Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1293

국가 사이버보안 역량 평가를 위한 평가항목 연구

배 선 하,† 박 상 돈, 김 소 정‡
국가보안기술연구소

A study on the Development for the National Cybersecurity Capability Assessment Criteria

Sunha Bae,† Sangdon Park, So Jeong Kim‡
National Security Research Institute

요 약

ICT가 사회 주요 기반 구조로 자리매김 함에 따라 사이버 공간을 보다 안전하고, 효과적으로 활용하기 위한 사이버보안 역량 강화 필요성이 대두되고 있다. 이에 미국을 비롯한 주요 선진국은 사이버보안 역량 강화에 지속적인 관심을 갖고, 역량 강화 방안을 마련하기 위한 연구가 활발히 진행 중에 있다. 사이버보안 역량 강화 방안 마련을 위해서는 먼저 우리나라 및 주요 국가에 대한 역량 평가를 통해 정확한 실태를 파악하고, 이를 기반으로 국가 정책 방향을 수립하고 법과 제도를 완비해야 할 것이다. 평가항목의 선정은 객관적인 사이버보안 역량 평가뿐만 아니라 향후 정책 방향을 제시하기에 매우 중요한 의미를 가진다. 그러나 사이버보안 역량에는 국가의 기반인 정책, 법·제도부터 기술, 문화, 인력 등 다양한 요소가 영향을 미치기 때문에 평가항목 선정에 어려움이 따른다. 이에 본 논문에서는 객관적인 국가의 사이버보안 역량 평가항목 도출을 위해 미국과 유럽 등지에서 연구된 사이버보안 역량 평가의 평가항목을 분석하고, 우리나라의 특성을 반영한 사이버보안 역량 평가를 위한 평가항목을 제안하였다.

ABSTRACT

As ICT is becoming a major social infrastructure, the need to strengthen cyber capabilities are emerging. In the major advanced countries including the United States, has a continuing interest in strengthening cyber capabilities and has studied in enhancements of cyber capabilities. The cyber capability assessment is necessary in order to determine the current level of the country, establish policy directions and legislations. The selection of criteria has very important meaning to suggest future policy direction as well as an objective assessment of cybersecurity capabilities. But there are variable criteria for national cyber capabilities assessment such as strategy, legislation, technology, society and culture, and human resources. In this paper we perform the analysis of criteria for the other country's cybersecurity assessments including the U.S. and Europe. And we proposed the criteria for the national cybersecurity assessment reflecting the our country's characteristics.

Keywords: national cybersecurity capability, assessment, criteria

I. 서 론

정보통신 기술의 발달로 사이버 공간에서의 국가간 신경전은 거세지고, 사이버 공간에 대한 중요성은 날로 커지고 있다. 사이버 공격은 날로 지능화, 고도화되고 있기에 우리나라도 이에 대응할 수 있는 사이버 방어 및 대응 역량을 강화할 필요성이 대두되고 있다.

사이버보안이란 정보의 비밀성, 무결성 및 이용가능성을 유지하기 위하여 사이버공간의 공격으로부터

접수일(2015년 9월 4일), 수정일(2015년 9월 24일), 게재확정일(2015년 9월 25일)
† 주저자, sunhabae@nsr.re.kr
‡ 교신저자, sjkim@nsr.re.kr(Corresponding author)

정보, 정보시스템 및 정보통신망을 보호하는 것을 말한다[1]. 효과적인 사이버보안 역량 강화 방안 마련을 위해서는 정확한 실태 파악이 먼저 선행될 필요가 있다.

국가 사이버보안 역량 평가이란 공개된 자료를 기반으로 사이버보안 역량 분야의 평가 항목에 따라 상대 평가를 수행하여 평가 대상국별 역량 점수 및 순위를 판별하는 것을 말한다. 우리나라와 주요국가의 사이버 공격 및 방어 역량 수준을 판별하고, 개선 및 보완이 필요한 분야에 대한 파악하여 우리나라의 사이버보안 역량 강화 마련을 위한 체계적인 지표를 제공한다.

그러나 이러한 국가의 사이버보안 역량 평가에는 이를 뒷받침하는 법, 제도, 경제나 관련 기술, 사회문화 등 다양한 항목이 영향을 미치게 된다. 때문에 사이버보안 역량 평가를 위해서는 다양한 분야의 평가항목에 대한 종합적인 분석할 수 있는 평가 방법론과 효과적인 평가를 위해 평가항목에 대한 연구가 필요하다.

먼저, 평가 방법론은 평가항목과 평가 척도가 다양한 경우 현실적으로 평가자가 객관적인 평가가 어렵기 때문에 중요한 의미를 갖는다. 평가자의 종합적인 분석을 도와 객관적 평가를 가능하게 하는 다기준 의사결정방법론 중 AHP와 TOPSIS를 융합한 방법론을 활용하였다[2].

평가항목은 향후 국가의 정책 방향 수립의 기초자료로 활용이 가능하고, 사이버보안 역량 강화 마련 시 참고자료로 활용이 가능하기 때문에 중요한 의미를 갖는다. 평가항목은 보편적으로 타당하고, 우리나라의 특성을 반영할 수 있어야한다.

본 논문에서는 평가 방법론과 평가항목 중 평가항목에 초점을 맞추고, 보편타당한 평가항목 선정을 위해 국내외 사이버보안 역량 평가의 평가항목을 분석하였다. 그리고 이를 기반으로 주요 역량 평가 동향과 우리나라의 사이버보안의 특성을 반영한 국가 사이버보안 역량 평가항목을 제안하였다.

II. 해외 사이버보안 역량 평가 연구 동향

사이버보안 역량 평가는 국가 사이버보안 역량 평가와 조직의 사이버보안 역량 성숙도 모델로 분류될 수 있다.

국가 사이버보안 역량 평가는 평가마다 다른 특징을 갖지만 대체적으로 대상을 국가로 설정하고, 국가간 역량 비교를 통해 현재 상태 점검을 목적으로 한다. 때문에 비교 가능한 평가항목을 선정하고, 구체적인 평가항목보다는 국가 또는 조직의 특성에 따른 차이를 고려하여 넓은 범위에서 평가항목을 선정하는 특징을 가지고 있다. 또한 최근의 국가 사이버보안 역량 평가는 사이버보안 분야 선진 국가아의 사이버보안 강화 방안과 모범 사례를 공유에도 초점을 맞추고 있다.

사이버보안 역량 성숙도 모델(CMM : Capacity Maturity Model)은 사이버보안 관리 프로세스를 체계화하고, 역량 강화 방향 제시를 목적으로 한다. 역량 성숙도 모델은 미국 카네기 멜론 대학(CMU)에서 발표한 업무 프로세스 관리 역량 향상을 위한 표준 모델로 업무 절차를 체계화하여 업무 역량을 향상시키기 위한 체계를 말한다[3]. 이러한 역량 성숙도 모델을 도입한 사이버보안 역량 성숙도 모델은 역시 모델 별로 다른 특징을 갖지만 대체적으로 평가 대상을 다양화하여 조직의 크기와 형태에 관계없이 적용 가능하도록 하고, 기관 또는 조직 특성에 맞도록 수정할 수 있게 지원한다. 또한 내부적인 자체 평가를 통해 현재 상태를 점검하고, 성숙도 단계마다 다음 단계로 향상하기 위한 방향을 제시하기 위해 구체적인 평가항목을 선정하는 특징을 가지고 있다.

본 논문에서는 국가 사이버보안 역량 평가 분야에서는 미국 헤리티지 재단의 군사력 지수, 유럽의 소프트웨어 연합인 BSA의 국가 사이버보안 대쉬보드와 호주전략정책연구원(ASPI)의 아태지역 사이버 성숙도 분석 결과를 소개한다. ASPI의 아태지역 사이

Table 1. Type of the cybersecurity capability assessment

	National Cybersecurity Capability Assessment	Cybersecurity Capability Model
Target	Country	Various(organization, enterprise, etc)
Purpose	Comparison of countries	Recommendation of the capability-building measure
Criteria	Fewer items, simple	Various items, specific
Result	Sharing of the assessment result between countries	No specific assessment result

버 성숙도 분석은 아태지역 국가의 사이버 성숙도를 분석한 것으로 성숙도 단계별 정의를 통한 역량 강화 방향 제시가 아닌 국가별 비교 평가에 초점을 맞춘 연구이기에 국가 사이버보안 역량 평가 분야로 분류하였다.

사이버보안 역량 성숙도 모델 분야에서는 미국 RAND 연구소의 사이버 방어 역량 성숙도 모델, 세계경제포럼(WEF)의 조직 사이버 복원 역량 성숙도 모델, 영국 옥스퍼드 대학의 사이버보안 역량 성숙도 모델, 미국 에너지부(DOE)의 사이버보안 역량 성숙도 모델을 소개한다.

2.1 국가 사이버보안 역량 평가

2.1.1 미 헤리티지 재단의 군사력 지수[4]

미 헤리티지 재단은 미국의 보수 성향 싱크탱크로 미국을 대상으로 한 주요 위협 국가의 군사력 현황을 비교 분석한 '미 군사력 지수 2015'를 발표하였다. '미 군사력 지수 2015'는 국가 예산 편성을 위한 정보 제공을 목적으로, 과거 타국에 대한 공격 사례를 기반으로 위협 지수를 평가하였다. 과거 공격이력을 정치적·군사적·경제적으로 분류하고, 공격 방식이나 기술력(침투 바이러스 형태) 및 정보 수집 역량을 기준으로 위협 지수를 결정하였다.

과거 사이버 공격 사례라는 객관적 근거에 기반한 평가 방식이기 때문에 평가 결과가 신뢰성을 가지는 반면, 공격력을 평가하기에 적합한 방식이라는 특징을 갖는다. 하지만 국가 사이버보안 역량 평가를 위해서는 공격 역량 외에도 기반 역량, 방어 역량 등 사이버보안에 영향을 미칠 수 있는 전반적인 항목에 대한 평가가 결합되어야 할 것이다.

