Journal of Digital Convergence
Vol. 19. No. 8, pp. 89-100, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.8.089

국가 사이버 역량평가 모델을 활용한 국내 사이버안보 정책 의제 도출 연구

송민경, 배선하, 김소정*
국가보안기술연구소

A study on national cybersecurity policy agenda in Korea using national cyber capability assessment model

Minkyoung Song, Sunha Bae, So-Jeong Kim*
National Security Research Institute

요 약 국가 사이버 역량평가는 국가 차원의 사이버역량 강화를 위해 필요한 요소와 그에 대한 국가별 수준에 대한 정보를 제공하기 때문에 국가 사이버안보 정책 개선을 위한 기초자료로 활용할 수 있다. 그러나 그간 우리나라를 평가대상국으로 포함하여 평가를 진행한 다양한 평가결과로부터 국내 사이버역량 개선을 위한 정책적 분석은 다소 부족하였다. 이에 본 논문에서는 미국 하버드 대학의 벨퍼센터에서 수행한 국가 사이버 추진력 지수(NCPI)의 평가결과에 대해 IPA(Importance-Performance Analysis) 기법을 변형·적용해봄으로써 우리나라 사이버안보 정책 개선 방안을 도출하고자 하였다. 분석 결과, 우리나라는 공격과 감시 목적의 사이버 기능 활용에 관한 정책 의제 형성이 필요하고, 인텔리전스와 방어에 관한 정책의 실효성을 향상하기 위한 노력이 필요하다는 결론을 얻을 수 있었다. 또한, 관련 정책 의제를 다루는 국내외 연구사례를 살펴봄으로써 정책개선 방향을 제시하며, 각 정책개선 방향에 관한 심층 연구를 추진할 것을 향후 과제로 제안하였다. 나아가 국가 사이버 역량평가 모델의 정책 분석적 활용을 향상하기 위해서는 국내 실정을 반영하는 자체 모델 개발·활용이 필요하며, 이때 본 연구에서 제안한 평가결과 분석 방안을 활용할 수 있을 것으로 기대한다.

주제어 : 사이버역량, 역량평가, 국가 사이버 추진력 지수(NCPI), 정책 분석, IPA 분석

Abstract The National Cyber Capability Assessment(NCCA) could be used as meaningful information for improving national cyber security policy because it provides information on the elements necessary for strengthening national cyber capabilities and the level of each country. However, there were few studies on improving cyber capabilities using the NCCA result in Korea. Therefore, we analyzed the result of National Cyber Power Index(NCPI) conducted by Belfer Center of Harvard Univ. by applying modified-IPA method to derive cybersecurity policy agendas for Korea. As a result, the need to set agendas on surveillance and offensive cyber capability and improve the effectiveness of policy implementation for intelligence and defense was drawn. Moreover, we suggested need for in-depth study of each policy agenda deduced from preceding research data as a future tasks. And it is expected to increase practical use of NCCA for domestic policy analysis by developing and using our own NCCA model which considered analysis framework proposed in this study.

Key Words : Cyber Power, Capability Assessment, National Cyber Power Index(NCPI), Policy Analysis, IPA Analysis

*Corresponding Author : So-Jeong Kim(sjkim@nsr.re.kr)
Received July 6, 2021
Revised July 20, 2021
Accepted August 20, 2021
Published August 28, 2021

1. 서론

국가 사이버역량 평가는 국가 차원의 사이버역량을 평가·분석하기 위한 기준을 마련하고, 국가별 현황을 직관적으로 살펴볼 수 있도록 정량화함으로써 주변 국가 대비 자국의 사이버역량 수준을 파악하는 것을 목적으로 한다. 국가 사이버 역량평가의 대표적인 해외 사례로는 국제전기통신연합(ITU)의 국가 사이버보안 지수(Global Cybersecurity Index, GCI)[1], 옥스퍼드 대학의 사이버 성숙도 모델(Cyber Security Capability Maturity Model, CMM)[2], 미국 포토맥 정책연구소의 사이버 준비 지수(Cyber Readiness Index, CRI)[3], 호주전략정책연구원의 사이버 성숙도 모델(Cyber Maturity in the Asia-Pacific region, C.M.)[4], 하버드 대학의 국가 사이버 추진력 지수(National Cyber Power Index, NCPI)[5] 등이 있다. 이들은 국가 차원의 사이버역량을 구성하는 항목을 선정하고, 항목별 국가의 역량을 점수화함으로써 전략개선, 역량구축 컨설팅, 경향 분석 등 다양한 목적에 평가결과를 활용하고 있다.

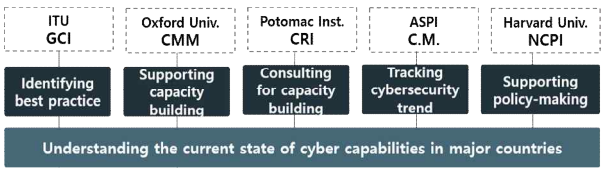

Fig. 1. National cyber capability assessment model usage

한편, 국가 사이버역량 평가는 평가수행기관에 따라 목적, 관점, 그리고 점수화 방법이 다르기 때문에 동일시기에 동일국가를 평가하더라도 서로 다른 결과가 도출될 수 있다는 한계가 지적되고 있다. 평가결과가 다양한 요인에 의해 영향을 받는다는 점은 국가 사이버역량 평가를 포함한 여러 평가모델이 내재하고 있는 한계이다. 그럼에도 불구하고 앞서 언급한 국내외 다수의 기관들이 평가모델을 개발하고 분석하는 노력을 지속하는 이유는 Fig. 1에서 제시한 바와 같이 평가모델이 국가별 점수와 순위를 산정하는 것을 넘어 각국의 현황자료를 체계적으로 확보하고 사이버안보 정책 경향을 추적하는 정책적 도구로서 가치가 있기 때문이다.

그러나 아직 우리나라에서는 국가 사이버역량 평가결과를 토대로 국내 사이버역량 향상 방안을 도출하는 연구나 공개된 분석사례를 찾기 어렵다. 이에 본 연구에서는 국가 사이버역량 평가결과로부터 국내 정책개선 방안을 도출해보고자 한다. 이를 위해 Table 1에 제시된 바와 같이 우리나라를 평가대상에 포함하며, 평가점수를 공개하고, 최신의 결과를 반영하는 하버드 대학의 NCPI 결과를 활용하였다. 특히 NCPI는 다른 평가보고서와는 달리 국가별 세부지표에 대한 점수를 별도의 파일로 공개하고 있기에 보다 구체적인 분석이 가능하다는 장점이 있다.

Table 1. Target selection criteria

Criteria	Assessment Model				
	GCI [1]	CMM [2]	CRI [3]	C.M. [4]	NCPI [5]
Does it covered Korea?	○			○	○
Are the scores publicly available?				○	○
Does it reflect the latest situation?	(2021)			(2017)	(2020)

본 논문의 구성은 다음과 같다. 2장에서 NCPI 평가모델과 우리나라의 평가결과를 구체적으로 살펴보았다. 3장에서는 NCPI 결과에 대한 분석방법으로 IPA 기법을 소개하고 이를 적용한 결과를 제시한다. 4장에서는 분석결과로써 NCPI 결과에 기반한 국내 사이버안보 정책개선 방안을 도출하였고, 5장에서 본 연구의 한계와 시사점을 제시하였다.

