 따라 한 기관이 가지고 있는 정보와 기관 내 담당 인력만으로는 사이버 위협에 대한 대응이 불가능해짐에 따라, 부처 간 협력, 민·관·군의 협력과 정보 공유가 필수적인 상황이 된 것이다. 이에 따라 미국은 정부부처조정위원회(GCCs) 및 분야별전문기관(SSAs)를 통해 연방 기관들 간의 협업을 장려하고 있으며, 민간분야에서도 분야별협력위원회(SCC)와 정보공유분석센터(ISACs)을 설립하여 공동체 차원에서 사이버보안 위협에 대응하고 있다. 일본 또한 최근 총무성 주도로 민관 정보공유분석센터(Telecom-ISAC)을 구축하고, 경찰청을 중심으로 방위 및 첨단기술 관련 기업 간 사이버 인텔리전스 공유 네트워크를 구축했을 뿐만 아니라 경제산업성 주도로 주요 인프라 관련 기업 간 사이버정보공유 이니셔티브(J-CSIP)를 구축하는 등 적극적으로 사이버 위협 정보 공유 기능을 강화하고 있다.

다섯째, 국제 협력을 통한 사이버보안 대응 체계를 구축하고자하는 움직임이 두드러지고 있다. 주요 선진국들은 제대로 된 사이버 위협 대응 체계를 구축하기 위해서는 타 국가와의 국제 협력이 반드시 필요함을 인식하고 있었으며, 이를 위해 각국의 국가 정보기관, 외교 담당 기관, 경찰 기관에 공통적으로 사이버위협 대응을 위한 국제 협력 및 수사 공조 기능을 부여하고 있었다. 더불어 거버넌스 특성에 따라 대통령 혹은 총리 산하의 사이버보안센터에 사이버보안 관련 국제 협력 기능을 부여하고 있는 국가도 있었다. 특히 독일이 EU, NATO 등과의 국제 협력을 통해 사이버보안 대응 체계 구축하기 위해 상당한 노력을 하고 있었으며, EU도 한 회원국이 사이버 공격을 당한 경우 EU차원에서 모든 회원국이 대응할 수 있다고 선언하는 등[37], 앞으로 국제 협력을 통한 사이버보안 대응 체계 구축은 선택이 아닌 필수가 될 것으로 보인다.

4차 산업혁명의 시대라고 불리는 현대 사회에서 사이버 보안 없는 국민 안전, 국가 방위, 국가 안보는 무용지물이 될 것이며, 앞으로 국가의 사이버보안 역량은 국가 경쟁력의 핵심 기반이 될 것으로 예상된다. 사이버 공간에서는 더 이상 어떤 국가도 우리의 안위를 보장해줄 수 없으며, 우리 스스로 사이버보안 능력과 역량을 갖춰야만 한다.

우리나라 사이버보안 정책은 주로 사건이 발생한 뒤 이에 대해 즉흥적으로 대책을 발표하고 법률을 제정하는 등 사후 대응의 형태로 형성되어왔기 때문에, 국가 사이버보안 거버넌스의 체계완결성이 부족한 것이 사실이며 각 기관들의 사이버보안 기능 수행의 근거도 명확하지 못한 편이다. 따라서 앞으로 국가 사이버보안 전략의 기조에 맞는 사이버보안에 대한 개념을 명확히 정의하고 사이버보안 컨트롤타워 및 관계 기관들의 법적 권한을 명확히 부여해줄 수 있는 사이버보안 기본법을 서둘러 마련해야 한다. 더불어 주요 선진국들이 부처 간, 기관 간 정보 공유 체계 및 협력 체계를 구축하고 있다는 점도 반영하여 부처 및 기관 사이에 협업 체계를 공고히 할 수 있는 법적 기구와 시스템을 마련하는 것도 입법적 차원에서 반드시 고려되어야 할 것이다.