2.1.2 BSA의 국가 사이버보안 대쉬보드[5]

유럽 소프트웨어 연합인 BSA(The Software Alliance)는 유럽 28개국을 대상으로 사이버보안 역량을 평가한 '사이버보안 대쉬보드'를 발표하였다. '사이버보안 대쉬보드'는 국제적인 표준 단계를 정립하여 EU 회원국에게 주변국과 비교하여 자국의 사이버보안 정책 평가 기회를 제공하기 위해 개발되었다.

평가항목을 법체계, 운영기구, 민관협력, 분야별 사이버보안 계획, 교육 5가지 테마로 분류하고, 해당 테마 별로 총 26가지 상세 평가항목을 선정하였다. BSA의 사이버보안 평가항목은 EU의 사이버보안 표준을 반영하고 있고, 26가지 세부항목 중 12가지가 법체계에 대한 항목으로 법체계 항목의 가중치가 다른 항목에 비해 높았다.

BSA는 각 항목에 대해서 '있음', '없음' 외에도 국가에 의한 공식적인 정책, 조직, 체계가 아니더라도 관련 정책, 조직, 체계가 있는 경우에는 '부분적으로 있음'으로 평가하여 평가의 객관성을 높였다.

BSA는 사이버보안 법체계 항목을 국가 사이버보안 정책, 주요 기반시설보호 정책, 정보보호 방안 구축 및 역량 실태 점검 법률 및 정책, 사이버보안 사고보고 의무화 법률 등으로 구체화하여 국내 역량 평가의 법 제도 항목 도출 시 활용도가 높을 것으로 사료된다.

Table 2. Criteria of EU Cybersecurity Dashboard by BSA

Category	Criteria
Legal Foundation	Is there a national cybersecurity strategy in place
	What year was the national cybersecurity strategy adopted
	Is there a critical infrastructure protection (CIP) strategy or plan in place
	Is there legislation/policy that requires the establishment of a written information security plan
	Is there legislation/policy that requires an inventory of "systems" and the classification of data
	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels
	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels
	Is there legislation/policy that requires a public report on cybersecurity capacity for the government
	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)
	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents
	Does legislation/policy include an

Category	Criteria
	appropriate definition for "critical infrastructure protection" (CIP)
	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements
Operational Entities	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)
	What year was the computer emergency response team (CERT) established
	Is there a national competent authority for network and information security (NIS)
	Is there an incident reporting platform for collecting cybersecurity incident data
	Are national cybersecurity exercises conducted
	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents
Public private Partnership	Is there a defined public private partnership (PPP) for cybersecurity
	Is industry organised (i.e. business or industry cybersecurity councils)
	Are new public private partnerships in planning or underway
Sector specific Cybersecurity plans	Is there a joint public private sector plan that addresses cybersecurity
	Have sector specific security priorities been defined
	Have any sector cybersecurity risk assessments been conducted
Education	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age

2.1.3 ITU의 세계 사이버 지수[6]

UN 산하 전문기구인 국제전기통신연합 ITU(International Telecommunication Union)에서 발표한 세계 사이버 지수 평가는 법·제도, 기술, 조직, 역량 구축, 국제협력 다섯 가지 항목에 대해서 평가하였다.

전세계 193개국에 대한 평가를 위해서 평가항목을 일반화 시켰으며, 협력 분야에 대한 평가항목을 다양화하였다. 협력 분야를 지역간 협력·기관간 협력·민관 협력·국제 협력으로 분류하고, 각각의 협력 단계에서 공유가 가능한 자산 항목을 정의하였다. 지역간 협력은 해당 국가가 양자간 다자간 협력 참여 여부와 정보·전문지식·기술·자원 공유가 이루어지는 지에 대해 평가한다.

기관간 협력은 해당 국가가 공식적인 기관 협력 참여 여부와 부서 또는 기관간 정보·전문지식·기술·자원 공유가 이루어지는 지에 대해 평가한다. 민관 협력은 민관 간 인력·절차·도구와 같은 사이버보안 자산을 공유하고, 정보·전문지식·기술·자원 공유가 이루어지는 지에 대해 평가 한다. 국제 협력은 국제적인 사이버보안 플랫폼 및 포럼 참여 여부에 대해 평가한다.

Table 3. Criteria of Global Cybersecurity Index by ITU

Category	Criteria	Specific Criteria
Legals	Criminal Legislation	Is there any criminal legislation regarding cyber activities
	Regulation & Compliance	Is there any regulation regarding cybersecurity and compliance requirements
Technical	CERT/CIRT/CSIRT	Is there one (or more) officially approved national or sector-specific CERT, CIRT or CSIRT team(s)
	Standards	Is there any officially-approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards
	Certification	Is there any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals
Organizational	Policy	Is there any officially recognised national or sector-specific cybersecurity strategy and/or policy
	Roadmap for Governance	IS there any officially recognised national or sector-specific governance roadmap for cybersecurity
	Responsible Agency	IS there any officially recognised national or sector-specific agency

Category	Criteria	Specific Criteria
		responsible for implementing a national cybersecurity strategy/policy/roadmap
	National Benchmarking	Is there any officially recognised national or sector-specific benchmarking exercises or referential used to measure cybersecurity development
Capacity Building	Standardization Development	Is there any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector
	Manpower Development	Is there any officially recognized national or sector-specific educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sector
	Professional Certification	Are there any public sector professionals certified under internationally recognized certification programs in cybersecurity
	Agency Certification	Are there any certified government and public sector agencies certified under internationally recognized standards in cybersecurity
Cooperation	Intra-state Cooperation	Are there any officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states
	Intra-agency Cooperation	Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector
	Public-Private Partnerships	Are there any officially recognized national or sector-specific programs for sharing cybersecurity assets between the public and private sector
	International Cooperation	Are there any officially recognized participation in regional and/or international cybersecurity platforms and forums

그러나 ITU의 세계 사이버 지수 평가항목 중 기술 항목은 세부항목을 표준 이행 체계와 인증 프로그램의 존재 여부로 분류하였으나, 이는 표준화 기구라는 ITU의 업무 성격을 반영한 것으로 기술의 발달과 직접적인 연관성이 있다고 보기는 어려운 측면이 있다. 우리나라 사이버보안 역량 평가에서는 표준 이행 체계와 인증 프로그램 및 체계 항목을 기술보다는 기술 정책으로 분류하여 평가하는 것이 보다 효과적일 것으로 보인다.

2.1.4 ASPI의 아태지역 사이버 성숙도[7]

호주전략정책연구원 ASPI(Australian Strategic Policy Institute)는 '아태지역 사이버 성숙도 2014'를 발표하였다. '아태지역 사이버 성숙도 2014'는 거버넌스, 군, 디지털 경제·산업, 사회 참여 4가지 항목에 대해서 9가지 세부항목으로 분류하여 평가하였다.

ASPI는 3단계에 걸쳐 평가항목 선정하였다. 1단계에서는 내부 전문가 협의를 통해 문항을 선정하고, 2단계에서는 1단계에서 선정된 문항을 정부그룹, 민간분야, 학계 전문가에게 공유하고, 논의 결과를 반영하여 국가 전체의 사이버 성숙도를 평가할 수 있는 평가 문항을 최종 선정하였다. 마지막 3단계에서는 정부기관과 민간 분야의 사이버 전문가를 통해 항목별 가중치를 산정하였다. 이 결과 최종적으로 9가지 문항이 선정되었고, 각 각의 평가항목은 가중치를 갖는다.

그러나 ASPI는 호주 국방부의 지원으로 설립된 국방안보 분야 정책연구소로 사이버보안 분야에 대한 평가항목 선정 시 군의 역할에 대한 비중을 높게 책정하여, 군을 정부의 사이버보안 조직의 일부가 아닌 독립적인 주체의 관점에서 평가했다는 특징을 가지고 있다. 또한 연구 개발 및 기술·표준·인증 관련한 평가항목이 없다는 한계점이 있다.

Table 4. Criteria of Cyber Maturity Model by ASPI

Category	Criteria	Specific Criteria
Governance	Organizational structure	Is there government's organizational structure for cyber matters, including policy, security, critical infrastructure protection, computer emergency response teams (CERTs), crime and consumer protection
	Legislation·Regulation	Is there existing legislation/regulation relating to cyber issues or internet service providers (ISPs) What level of content control doe the state conduct or support
	International Cooperation	How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums
	CERTs	Is there a publicly accessible cybersecurity assistance service, such as a CERT
Military	Military's role	What is the military's role in cyberspace, cyber policy and cybersecurity
Business	Public private Partnership	Is there dialogue between government and industry on cyber issues What is the level/quality of interaction
	Digital economy	Is the digital economy a significant part of economic activity How has the country engaged in the digital economy
Social	Public awareness	Is there public awareness, debate and media coverage of cyber issues
	Internet connectivity	What percentage of the population has internet connectivity

2.2 사이버보안 역량 성숙도 모델

2.2.1 RAND의 사이버 방어 역량 성숙도 모델[8]

RAND는 미국의 대표적인 싱크탱크로서 2012년 사이버 방어 역량 평가에 대한 연구를 발표하였다. RAND는 국방 분야에 대한 사이버 역량 평가를 위해서 국방 개발 분야(DLoDs, Defence Lines of Development)를 활용하여, 규정, 조직, 훈련, 무기, 리더쉽/교육, 인력, 시설, 상호운용성 8가지 항목으로 분류하여 유럽 연합을 대상으로 한 군의 사이버 방어 역량에 대하여 평가하였다.

그러나 EU는 유럽의 공동안보·방위정책의 일환으로 사이버 방어에 접근하고 있기에 RAND의 사이버 '방어(Defense)'가 사이버 공격에 대한 대응을 위한 국방부와 군의 역할로 제한되지 않고, 전반적인 사이버 방어로 해석하는 것이 바람직 할 것이다.