2. 국가 사이버 추진력 지수(NCPI) 소개

2.1 NCPI 개요

2020년 9월, 미국 하버드케네디스쿨의 벨퍼센터는 중국사이버정책이니셔티브의 일환으로 전 세계 30여 개국의 사이버추진력을 평가한 NCPI를 발표하였다[5]. NCPI는 Table 2에 제시된 7개의 국가목표(감시, 방어, 정보통제, 인텔리전스[1], 산업, 공격, 규범)를 달성하기 위해 사이버수단을 활용할 수 있는 국가를 사이버강국으로 정의하고, 이에 대한 국가의 의지와 역량을 각각 사이버 의지지수(Cyber Intent Index, CII)와 사이버 역량지수(Cyber Capability Index, CCI)로 측정하여 점수화하였다.

1) 국가안보와 관련된 타국의 정보를 수집하는 일련의 국가 활동으로, 국내에서 정보 또는 첩보로 번역·혼용되고 있어 그 모호성을 최소화하기 위해 영어 발음을 한글화하여 표기함

Table 2. 7 objectives to achieve through cyberspace by states
(Source: NCPI 2020 report of Harvard Univ.[5])

#	Objectives	Definition
1	Surveillance	Surveilling and Monitoring Domestic Groups
2	Defense	Strengthening and Enhancing National Cyber Defense
3	Control	Controlling and Manipulating the Information Environment
4	Intelligence	Intelligence Gathering and Collection in other Countries for National Security
5	Commercial	Growing National Cyber and Technology Competence
6	Offense	Destroying or Disabling an Adversary's Infrastructure and Capabilities
7	Norms	Defining International Cyber Norms and Technical Standards

CII는 국가별 공개된 전략이나 표명, 자금지원 자료, 사이버 공격 자료를 근거로 하는 32개 지표를 통해 국가목표에 사이버역량을 활용하고자 하는 의지의 정도를 나타낸다. CCI는 공격증거, 국가온라인컨텐츠, 거버넌스 체계, 정책·법률 프레임워크 등 27개의 공개데이터(국가 산출물)를 지표로 하여 국가목표 달성에 요구되는 사이버역량 수준을 점수화한다. NCPI 최종 점수는 CII와 CCI의 곱으로 최종 산정되며, 의지와 역량 모두 높은 국가가 높은 NCPI 점수를 획득하게 된다.

$$NCPI = \frac{1}{7}\sum_{\chi=1}^{7} CII_{\chi} \times CCI_{\chi} \ (x\,means\,7\,objectives\,of\,NCPI)$$

NCPI 평가 결과, 미국, 중국, 영국, 러시아, 네덜란드 순으로 최종 점수가 산정되었고, CII와 CCI 점수별 상위 10개국은 Table 3과 같다.

Table 3. Top 10 ranking by index

#	CII(score)	CCI(score)
1	China(80.3)	US(65.8)
2	US(76.7)	China(55.9)
3	UK(76.0)	UK(44.9)
4	Russia(71.0)	Germany(43.5)
5	Netherlands(60.9)	France(43.0)
6	Israel(59.6)	South Korea(40.0)
7	Spain(58.7)	Singapore(39.1)
8	Australia(56.6)	Japan(38.3)
9	Canada(54.7)	Netherlands(38.0)
10	Iran(51.1)	Russia(37.7)

우리나라는 CII 18위(39.3점), CCI 6위(40.0점)로 높은 역량 대비 낮은 의지를 보유한 국가로 평가되면서 종합 16위를 기록하였다. 한편, NCPI 평가보고서는 국가별 의지(CII)와 역량(CCI) 점수의 분포에 따라 의지와 역량이 모두 높은 국가로 미국·영국·중국·프랑스·독일, 역량은 높지만 의지가 낮은 국가로 한국, 의지는 높지만 역량이 낮은 국가로 러시아·이란·이스라엘·네덜란드, 의지와 역량 모두 낮은 국가로 이집트·리투아니아를 선정하였다.

2.2 우리나라 상세 평가결과

본 절에서는 우리나라 관점에서 NCPI 평가결과를 재해석하기 위해 벨퍼센터에서 별도로 제공하는 세부 평가결과 파일[6]을 참고하여 국가목표별, 지표별 점수를 Table 4와 같이 재정리하였다.

Table 4. Detailed score of Korea by objectives

National Objectives	CII		CCI	
	average score	score of Korea	average score	score of Korea
Surveillance	40.8	23	42.9	47.7▲
Defense	74.5	63	54.5	59.6▲
Control	33.8	14	26.9	34.4▲
Intelligence	45.7	67▲	23.2	23.9▲
Commercial	35.1	32	20.7	41.5▲
Offense	26.6	15	33.8	34.8▲
Norms	61.9	61	30.4	37.4▲

우리나라는 7가지 국가목표 모두 평균보다 높은 역량 수준을 확보한 것으로 평가되었으나 의지는 낮게 평가되었는데, 특히 감시, 정보통제, 공격 항목은 30개 국가의 평균점수의 절반에 해당하는 점수로 평가되었다.

2.2.1 사이버 의지지수(CII)

NCPI의 CII는 Table 5의 지표로 구성되며, 점수의 50%는 사이버공격 사례, 나머지 50%는 전략·계획·법에 대한 분석을 통해 산정된다. 우리나라는 알려진 사이버공격 사례가 없고, 감시나 정보통제 등에 대한 의지를 공개적으로 표명하고 있지 않기에 CII 점수가 전반적으로 낮게 평가된 것으로 보인다.

2.2.2 사이버 역량지수(CCI)

NCPI의 CCI는 국가목표에 관련된 27개의 정량지표에 따라 점수화되며, Table 6에서도 확인할 수 있듯이 하나의 지표가 여러 국가목표에 관련이 있어 여러 항목에 동시에 영향을 미치는 구조이다. 우리나라는 산업과 정보통제에 높은 역량을 보이는 반면, 그 외 다른 항목에