References

[1] Boannews(2018.04.17.), "Although the summit is approaching, the cyber attack, which is presumed to be North Korea, is ongoing". http://www.boannews.com/media/view.asp?idx=68529&kind=1

[2] arsTECHNICA(2018.04.28.), "As two Koreas shake hands, Hidden Cobra hackers wage espionage compaign". https://arstechnica.com/tech-policy/2018/04/as-two-koreas-shake-hands-hidden-cobra-hackers-wage-espionage-campaign/

[3] Stephen J. Cimbala & Roger N. McDermott, "A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War", Comparative Strategy, pp.95-111, 2015

[4] Sangbae Kim, "Cybersecurity Strategies of Major Powers in World

Politics: From the Comparative Perspective of National Strategies", Journal of International and Area Studies, vol. 26, No. 3, pp.67-108, 2017
〔5〕 Deloitte, "2016 Deloitte Asia-Pacific Defense Outlook", 2016
〔6〕 Sangdon Park, Injung Kim, "A Study on Tasks for the Legal Imporvement for the Governance System in Cybersecurity", Convergence security journal, Vol. 13, No. 4, pp.1-3, 2013.
〔7〕 Korea Internet&Security Agency, "A Comparative Law Study on the Cybersecurity Response System", 2015
〔8〕 Ji-Hyun Kim, "Proposal of Cyber Security Control Tower System in view of Korea's Constitutional Law", Journal of Security Engineering, Vol. 11, No.1, pp.25-40, 2014
〔9〕 Sim, Kwang-ho, Lee, Cheouljoo, Park, Jae-Hyung, "Cyber Terror and Shadow Risk: A Study on the Design of Governance System for the National Cyber Security of Korea", The Journal of Political Science & Communication, Vo.16, No.1, pp.265-296, 2013
〔10〕 Jong-In Lim, "Cyber security policy proposal for the Hyper-connectivity society", Policy study of National Science and Technology Advisory Council, Vol. 2014, No. 5, 2014
〔11〕 The White House, "National Security Strategy", 2015.02.
〔12〕 The Department of Defense, "The DoD Cyber Strategy", 2015.04.
〔13〕 The White House, "Cybersecurity National Action Plan", 2016.02. Homeland Security, "NATIONAL CYBER INCIDENT RESPONSE PLAN", 2016.12.
〔14〕 Homeland Security, "NATIONAL CYBER INCIDENT RESPONSE PLAN", 2016. 12.
〔15〕 Homeland Security, "Comprehensive National Cybersecurity Initiative", 2008.01.
〔16〕 European Commission, "Cybersecurity Strategy of the European Union : An Open, Ssfe and Secure Cyberspace", 2013.07.
〔17〕 European Parliament and of the Council, "Directive on Network Information Security", 2016.07.
〔18〕 Federal Ministry of the Interior, "Cyber Security Strategy for Germany", 2011.02.
〔19〕 Bundesministerium des Innern, "Cyber-Sicherheitsstrategie für Deutschland", 2016.11.
〔20〕 Cabinet Office, "The UK Cyber Security Strategy 2011-2016", 2011.
〔21〕 HM Government, "National Cyber Security Strategy 2016-2021", 2016.11.
〔22〕 HSCIC, "Health and Social Care Information Centre Strategy 2015-2020", 2015.03.
〔23〕 UK Cabinet Office, "A National Information Assurance Strategy", 2007.06.
〔24〕 務省,"識情報社會の實現に向けた情報通信政策の在り方", 2012. http://www.soumu.go.jp/main_content/000169616.pdf
〔25〕 Information Security Policy Council, "Japan Cybersecurity Strategy : Towards a world-leading, resilient and vigorous cyberspace", 2013.06.10.
〔26〕 Cabinet Decision, "Japan Cybersecurity Strategy", 2015.10.04.
〔27〕 Ministry of Defense, "NATIONAL DEFENSE PROGRAM GUIDELINES for FY 2014 and beyond", 2013.12.17.
〔28〕 Mikk Raud, "China and Cyber: Attitudes, Strategies, Organisation", CCDCOE, 2016
〔29〕 Youn Bonghan, "A Study on China's Cyber Security Legislation and Policy: Implications of China's New Cyber Security Law and Our Responses", Policy Study, Vol 189, 53p, 2016