RAND는 사이버공간을 군의 작전 공간으로 분류하여 무력 공격으로의 사이버 공격 정의 여부 및 국방 사이버 조직 존재 항목 등 군의 사이버보안 역량을 중심으로 항목을 선정하였다는 특징을 가지고 있다. RAND는 평가항목별로 가중치를 정의하여 항목별 상대적 중요성을 나타내고, 또한 항목별로 성숙도 진행 곡선을 정의하여 항목별 난이도를 나타내었다. 성숙도 진행 곡선이란 항목별로 단계를 진전시키기 위한 누적 점수 곡선으로, 진행 곡선이 선형인 경우에는 단계별로 진전 난이도가 동일한 것을 나타내고, 포물선인 경우 형태에 따라 성숙도가 낮은 단계에서 다음단계로의 진전이 어려운 항목과 성숙도가 높은 단계에서 다음단계로 진전이 어려운 항목을 나타낸다.

또한 시설 항목을 세분화하여 국내에 존재하는 물리적 시설 및 연구 개발 시설의 존재 여부 외에 협력을 통해 활용 가능한 EU 및 NATO 자산 활용 가능 여부를 평가항목을 선정하여 국제 협력을 통한 활용 가능한 자산에 대해서도 평가하였다.

Table 5. Criteria of Military Cyber Defence Capabilities by RAND

Category	Criteria
Doctrine	Familiarity with cyber defence issues
	Existence of cybersecurity strategy
	Specific cyber defence strategy
	National critical information infrastructure protection strategy
	Computer network operations doctrine
	Cyber deterrence doctrine
	Cyber-attacks as armed attack
	Cyber-attacks as armed attack
	International strategy
Organization	Existence of national steering group
	Cyber-security organization in defence
	Responsibility for defence & offence
	Responsibility for defence & offence
	Function of unit
	Expertise from other organizations in unit
	Expertise from private sector in unit
	linked to national cybercrime capability

Category	Criteria
	Co-ordination (linked to n/g CERT)
	Linked to other incident response
Training	CS covered in syllabus at command level
	Specific cyber defence training competency/career path or skills profile
	Participation in EU exercises
	Estimate of theoretical academic expertise at national level
	Estimate of applied expertise at national level
	Conduct national level recruitment competitions
	Sharing good practice / Lessons learned
	Breadth of participants
Materiel	Reliance upon privately owned assets
	Perception of role of private sector
Personnel	Recruitment and retention for cyber defence specialists
	Identity and access management
	Insider threat management
	Personnel vetting and assurance
	Vetting contractors and third parties
	Recruitment and employment of 'black' or 'grey' hats
Leadership	Tactical level of authorization for cyber defence capabilities
	Operational level of authorization for cyber defence capabilities
	Strategic level of authorization for cyber defence capabilities
	Escalation mechanism for national incidents
	Feasible to apply a non-national decision to your own network
	Court order required for surveillance of private sector networks
	Civil servant authority required for surveillance of private sector networks
	Other level of authority required for surveillance of private sector networks
Facilities	Existence of a national range
	Dedicated physical facility to address cyber defence
	Existence of a facility to develop & test offensive capabilities
	Existence of a national level forensics research facility
	Use of own assets for cyber defence in Common Security and Defence Policy missions
	Use of NATO assets for cyber defence in common security and defence policy missions
	Bilateral arrangements with pMS for cyber defence in common security and defence
	Policy missions
	Bilateral arrangements with non-EU for Cyber Defence in Common Security and Defence Policy missions
Interoperability	Sufficient development of Cyber Defence interoperability
	Tactical level of interoperability
	Operational level of interoperability
	Strategic level of interoperability

2.2.2 WEF의 조직의 사이버 복원 성숙도 모델[9]

세계경제포럼인 WEF(World Economic Forum)은 사이버보안 분야의 '조직 사이버 복원 성숙도 모델'을 발표하였다. '조직 사이버 복원 성숙도 모델'은 늘어나는 사이버보안 위험에 대항하여 복원력을 갖추기 위해 조직에 사이버 복원(Resiliency) 프로그램 개발 가이드를 제공하고자 개발되었다.

평가항목은 거버넌스, 프로그램, 네트워크 3가지로 항목으로 분류하고, 18개의 세부항목으로 평가하였다. 세계경제포럼의 평가항목은 국가의 사이버보안 성숙도를 평가하기 위한 항목이 아닌 조직의 사이버 복원력을 평가하기 위한 항목이라는 점에서 타 사이버보안 역량 성숙도 모델과는 차이점이 있다.

WEF의 사이버 복원 성숙도 모델 평가는 최고 책임자와 관리부서의 사이버보안 의무 이행 여부와 책임 숙지에 대한 평가항목이 19가지 항목 중 6개를 차지하고 있어 이에 대한 평가가 주를 이루고 있다. 또한 사고 대응·모니터링·교육 및 훈련·위험 관리 등을 프로그램으로 분류하여 해당 프로그램의 수행 여부와 정책에 대한 반영 여부에 대하여 평가했다는 특징을 갖고 있다.

Table 6. Criteria of Maturity Model for Organizational Cyber Resilience by WEF

Category	Criteria
Governance	The chief executive and executive management team are responsible for overseeing the development and confirming the implementation of a Programme of best practices for cyber risk management
	The chief executive and executive management team ensure that the Programme is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued
	The chief executive and the executive

Category	Criteria
	management team demonstrate visible and active commitment to the implementation of the Principles
	Executives and managers are responsible for understanding at the appropriate level how cyber risks could impact and originate from their line of business
	Senior leadership understands who is responsible for managing cyber risk when managing security incidents
	The organization has access to cyber expertise at its highest management levels
	The organization undertakes to continuously improve the integration of its cyber risk management with its other risk management initiatives
	The chief executive (or equivalent) has a clear decision path for action and communication in response to a significant security failure or accident
Program	The organization conducts comprehensive assessments of its vulnerabilities to internal and external cyber risks appropriate for its industry and sector
	The organization monitors the effectiveness of its cyber risk management strategy
	The organization periodically internally verifies its compliance with rules and regulations
	The organization's commitment to the Programme is reflected in its policies and practices
	Managers, employees and agents receive specific training on the Programme, tailored to relevant needs and circumstances
	The organization has identified its data and information as vital assets, and organizes its Programme around the recognition that data and information have value that can be separately recognized and protected
	The risk management Programme includes all material third-party relationships and information flows
	The organization conducts comprehensive internal short- and long-term cyber risk impact assessments
Network	The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization's specific cyber risk management standards or industry best practices, in line with the Principles, and formalizes this requirement using contractual obligations
	The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents
	The risk management Programme includes all material third-party relationships and information flows

2.2.3 옥스퍼드 대학의 사이버보안 성숙도 모델[10]

영국의 옥스퍼드 대학 인터넷 연구소의 글로벌 사이버보안 역량 센터에서 '사이버보안 역량 성숙도 모델'을 발표하였다. '사이버보안 역량 성숙도 모델'은 사이버보안 정책, 사이버 문화·사회, 사이버보안 교육·훈련·기술, 법·규제 구조, 조직·기술·표준으로 분류하여 평가하였다. 옥스퍼드 대학의 '사이버보안 성숙도 모델'의 평가항목은 사이버보안 관련 연구 기관의 결과를 통합하여 선정된 항목으로 보편적인 평가항목을 선정했다는 의미를 갖는다. 사이버보안 정책부터 사회·문화, 교육·훈련, 법·규제, 기술 등 사이버보안 역량에 영향을 미치는 항목에 대해서 전반적으로 검토하여 평가항목을 선정하였다.

또한 평가항목 선정 기준을 마련하고, 전문가 설문을 통해 평가항목간 우선순위를 선정하여 최종 항목을 도출하였다. 평가항목은 평가항목에 대한 증거 수집 가능 여부, 과학적 평가 가능성 및 측정 난이도, 해당 항목의 향후 사이버보안 역량 구축에 미치는 영향력을 기준으로 선정하였다.

또한 사이버보안 정책과 법·규제에 대한 항목을 분리하여 보다 체계적으로 평가항목을 선정하였다. 정책 항목에서는 넓은 범위에서의 정책과 계획에 대하여 평가하고, 법·규제 항목에서는 법과 규정을 통해 제재가 필요한 항목에 대해여 평가하였다. 정책 분야에서는 국가적인 사이버보안 정책의 유무부터 사고대응, 주요 기반 시설 보호, 디지털 이중화(Digital Duplexing), 사이버 방어, 위기관리에 대한 정책의 존재 유무와 관련 조직에 대하여 평가하였다. 법·규제 분야에서는 사이버 범죄와 개인정보보호를 위한 법제도와 정보 공유를 위한 사이버보안 사고보고 의무 규정에 대하여 평가하였다. 옥스퍼드의 평가항목은 기존 연구의 통합 결과로 국내 사이버보안 역량 평가의 항목 도출 시 기준 항목으로 활용할 가치가 있다고 판단된다.