Table 5. CII indicators and score(ranking) of Korea by objectives

Objectives	CII indicators(a brief summary)	Score (Ranking)
Surveillance	having related policy/law enforcement agency, acknowledging related cyber capabilities, establishing related strategy/plan/law, consistency of objective in strategy, related cyber attack experience, etc.	23 (24th)
Defense	establishing related plan, undertaking cyber awareness campaigns, describing national active cyber defense-style, consistency of objective in stategy, etc.	63 (18th)
Control	data law protection strength, having related strategy or acknowledging related cyber capabilities, having military cyber unit or command, acknowledging related cyber capabilities, consistency of objective in strategy, related cyber attack experience, etc.	14 (20th)
Intelligence	having realted strategy/planning documents, acknowledging related cyber capabilities by military cyber unit/intelligence agency, consistency of objective in stategy, related cyber attack experience, etc.	67 (11th)
Commercial	quality of participation across all 22 ISO-IEC Joint Technical Committees, having public-private partnership initiative for domestic cyber issue, investing in or funding cyber research, consistency of objective in stategy, etc.	32 (17th)
Offense	having realted strategy/planning documents, acknowledging related cyber capabilities by military cyber unit/intelligence agency, consistency of objective in stategy, related cyber attack experience, etc.	15 (15th)
Norms	participating in UN GGE consultations/Internet Governance Forum(IGF)/Global Forum for Cyber Expertise capabity building activities, quality of participation across all 22 ISO/IEC Joint Technical Committees, participating in bilateral/multilateral cyber defense exercises, consistency of objective in stategy, etc.	61 (15th)

Table 6. CCI indicators and score(ranking) of Korea by indicators

CCI		National Objectives						
Indicators	Score(ranking) of Korea	Surveillance	Defense	Control	Intelligence	Commercial	Offense	Norms
Overall score(ranking) by objectives		47.7(13th)	59.6(11th)	34.4(4th)	23.9(11th)	41.5(2nd)	34.8(14th)	37.4(9th)
Cyber security laws	1(15th)	○	○					○
State-sponsored attacks	0(9th)	○		○	○	○	○	
Bilateral cyber agreements	27(8th)							○
Multilateral cyber agreements	8(7th)							○
Cyber military doctrine	0(20th)						○	
National cyber command	4(1st)						○	
Global top 100 tecgnology firms	3(4th)				○	○		○
High-tech exports	36(4th)				○	○	○	○
Skilled employees in the technology industry	62.9(18th)		○		○	○		
Cyber military staffing	1000(10th)				○		○	
Global top 500 cybersecurity firms	0(8th)					○		
Computer infection rates	0.08(5th)		○					
Mobile infection reates	0.03(7th)		○					
Population % on social media	0.85(1st)	○		○				
Population % on the internet	0.95(2nd)	○	○	○				
Existence of private sector surveillance technology	5(20th)	○			○			
Top websites in Alexa top 50	0(9th)			○		○		
Top news sites in Alexa top 50	1(5th)			○				
Successful Google content removal requests	749(7th)			○				
Freedom on the net score	64(12th)	○						
Patent applications	3188.6(4th)					○		
speed of broadband	6.1(8th)		○					
speed of broadband	9.7(1st)		○					
E-commerce economy	1390.7(6th)					○		
Vulnerabilities listed in Shodan affecting domestic machines	31.1(27th)		○					
Existence of CSIRTs	4(1st)		○					
Global Soft Power	48.3(14th)							○

서는 중간 정도의 역량을 확보한 것으로 도출되었다.

한편, CCI는 일반적인 지표의 조합을 통해 7대 국가목표에 대한 역량을 평가한다는 특징이 있다. 일례로 인적자원 지표는 일반적인 정보보호 인력 수급에 관한 지표로, NCPI에서는 정보보호 인력 수급에 어려움이 있는 국가는 방어, 인텔리전스, 산업적 목적 달성을 위한 역량에 부정적인 영향이 미칠 수 있다고 가정할 뿐, 각 목적에 특화된 인력 수급을 의미하는 것은 아니다.

3. 분석방법

3.1 IPA 분석기법과 CII-CCI 매트릭스화 방법

자료 속 정보로부터 분석의 목적에 맞는 정보를 식별, 분류하고 그로부터 효율적이고 효과적인 정보를 재탄생시키는 분석방법으로 매트릭스 분석이 있다[7,8]. 그중에서도 NCPI 평가처럼 국가별 CII 점수와 CCI 점수, 즉 두 개의 항목에 대한 점수 정보를 제공하는 자료를 분석할 수 있는 대표적인 매트릭스 분석방법으로 IPA(Importance-Performance Analysis)가 있다. IPA 기법은 경영진단을 목적으로 처음 도입[9]되었는데, 중요도(Importance)나 성취도(Performance)만을 고려하여 대상의 속성을 평가하거나 개선점을 제시했던 이전 연구에서 벗어나, 두 개념을 매트릭스화하는 비교적 간단한 방법으로 중요도와 성취도를 함께 고려함으로써 특정 조치 또는 개선의 우선순위를 도출할 수 있다는 점에서 유용성이 있다.

IPA 매트릭스는 중요도와 성취도 값을 각각 x축, y축으로 구성하고, 두 축을 중앙값 또는 평균값에서 수직 교차시킴으로써 도식화된다. 이때, 연구대상을 구성하는 각 요인은 매트릭스의 사분면 중 한 군데에 위치하게 되는데, 위치한 사분면에 따라 우선순위가 달리 해석된다. 중요도와 성취도가 모두 높은 Ⅰ사분면은 차별적인 경쟁우위 요소로, 지속적인 유지·관리가 필요한 영역이다. 중요도는 낮지만 성취도가 높은 Ⅱ사분면 역시 장점으로 작용할 수 있겠으나, 상대적으로 중요도가 낮기에 과잉 투자 여부를 확인할 필요가 있다. 한편, 성취도가 낮게 평가된 Ⅲ~Ⅳ분면의 경우, 중요도가 높은 Ⅳ사분면의 요소는 즉각적인 개선이, 비교적 중요도가 낮은 Ⅲ사분면에 대해서는 중장기적인 관점의 개선이 필요한 영역이라고 할 수 있다.

본 연구에서는 IPA 매트릭스의 해석방법에 착안하여 CII와 CCI로 구성된 매트릭스를 활용, 7개 국가목표별 점수를 사분면에 위치시켜봄으로써 우리나라의 사이버안보 정책적 의지와 실질적 역량을 모두 고려한 개선방안을 도출해보고자 한다.

