국가 사이버보안 전략 수립과 개선을 위한 참조 모델 개발

윤재석*

요 약

세계 많은 국가들은 사이버위협으로 인한 피해를 사전에 예방하고, 사고 발생 시 그 피해를 최소화하기 위해 국가 차원의 사이버보안 전략을 수립하여 이행하고 있다. 그러나 국가 사이버보안 전략은 해당 국가가 처한 환경과 필요에 따라 그 수준과 범위에 있어 상당한 편차를 보이고 있다. 어느 한 곳의 취약점은 전 세계적인 문제로 이어질 수 있다는 점에서 국가 사이버보안 전략 수립을 지원하고 개선하기 위해 국제기구를 비롯한 관련 기구, 기관에서 다양한 지침서가 개발되었다. 본 논문에서는 국가 사이버보안 전략 수립을 위해 발표된 각종 지침서를 분석하고, 주요 공통요소를 도출한 참조 모델을 제시하였다. 아울러 이를 우리나라 정책과 비교하여 미흡한 부분에 대한 보완대책을 제안하였다.

Developing Reference Model for National Cybersecurity Strategy Establishment and Improvement

Jaesuk YUN*

ABSTRACT

A number of countries have been developing and implementing national cybersecurity strategy to prevent damages caused by cyber threats and to minimize damages when they happened. However, there are a lot of differences and disparities in respective strategies with their own background and needs. A vulnerability in some places can be a global problem, so various guidelines have been developed by relevant organizations including international organizations to support the establishment of national cybersecurity strategies and improvement of them. In this paper, with analysis on the guidelines for the establishment of national cybersecurity strategies, reference model consisting of common elements of strategies was suggested. And several recommendations for the improvement measures for Korean national cybersecurity strategies were explained with a comparison of the reference model.

Key words : National cybersecurity strategy, Reference model, Critical infrastructure protection, CSIRT, ISMS

접수일(2016년 5월 31일), 수정일(1차: 2016년 6월 18일), 게재확정일(2016년 6월 23일)

* 한국인터넷진흥원

1. 서 론

인터넷 경제가 발전하면서 전 세계적으로 디지털 환경을 통해 수많은 경제적, 사회적 혜택을 향유할 수 있는 기회가 창출되고 있다. 특히 사물인터넷, 클라우드 등과 같은 새로운 정보통신기술의 발전에 따라 다양하고 새로운 서비스가 활발히 시장에 나타나고 있다. 그러나 사이버범죄로 인한 피해가 2019년 2조 달러에 달할 것으로 예측되는 등 개인과 사회는 물론, 주요 기반시설에 대한 사이버공격으로 인한 국가 안보차원의 위험도 증가하고 있다[1].

이에 세계 많은 국가들은 사이버위협으로 인한 피해를 사전에 예방하고, 사고 발생 시 그 피해를 최소화하기 위해 국가 차원의 사이버보안 전략을 수립하여 이행하고 있다. 그러나 국가 사이버 보안 전략은 해당 국가가 처한 환경과 필요에 따라 그 수준과 범위에 있어 상당한 편차를 보이고 있다. 사이버위협으로 인한 피해가 비단 한 개별 국가에 국한되지 않고 순식간에 전 세계로 파급된다는 점에서 일련의 공통적인 대응요소가 마련될 필요가 있다. 국경을 뛰어넘는 사이버위협과 그 파급력은 사물인터넷과 비약적인 통신 속도의 증가로 파괴력이 상당하기 때문에 이에 즉각 대응하기 위한 프레임워크를 마련하고 전 세계적으로 통용될 수 있는 최소한의 규제 거버넌스를 구축함으로써 피해를 줄일 수 있다. 또한 아직 국가차원에서 사이버보안 전략을 마련하지 못한 국가들은 이를 참조하여 정책방안을 마련함으로써 사이버위협에 보다 효과적으로 대응할 수 있다.