[30] Lindsay, Jon R., Tai Ming Cheung and Derek S. Reveron. "China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain". Oxford University Press, 2015.
[31] Politburo Standing Committee, "National Cyberspace Security Strategy(國家网絡空間安全戰略)", 2016.12.
[32] Ministry of Public Security, "China International strategy of Cooperation on Cyberspace", 2017.03.
[33] Homeland Security, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
[34] Yang. Jeong-yoon, Park. Sang-don, Kim. So-jeong, "Analysis on the U.S. Legislation Relating to Cybersecurity: Overview and Discussion of Five Acts Including National Cybersecurity Protection Act PDF icon", National Assembly Research Service, Vol 7, No.2, p.316, 2015
[35] Senior National Assembly Intelligence Committee member, Review Report on the National Legislation and National Cyber Safety Management, p.3, 2014
[36] Park Sangdon, "A Review on the Role Expansion of German Federal Office for Information Security(Bundesamt für Sicherheit in der Informationstechnik, BSI) in 2017", Journal of Security Engineering, Vol.15, No.2, pp.69-80, 2018
[37] EUROPEAN COMMISSION press release(2017.09.19.), "State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks", Brussels. http://europa.eu/rapid/press-release_IP-17-3193_en.htm
[38] Korea Internet Development Institute, National Institute of Security Technology, "2017 National Information Security White Paper", 2017

[부 록] 주요국 사이버보안 전략/법률 참고 목록

본 연구에서 주요국 사이버보안 거버넌스 분석을 위해 참조한 미국, 독일, 영국, 일본, 중국, 한국 등 6개국의 국가차원의 사이버보안 전략 및 법률은 다음과 같다.

〈미국〉

(전략)
[1] National Security Strategy 2015
[2] The DoD Cyber Strategy 2015
[3] Cybersecurity National Action Plan 2016
[4] National Cyber Incident Response Plan 2017
[5] The Comprehensive National Cybersecurity Initiative

(법률)
[6] Cybersecurity Enhancement Act of 2010
[7] National Cybersecurity Protection Act of 2014
[8] Federal Information Security Modernization Act of 2014
[9] Cybersecurity Workforce Assessment Act, 2014
[10] Cybersecurity Information Sharing Act of 2015
[11] Cybersecurity Act
[12] Development Cyber Security Research and Development Act
[13] National Security Act
[14] State Department Basic Authorities Act
[15] Gramm-Leach-Bliley Act
[16] The Health Insurance Portability and Accountability Act
[17] Economic Espionage Act
[18] Counterintelligence Enhancement Act
[19] Federal Information Security Modernization Act
[20] The Computer Security Act
[21] Management Act
[22] National Defense Authorization Act
[23] Intelligence Reform and Terrorism Prevention Act

〈독일〉

(전략)
[1] EU Cybersecurity Strategy(2013)

〔2〕 EU Directive on Network Information Security(2016)
〔3〕 Cyber Security Strategy for Germany (2011)
〔4〕 Cyber Security Strategy for Germany (2016)
(법률)
〔5〕 Act on the Federal Office for Information Security
〔6〕 Telecommunications Act
〔7〕 Federal Criminal Police Act
〔8〕 German Federal Data Protection Act
〔9〕 German Federal Data Protection Act
〔10〕 Financial Services and integration Act
〔11〕 E-Health Act
〔12〕 IT-Security Act
〔13〕 BND-Gesetz - BNDG

〈영국〉

(전략)
〔1〕 UK Government Strategy for Information Assurance (2007)
〔2〕 The UK Cyber Security Strategy (2011)
〔3〕 National Cyber Security Strategy 2016-2021(2016)
〔4〕 HSCIC Strategy 2015-2020 (2015)
(법률)
〔5〕 Justice and Security Act
〔6〕 Investigatory Powers Act
〔7〕 Data Protection Act
〔8〕 Freedom of Information Act
〔9〕 Financial Services and Markets Act
〔10〕 National Audit Act
〔11〕 Security Service Act
〔12〕 Anti-terrorism, Crime and Security Act
〔13〕 Intelligence Service Act