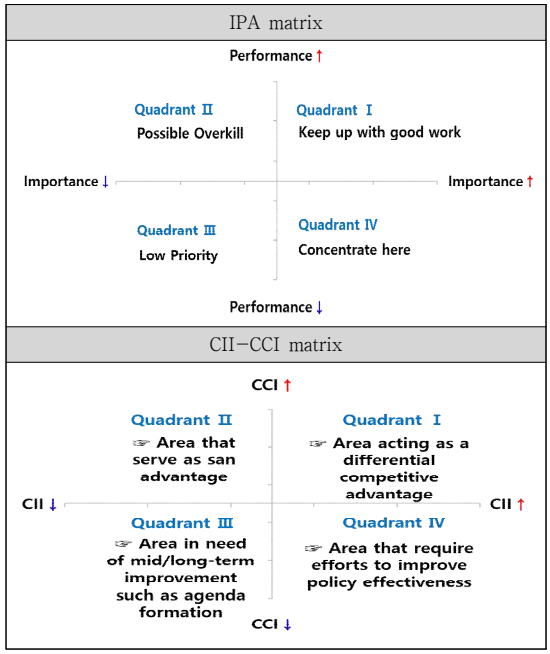

Fig. 2. Comparison IPA matrix and CII-CCI matrix

CII-CCI 매트릭스의 사분면별 해석방법은 다음과 같다. (1) Ⅰ사분면은 의지와 역량이 모두 높게 평가된 영역으로 국내 사이버안보 정책에서 차별적인 우위 요소로 작용할 수 있어 지속적인 유지·관리가 필요한 영역이다. (2) Ⅱ사분면은 의지는 낮지만 역량은 높게 평가된 경우로, 이 역시 강점이라 할 수 있으나 관련 항목에 지속적인 투자가 이루어지고 있다면 과잉 투자의 여지가 있으며, 적은 비용으로도 높은 역량을 보이는 것이라면 지속적인 관리가 필요한 영역이다. (3)Ⅲ사분면은 의지와 역량이 모두 낮은 경우로 약점으로 작용할 수 있으나 개선의 우선순위가 높은 편은 아니며, 중장기적 관점에서의 개선이 필요한 영역이다. (4)끝으로 Ⅳ사분면은 의지는 높지만 역량이 낮은 영역으로 정책 실현에 어려움을 겪고 있다고 해석될 수 있으며, 따라서 향후 적극적이고 즉각적인 개선의 노력이 필요한 영역이라고 할 수 있다.

3.2 CII-CCI 매트릭스 도식화 결과

본 절에서는 CII 및 CCI 점수를 CII-CCI 매트릭스로 도식화하고, 7개 국가목표를 사분면에 위치시키고자 한다. 그러나 같은 15위로 평가된 CII-공격과 CII-규범이

각각 15점과 61점으로 평가된 것처럼, 7개 국가목표가 서로 다른 기준에 따라 점수화되면서 단순히 점수로만 항목을 사분면에 위치시킬 경우 다른 국가와 비교한 상대적인 의지 및 역량 순위를 고려하지 못한다는 제한이 있다. 이에 본 논문에서는 7개 국가목표별 CII와 CCI 점수를 전체 국가의 평균값으로 나누어 Table 7의 조정된 CII 및 CCI 점수를 활용하였고, 그 결과 Fig. 3의 CII-CCI 매트릭스를 구성할 수 있었다.

Table 7. Adjusted score for CII-CCI matrix

National Objectives	CII	CCI
	adj. score	adj. score
Surveillance	0.56	1.11
Defense	0.85	1.09
Control	0.41	1.28
Intelligence	1.47	1.03
Commercial	0.91	2.00
Offense	0.56	1.03
Norms	0.99	1.23

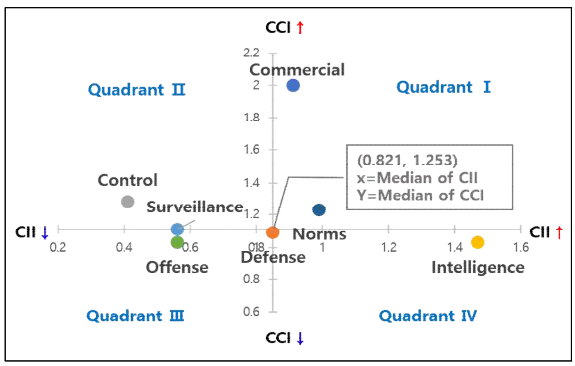

Fig. 3. CII-CCI matrix of Korea result in NCPI

우리나라는 Ⅰ사분면에 산업과 규범 항목이 위치하면서 기술경쟁력과 이를 통한 경제적 성과 창출, 그리고 국제적인 규범 형성에 차별적인 경쟁우위가 있는 것으로 나타났다. 또한, 의지는 낮지만 역량이 높게 평가(Ⅱ사분면)되면서 지속적인 유지·관리가 필요한 항목으로 정보통제 항목이 도출되었다. 반면, 인텔리전스, 방어 활동의 경우 의지는 높지만 역량은 낮게 평가(Ⅳ사분면)되면서, 정책의 효율적, 효과적인 이행을 위한 즉각적인 개선 노력이 필요한 항목으로 도출되었으며, 감시와 공격항목은 의지와 역량 모두 낮게 평가(Ⅲ사분면)되어 향후 정책 형성이 필요한 것으로 나타났다.

일반적으로 정책은 ①의제설정→②정책결정→③정책집행→④정책평가의 4단계로 발전하는데[10], CII-CCI 매트릭스의 Ⅰ사분면은 정책의지와 역량이 모두 높기 때문에 정책집행 이후 역량이 향상된 것으로 간주하고, Ⅱ사분면은 이미 충분한 역량을 보유하였기에 의제설정에 대한 우선순위가 낮은 항목으로 간주하여 국가 사이버안보 정책 개선을 위한 분석에서는 제외하였다. 따라서 다음 장에서는 역량이 낮게 평가된 Ⅲ~Ⅳ 사분면을 중심으로 주요국과 우리나라의 정책 현황을 비교해봄으로써 NCPI 결과에 기반한 국내 사이버 정책 개선 방향을 제시하고자 한다. 의지는 있으나 역량이 낮게 평가된 Ⅳ사분면은 해당 항목의 역량(CCI) 지표 중 낮게 평가된 지표를 식별하고 이를 개선하기 위해 작성된 국내연구사례의 주요 내용을 제시하고, 의지와 역량 모두 낮게 평가된 Ⅲ사분면은 의지(CII)와 역량(CCI) 지표를 종합적으로 고려하여 관련 정책 의제 발굴에 참고할 수 있는 주요 사례를 제시하고자 한다.

4. 분석결과

4.1 (Ⅳ사분면) 정책 실효성 향상 노력이 필요한 항목

4.1.1 인텔리전스

NCPI 평가에서 인텔리전스는 국가안보 목적의 국외 정보수집 역량으로, 사이버수단을 이용하여 외교·군사·조약의 측면에서 타국에 대한 상황인식 및 이해 향상 수준을 반영한다. 우리나라는 국가정보원법에 따라 국가정보원이 국외 정보 및 국내 보안정보 수집·작성 및 배포 업무를 수행하였다[2]. 또한, 통신비밀보호법에서 안보목적의 감청과 통신제한조치를 정의하고, 관련 국가활동 수행 의지를 드러내고 있기에 CII 점수가 높게 평가된 것으로 보인다.

그러나 CCI 점수는 낮게 평가되었는데, 인텔리전스 항목에 대한 CCI 평가지표는 ①국가지원 사이버공격, ②글로벌기술기업, ③하이테크수출, ④인적자원, ⑤사이버군사입력, ⑥감시기술존재여부로 구성된다. 이 중 우리나라가 특히 낮은 점수로 평가된 항목은 숙련된 사이버 인력 확보의 용이성을 평가하는 인적자원 지표(18위)와 자국 내 운영되는 감시 기술 기업의 수를 의미하는 감시기

2) 2020년 10월 15일 전부개정되면서 국정원의 직무 범위가 국외 및 북한에 관한 정보, 방첩·대테러·국제범죄조직에 관한 정보, 국제 및 국가배후 해킹조직 등 사이버안보 및 위성자산 등 안보 관련 우주 정보 구체화·축소되었으나, 본 분석에서는 NCPI 평가가 2019년도에 진행되었기에 개정 전 법령을 토대로 작성하였다.