이를 위해 UN 산하 ICT 전문 기구인 ITU를 비롯하여 경제협력개발기구(OECD), 북대서양조약기구(NATO), 유럽정보보호 전문기관인 ENISA 등에서 국가 사이버보안 전략 수립을 위한 가이드를 다수 발간하였다. 아울러 국가 간 전략 비교를 통한 장단점 분석[5][7], 전략 이행과정의 문제점을 개선하기 위한 평가 방법론에 대한 연구[13] 등이 진행되고 있다. 그러나 국가 전략 수립을 위해 일관적으로 고려해야 하는 요소에 대한 연구는 다소 미진한 상황이다.

본 연구에서는 전 세계 국가 사이버보안 전략 수립 현황을 살펴보고, 국제기구 등에서 발표한 관련 가이드라인과 지침 등을 분석하여 공통요소를 도출한 참조모델을 제시하도록 한다. 아울러 이를 우리나라 정책과 비교하여 미흡한 부분에 대한 보완책을 제안하도록 한다.

2. 전 세계 사이버보안 전략 수립 현황

ITU의 조사에 따르면 현재 회원국 193개 국가 중 72개 국가에서 사이버보안 전략을 수립한 것으로 나타났다[2]. ENISA에 의하면 유럽연합 28개 회원국 중 23개 국가, 그 외 지역 국가는 34개에 이르는 것으로 조사되었다[3]. 한편 NATO에 따르면 국가 사이버보안 전략을 수립한 국가는 65개에 이른다[4]. 조사별로 편차가 있기는 하지만 대략적으로 50여개에서 70여개에 이르는 국가가 사이버보안 전략을 수립한 것으로 파악되었다.

<표 1> 전 세계 국가 사이버보안 전략 수립 현황

	ITU	ENISA	NATO
Member states	72	23	21
Non member states	-	34	44
Total	72	57	65

사이버보안 전략의 수준과 범위는 국가별로 그 시기와 환경에 따라 상당한 차이를 보이고 있다. 2000년대 초 중반에 수립된 여러 국가의 사이버보안 전략은 주로 급격한 컴퓨팅 연산 능력과 네트워크 발전에 따라 발생하는 피해에 대응하기 위해 컴퓨터침해대응팀(Computer Security Incident Response Team: CSIRT) 설립 혹은 사이버범죄에 대응하기 위한 법적 규제 프레임워크 구축에 중점을 두고 있다[5]. 이후 새로운 ICT 서비스의 출현과 확대에 따라 사이버보안 이슈가 국가차원의 안전 문제로 부상하고, 이를 국가 안보, 경제적 이슈, 그리고 공공의 안녕의 관점에서 바라보는 인식의 확장이 일어나게 된다[6].

이에 따라 국가 사이버보안 전략에서 공통적으로 나타나는 요소는 크게 ① 모든 정부의 역량을 포괄하는 정책의 수립 ② 민간과 공공에 걸쳐 모든 이해 관계자들이 역할과 책임을 체계적으로 정립 ③ 국제적

공조 노력의 강조 등이다[7]. 그러나 사이버공간과 보안에 대한 개념 정의, 국가 사이버보안을 수행할 기관 지정과 역할과 책임의 정의, 그리고 개별 국가에서 어떤 요소에 더욱 중점을 둘지에 따라 전략수립과 실제 이행상황은 다양한 편차가 나타나고 있다.

3. 국가 사이버보안 전략 참조모델

3.1 국가 사이버보안 전략 사례

국가 사이버보안 전략을 수립을 지원하기 위해 여러 국제기구, 기관에서 다양한 지침서, 가이드라인, 권고 등 여러 종류의 참조 모델을 개발하였다. 그 범위는 <표 2>와 같이 국가 사이버보안 전략 수립을 위한 가이드에서 컴퓨터침해사고대응팀(CSIRT) 구축 및 운영 방법론, 주요 정보통신기반시설 식별 및 보호 방법, 사이버보안 성숙도 측정, 사이버보안 인식도 제고, 디지털 보안 위험관리, 개인정보보호 등으로 다양하다.