〈일본〉

(전략)
〔1〕 Active Japan ICT (2012)
〔2〕 Japan Cybersecurity Strategy (2014)
〔3〕 Japan Cybersecurity Strategy (2015)
〔4〕 NATIONAL DEFENSE PROGRAM GUIDELINES for FY 2014 and beyond(2013)
(법률)
〔5〕 Basic Act on the Formation of an Advanced Information and Telecommunications Network Society
〔6〕 Important Action Plan for Information Security Third Action Plan for Measures
〔7〕 The Basic Act on Cybersecurity
〔8〕 Amended Personal Information Protection Law
〔9〕 Financial Services Agency Establishment Act
〔10〕 Ministry of Health, Labour and Welfare Establishment Act
〔11〕 Unfair Competition Prevention Act

〈중국〉

(전략)
〔1〕 National Cyberspace Security Strategy (2016)
〔2〕 China International strategy of Cooperation on Cyberspace (2017)
(법률)
〔3〕 People's Republic of China Network Security Law
〔4〕 Information Security Regulations
〔5〕 Information security technology and privacy guidelines
〔6〕 Consumer Rights Protection Law
〔7〕 The Legislation of Electronic Financial Transactions
〔8〕 Electronic Bank Safety Assessment Guidelines
〔9〕 Anti-Unfair competition Law
〔10〕 National Intelligence Law of China
〔11〕 Regulation about prohibiting infringement of trade secret

〈한국〉

(전략)
〔1〕 National Cyber Security Master Plan (2011)
〔2〕 Comprehensive Measures for Information Security Industry Development (2013)
〔3〕 K-ICT Security Development Strategy (2015)
〔4〕 National Cyber Security Strengthening Plan (2015)
〔5〕 The 1st Information Security Industry Promotion Plan (2016)
〔6〕 ICT-based Future Healthcare Policy Roadmap (2016)

(법률)
〔7〕 National Intelligence Service Korea Act
〔8〕 National Cyber Safety Management Regulations
〔9〕 Act on the protection of the Information and Communications Infrastructure
〔10〕 Act on Information and Communications Network
〔11〕 Framework Act on National Informatization
〔12〕 Personal Information Protection Act
〔13〕 Act on Promotion of Information Protection Industry
〔14〕 Act on the Establishment of the Financial Services Commission
〔15〕 Electronic financial transaction law
〔16〕 Act on the Prevention and Protection of Industrial Technology Spill
〔17〕 E-government Act
〔18〕 Basic Act on Government Business Evaluation
〔19〕 Information security system evaluation and certification guidelines
〔20〕 Criminal law
〔21〕 Armed Forces Cyber Command order

〈저자소개〉

주 문 호 (Moon-ho Joo) 학생회원
2014년 8월: 고려대학교 정보통신대학 컴퓨터공학 학사
2017년 8월: 고려대학교 정보보호대학원 박사과정 수료
2017년 9월~현재: 고려대학교 정보보호연구원 전문연구요원
〈관심분야〉 정보보호정책, 개인정보보호, 금융보안, 융합기술보안, 사이버법률, 사이버국방 등

권 헌 영 (Hun-Yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 졸업
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2008~2015년: 광운대학교 법학과 교수
2015년 9월~현재: 고려대학교 정보보호대학원 교수
現 공공데이터법제도전문위원회 위원장, 개인정보분쟁조정위원회 위원, 한국교육학술정보원 이사, 한국인터넷윤리학회장 및 사이버커뮤니케이션학회 부회장 등 역임
〈관심분야〉 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부

임 종 인 (Jong In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보보호대학원 교수/사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 한국 CISO협회장, 국방부 정보화책임관자문위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등