술존재여부 지표(20위)이다.

우선 인적자원 지표와 관련하여 우리나라는 사이버 전문인력에 대한 수급 불균형 문제를 일찍이 인식하고, 관련하여 교육·훈련체계 개선, 인력양성 프로그램 확대 등을 위한 다양한 정책을 추진하여왔다. 그러나 아직도 사이버 전문인력을 위한 생태계 조성에 대한 한계나 정보보호 인력난 등이 제기되고 있는 실정이다[11]. 또한, 감시기술존재여부 지표에서도 알 수 있듯이 우리나라는 감시 기술을 제공하는 기업을 많이 확보하지는 못한 편이다. 따라서 향후 국내 인텔리전스 역량 강화를 위해 인적자원과 감시기술 지표에 대한 개선이 필요하며, 이에 관련 국내 연구사례를 Table 8과 같이 제시한다.

Table 8. Considerations for improving intelligence CCI score

indicators	related study
Skilled employees	The need to establish an national education system that systematically linked from training to manpower supply[12,13] Designing a refresher course to support job transition to cybersecurity experts[14] Introducing training of step-by-step training system and certification system[15]
surveillance technology	The need to reform the institutional arrangements for the supervision/use of intelligence/surveillance activities to improve the negative public perception of that activities and accelerate developing and utilizing the related technology[16]

우선, 인적자원에 대한 국내 주요 연구사례에서 공통으로 지적되는 사항은 교육체계의 일관성이나 교육과 직무 간 연계성 부족이다. 이를 개선하기 위해 연구된 국내 사례에서는 교육부터 인력공급 과정 전반의 일관성이 보장된 교육체계 마련[12,13], 사이버보안 분야의 전문성을 향상할 수 있는 재교육 프로그램 개발[14], 교육인증체계 확보[15] 등에 대한 필요성이 제기되었다. 인적자원 지표 개선에 관한 대표적인 사례로는 미국의 국가 사이버보안 교육 계획(NICE)[17]과 NICE 인력체계의 활용을 촉진하고 교육·훈련체계의 일관성을 증대하기 위한 계획이 담긴 사이버보안 인력에 관한 행정명령(E.O. 13870)[18]이 있다. 관련 내용을 살펴보면 미국은 사이버보안 분야에 대한 교육-훈련-직무 전반의 연계성을 확보하고 숙련된 전문가들에 인센티브를 제공함으로써 고급 사이버보안 인력을 확보하고 유지하고자 함을 알 수 있다. 향후 우리나라에서도 사이버보안 업무에 필요한 직무 범위 수요를 식별하고, 이를 토대로 사이버보안 교육-훈련-직무 전반에 대한 연계성을 확보하기 위한 노력이 필요할 것으로 보인다.

한편, 감시기술에 대해서는 이에 대한 국민 인식을 긍정적으로 개선하는 것이 가장 시급한 사안으로 꼽히고 있는데, 이를 위해서는 인텔리전스나 감시 활동에 대한 감독과 활용을 제도화함으로써 투명성을 향상할 필요가 있으며[16], 이로부터 관련 기술과 산업의 발전도 이끌 수 있을 것으로 판단된다.

4.1.2 방어

NCPI 평가에서 방어는 국가 자산 및 시스템 방어, 복원력 구축, 사이버 위협 국가에 대한 인식제고 수준 등을 의미하는데, 우리나라는 아주 근소한 차이로 CCI 점수가 낮게 평가되면서 Ⅳ사분면에 위치하였다. 방어 항목을 구성하는 CCI 지표는 ①사이버관련 법률, ②인적자원, ③컴퓨터감염률, ④모바일감염률, ⑤인터넷보급률, ⑥광대역속도, ⑦모바일속도, 쇼단 노출 취약점목록, ⑨CSIRT가 있다. 대부분 높은 역량으로 평가되었는데, 쇼단 노출 취약점목록 지표에서 유독 낮은 점수(27위)로 평가된 것이 방어항목의 CCI 점수가 낮게 평가된 원인으로 보인다. 해당 지표는 일종의 검색엔진으로 인터넷에 연결되어 있는 기기의 포트나 취약점 정보를 검색할 수 있는 쇼단[3]에 등록된 취약점 개수로 IoT 기기의 취약성을 의미하며, 우리나라는 미국과 러시아에 이어 세 번째로 많은 취약점이 노출된 것으로 나타났다.

따라서 국내 사이버 방어역량 향상을 위해 IoT 보안 정책의 실효성 향상이 필요하며, 이에 IoT 보안 수준 향상을 위한 국내 연구는 Table 9와 같다.

Table 9. Considerations for improving defense CCI score

indicators	related study
Vulnerabi-lities listed in Shodan	Deriving the security requirements by analyzing the attack path and possibility according to the characteristics of the IoT environment[19] The need to establish a lagal and insitutional basis for post-security management after product launch[20,21]

Table 9의 연구사례는 IoT 기기가 생활에 밀접하게 연결되어 있고, 제품이 다양하며, 저전력으로 동작하는 특성이 있어 기존 보안체계를 그대로 적용하는 데 한계가 있음을 공통으로 지적한다. 또한, IoT 환경 특성별 가

3) 쇼단은 일종의 검색 엔진으로 인터넷에 연결되어 있는 기기(IoT 기기)의 포트나 취약점 정보를 검색할 수 있는 서비스를 제공하며, 다음 링크(https://www.shodan.io/)를 통해 접속 가능하다.

능한 공격 경로를 분석함으로써 보안 요구사항을 도출하는 기술적 조치와[19] 개발된 패치를 이미 판매된 제품에 배포·적용할 수 있는 제도적 조치[20,21]가 함께 논의될 때, IoT 보안이 달성됨을 보여준다. 따라서 향후 IoT 보안정책의 실효성을 향상하기 위해서는 관련 기술과 표준의 개발도 중요하지만, 이를 적용할 수 있는 법제도적 장치가 함께 고려되어야 할 것이다.

4.2 (Ⅲ사분면) 중장기적 관점에서의 정책 의제 형성이 필요한 항목

4.2.1 공격

국가 차원의 사이버 공격 역량 개발에 관한 논의는 자칫 사이버 무기에 대한 글로벌 경쟁 체제의 심화 및 위협의 에스컬레이션 문제를 초래할 수 있기에 그간 공개적으로 논의되어오지는 않았다. 그러나 최근 미국과 영국 등 주요 국가들을 중심으로 억지력을 확보하기 위해 사이버 공격에 대한 역공격이 가능함을 공개적으로 표명하는 사례가 증가하고 있으며, 대표적인 사례로 미국의 전진 방어(Defending forward)[4] 전략, 영국의 국가사이버부대(National Cyber Force, NCF)[5] 설립 공식화 등이 있다.