<표 2> 사이버보안 가이드라인 발간 현황

Org.	Subject
Carnegie Mellon	Handbook for Computer Security Incident Response Teams (CSIRTs)
Commonwealth Cybercrime Initiative (CCI)	Harare Scheme on Mutual Legal Assistance in Criminal Matters
	Commonwealth Network of Contact Persons Framework
Commonwealth Telecommunications Organisation (CTO)	Commonwealth Approach for Developing National Cyber Security Strategies
ENISA	National Cyber Security Strategies: Practical Guide on Development and Execution
	An Evaluation Framework For National Cyber Security Strategies
	NCSS, Setting the course for national efforts to strengthen security in cyberspace
	Methodologies for the identification of Critical Information Infrastructure assets and services
Global Cyber Security Capacity Centre	Cyber Security Capability Maturity Model
ITU	National Cybersecurity Strategy Guide
	Global Cybersecurity Index
MS	Developing a National Strategy for Cybersecurity
NATO CCD COE	National Cyber Security Framework Manual
	National Cyber Security Strategy Guidelines
NIST	Framework for Improving Critical Infrastructure Cybersecurity
OAS	Cyber Security Awareness Campaign Toolkit
	Report Cybersecurity and Critical Infrastructure in the Americas
	CSIRT Best Practice Guide
OECD	Recommendation of the Council on the Protection of Critical Information Infrastructures
	Report on The Development of Policies for the Protection of Critical Information Infrastructures
	Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity
	Companion document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity
	Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder flows of Personal Data (Privacy Guidelines)
Potomac Institute	Cyber Readiness Index
UNCTAD	A framework for information and communications technology policy reviews
	Global Cyberlaw Tracker
WEF	Global Agenda Council on Risk & Resilience: Resilience Insights

본 연구에서 제시하고자 하는 사이버보안 전략 수립을 위한 참조 모델의 역할은 ① 개별 국가 수준을 넘어 전 세계적으로 적용될 수 있는 레퍼런스 가이드, ② 새로운 전략 수립과 기존 전략의 개선을 위한 레퍼런스 가이드, ③ 평가도구 개발과 개선사항 도출, 개선 방법에 대한 권고 제시, ④ 기존 모델, 가이드라인, 평가 도구와 연계, ⑤ 우수사례지표(Good Practice Indicators: GPI)를 통한 개선사항 평가 등으로 구분할 수 있다.

이들 가이드를 통해 정책결정자들은 국가 차원에서 어떻게 국가 사이버보안 전략을 수립하고, 이를 이행하는지에 대해 도움을 얻을 수 있다. 또한 다른 모범사례와 비교를 통해 국가 사이버보안 역량 수준을 평가하고 개선점을 도출할 수 있다.

개별 국가들은 자신들의 국가 사이버보안 수요와 필요요건에 따라 중점적으로 추진할 각자의 전략 분야를 결정해야 할 필요가 있다. 그러나 국가 사이버보안 전략은 일반적으로 통용될 수 있는 합의에 기반 하는 것이 바람직하다. 국가 사이버보안 레퍼런스 모델 수립을 위해 고려해야 할 주안점은 ① 국가별로 국가 사이버보안 전략 수립의 목표 도출, ② 국가 사이버보안 개발과 이행을 위한 체계적인 프로세스 확립, ③ 국가 사이버보안 전략이 포괄해야 하는 전략 분야 판별, ④ 국가 사이버보안 전략의 실행을 위한 인력과 자원의 할당 등으로 요약할 수 있다.

3.2 국가 사이버보안 전략 수립 참조 모델

앞서 제시한 국제기구 및 기관, 단체에서 발간한 사이버보안 가이드와 지침 등은 그 수준과 내용면에서 다양하다. 참조모델 수립을 위해 그간 발표된 사이버보안 전략 등을 분석하고, ITU, OECD, Oxford 대학 등 이 분야 전문가들의 의견 수렴을 거쳐 사이버보안 전략 수립에 있어 필요한 요소들로서 ① 국가 사이버보안 거버넌스, ② 국가 사이버보안 프레임워크, ③ 주요기반시설 보호, ④ 침해사고 대응, ⑤ 연구개발 역량 배양, ⑥ 인식제고, ⑦ 법적 체계 구축, ⑧ 국제 공조 등을 도출하였다.