Table 7. Criteria of Cybersecurity Capability Maturity Model by Oxford

Category	Criteria	Specific Criteria
Cybersecurity Policy and Strategy	National cybersecurity strategy	Strategy development
		Organization
		Content
	Incident response	Identification and designation
		Organization
		Coordination
	Critical National Infrastructure (CNI) protection	Identification
		Organization
		Response planning
		Coordination
		Risk management
	Crisis management	Planning
		Evaluation
	Cyber defence consideration	Strategy
		Organization
		Coordination
	Digital redundancy	Planning
		Organization
Cyber Culture and Society	Cybersecurity mind-set	Government
		Private sector
		Society[at-large]
	Cybersecurity awareness	Awareness raising
	Confidence and trust on the Internet	Trust in use of online services
		Trust in e-government
		Trust in e-commerce
	Privacy online	Privacy standards
		Employee privacy
Cybersecurity Education, Training and Skills	National availability of cyber education and training	Education
		Training
	National development of cybersecurity education	National development of cybersecurity education
	Training and educational initiatives within public and private sector	Training employees in cybersecurity
	Corporate governance, knowledge and standards	Private and state owned companies' understanding of cybersecurity
Legal and Regulatory Frameworks	Cybersecurity legal frameworks	Legislative frameworks for ICT security
		Privacy, data protection & other human rights
		Substantive cybercrime law
		Procedural cybercrime law
	Legal investigation	Law enforcement
		Prosecution services
		Courts
	Responsible reporting	Responsible disclosure
Organizations, Technologies and Standards	Adherence to standards	Implementation of standards and minimal acceptable practices
		Procurement
		Software development
	Cybersecurity coordinating organizations	Command and control center
		Incident response Capacity
	Cybersecurity marketplace	Cybersecurity technologies
		Cybercrime insurance
	National infrastructure resilience	Infrastructure technology
		National resilience

2.2.4 미 DOE의 사이버보안 성숙도 모델[11][12]

미국 에너지부인 DOE(U.S. Department of Energy)는 국토안보부와 카네기 멜론 대학교와 공동 연구를 통해 '사이버보안 성숙도 모델'을 발표하였고, 10가지 평가항목에 대하여 37가지 세부항목으로 분류하여 평가하였다. 평가항목은 위험 관리, 자산·변화 및 형상 관리, ID 및 접근 관리, 위협 및 취약점 관리, 상황 인지, 정보 공유 및 소통, 이벤트 사고 대응·지속적 운영, 공급 체인·외부 의존도 관리, 인력 관리, 사이버보안 프로그램 관리로 분류하였고, 세부항목별로 성숙도 단계에 따라 평가가 필요한 항목에 대해 정의하였다.

DOE의 '사이버보안 성숙도 모델'은 성숙도 단계에 따른 평가항목이 다양하기 때문에 국가뿐만 아니라 조직의 분야, 형태, 크기에 관계없이 평가가 가능하도록 평가항목을 선정하였다는 특징을 가지고 있다. 또한 평가항목 마다 활동 관리 항목을 세부 항목으로 선정하여 해당 평가항목의 지속적인 수행을 위한 관

리 방안을 제시하였다. 그러나 국가별 평가에 적용하기에는 평가항목이 너무 구체적이고, 전문적인 근거 자료가 필요하다는 한계점이 있다.

DOE의 '사이버보안 성숙도 모델'은 정부 주관으로 개발되었지만, 역량 성숙도 모델의 창시자인 카네기 멜론 대학과 산업 분야 전문가가 개발에 함께 참여하여 통합 연구를 수행하였다. 또한 에너지 분야 17개의 사이트에 사전 적용 시험을 수행하고, 실 사용자를 대상으로 한 검토 결과를 모델에 반영하여 모델을 개선하였다. 향후 국내 사이버보안 역량 평가도 정부·학계·산업계가 연계하여 지속적으로 개선 및 발전시키는 방향으로 연구가 진행될 필요가 있겠다.

Table 8. Criteria of Cybersecurity Capability Maturity Model by DOE

Category	Criteria
Risk Management	Establish cybersecurity risk management strategy
	Manage cybersecurity risk
	Management activities
Asset, Change, and Configuration Management	Manage asset inventory
	Manage asset configuration
	Manage changes to assets
	Management activities
Identity and Access Management	Establish and maintain identities
	Control access
	Management activities
Threat and Vulnerability Management	Identify and respond to threats
	Reduce cybersecurity vulnerabilities
	Management activities
Situational Awareness	Perform logging
	Perform monitoring
	Establish and maintain a common operating picture
	Management activities
Information Sharing and Communications	Share cybersecurity information
	Management activities
Event and Incident Response, Continuity of Operations	Detect cybersecurity events
	Escalate cybersecurity events and declare incidents
	Respond to incidents and escalated cybersecurity events
	Plan for continuity
	Management activities
Supply Chain and External Dependencies Management	Identify dependencies
	Manage dependency risk
	Management activities
Workforce	Assign cybersecurity responsibilities
Management	Control the workforce life cycle
	Develop cybersecurity workforce
	Increase cybersecurity awareness
	Management activities
Cybersecurity Program Management	Establish cybersecurity program strategy
	Sponsor cybersecurity program
	Establish and maintain cybersecurity architecture
	Perform secure software development
	Management activities

2.3 해외 사이버보안 역량 평가 종합 분석

Table 9는 해외 사이버보안 역량 평가를 종합한 결과이다. 평가별로 평가 대상·목적에 따라 다른 평가항목·결과를 갖지만 일반적인 특징은 다음 3가지이다.

먼저, 평가 객관성 확보를 위해 민관 분야 전문가를 통한 보편타당한 항목을 선정하고, 사이버보안에 영향을 미치는 다양한 분야에 대하여 전반적으로 평가하였다.

둘째, 국가의 사이버보안 구축 및 강화를 위한 방안을 평가항목으로 선정하여 사이버보안 역량 강화 방안 마련을 위한 기초 자료로 활용될 수 있도록 하였다.

마지막으로 평가를 통해 국가 및 조직간 경쟁을 유발하여 사이버보안 인식 제고 및 역량 강화에 기여하고, 국가별 역량 강화 방안 및 모범 사례를 공유하여 국가간 협력 체계를 강화하였다.

평가 형태별 대표적인 특징은 평가 형태에 따라 대상과 목적이 다르다는 것이다. 국가 사이버보안 역량 평가는 주로 국가의 사이버보안 점검을 목적으로 하는 반면, 사이버보안 역량 성숙도 모델은 주로 조직 및 기관의 사이버보안 점검을 목적으로 한다. 특히, WEF와 DOE의 사이버보안 역량 성숙도 모델은 현재 우리나라에서 공공기관을 대상으로 시행중인 관리실태 평가와 평가 목적이 조직의 안정성을 점검하기 위한 것이라는 점에서 유사한 면을 가지고 있다.

Table 9. Overall result for international cybersecurity capability assessment

	National Cybersecurity Capability Assesment				Cybersecurity Capability Maturity Model			
	Heritage	BSA	ITU	ASPI	RAND	WEF	Oxford	DOE
Target	Principal threats countries to U.S.	28 countries in EU	193 countries	14 countries in Asia Pacific area	10 countries in EU and EU, NATO organization	Country, Organization, Enterprise, etc.	Country, Organization, Enterprise etc.	Country, Organization, Enterprise etc.
Purpose	Calculation of threat index	Comparison between countries and standard formulation	Sharing information of best practices and the enhancement strategy for cybersecurity capability	Cyber maturity assessment of Asia Pacific countries	Assesment Military's cyber defence capability and suggestion of directions	Assesment cyber resilience and suggestion of directions	Check the status of capability and suggestion of the enhancement strategy	Check the status of capability and suggestion of the enhancement strategy
Criteria	Previous cyber attack practices	5 criteria 25 specific criteria	5 criteria 13 specific criteria	4 criteria 9 specific criteria	8 criteria 55 specific criteria	3 criteria 18 specific criteria	5 criteria 42 specific criteria	10 criteria 37 specific criteria
Result	Threats index and cyber offence capability index	Assessment result for each criteria No ranking of countries	Ranking of countries	Ranking of countries	Maturity level for each country	N/A	N/A	N/A
Characteristic	Assessment based offence capability	Assessment focused on legal framework	Diversified criteria of cooperation category	Calculation of weight for each criteria through survey by experts	Selection of criteria focused on the military's role Calculation of weight and difficulty level for each criteria	Assessment focused on cyber resilience	Integration existing cyber capability assessment result	Applied critical infrastructure and reflect feedback
Implication	Need for the selection of overall assesment criteria in addition offence capability	Selection of major legal framework for cybersecurity	Need for the review of various cooperation criteria	Need for the criteria of R&D and technology	Departmentalization of the facility criteria(assessment of possible cooperation facilities at other countries)	Definition of role and responsibility for CSO and the organization	Reference available when we select our country assessment criteria since integration e results	Need for continuous improvement through public-private partnerships

III. 국내 기존 사이버보안 역량 평가 연구 동향

국가보안기술연구소는 역량 평가 관련 해외 동향을 반영하여 지난 2010년부터 사이버 역량 측정 및 평가를 통해 객관적이고 정량적인 자료를 토대로 국가 사이버 안보 정책을 수립하기 위하여 국가 사이버 역량 평가 모델에 대하여 연구해왔다. 국가보안기술연구소의 사이버 역량 평가 모델 개발로 주변국과 우리나라의 사이버 역량을 비교를 시도하였고, 공격과 방어 측면에서 개선점 및 강화 방안을 마련할 수 있는 기초를 마련하였다.

국가 사이버 역량 평가는 1차, 2차로 나뉘어 진행되었고, 1차에는 기반 능력, 실행 능력 2가지로 분류하여 평가하였다. 세부 항목은Table 10과 같다[13]. 2차에는 기반 역량, 공격 역량, 방어 역량 3가지로 분류하여 평가하였고 세부항목은 Table 11과 같다[14].

1차 항목은 법, 교육, 조직 등 기반 능력과 공격, 방어, 기술에 이르기 까지 사이버보안에 영향을 미치는 항목을 넓은 범위에서 검토 및 선정하여 평가하였다. 1차 평가항목은 RAND의 역량 평가와 유사하게 사이버공간을 작전 공간으로 분류하고, 사이버 무기 및 공격 항목을 선정하여 평가하였다. 또한 일부 항목은 시대의 흐름에 맞게 수정이 필요할 것으로 사료된다. 교육 항목은 사이버보안 관계자에 대한 교육 수준을 평가하였으나, 지속적인 보안 인력 양성을 위해 기존 관계자뿐만 아니라 보안 인력 양성 체계 구축 여부에 대한 평가가 이루어져야 할 것이다. 협력 항목에서도 국제 협력 외에도 정부 부처 및 기업의 사이버보안 수준 향상을 위한 민관 협력에 대해서도 평가가 필요하다.