한편, 공격 역량을 평가하는 지표로는 ①국가지원 사이버공격, ②사이버군사교리, ③사이버사령부, ④하이테크 수출(4위), ⑤사이버군사인력이 있는데, 이 중 우리나라에서 가장 낮게 평가된 지표는 사이버군사교리(20위)이다. 동 지표는 사이버공간에서의 공격적 또는 방어적 군사 역량에 관한 군사이버전략 개발 여부와 전략의 실효성에 따라 0~4점으로 평가되는데, 우리나라는 관련 전략이 없는 것으로 평가되어 0점을 획득하였다. 동 지표에서 4점으로 평가된 국가로는 미국, 영국, 러시아, 독일, 프랑스가 있다. 이들 국가는 일찍이 사이버공간을 새로운 작전 영역으로 간주하여 사이버공격에 대한 예방과 대응을 강조하면서, 사이버안보 문제에 대해 '군사화'하는 경향을 보이기도 한다[22].

우리나라는 예방과 보호 활동에 초점을 둔 사이버안보 정책을 추진 중이지만, 향후 공세적 대응과 억지력 확보에 관한 정책 의제 발굴을 위해서는 관련 주요국 현황 파악을 선행할 필요가 있다. 이에 특히 우리나라가 낮게 평가된 지표인 사이버군사교리에 대해 높은 점수를 확보한 미국, 영국, 독일, 프랑스의 공격적 사이버 대응을 위한 주요 정책 사례를 Table 10에 정리하였다.

Table 10. List of case of major countries that could be referenced for the discovery of offensive cyber agenda

States	related policy contents
US	**DoD Strategy for Operating in Cyberspace(2011. 7.)**[23]−raising the need for active cyber defense **JP 3−12, Cyberspace Operations(2013. 2.)** [24]−defining Offensive Cyberspace Operations(OCO) as one of the military operation in cyberspace **DoD Cyber Strategy(2015. 4.)**[25]−stating that operational activities are possible to prevent cyber attacks in cooperation with the information community before they occur **DoD Cyber Strategy 2018(2018. 9.)**[26] −allowing preemptive attacks to prevent malicious cyber activities that occur below the level of armed conflict
UK	**National Cyber Security Strategy(2016. 11)**[27]−Explicitly strengthened offensive cyber capabilities to secure deterrence (National Offensive Cyber Programme) **Defence in a Competitive Age(2021. 3.)**[28] official creating of a National Cyber Force(NCF) as a offensive cyber operation unit
Germany	**Cyber security strategy for Germany 2016(2016. 4.)**− defining cyber defense as covering the defensive and offensive capabilities in cyberspace[29]
France	**French military cyber strategy(2019. 1.)**− outlining defensive and offensive cyber warfare[30]

미국은 사이버 위협에 대한 선제적 공격이 가능함을 표명하는 동시에 국제적으로는 사이버안보 규범 논의를 이끄는 사이버안보 전략을 수립하고 있으며[22], 미국 국방부(Department of Defense)는 공격적 사이버 작전 교리와 원칙을 마련하고 이를 표명하는 전략을 꾸준히 발표하고 있다[23~26]. 영국은 2016년 국가사이버안보 전략에 공격적 사이버 역량 강화 목표를 표명[27]한 이후 최근에는 국방 전반에 사이버역량을 통합하고, 사이버공격 기능을 수행하는 부대의 설립을 표명하는데 이르렀다[28]. 독일은 일찍이 공격적인 사이버역량을 보유한 조직을 보유하고 있음을 밝힌 바 있으며[29,31], 프랑스는 2019년부터 사이버 군사 전략에서 방어적/공격적 사이버전을 각각 정의하며 공세적 대응 전략을 추구하기 시작하였다[30].

우리나라는 미국이나 영국 등과 마찬가지로 높은 디지털화 수준으로 인해 많은 사이버 공격에 노출되어 있다. 따라서 예방과 보호 활동을 넘어 억지력을 확보하는 측면에서 선제적 사이버 공격 대응에 관한 기준·절차·군사

4) 2018년 발표한 미국 국방부의 사이버 전략(DoD Cyber Strategy 2018)에 처음으로 명시된 개념으로, 사이버 공격 예방을 위한 선제적 공격을 허용함

5) 공격적 사이버 작전 수행을 위해 영국의 정보통신본부(GCHQ), 국방부, 비밀정보부(Secret Intelligence Service) 및 국방과학기술연구소(Defence Science and Technology Laboratory)의 인력과 예산을 결집하여 설립된 조직

교리의 확립, 정보기관과 국방기관 간 협력적 대응 등 관련 논의가 필요하며, 나아가 향후 공세적 사이버 대응에 관한 국제적 논의가 예상되는 바, 이에 관한 국내 입장과 기준을 사전에 마련할 수 있는 정책적 연구가 필요하다고 판단된다.

4.2.2 감시

끝으로 논의할 사안은 감시에 관한 항목으로, NCPI는 이를 국내 위협 및 행위자에 대한 정보를 탐지하고 수집하는 국가 능력으로 설명한다. 국가적 감시 활동은 시민에 대한 감시, 인터넷 트래픽 추적, 암호화 해제, 해외정보활동·범죄·테러 활동 탐지 및 방해 등 다양한 범위의 목적에 활용될 수 있다. 우리나라의 경우 국내 정보수집에 관한 부정적 인식으로 인해 관련 국가 활동에 관한 법·제도적 논의가 저해되고 있어 의지 점수가 낮게 평가된 것으로 보인다.

감시에 대한 CCI 세부지표를 살펴보면, 우리나라는 인터넷보급률과 소셜미디어 사용인구 비율이 높아 국내 정보 수집에 유리한 환경인데도 불구하고, 국내 위치한 감시 기술 기업이 적고 콘텐츠 규제나 국내 정보수집 활동에 대한 법적 기반 마련 부족으로 최종적으로 비교적 낮은 점수로 평가되었다고 해석된다. Table 11은 법제적 관점에서 국내 정보수집을 다룬 국내 연구사례이다.

Table 11. Considerations for discovering agendas of surveillance

indicators	related study
cybersecurity law(related surveillance)	the need of improvement the legal system to secure transparency and restriction on the scope and authority of information collection[32] the necessity of integrated management system for national security threat information and a system of checks and balances[33] social consensus should be preceded before legislation is enacted ensuring values such as fairness, transparency, and human rights[34] a need to improve the legal system, such as separation of investigative powers, strengthening of budget transparency[35]

최근 코로나-19로 인해 디지털 감시에 대한 이슈가 불거지면서, 감염병 확산 방지라는 사회적 가치와 개인정보보호 및 인권 대립 문제, 감시에 대한 적법성 확보 문제가 다시 한번 제기되기도 하였는데[34], 이전에도 사이버범죄 수사나 테러 방지 활동에서 발생할 수 있는 인권과 안보의 균형 문제, 적법성 확보 문제에 관한 적극적인 연구 활동을 통해 우리나라 실정에 맞는 법·제도적 규율 방안을 마련해야 한다는 필요성은 꾸준히 제기되어 왔다[32,33]. 특히 국내에서는 정보수집에 관한 부정적인 인식이 높아 관련 법제 마련 이전에 사회적 합의가 필요하다는 연구도 찾아볼 수 있었다[34]. 이렇듯 향후 국내 정보수집에 관한 논의를 회피하기보다 오히려 더욱 적극적이고 공개적인 연구를 통해 공감할 수 있는 정책 의제를 도출하고, 이를 규율하는 법제도를 마련해나가는 과정에서 투명성을 보장할 필요가 있다. 결국, 정보수집 범위, 권한 및 감독체계에 대한 법제적 개선에 앞서 국민 정서를 살피고 사회적 합의를 이끌기 위해 중장기적으로 개선방안을 모색해야 할 것이다.