먼저 국가 사이버보안 거버넌스의 구성 요소는 정책 수립과 이행을 위한 체계 구축, 역할과 책임의 범위, 자원의 배분, 그리고 순환구조를 이루기 위한 검토 및 개선 등으로 나누어볼 수 있다. 두 번째로 국가 사이버보안 프레임워크는 세부적으로 어떠한 분야에 정부 차원에서 중점을 두어야 하는지, 그리고 주요 사이버 기반시설에 대한 보호 대책의 체계 등이 포함될 수 있다. 세 번째는 주요 기반시설에 대한 보호대책으로서, 에너지, 수력, 운송, 정보통신 등 국가 기반시설에 대한 판별 및 보호 대책이 포함된다. 네 번째는 사이버 침해 사고에 대한 대응이다. 다섯 번째는 국가 사이버보안 기술역량 배양, 여섯 번째는 인식 제고, 일곱 번째는 법적 체계, 그리고 마지막 여덟 번째는 다른 국가, 정부와의 국제공조이다. 이를 통해 <표 3>과 같이 국가 사이버보안 전략 개발을 위한 참조 모델을 도출할 수 있다.

<표 3> 국가 사이버보안 전략 수립을 위한 참조모델

	Area	Description
1	National Cybersecurity Governance	A. Framework and implementation plan B. Determination of responsibilities and roles C. Allocation of resources D. Review cycle
2	National Cybersecurity Framework	A. Main area governments should focus on B. Framework for the protection of national cyber infrastructures
3	Critical Infrastructure Protection(CIP)	A. Programs to identify and protect critical services (e.g. energy, water, transports, telecommunications, etc.)
4	Incident Response	A. Detection of and response to cyber incidents
5	Capability Development	A. Advancement of national cybersecurity R&D programs
6	Awareness	A. Programs to foster awareness of cybersecurity
7	Legal Framework	A. Formalization of the framework B. Definition of illegal cyber activities C. Establishment & Operation of the agencies that will enforce the legal framework
8	International Cooperation	A. Outreach, partnership, and information sharing activities between different governments

4. 국내 정책 및 참조모델 비교분석

우리나라에서 국가차원의 사이버보안 종합계획은 대표적으로 2009년 9월 발표한 '국가 사이버위기 종합대책', 2011년 8월 발표한 '국가 사이버안보 마스터플랜', 그리고 2013년 7월 발표한 '국가 사이버안보 종합대책' 등을 들 수 있다.

4.1 국가 사이버위기 종합대책 주요내용

국가 사이버위기 종합대책은 2009년 발생한 '7.7 DDoS공격'을 계기로 수립되었다. 주요 내용을 살펴보면, 우선 평시 국가기관 간 사이버위기관리 기능을 보다 명확히 한 점을 들 수 있는데, 즉 정보기관인 국가정보원이 사이버위기대응 총괄 역할을 수행하고, 방송통신위원회는 좀비 PC 제거 및 국민대상 사이버안전홍보 및 계도업무를 담당하며, 국방부가 사이버부대를 편성하여 군사 분야를 보강하게 하였다. 또한, 민간분야에서 사이버안전 수준을 제고하기 위해 학교와 직장, 그리고 민방위 훈련 시 사이버보안교육을 확대하고, 기업 정보보호 등을 위해 사이버보안관을 양성하며, 자동차·조선 등 산업별 협회에 보안 관제센터를 설립하여 사이버침해 차단 및 산업기밀 보호 활동을 강화하도록 하였다.

당면 과제로는 사이버위기 관리체계를 강화하였는데, 국가 사이버위기 발생 시 민·관 합동 범정부 대책기구를 구성하여 위협분석 및 경보발령, 외국과 공조체계 가동 등을 총괄하며, 언론창구는 방송통신위원회로 일원화하는 등 위기관리체계를 정비하였다. 또한, 악성프로그램 삭제요청권, 침해사고 발생 시 시스템 접근 요청권 등의 법적 근거를 마련하고 국가위기관리 기본지침 등 정부 규정을 개정하여 대책기구 구성, 경보발령 요건 구체화 등을 보완키로 하였다.