Table 10. Criteria of the first Cyber Capability Assessment

Category	Criteria	Specific Criteria
Basic	Organization	Scale of Control tower & Professional Organization
		Level of interorganizational cooperation
	Budget	National budget for offense and defense capability
	Work Force	Size and level of direct/indirect workforce to participate in offense & defense cyber war
	Law(Authority)	Lawful authority to support organization, budget, work force and system
	Education	Level of education for staffs of cybersecurity
Implementation	Offense	Paralyze the subject country's system(computer, network)
	Defense	Combine the detection skill with deterrent
	Weapons	Diversity & performance level of cyber weapons
	Creed / Strategy	Capability to dispatch work force and use weapons in a battle systematically
	Fundamental Technology	Computer skills, telecommunication performance.
		Scope, frequency, strength,, and practicality for the national level of training and professional training organization.
	Training	Scope, frequency, strength, and practicality for the national level of training and professional training organization
	International cooperation	The number of cooperating countries related to cyber offense and defense
	Ripple Effect	Skill of transmitting information
		Mass media effect
		Information ripple effect caused by frequent internet usage

2차 항목은 1차 항목에 비해 기반 능력 분야 항목을 축소하고, 실행 능력을 공격과 방어로 분류고, 세부항목을 구체화하였다는 특징을 가지고 있다. 조직 공격을 위한 정보 수집 및 침투 기술 수준과 방어를 위한 예방 및 탐지 기술 평가항목을 선정하여 평가하였다. 2차 항목은 넓은 범위에서 국가의 사이버보안 역량 평가를 위한 항목이라기보다는 사이버보안 기술 역량에 초점을 맞춘 평가항목이다.

Table 11. Criteria of the second Cyber Capability Assessment

Category	Criteria	Specific Criteria
Basic	Domain (Infrastructure)	Level of network
		Level of system
	Resource (Budget)	National budget for IT
		National budget for information security
	Population (Organization)	Size and level of direct workforce to participate in offense & defense cyber war
		Size and level of indirect workforce to offense & defense cyber war(Security companies, IT-related departments, the hacker community)
		Existence of control tower
	Etc	International cooperation
		Training
Offence	Information Gathering	Level of digital snooping
		Level of social engineering
		Level of trojan horse
	Penetration	Level of vulnerability exploit
		Level of worms virus
		Level of security system bypass capability
	Destruction / disable	Level of DDos
		Level of system destruction
		Level of EMP
Defence	prevention	Level of software certification
		Secure server penetration
		Patch penetration (MS patches)
	Detection	Level of intrusion detection system
		Level of security control
		Level of vaccine
	Response	CERT activities
		Forensic experts
		Level of malware analysis

IV. 국가 사이버보안 역량 평가항목 제안

4.1 평가항목 선정 기준

평가항목은 3가지 기준을 바탕으로 도출하였다. 먼저, 국가 사이버보안 역량 평가는 국가의 사이버보안 역량 평가를 목적으로 하기 때문에 우리나라와 다른 국가에 공통적으로 적용하기 위해 객관적이며 보편적인 항목을 평가항목으로 도출하였다. 객관적이며 보편적인 항목 선정을 위해 앞서 분석한 해외 역량 평가 항목 중 다수의 해외 역량 평가에서 평가항목으로 도출된 항목을 선정하였다. 해외 역량 평가의 평가항목 전체는 Table 12와 같다. 평가별로 해당 세부 항목이 항목으로 선정된 평가는 'O'로 표기하고, 선정되지 않은 평가는 'X'로 표기하였다. 합계는 해당 세부 항목이 8개의 평가 중 평가항목으로 선정된 횟수이다.

정책 항목은 대부분의 평가에서 평가항목으로 선정되어 합계가 4개 이상인 평가항목을 세부항목으로 도출하였다. 법·제도 항목은 일부 평가에서만 평가항목으로 다루고 있기 때문에 합계가 2개 이상인 평가항목을 세부항목으로 도출하였다. 정책과 법·제도 항목을 제외한 나머지 항목에 대해서는 합계가 3개 이상인 평가항목을 세부 항목으로 도출하였다.

둘째, 정량적 또는 정성적으로 평가가 가능한 항목으로 선정하였다. 해당 항목이 과학적으로 평가 가능한지 여부와 역량 보유에 대한 입증이 가능한지, 여부를 판단하여 선정하였다.

셋째, 우리나라의 사이버 공간의 특성을 반영한 항목으로 선정하였다. 국가 사이버보안 역량 평가는 국가별 비교 평가 목적도 가지고 있지만, 국가 사이버보안 역량 실태와 정책의 종합적 검토하고, 이를 통해 우리나라의 강점과 약점을 식별하여 향후 정책 방향 수립 기준을 마련하는데 보다 더 큰 의미가 있다고 할 수 있겠다. 국가 사이버보안 역량 평가와 사이버보안 성숙도 모델 모두 형태에 관계없이 평가항목은 향후 사이버보안 역량 강화 방안 및 사이버보안 발전 방향 정립에 영향을 미치게 된다. 더욱이 사이버보안 성숙도 모델 형태의 역량 평가는 단계별로 성숙도를 정의하여 구체적인 발전 방향을 제시하고 있다. 이에 국내 사이버보안 역량 평가항목 도출 시 우리나라의 사이버 공간의 특성을 반영하여 향후 사이버보안 정책 방향 수립 및 효과적인 사이버보안 역량 강화 방안 마련에 활용될 수 있도록 도출하였다.

Table 12. Overall Criteria of Cybersecurity Capability Assessment

Category	Criteria	Specific Criteria	Heritage	BSA	ITU	ASPI	RAND	WEF	Oxford	DOE	Sum
Policy	National cybersecurity	National cybersecurity policy	X	O	O	△	O	X	O	O	5.5
	Critical infrastructure	Critical Information Infrastructure Protection policy	X	O	X	△	O	X	O	△	4
	Risk management	Risk management framework	X	O	X	X	X	O	O	O	4
	Incident response	Cybersecurity incident response strategy	X	O	X	X	X	O	O	O	4
	Regulatory compliance and audit	Regulatory compliance of cybersecurity and audit	X	O	O	X	X	O	X	O	4
	What year was the national cybersecurity policy adopted	What year was the national cybersecurity policy adopted	X	O	X	X	X	X	X	X	1
	Capability assessment	Policy for check status through assessment and public report of cybersecurity capability	X	O	X	X	X	X	X	O	2
	CIO or CSO	Strategy for Chief Information Officer or Chief Security Officer	X	O	X	X	X	X	X	X	1
	Sector specific cybersecurity plan	Sector specific cybersecurity strategy or policy of requirement for plan	X	O	O	X	O	X	X	X	3
	National or sector specific governance	Establish National or sector specific governance roadmap	X	X	O	X	X	X	X	X	1
	Network operations and management	Computer network or Internet Service Providers Management policy	X	X	X	O	O	X	X	X	2
	Cyber deterrence	Cyber deterrence policy	X	X	X	X	O	X	X	X	1
	Cyber defence	Cyber defence policy	X	X	X	X	O	X	O	X	2
	Cyber attacks as armed attack	Armed attack policy in cyberspace	X	X	X	X	O	X	X	X	1
Law	Information protection law	Legislative framework for information protection and privacy protection	X	O	X	X	X	X	O	X	2
	Cybercrime law	Legislative framework for cybercrime response	X	X	O	△	X	X	O	X	2.5
	Incident reporting regulatory	Regulatory of public report about cyber incident	X	O	X	X	X	X	O	O	3
	ICT security law	Legislative frameworks for ICT Security	X	X	X	X	X	X	O	X	1
	Law enhancement	Process for law enhancement or prosecution services	X	X	X	X	X	X	O	X	1
Organization	Dedicated organization for cybersecurity	Dedicated organization for cybersecurity(policy, infrastructure protection, crime, etc.)	X	O	O	O	O	O	O	O	7
	Role of organization	Definition of the role and responsibility for cybersecurity organizations	X	X	O	X	O	X	X	O	3
	CERTs	National CERT or CSIRT	X	O	O	O	O	X	O	O	6
	What year established CERT	What year established CERT	X	O	X	X	X	X	X	X	1
	Platform for incident reporting	Cybersecurity incident reporting platform for data collection	X	O	X	X	X	X	X	O	2
	Military organization	Military cybersecurity organization	X	X	X	O	O	X	X	X	2
	Responsibility for offence and defence	Definition of responsibility for cyber offence and defence	X	X	X	X	O	X	X	X	1
	Location of agency	Location of agency	X	X	X	X	O	X	X	X	1
	Linked to cybercrime	Linked to national cybercrime capability	X	X	X	X	O	X	X	X	1