5. 결론

본 연구는 주요 국가 사이버 역량평가 모델과 그 활용방안을 소개하고, 실제 진행되었던 평가결과를 토대로 국내 사이버안보 정책 개선 방향을 도출하였다는 데 의미가 있다. 그간 많은 기관에서 국가 차원의 사이버역량을 평가하고 그 결과를 공개하고 있는데, 이러한 평가결과는 국가별 역량 수준을 점수화·순위화하는 데에만 의미가 있지 않으며, 어떻게 활용하느냐에 따라 국제협력, 정보공유, 정책분석 도구로 활용이 가능하다. 그 이유는 평가모델 자체가 국가 차원의 사이버역량을 구성하는 요인(평가항목)을 식별하고, 역량 강화를 위해 우선시 고려되어야 할 요인(가중치)과 국가별 실태(평가점수 및 모범사례)에 대한 정보를 제공하기 때문이다.

우리나라는 2010년부터 국가 사이버역량 평가모델을 개발[36,37]하고 있으나, 구체적인 평가모델이나 결과를 공개하지는 않기에 그간 국제협력, 정보공유 및 정책분석 도구로의 활용이 제한된 것으로 보인다. 그러나 최근 정책의 효율성과 효과성을 검토하고 이로부터 정책을 개선하는 증거기반의 정책평가에 대한 수요가 증가하고 있음에 따라 국내 정책 개선을 위한 분석도구로 활용할 수 있도록 평가모델과 평가결과를 공개할 필요가 있다.

한편, 동 연구는 NCPI 평가보고서에 제시되지 않은 지표별 우리나라의 상세 점수와 순위를 표로 제시하고, 그 결과를 CII-CCI 매트릭스로 도식화하여 항목별 사분면에 위치시킴으로써 우리나라 관점에서 NCPI 결과를 재해석하고, 나아가 CII와 CCI 점수 모두를 고려하여 국내 사이버안보 정책 의제를 도출하였다는 데 의의가 있다. 그 결과, 공격과 감시 목적의 사이버 기능 활용에 관한 정책의제 형성이 필요하며 의제 형성 시 공격 정책은

억지력 확보 목적의 공격적 사이버 대응에 관한 기준·절차·군사교리와 정보기관과 국방기관 간 협력적 대응방안을, 감시 정책은 국내 정보수집에 관한 부정적 인식을 고려하여 인권과 안보의 균형, 적법성 확보, 투명성 강화방안을 고려해야 함을 제시할 수 있었다. 한편, 인텔리전스와 방어 목적의 사이버역량 강화를 위해서는 관련 정책의 실효성을 높이기 위한 노력이 필요하며, 특히 낮게 평가된 CCI 지표인 인력수급문제와 IoT 보안 문제를 해결하기 위해 교육부터 채용의 전 과정에 일관된 사이버보안 교육체계를 마련하고, IoT 패치 개발과 같은 기술적 측면과 이를 배포할 수 있는 제도적 측면을 동시에 고려하는 IoT 보안체계를 확립할 것을 제안할 수 있었다.

그러나 동 연구는 두 가지 측면에서 한계가 있다. 하나는 CII-CCI 매트릭스의 Ⅲ~Ⅳ사분면에 위치한 4개의 항목에 대한 개선 방안을 도출하는 과정에서, 논문의 전체적인 구성과 지면의 한계로 각 항목에 대한 심층적인 분석으로까지는 이어지지 못했다는 점이다. 본 논문은 국가 사이버역량 평가를 소개하고 이에 대한 정책적 활용을 모색하고, 이를 실제 NCPI 평가에 도입해봄으로써 우리나라는 어떠한 분야에 대한 개선이 필요한 것으로 도출되는지를 거시적으로 제시하는 데 중점을 두었기 때문에 국내 정책 개선에 대해서는 관련 선행 연구로부터 향후 고려할 필요가 있는 주요 의제들을 식별·제시하는 데 그쳤다. 따라서 본 연구에서 도출된 정책 의제 각각에 대한 심층적인 정책 분석과 이로부터 구체적인 정책 대안을 제시하는 연구를 후속연구로 제안한다. 또 다른 한계는 미국의 관점에서 구성된 평가항목과 평가점수를 그대로 활용함에 따라 우리나라에서 바라보는 사이버안보 관점이나 공개되지 않은 자료를 반영하지 못했다는 점이다. 결국, 국내 관점의 사이버안보 정책분석 및 평가를 지속하고 이를 토대로 실제 국내 정책을 개선하기 위해서는 우리나라 관점의 국가 사이버역량 모델을 개발하고 관련 자료를 직접 수집·분석하여 평가결과를 도출할 필요가 있으며, 이 역시 후속 연구과제로 제안한다.

REFERENCES

[1] International Telecommunication Union. (2021). *Global Cybersecurity Index 2020.* Geneva : ITU.

[2] University of Oxford Global Cyber Security Capacity Centre. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition.* Oxford : University of Oxford.

[3] M. Hathaway, C. Demchak, J. Kerben, J. McArdle & F. Spidalieri. (2015) *Cyber Readiness Index 2.0 – A plan for cyber readiness : A baseline and an index*, Arlington Country : Photomac Institute for Policy Studies.

[4] Australian Strategic Policy Institute. (2017). *Cyber maturity in the Asia-Pacific region 2017.* Barton : ASPI

[5] Harvard Kennedy School Belfer Center. (2020). *National Cyber Power Index 2020-Methodology and Analytical Considerations.* Cambridge.

[6] A. Schwerzennach, J. Voo, I. Hemani, S. Jones, W. DeSombre & D. Cassidy. (2020). *Codebook_NCPI_2020.* Cambridge : Harvard Kennedy School Belfer Center for Science and International Affairs.
DOI : 10.7910.DVN.LT55JY

[7] S. E. Min. (2016). Understanding Matrix Analysis As a Qualitative Analysis Methods. *Journal of Qualitative Inquiry, 2(2).* 161-191.

[8] D. Y. Lee & K. H. Kim. (2021). Information Analysis Framework for Supporting Evidence-based Research and Development Policy: Practical Considerations for Rationality in the Policy Process. *Information Policy, 28(1).* 77-93.

[9] J. A. Martilla & J. C. James. (1977) Importance-Performance Analysis. *Journal of Marketing, 31.* 77-79.