2010년까지 추진할 과제로 정부의 사이버안보 리더십을 강화하기 위해 사이버대응 조직을 보강하고 사이버보안관 3,000명 등의 전문 인력 양성 기반을 조성하며, 사이버공격 탐지 사각 지대 해소 등 사이버방어 환경을 개선키로 하였다. 또한 중앙정부의 망 분리 사업을 예정대로 추진하되, 지방정부의 보안 관리도 중요하기 때문에 지자체의 망 분리도 정부가 지원하여 추진하기로 하였다. 한편 주요 중장기 과제로 법제도 정비는 물론, 정보화 예산 대비 정보보호 예산을 단계적으로 확대하고, 정보보호 설비투자 제고를 위해 조세감면도 지속 지원키로 하며, 전력·통신 등 국가기능 유지 핵심시설의 보안체계도 고도화하기로 하였다. 특히 새로운 정보화 투자도 중요하지만, 사이버전 환경 변화를 고려하여 기존의 정보통신망과 기반시설 보호를 강화하기 위해 사이버공격 대응기술 개발·활용, 사이버보안 예산 증액 및 관련 교육 강화를 보다 적극적으로 추진하기로 하였다[8].

4.2 국가 사이버안보 마스터플랜 주요내용

국가 사이버안보 마스터플랜은 국가안보를 위협하는 사이버공격에 종합적이고 체계적으로 대응하기 위해 2011년 8월 발표되었다. 마스터플랜에는 국가차원의 사이버위협 대응체계 정비 및 관련 부처별 역할 정립, 분야별 중점 추진과제 등이 포함되었는데 먼저 대응체계 정비 및 부처별 역할 정립에 있어서는 각종 사이버위협에 총력 대응할 수 있도록 '국가사이버안전센터'를 중심으로 관계 부처 간 협력·공조와 민간 전문가 참여를 확대해 나가는 한편, 국가정보원의 컨트롤타워 기능과 부처별 역할을 명확히 하여 지속적으로 제기되었던 기관간의 업무 혼선·중복 및 사각지대 발생의 문제점을 해소하기로 하였다. 즉, 평상시는 물론 위기 상황 시 총괄 역할을 국가정보원으로 하고, 방송통신 분야는 방송통신위원회, 금융부문은 금융위원회, 국방 분야에서는 국방부, 그리고 전자정부대민서비스와 정부전산센터 등 행정 분야에서는 행정안전부가 주무 담당부서의 역할을 담당하기로 하였다. 그리고 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·추진키로 하였는데, 예방 측면에서 전력, 금융, 의료 등 기반시스템 운영기관 및 기업들의 중요 정보 암호화 등 보호조치를 강화하고, 주요 핵심시설에 대한 백업센터 및 재해복구시스템 확대 구축과 정부 S/W개발 단계에서의 보안취약점 사전 진단 제도의 의무화 등을 추진하는 한편, 국제공조 강화를 통해 사이버도발 억지력을 확보해 나가기로 하였다. 탐지 측면에서는 범국가적 사이버공격에 대응하기 위해 3線 방어체계(국제관문국·인터넷연동망 ↔ 인터넷서비스 사업자(ISP) ↔ 기업·

개인) 개념을 도입하여 공격 트래픽을 단계별로 탐지·차단하기로 하였다. 또한 지자체 정보시스템의 사이버공격 탐지도 실시하고 보험·카드사 등 제2금융권 전산망에도 보안관제를 확대해 나가는 한편, 북한産 불법S/W 유통 감시·차단 활동을 강화하고 금융·통신 등 민간 주요시스템은 전문 업체를 활용한 보안점검을 年 1회 이상 이행토록 의무화하기로 하였다. 대응 측면에서는 조직적인 해커공격에 대해 외부전문가가 참여하는 '민·관 합동 대응반'을 운영하고 주요 국가 및 국제기구와의 협력을 강화하여 고도화되는 해킹에 총력 대응하기로 하였다. 제도 측면에서는 국가·공공기관 대상 정보보안 평가제도 개선, 민간기업 정보보호 관리체계(ISMS) 인증 활성화, 금융 분야 'IT부문평가' 대상기관 확대 등을 추진하고, 민간기업 해킹사고 발생 시 경영자의 책임을 명확히 하는 한편, 용역업체에 의한 사고 시 민·형사상 책임을 함께 묻도록 하는 등 용역사업 및 민간분야 보안 관리를 강화키로 하였다. 아울러 범정부 차원의 '사이버안전의 날' 제정·시행과 '클린 인터넷 운동' 활성화 등을 통해 사회 전반의 사이버안보에 대한 마인드 확산에 주력하기로 하고, 사이버위협 대응을 보다 효율화하기 위해 관련 법령의 정비도 추진해 나가기로 하였다. 마지막으로 기반 측면에서도 각 정부기관의 정보보안 인력 증원 및 금융위원회 보안업무 전담조직 신설, 한국인터넷진흥원의 정보보호 정규직 비율 상향, 원전 등 국가 핵심 기반시설 운영기관의 보안 전담인력 확보 등을 추진하는 한편, 정보보호학과 증설 및 계약형 석사과정 확대, S/W 분리발주 정착, 국내 정보보호제품의 해외수출 지원 및 정보보호 R&D 확대 등 관련 산업 및 연구 활성화 지원도 강화키로 하였다[9].