Category	Criteria	Specific Criteria	Heritage	BSA	ITU	ASPI	RAND	WEF	Oxford	DOE	Sum
Budget	Cybersecurity budget	National cybersecurity Budget(Compare with IT budget)	O	X	X	X	X	X	X	X	1
Education·Training	Framework for education and training	National cybersecurity education and training framework including curriculum of university and vocational training	X	O	O	X	O	O	O	O	6
	Various eduction program	Various education programs(various sector and level) and on/offline education program	X	X	O	X	X	O	O	O	4
	Public awareness	Campaign or education for increasing cybersecurity awareness	X	O	O	O	X	X	O	O	5
	Sharing of best practices	Program for sharing best practices	X	X	O	X	O	O	X	O	4
	International training	Participation in international organization's training	X	X	X	X	O	X	X	X	1
	Assessment of experts level	Estimate of applied expertise at national level	X	X	X	X	O	X	X	X	1
	National level recruitment	Conduct national level recruitment competitions	X	X	X	X	O	X	X	X	1
Technology·Standard·Certification	R&D manpower and technical level	R&D Organization for cybersecurity technologies and the level of technologies for cybersecurity	△	X	O	X	O	X	O	O	4.5
	Standard formulation and implementation framework	National framework for standard formulation and implementation	X	O	O	X	X	X	O	O	4
	Certification agency and policy	Officially approved national cybersecurity certification agency and the policy for certification requirement	X	O	O	X	X	X	X	O	3
	Internet connectivity	Network penetration and smartphone penetration	X	X	X	O	X	X	X	X	1
	Secure software	Security software development framework and development requirements policy	X	X	X	X	X	X	O	O	2
	Technology for cybersecurity	Development level of technologies for cybersecurity	X	X	X	X	X	X	O	O	2
	Technology for resilience	Level of technologies for resilience in critical infrastructure	X	X	X	X	X	X	O	X	1
	Previous attack practices	Level of offence technologies in previous attack practices	O	X	X	X	X	X	X	X	1
Cooperation	Public private partnership	Framework for public private partnership(Sharing resource and information)	X	O	O	O	O	X	O	O	6
	Intra-agency partnership	Framework for intra-agency partnership	X	X	O	X	X	O	X	O	3
	International partnership	Participation of international cybersecurity organization or forum	X	X	O	O	O	X	X	X	3
	Intra-state partnership	Framework for Intra-state partnership	X	X	O	X	X	X	X	X	1
	Connectivity with risk management framework and information sharing	Risk management framework with shared information from other organizations	X	X	X	X	X	O	X	O	2
	Cooperation organization	Definition of the cooperation organizations	X	X	X	X	X	X	O	X	1

Category	Criteria	Specific Criteria	Heritage	BSA	ITU	ASPI	RAND	WEF	Oxford	DOE	Sum
Cyber culture·society	Familiarity with cyber defence issues	Familiarity with cyber defence issues	X	X	X	X	O	X	X	X	1
	Cybersecurity mind-set	Position of cybersecurity mind-set	X	X	X	X	X	X	O	X	1
	Confidence and trust on the internet	Confidence and trust on the e-Commerce, online service, e-Goverment	X	X	X	X	X	X	O	X	1
	Protection of privacy	Regulatory for privacy, data protection	△	X	X	X	X	X	O	X	1.5
Industry	Industry for cybersecurity	Industry or market for cybersecurity	X	O	X	X	X	X	O	X	2
	Digital economy	Digital economy rate in the whole economy	X	X	X	O	X	X	X	X	1
	Management of vulnerabilities and impact of accident	Management of vulnerabilities and impact of significant security failure or accident	X	X	X	X	X	O	X	X	1
Material	Reliance upon private assets	Reliance upon privately owned assets	X	X	X	X	O	X	X	X	1
	Perception of role of private sector	Perception of role of private sector	X	X	X	X	O	X	X	X	1
Personnel management	Recruitment and retention	Recruitment and retention for cybersecurity specialists	X	X	X	X	O	X	X	O	2
	ID and Access management	Personnel vetting and assurance Identity and access management	X	X	X	X	O	X	X	O	2
	External dependencies management	Vetting contractors and third parties	X	X	X	X	O	X	X	O	2
	Professional training for hacker	Recruitment and employment of 'black' or 'grey' hats	X	X	X	X	O	X	X	X	1
Leadership	Authorization for cyber defence capabilities	Authorization for cyber defence capabilities(Tactical level, Operational level, Strategic level)	X	X	X	X	O	X	X	X	1
	Escalation mechanism	Escalation mechanism for national incidents	X	X	X	X	O	X	X	X	1
	surveillance of private sector networks	Level of authority required for surveillance of private sector networks	X	X	X	X	O	X	X	X	1
Facility	Cybersecurity facility	Physical facility for cyber defence	X	X	X	X	O	X	X	X	1
Etc	Interoperability	Tactical·operational·strategic interoperability	X	X	X	X	O	X	X	X	1
	Review of the program modification	Programme is reviewed for effectiveness and, when shortcomings are identified, corrective action	X	X	X	X	X	O	X	X	1

4.1 국내 사이버보안 특징 반영

우리나라는 세계 최고의 인터넷 속도를 보유하고, 전자정부, IoT, 스마트 그리드 분야에서도 선진 기술을 보유한 사이버 강국이다. BAH 사이버 역량 평가에서도 한국은 기술 분야에서는 2위에 랭크되어 있다[15]. 또한 인구 수 대비 인터넷 보급율과 모바일 사용 비율이 높고, 스마트폰 보급률은 세계 2위로 매우 높은 수준이다[16]. 이에 따라 네트워크 의존도는 지속적으로 증가하고, 그에 따른 취약성도 증가하고 있는 추세이다.

그러나 진보된 IT 기술 및 네트워크 보급률에 비해 사이버보안 수준이 발맞춰 가고 있지 못한 것이 현실이다. 한국과학기술평가원이 분석한 스위스국제경영개발원의 세계 경쟁력 연감 분석에 따르면 사이버보안이 기업에서 적절히 다루어지는 정도가 세계 60개국 중 58위로 과학·기술 인프라 세부 지표 가운데 가장 낮은 순위를 기록하였다[17]. 정부 정책 관련 만족도가 낮고, 연이은 개인정보 유출 사고 등 전반적으로 정보보호에 대한 인식이 낮은 것으로 나타났다. 이렇듯 우리나라는 기업의 정보보호 수준이 낮고, 정보보호에 대한 인식이 부족하다는 특성을 갖고 있다.

또한 우리나라의 정보보호 인력은 수요에 비해 턱없이 부족한 상황이다. 해마다 증가하는 보안사고로 보안전문 인력이 수요는 크게 증가하고 있지만, 공급이 이에 미치기 어려운 실정이다. 2015 정보보호백서에 따르면 정보보호 전담 조직이 신설되지 못하는 이유로 예산·인력 부족이 85.2%로 압도적으로 우세했고, 정보보호 담당자의 업무 수행 중 가장 큰 애로사항도 기술인력·예산 부족이 42.6%로 가장 높게 나타났다[18].

우리나라 특성을 예산, 교육·훈련, 기술 항목에 반영하여 향후 사이버보안 정책 방향 수립 시 정보보안 인력 수급, 인식 제고 및 예산 항목에 대한 검토가 이루어지도록 평가항목을 도출하였다.

4.2 평가항목 제안

최종적으로 제안하는 국가 사이버보안 역량 평가항목은 Table 13과 같다. 각 세부 항목의 발전 수준에 대하여 평가한다.

Table 13. Criteria of National Cybersecurity Capability Assessment

Category	Criteria	Specific Criteria
Policy	National cybersecurity	National cybersecurity policy
	Critical infrastructure	Critical information infrastructure protection policy or strategy
	Risk management	Risk management framework
	Incident response	Cybersecurity incident response strategy
	Regulatory compliance and audit	Regulatory compliance of cybersecurity and audit
Law	Cybersecurity basic law	Basic law for cybersecurity
	Information protection law	Legislative framework for information protection and privacy protection
	Cybercrime law	Legislative framework for cybercrime response
	Incident reporting regulation	Regulatory of public report about cyber incident
Organization	Dedicated organization for cybersecurity	Dedicated organization for cybersecurity(policy, infrastructure protection, crime, etc.)
	CERTs	National CERT or CSIRT
Budget	Cybersecurity budget	National cybersecurity budget(Compare with IT budget)
Education·Training	Framework for education and training	National cybersecurity education and training framework including curriculum of university and vocational training
	Various eduction program	Various education programs(various sector and level) and on/offline education program
	Public awareness	Campaign or education for increasing cybersecurity awareness
	Sharing of best practices	Program for sharing best practices
Technology·Standard·C	R&D manpower and technical level	R&D organization for cybersecurity technologies and the development level of technologies for cybersecurity
	Standard formulation	National framework for standard formulation and

Category	Criteria	Specific Criteria
ertification	and implementation framework	implementation
	Certification agency and policy	Officially approved national cybersecurity certification agency and the policy for certification requirement
Cooperation	Public private partnership	Framework for public private partnership(Sharing resource and information)
	Intra-agency partnership	Framework for intra-agency partnership
	International partnership	Participation of international cybersecurity organization or forum

4.2.1 정책

국가 사이버보안 역량 평가에서는 정책과 법·제도 항목을 분류하고, 정책 항목에서는 8개의 해외 역량 평가 중 4개 이상의 평가에서 항목으로 선정된 사이버보안 정책 및 전략 발전 수준, 기반시설보호 정책 및 전략 발전 수준, 사고 대응, 위기관리 체계 발전 수준, 사이버보안 규정 준수 관리 및 감사 체계 발전 수준을 세부 항목으로 도출하였다.

국가 사이버보안 정책 발전 수준 항목은 앞서 살펴본 8개의 해외 역량 평가 중 5.5개의 평가에서 평가항목으로 선정되어 국가 사이버보안 역량 평가를 위한 기본 항목이라고 할 수 있겠다. BSA는 국가 사이버보안 정책 존재 여부 및 채택 시기에 대해서도 평가하였고, ASPI는 국가 사이버보안 정책 및 주요기반시설 보호 정책 발전 수준은 아니지만 관련 조직 구조를 평가항목으로 선정하고, 가장 높은 가중치를 부여하였다.

주요기반시설에 대한 위협은 국가 안보를 위협하고, 큰 혼란과 피해를 야기할 수 있는 만큼 그 중요성이 날로 커지고 있는 실정이다. 이를 반영하여 9개의 평가 중 BSA, RAND, 옥스포드 대학의 역량 평가에 항목으로 선정되었고, DOE의 역량 평가는 에너지부의 주관으로 개발되어 주요 기반 시설인 에너지 분야에 사전 적용 시험을 하는 등 주요 기반 시설 보호와 밀접한 관련이 있다.