[10] C. O. Jones. (1984). *An Introduction to the Study of Public Policy.* Monterey, CA : Brooks/Cole.

[11] K. H. Park. (2021). *Cybersecurity manpower* shortage.. *Need to secure AI convergence security technology.* Information Telecommunication News(Online), https://www.koit/co.kr/news/articleView.html?dxno=83972

[12] S. Hong. (2018). A Study on the Framework of Comparing New Cybersecurity Wrokforce Development Policy Basled on the ATE Programs of U.S.. *Journal of The Korea Institute of Information Security & Cryptology, 28(1).* 249-267.
DOI : 10.13089/JKIISC.2018.28.1.249

[13] S. Hong & J. Kim. (2020). A Study on the Laws and Regulations in Korea through the Analysis of Cybersecurity Workforce Developing Laws and Regulations in U.S.. *Journal of The Korea Institute of Information Security & Cryptology, 30(1),* 123-139.
DOI : 10.13089/JKIISC.2020.30.1.123

[14] J. Ji, S. Park, H. Yu & H. Chang. (2018). A Study on the Design of Re-training Courses for Nurturing Cybersecurity Professionals from Other Occupational Groups. *Convergence security journal, 18(1),* 43-60.

[15] K. H. Lee & H. T. Kim. (2017). Measures for Training Military Information Security Professional Personnel for Cyber Security. *Convergence security journal, 17(2).* 145-151.

DOI : 10.22693/NIAIP.2021.28.1.077

[16] N. S. Chang & S. K. Cho. (2010). Concept of Intelligence and the Role of Intelligence Agency. *National Security and Strategy, 10(4).* 33-76.

[17] National Institute of Standards and Technology(NIST). (2017). *National Initiative for Cybersecurity Education(NICE) Cybersecurity Workforce Framework*. DOI : 10.6028/NIST.SP.800-181

[18] Executive Office of the President of U.S. (2019). *America's Cybersecurity Workforce* (Executive Order 13870 of May 2, 2019).

[19] Y. H. Jeon. (2017). A Study on the Security Modeling of Internet of Things(IoT). *Journal of Korean Institute of Information Technology*, 15(2). 7-27. DOI : 10.14801/jkiit.2017.15.12.17

[20] D. Lee & N. Park. (2017). Proposal of Technology and Policy Post-Security Management Framework for Secure IoT Environment. *The Journal of Korean Institute of Information Technology, 15(4).* 127-138. DOI : 10.14801/JKIIT.2017.15.4.127

[21] D. Lee & N. Park. (2017). Institutional Improvements for Security of IoT Devices. *Journal of the Korea Institute of Information Security & Cryptology, 27(3),* 607-615. DOI : 10.13089/JKIISC.2017.27.3.607

[22] S. B. Kim. (2017). Cybersecurity Strategies of Major Powers in World Politics: From the Comparative Perspective of National Strategies. *Journal of International Area Studes, 26(3),* 67-108.

[23] Department of Defense(DoD). (2011). *Department of Defense Strategy for Operating in Cyberspace*. https://csrc.nist.gov/CSRC/media/Projects/ISPAB.documents/COC-Strategy-for-Operating-in-Cyberspace.pdf.

[24] Joint Chiefs of Staff. (2013). *JP 3-12 Cyberspace Operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

[25] The department of defense(DoD). (2015). *DoD Cyber Strategy*. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

[26] The department of defense(DoD). (2018). *Department of defense cyber strategy 2018*, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FIANL.PDF

[27] Cabinet office. (2016). *National cyber security strategy 2016 to 2021*, https://www.gov/uk/goverment/publications/national-cyber-security-strategy-2016-to-2021

[28] Ministry of Defence. (2021). *Defence in a Competitive age*. https://www.gov/uk/government/publications/defence-in-a-competitive-age

[29] Net Politics & Digital and Cyberspace Policy Program. (2018). *Germany develops offensive cyber capabilities without a coherent strategy of what to do with them.* Councile Foreign Relations(CFR, Online), https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them

[30] A. Laudrain. (2019). *France's new offensive cyber doctrine*. LAWFARE(Online), https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

[31] Atlantic Council. (2012). *Germany reveals offensive cyberwarfare capability*. https://www.atlanticcouncil/orgblogs/natosource/germany-reveals-offensive-cyberwarfare-capability/

[32] H. Kim & M. Kim. (2017). The Act on Anti-Terrorism in the Age of Big Data and Mass Surveillance. J*ournal of Cybercommunication Academic Society, 34(3).* 41-89.

[33] S. G. Hwang. (2019). A Proposal for Reform and Problems of Cybersecurity-related Legal System. *Journal of Law & Economic Regulation, 12(1).* 44-61. DOI : 10.22732/CeLPU.2019.12.144

[34] J. Lee. (2020). Digital Surveillance 2020. *2020 KISA REPORT, 12.* 1-15.

[35] H. D. Kwon. (2020). Protection the rights of the people against the secret service activities -Focusing on German Legislation-. *Chung-Ang Journal of Legal Studies, 44(1).* 5-37.

[36] J. M. Kang, H. U. Hwang, J. M. Lee, Y. T. Yun, B. C. Bae & S. Y. Jung. (2012). A Study on National Cyber Capability Assessment Methodology. *Journal of the Korea Institute of Information Security and Cryptology, 22(5),* 1039-1055.

[37] S. Bae, S. Park & S. J. Kim. (2015). A study on the development for the national cybersecurity capability assessment criteria. *Journal of the Korea Institute of Information Security & Cryptology, 25(5)*, 1293-1314.

송 민 경(Minkyoung Song) [정회원]

비공개

- 2017년 8월 : 과학기술연합대학원대학교 과학기술경영정책(이학석사)
- 2017년 12월 ~ 현재 : 국가보안기술연구소 연구원
- 관심분야 : 사이버안보정책, 정책분석/평가
- E-Mail : mksong@nsr.re.kr

배 선 하(Sunha Bae) [정회원]

비공개

· 2009년 1월 : 한국과학기술원 전기 및 전자공학과(공학석사)
· 2009년 ~ 2012년 : LIG 넥스원 연구원
· 2013년 ~ 2014년 : 두산중공업 기술연구원 연구원
· 2015년 2월 ~ 현재 : 국가보안기술연구소 선임기술원
· 관심분야 : 사이버안보전략/정책, 주요기반시설보호정책
· E-Mail : sunhabae@nar.re.kr

김 소 정(So-Jeong Kim) [정회원]

비공개

· 2001년 2월 : 경희대학교 평화복지대학원 동북아학과(정치학석사)
· 2005년 2월 : 고려대학교 정보보호대학원 정보보호정책학과(공학박사)
· 2001년 ~ 2002년 : 한국전파진흥협회 ITU-WRC 담당 연구원
· 2004년 5월 ~ 현재 : 국가보안기술연구소 정책연구실장
· 관심분야 : 사이버안보전략/정책, 국제안보정책
· E-Mail : sjkim@nsr.re.kr