4.3 국가 사이버안보 종합대책 주요내용

2013년 7월에 발표된 국가 사이버안보 종합대책은 '3.20 사이버테러' 및 '6.25 사이버공격' 등을 계기로 청와대와 국가정보원, 미래창조과학부와 국방부, 안전행정부 등 16개 관계부처 합동으로 수립하였다. 종합대책은 '선진 사이버안보 강국 실현'을 목표로 4대 전략에 따라 수립되었는데 첫째, 사이버위협 대응체계 즉응성 강화를 위해 사이버안보 컨트롤타워는 청와대가 맡기로 하였고, 실무총괄은 국가정보원이 담당하며, 미래창조과학부와 국방부 등 관계 중앙행정기관이 소관 분야를 각각 담당토록 하는 대응체계를 확립하였고 청와대와 국가정보원, 그리고 미래창조과학부 등 대응기관이 사이버상황을 즉시 파악하여 대처할 수 있도록 동시 상황전파 체계를 구축하였으며, 중요 사고에 대해서는 '民·官·軍 합동대응팀'을 중심으로 상호협력 및 공조를 강화하기로 하였다. 둘째, 기관 간 원활한 정보공유가 부족하다는 지적에 따라 유관기관 스마트 협력체계를 구축하기 위해 국가차원의 '사이버위협정보 공유시스템'을 2014년까지 구축하고, 이를 토대로 민간 부문과의 정보제공·협력도 강화해 나가기로 하였다. 셋째, 사이버공간 보호대책 견고성 보강을 위해 2017년까지 집적정보통신시설(IDC)·의료기관 등을 포함한 주요정보통신기반시설을 209개 수준에서 400개로 확대하고 국가기반시설에 대해 인터넷망과 분리·운영하는 한편, 전력·교통 등 테마별로 특화된 위기대응훈련을 실시키로 하였다. 주요 민간 기업에 대해서는 정보보호 관리체계(ISMS) 인증 대상을 150개에서 500개로 확대하고 중소기업을 대상으로 보안취약점 점검 및 교육지원 등을 통해 국가전반의 보안수준을 향상시켜 나가기로 하였다. 넷째, 사이버안보를 위한 창조적 기반을 조성하기 위해 최정예 정보보호 전문가 양성사업 확대 및 영재교육원 설립 등 다양한 인력양성 프로그램을 추진하여 2017년까지 사이버 전문 인력 5,000명을 양성하고, 미래시장 선점을 위해 암호, 인증, 인식, 감시, 탐지 등 5대 기반 분야, 그리고 스마트폰, 사물인터넷(IoT/M2M), 클라우드, 지능형교통체계(ITS), 사회기반 등 5대 신성장 분야의 10대 정보보호 핵심기술 선정과 연구개발을 통해 기술 경쟁력도 강화해 나가기로 하였다[10].

4.4 우리나라 사이버보안 전략 비교 및 제언

앞서 도출한 참조모델과 우리나라의 국가 사이버보안 전략을 비교, 분석하면 다음과 같은 미비 사항을 도출할 수 있다.