사고 대응과 위기관리 체계 발전 수준 항목은 8개 평가 중 4개 평가에 평가항목으로 선정되었다. 미국 NIST는 통합적 사이버 위기관리 체계 필요성을 강조하며, 위험 관리 프레임워크를 기반으로 정부기관의 사이버보안을 강화하고자 노력하고 있으며, 이는 FISMA 체계의 근간이기도 하다. 체계적인 사고 대응 및 지속적인 위기관리를 위해 관련 정책에 대한 평가가 필요하다.

4.2.2 법・제도

법·제도 항목에서는 정보시스템 및 사이버보안을 위한 기본법과 정보보호, 사이버 범죄, 사이버보안 사고보고 의무에 관한 법률 및 규정의 발전 수준을 평가항목으로 도출하였다.

사이버보안 기본법은 사이버보안의 기본 방향 및 정책 수립·추진에 필요한 사항을 규정한 법률로 기존의 역량 평가에서는 항목으로 도출되지는 않았지만, 국가 정보보호를 위한 가장 기본적인 법률이자 다른 하위 법률 제정의 근간이 되는 법률이기 때문에 평가항목으로 도출하였다.

정보보호에 관한 법률은 개인정보를 포함한 데이터의 보호를 말하며, 옥스포드 대학 역량 평가에서 평가항목으로 선정되었고, BSA는 정보보호에 관한 법률의 발전 수주을 평가항목으로 선정하여 평가하였다.

우리나라는 수차례 은행 및 카드사 고객 정보 유출 등 개인정보 유출 피해가 광범위하게 발생하였고 개인정보 보호 강화를 위해 '개인정보보호법'을 제정 및 시행하고 있다. 개인정보보호법은 개인정보 유출로 인한 피해를 방지할 뿐만 아니라 개인정보의 중요성 및 보호의 필요성에 널리 알리는 데에도 기여하였다. 네트워크 보급률이 높고, 국민의 네트워크 의존도가 높은 우리나라에서는 사이버 공간에 대한 신뢰 구축을 위해 개인정보보호는 필수적이다.

사이버범죄는 갈수록 증가하고 있는 데에 비해 기존의 범죄와는 다르게 형태와 피해 규모에 대한 파악이 어려운 실정이다. 이에 사이버범죄 방지 및 대응을 위해서는 사이버범죄에 관한 법률이 필수적이라고 할 수 있겠다. 이에 옥스포드 대학과 ITU는 사이버범죄에 관한 법률의 발전 수준을 평가항목으로 선정하여 평가하였다. ASPI는 사이버범죄 법률 존재 여부는 아니지만 관련 조직 구조의 존재 여부를 평가항목으로 선정하고 평가하였다.

사이버보안 사고보고 의무는 국가 차원을 넘어 범세계적 이슈로 사고 재발을 막고 위기관리 및 대응을 위해 반드시 필요한 사항이다.

4.2.3 조직

조직 항목에서는 사이버보안 전담 조직의 발전 수준과 CERTs의 발전 수준을 세부항목으로 도출하였다.

사이버보안 전담 조직은 8개의 해외 역량 평가 중 7개의 평가에서 항목으로 선정되었고, CERTs는 6개에서 항목으로 선정되어 국가 사이버보안 역량 평가를 위한 기본 항목이다. 책임기관은 직접적인 업무 집행 및 결정과 그에 따른 책임을 지는 기관으로, 이를 규정함으로써 권한과 책임을 명확화하고 조직 간의 중복 및 충돌을 예방하여 행정 운영의 효율성을 향상시킬 수 있다.

4.2.4 예산

예산 항목은 기존의 역량 평가에서는 항목으로 도출되지 않았지만 국가 정책에서 예산의 중요성을 고려하여 세부항목으로 도출하였다.

국가 예산은 국가가 어떤 정책이나 목적을 위해 얼마나 지출하고, 이를 위한 재원 조달 방법을 나타낸 것이다. 즉, 예산은 사용할 수 있는 자금 한도를 나타내며, 예산 금액과 활동의 범위가 비례하므로 '권한기능'이라고 할 수 있다[19]. 이러한 예산은 단순한 자금의 의미를 넘어 넓은 의미에서 한 국가의 미래 형성 방향 설정의 의미를 포함하고 있다. 즉, 더 많은 예산을 책정한다는 것은 국가가 해당 정책과 목적을 적극적으로 지원하여, 해당 정책과 목적으로 미래를 성장시키겠다는 의지가 반영된 것이다.

때문에 사이버보안에 대한 예산은 국가의 사이버보안에 대한 의지를 나타내며 향후 사이버보안의 발전 가능성을 나타내는 지표라고 할 수 있겠다. 또한 국가 예산은 정량적 지표로서 평가 결과에 보다 높은 객관성을 부여할 것으로 보인다.

4.2.5 교육・훈련

교육·훈련 항목에서는 사이버보안 인력 양성 체계 구축, 교육의 다양성 확보, 인식제고, 모범 사례 공유 프로그램의 발전 수준을 세부 항목으로 도출하였다.

미국은 2011년 '국가 사이버보안 교육 프로젝트 전략 수행계획(NICE, The National Initiative for Cybersecurity Education)'을 발표하고, 사이버보안 인력 양성을 위한 교육 및 훈련을 체계적으로 추진하고 있다[20].

우리나라의 부족한 정보보호 인력 수급을 위해서는 종합적인 교육·훈련 체계가 마련되어야 한다. 따라서 대학 커리큘럼, 직업 훈련 등의 교육 체계를 마련하여 지속적이고, 종합적인 사이버보안 인력을 양성 체계 구축 여부와 다양한 사이버보안 분야 대하여 초급에서 전문적이고 고도화된 교육까지의 수준별 교육을 IT 기술을 이용한 온·오프라인 등의 다양한 형태로 지원하는 지의 여부를 평가항목으로 도출하였다.

또한 국가가 국내외의 모범 사례 공유를 통해 국가의 사이버보안 역량 향상 및 조직 및 기관에서도 활발하게 사이버보안 이루어질 수 있도록 하는 지원 여부와 지속적으로 사이버보안 인식 제고 활동을 통해 사이버보안의 중요성을 알리고, 정부·기업뿐만 아니라 일반 이용자도 사이버보안에 적극 참여를 유도 수준을 평가항목으로 도출하여 향후 사이버보안 정책 수립 방향을 제시하였다.

특히 교육·훈련 항목 평가 분석 결과는 국가 사이버 전문 인력 양성 기관인 사이버안전훈련센터의 활동 방향 정립 시 기초자료로 활용이 가능하다.

4.2.6 기술・표준・인증

기술·표준·인증 항목에서는 연구·개발 조직, 표준·인증기관 발전 수준과 기술 보유 수준을 세부 항목으로 도출하였다.

사이버보안 연구 개발 인력 조직 보유 및 기술 보유는 사이버 위협 탐지 및 사이버보안 테러 대응 기술 등 사이버보안 핵심 기술 확보를 통해 사이버보안 기반 강화에 기여하고, 이는 사이버보안 산업 경쟁력 확보 및 발전에도 영향을 미친다.

미국은 2009년에 발표한 '사이버공간 정책 재검토(CPR, Cyberspace Policy Review)' 명령에 따라 대통령실 주도로 사이버보안 연구 개발 전략을 수립하고 있다[20]. 또한 '네트워크 및 정보기술연구개발' 프로그램인 IT 이니셔티브를 만들고 '사이버보안 정보 신뢰', '고신뢰성 소프트웨어 및 시스템'을 주요 연구개발 분야로 선정하여 사이버보안 기술 연구 개발을 수행하고 있다[21].

사이버보안 연구 개발 조직의 존재 여부는 사이버보안 인력 양성에도 기여한다. 고급 인력의 사이버보안 분야에서의 커리어 패스를 마련하므로서 사이버보안 분야에 대한 관심을 증대시킬 수 있기에 평가항목으로 도출 하였다. 또한 기술 연구뿐만 아닌 체계적

인 사이버보안 정책 개발을 위한 정책 연구 개발 조직의 존재 여부도 향후 평가항목으로 선정될 필요가 있다.

표준·인증 기관의 발전 수준 항목은 8개 평가 중 4개의 평가에서 평가항목으로 선정되었다. 표준·인증 기관의 설립은 기술의 발전 및 사이버보안 인력, 조직, 기술의 신뢰성 확보에 기여할 것이라 사료된다.

4.2.7 협력

협력 항목에서는 민관 협력, 부처간 협력, 국제 협력 체계 발전 수준을 세부 항목으로 도출하였다.

민관 협력 항목은 8개의 해외 역량 평가 중 6개의 평가에서 항목으로 선정된 만큼 국가 사이버보안 역량 평가를 위한 기본 항목이라고 할 수 있겠다. 특히 주요 기반시설의 사이버보안 강화와 인력양성 측면에서는 정부와 기업의 공조체계 구축은 반드시 필요한 항목이다.

부처간 협력은 국가의 사이버보안 역량 강화를 위해서 중복 부서를 통합 연계하여 역량을 통합하고, 책임 소재를 명확하게 하여 사이버보안 업무 대응 효율 증대에 기여할 수 있다.

미국은 2010년 국토안보부, 국방부가 미국 전역에 걸쳐 사이버보안 강화를 위한 공동 계획에 합의하고 부처간 협력 강화를 위해 노력하고 있다.

우리나라도 부처간 협력의 중요성을 인식하고, 관련 법률을 제안하고, 대응 체계를 마련하고 있다. 향후 지속적인 부처간 협력을 강화하기 위해 부처간 협력 항목을 평가항목으로 도출하였다.

국제 협력 또한 3개의 평가에서 항목으로 선정되었다. 사이버보안은 이제 국가를 넘어서 범세계적 이슈로 전세계의 공동 대응과 협력이 필요하다. 사이버보안 국제 협력 조직 참여는 정보 공유 및 협력 연대 강화에 기여할 것으로 보인다.

4.3 평가의 한계점

3.3절에서 보다 객관적이 체계적인 국가 사이버보안 역량 평가를 위한 평가항목을 제안하였다. 그러나 국가의 사이버보안 역량 평가 특성상 근본적인 평가의 한계점을 가지고 있다.

먼저, 국가의 사이버보안 역량 평가를 위한 근거 자료가 부족하다는 것이다. 많은 국가가 구체적인 사이버보안 실태를 공개하지 않고 있으며, 공개된 자료도 국가별로 시기적으로 일치하지 않아서 비교 평가가 어렵다.

둘째, 평가 결과의 신뢰성과 타당성을 입증할 객관적인 검증 절차가 없다는 것이다. 때문에 각 역량 평가 별로 평가 방법론과 근거 자료가 달라 동일 항목에 대해서도 다른 결과가 도출된다. 그러나 각각의 방법론과 모든 근거 자료의 신뢰성을 입증하는 데는 현실적인 어려움이 존재한다.

셋째, 전문가를 통한 정성적 평가라는 한계점을 갖는다. 국가 사이버보안 역량 평가의 평가항목은 각 항목에 대해서 수치화하여 정량적인 표현이 어렵고, 때문에 전문가를 통한 정성적 평가가 일반적이다. 그러나 국가의 사이버보안 역량을 평가하기 위해 전체적인 지식을 보유한 전문가가 매우 극소수일 뿐만 아니라 전문가의 편향적인 성향이 개입될 여지가 있어 원칙적 한계를 가지고 있다.

또한 본 논문에서 제안한 국가 사이버보안 역량 평가는 국가의 사이버보안 역량 평가 실태 평가 및 국가간 비교를 위한 평가항목으로 국가가 아닌 기업 및 조직에 적용하기에는 한계가 있다.

그러나 국가 사이버보안 역량 평가는 국가간 비교 평가 결과에만 목적이 있지 않고, 평가항목을 통한 향후 정책 방향에 대한 제안 및 사이버보안 역량 강화 방안 마련 기초 자료로 활용이 가능하기 때문에 평가항목 선정은 중요한 의미를 갖는다. 또한 국가 사이버보안 역량 평가는 향후 기업 및 조직에서 적용 가능한 사이버보안 역량 성숙도 모델 구축 시에도 활용이 가능하다.

V. 결 론

사이버보안 역량 평가는 법, 정책, 사회, 기술 등 다양한 항목이 평가에 영향을 미치게 된다. 이에 사이버보안 역량 평가를 국가 사이버보안 역량 평가와 사이버보안 성숙도 평가로 분류하고, 해외 사이버보안 역량 평가 사례로 미 헤리티지 재단의 '2015 군사력 지수', BSA의 '사이버보안 대쉬보드', ITU의 '세계 사이버 지수', ASPI의 '아태지역 사이버 성숙도', RAND의 '사이버방어 역량 성숙도 모델', WEF의 '조직 사이버복원 성숙도 모델', 옥스포드 대학의 '사이버보안 역량 성숙도 모델', 미국 에너지부의 '사이버보안 역량 성숙도 모델'을 분석하였다. 그 결과 보편적이고 일반적인 평가항목과 우리나라의 사이버공간 특성을 반영한 평가항목을 배합하여 새로운 국가 사

이버보안 역량 평가항목을 도출하였다.

제안한 평가항목은 정책, 법제도, 조직, 예산, 교육·훈련, 기술·표준·인증, 협력 7가지 평가항목에 대해 18개의 세부항목으로 분류하였다. 기존 해외 역량 평가 연구에서 기본항목으로 선정된 정책, 법, 조직, 협력 항목을 바탕으로 정량적 지표를 통한 평가 결과 객관성 확보를 위한 예산 항목과 향후 정책 방향 수립 지원을 위한 연구·개발 조직 존재 유무, 기술, 표준, 인증 항목을 추가하였다.

국가 사이버보안 역량 평가항목 및 평가 결과는 사이버보안 정책 결정자들을 위한 기초자료로 활용이 가능하고, 사이버보안 역량 강화 방안 마련 시에도 참고자료로 활용이 가능하다.

그러나 역량 평가의 특성상 근본적인 한계가 존재한다. 공개된 근거 자료가 부족하고, 평가 결과에 대한 신뢰성 입증이 어려우며, 평가를 위한 국가 사이버보안 전반에 걸친 전문 지식을 보유한 전문가가 부족하고, 전문가를 대상으로 한 정성적 평가이기에 전문가의 편향적인 성향이 개입될 여지가 있다.

향후 도출된 평가항목을 바탕으로 사이버보안 법·정책·기술 전문가를 대상으로 우리나라와 주요 국가를 대상으로 국가 사이버보안 역량 평가를 수행할 예정이다. 또한 평가 결과의 객관성 부여를 위해 평가 대상국의 평가항목 관련 근거 자료 확보가 필요하고, 항목별로 측정 기준 또는 평가 기준을 마련하는 연구가 필요할 것으로 보인다.

도출된 평가항목은 국가의 사이버보안 역량을 평가하기 위한 항목으로, 향후 해당 항목들을 조직 또는 기관에서 활용할 수 있도록 확대하는 방안에 대한 추가적인 연구가 필요할 것으로 사료된다.

References

〔1〕 Pil Woon Jung, "A Critical Analysis on the Concept of Cyber Security," Yonsei Journal of Mediccal and Science Technology Law, vol.2, no.2,, pp.1-25, 2011.

〔2〕 Sunha Bae, Sangdon Park, and So Jeong KIM, "The enhancement Strategy on National Cyber Capability Using Hybrid Methodology of AHP and TOPSIS," Convergence Security Journal, vol.15, no.4, pp.43-55, Jun. 2015.

〔3〕 Paulk, Mark C., Weber, Charles V, Curtis, Bill, Chrissis, Mary Beth "Capability Maturity Model for Software (Version 1.1)," Software, IEEE, vol.10, no.4, pp18-27, Jul. 1993.

〔4〕 The Heritage Foundation, "2015 Index of U.S. Military Strength", pp.74-78, Feb. 2015.

〔5〕 BSA The software alliance, "EU Cybersecurity Dashboard 2015," pp.1-16, May, 2015.

〔6〕 Peña-López, Ismael. "Global Cybersecurity Index and Cyberwellness profiles Report," WSIS Forum'15 Geneva, pp.1-37, May, 2015.

〔7〕 Tobias Feakin, Jessica Woodall and Klée Aiken, "Cyber maturity in the Asia-Pacific Region 2014," ASPI, pp.1-76, Apr. 2015.

〔8〕 Neil Robinson, Agnieszka Walczak, and Sophie-Charlotte Brune, "Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)," RAND Corporation, pp.1-22, 2013.

〔9〕 Collaboration with Deloitte, "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience," World Economy Forum, pp.18-20, 2012.

〔10〕 Taylor Roberts, "Cyber Security Capability Maturity Model (CMM)", Global Cyber Securiy Capacity Center University of Oxford, pp.1-44, May, 2015.

〔11〕 U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2)," v1.1, pp.1-76, Feb. 2014.

〔12〕 U.S. Department of Energy, "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)," v1.1, pp.1-52, Feb. 2014.

〔13〕 Seo, H. J., SoonJa Hong, and Yoon-Cheol Choy. "A Study on the methodology to evaluate the level of nation's capability for cyber war." The 12th International Workshop on Information Security Applications (WISA2011), Aug. 2011.

〔14〕 Jungmin Kang, "A Study on National Cyber

Capability Assessment Methodology," Journal of KIISC, vol. 22, no. 5, pp. 1039-1055, 2012.
〔15〕 Booz Allen Hamilton, "Cyber Power Index," Mar. 2011.
〔16〕 KT Economic Management Institute, "Tap On The Door of Mobile First World", pp. 6, Jan. 2015.
〔17〕 KISTEP, "The Analysis of The World Competitiveness 2014 by IMD", vol.11, pp. 7, Mar. 2015.
〔18〕 NIS, "Whitepaper of national Cybersecurity 2015", pp. 275-303, May, 2015.
〔19〕 Taekyu Lee, Corporate Finance based on Business Management, Knowledge and sensiblity, pp.227-228, Feb. 2014.
〔20〕 So Jeong KIM, Seokjin Choi "Study on the National Cybersecurity Strategies of Obama Administraton," Journal of Foreign Affairs and National Security, vol.7, no.2, pp.173-200, 2011.
〔21〕 https://www.nitrd.gov/nitrdgroups/index.php?title=High_Confidence_Software_and_Systems_Coordinating_Group_(HCSS_CG)

〈저자소개〉

사 진

배 선 하 (Sunha Bae) 정회원
2007년 2월: 한양대학교 미디어통신공학과(학사)
2009년 1월: 한국과학기술원 전기 및 전자공학과(석사)
2009년 1월~2013년 2월: LIG 넥스원 주임연구원
2013년 4월~2014년 1월: 두산중공업 기술연구원 주임연구원
2015년 2월~현재: 국가보안기술연구소 기술원
〈관심분야〉 정보보호, 전자공학, 제어시스템

사 진

박상돈(Sangdon Park) 정회원
2002년 2월: 성균관대학교 법학과(학사)
2004년 8월: 성균관대학교 법학과(석사)
2010년 2월: 성균관대학교 법학과 박사과정 수료
2008년~ 현재: 국가보안기술연구소 선임연구원
〈관심분야〉 정보보호 법제도

사 진

김소정(So Jeong Kim) 정회원
1998년 2월: 부산대학교 사학과(학사)
2001년 2월: 경희대학교 평화복지대학원 동북아학과(석사)
2005년 2월: 고려대학교 정보보호대학원 정보보호정책학과(박사)
2001년~2002년: 한국전파진흥협회 ITU-WRC 담당 연구원
2004년~ 현재 국가보안기술연구소 정책연구실장, 선임연구원
〈관심분야〉 사이버안보 전략, 정보보호정책, 기반보호정책