첫째, 사이버보안 거버넌스 측면에서 살펴보면 전략 수립과 이행, 그리고 각 행위 주체의 역할과 책임은 비교적 잘 제시하고 있지만, 자원의 할당과 추후 검토, 보완 등에 대한 적시는 미흡한 것으로 나타났다.

둘째, 보안기술 개발 노력에 대한 구체적인 방안 제

시는 비교적 미비한 것으로 나타났다.

셋째, 법적 체계 구축에 대한 제시는 비교적 미흡한 것으로 나타났는데, 이는 기존에 정립된 사이버보안상의 법률 체계를 모두 포괄하지 않기 때문인 것으로 보인다.

넷째, 국제 협력과 관련된 대책은 비교적 잘 제시된 것으로 나타났지만, 구체적인 실행방안에 대한 제시는 다소 미흡한 것으로 분석된다.

<표 4> 우리나라 사이버보안 전략 비교

	Area		NCS(Sept. 2009)	NCS(Aug 2011)	NCS(July 2013)
1	National Cybersecurity Governance	A	○	○	○
		B	○	○	○
		C	X	○	X
		D	X	X	X
2	National Cybersecurity Framework	A	○	○	○
		B	○	○	○
3	Critical Infrastructure Protection(CIP)	A	○	△	○
4	Incident Response	A	○	△	○
5	Capability Development	A	△	X	○
6	Awareness	A	○	○	△
7	Legal Framework	A	△	△	△
		B	X	X	△
		C	△	△	△
8	International Cooperation	A	△	○	X

이상의 내용에서 다음과 같은 제안사항을 도출할 수 있다.

먼저 사이버보안 거버넌스 측면에 해당 기관의 역할과 책임이 보다 명확하고 구체적으로 정립되어 이행되어야 할 필요가 있다. 또한 전 부문을 포괄할 수 있는 국가 사이버보안 전략의 수립과 세부 이행과제의 정립, 산재된 사이버보안 관련 법률의 통합을 통한 효율성 제고, 사이버보안 분야 국제적 공조 및 협력을 증진하기 위한 체계 구축, 국가 사이버보안 전략 수립과 이행에 따른 평가와 성과 점검, 그리고 이를 다시 정책에 반영하는 환류체계의 구축 등이 필요하다.

5. 결 론

상이한 환경에 따라 규제 환경도 마찬가지로 다르게 나타날 수 있다. 그러나 사이버보안 위협의 파급력을 고려할 때 이를 능동적으로 대응하기 위한 글로벌 차원의 규제 프레임을 상정하고 개별 국가의 상황에 맞는 전략적 보안정책 입안과 수행이 필요하다. 아울러 개별 국가 정부 차원에서 사이버보안 정책 수립을 위해 필요한 요건을 도출하고 이행하기 위한 절차를 수립하는 것이 중요하다.

본 연구는 국제기구와 여러 관련 기관이 마련한 사이버보안 전략 수립 지원 자료를 분석하여 국가 차원의 전략 수립을 위한 참조모델을 제시하였다. 그리고 이를 우리나라 정책과 비교하여 미비점을 판별하고, 개선 필요사항을 도출하여 대안을 제시했다는 점에서 의의가 있다. 아울러 본 연구는 우리나라 기업이 개도국에 진출 시 국가 차원의 사이버보안 전략 수립을 위한 참고자료로 활용할 수 있을 것으로 기대된다.

본 연구는 우리나라 사이버보안 정책에 대한 전체 내용에 대한 접근이 제한되어 보다 세밀한 분석이 이루어지지 못했다는 한계가 있다. 이에 따라 향후 후속 연구과제로서 논문에 제시된 3개 국가 전략을 포함, 그간 우리나라 정부에서 발표한 사이버보안 관련 정책과 전략을 포괄하여 FGI, 서베이 등 구체적인 방법론 적용을 통해 보다 세부적으로 분석하는 것이 필요하다. 아울러 전 세계 지역별 혹은 수준별 국가 사이버보안 전략에 대한 구분과 비교 분석 등을 통해 차이점과 유사점을 판별하고, 국내 정책의 미흡한 부분에 대한 개선대책을 제시할 수 있을 것으로 보인다. 그리고 시기별, 지역별 주변 환경과 글로벌 차원의 사이버전략 수립 변화내용을 살펴봄으로써 보다 시의 적절한 사이버보안 정책 수립과 이행방안 마련이 가능할 것으로 판단된다. 마지막으로 국가 사이버보안전략 수립과 이행에 있어 성과 평가에 대한 보다 정량화된 모델 개발

을 통해 보다 효율적인 정책 이행이 가능할 것으로 예측된다.

참고문헌

[1] “Cybercrime Will Cost Businesses Over $2 Trillion by 2019.” Juniper Research. Accessed May 24, 2016. http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[2] “National Strategies Repository.” ITU. Accessed May 12, 2016. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

[3] “National Cyber Security Strategies (NCSSs) Map”, ENISA. Accessed May 21, 2016. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[4] “Cyber Security Strategy Documents”, NATO CCDCOE. Accessed May 23, 2016. https://ccdcoe.org/strategies-policies.html.

[5] Newmeyer, Kevin P. “Elements of National Cybersecurity Strategy for Developing Nations.” National Cybersecurity Institute Journal Volume 1, No3. (n.d.): 9 - 19.

[6] Mulligan, D. K., & Schneider, F.B., Doctrine for cybersecurity. Daedalus 140(4), 70-92. 2011.

[7] Luiijf, E., Besseling, K. and de Graaf, P. 'Nineteen national cyber security strategies', International journal of critical infrastructures, Vol. 9(1/2), 3-31. 2013.

[8] 방송통신위원회, 국가 사이버위기 종합대책, 2009. 9.

[9] 방송통신위원회, 국가 사이버안보 마스터 플랜, 2011. 8.

[10] 미래부 등 관계부처 합동, 국가 사이버안보 종합대책, 2013. 7.

[11] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski., Handbook for Computer Security Incident Response Teams (CSIRTs). CMU/SEI-2003-HB-002. Carnegie Mellon University, 2003.

[12] Hasna ELKHANNOUBI, Mustapha BELAISSAOUI, “A Framework for an Effective Cybersecurity Strategy Implementation.” Journal of Information Assurance & Security. 2016, Vol. 11 Issue 4, p233-241.

[13] JungMin Kang, HyunUk Hwang, JongMoon Lee, YoungTae Yun, ByungChul Bae, and SoonYoung Jung. “A Study on National Cyber Capability Assessment Methodology.” Journal of the Korea Institute of Information Security and Cryptology 22, no. 5 (2012): 1039 - 1055.

[14] Wamala, Frederick. “ITU NATIONAL CYBERSECURITY STRATEGY GUIDE,” September 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf.

[15] Wamala, Frederick. “ITU NATIONAL CYBERSECURITY STRATEGY GUIDE,” September 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf.

[16] Loukas, George. Cyber-Physical Attacks: A Growing Invisible Threat. Butterworth-Heinemann, 2015.

[17] “Cyber Security Strategy Documents”, NATO CCDCOE. Accessed May 23, 2016. https://ccdcoe.org/strategies-policies.html.

[18] “National Cyber Security Strategies : Practical Guide on Development and Execution.” ENISA, December 2012.

[19] Liveri, Dimitra, Anna Sarri, An Evaluation Framework for National Cyber Security Strategies, ENISA, 2014. http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

[20] “National Cyber Security Strategies : Practical Guide on Development and Execution.” ENISA,

December 2012.
[21] “Cybersecurity Policy Making at a Turning Point : Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy”, OECD, 2012.
[22] “Framework for Improving Critical Infrastructure Cybersecurity.” NIST, February 2014.
[23] Demchak, Chris, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri., “CYBER READINESS INDEX 2.0,” 2015. http://potomacinstitute.org/images/CRIndex2.0.pdf .
[24] “Recommendation of the Council on the Protection of Critical Information Infrastructures.” OECD, June 2008.

[저 자 소 개]

윤 재 석 (Jaesuk YUN)

1998년 2월 동국대 영어영문 학사
1998년 2월 서강대 신문방송 석사
2011년 2월 고려대 정보보호대학원 박사 수료

email : jsyun@kisa.or.kr