2024.09.13.

국회미래연구원 | 국회미래의제 | 24-03호

사이버안보 개념의 확장과 주요국의 사이버안보 전략 변화 : 한국 사이버안보에의 함의와 의회에의 제언

차정미, 유지연

국회미래연구원
NATIONAL ASSEMBLY FUTURES INSTITUTE

국회 미래의제

사이버안보 개념의 확장과 주요국의 사이버안보 전략 변화 : 한국 사이버안보에의 함의와 의회에의 제언

차정미 국제전략연구센터장
유지연 상명대학교 교수

요약

'사이버 안보가 곧 국가안보(cybersecurity is national security)'라는 인식과 강조는 기술의 발전과 사이버 공간 위협의 치명성, 전면성으로 인한 글로벌 추세이다. 사이버 안보는 경제적 안보, 환경 안보, 군사안보, 사회안전, 물리적 안전, 정체성 안보, 감정 안보 등 많은 다양한 안보들과 직접 연결되어 있다. 기술의 발전과 디지털 연결성의 지속적 증대는 사이버 공간의 안보가 국가와 개인의 경제, 생활, 나아가 생명까지도 위협할 수 있는 다양한 위험들을 동시에 증대시키고 있다. 한국은 세계에서 사이버 공격을 가장 많이 받는 국가중 하나이다. 사이버안보가 국가안보와 개인안전, 경제사회에 미치는 파괴력이 점점 더 커지는 현실 속에서 한국은 그 어느 때보다 사이버 안보 강화를 위한 역량과 체계를 구축해 가야 한다.

본 연구는 주요국 사이버 안보 전략의 변화와 방향을 살펴보고 한국 사이버안보전략에의 시사점과 국회의 역할을 논한다. 우선 키워드 분석, 키워드 네트워크 분석을 통해 주요국의 사이버안보 개념의 확장과 사이버안보전략 중점 변화를 고찰하였다. 분석 결과 초기 정보 보안과 네트워크 방어에 초점을 맞추었던 사이버안보전략이 공급망과 기술산업 역량강화, 사이버안보 생태계 구축, 전사회적 접근, 글로벌 협력 등으로 확장되고 있음을 볼 수 있다. 또한 진화하는 기술과 변화하는 위협 환경에 대응하기 위해, 법적 강제와 민관협력 생태계 구축 등 실행력을 높이는 방향으로 나아가고 있다.

세계 주요국들은 또한 사이버 안보법 제정 등 실행력 강화를 위한 제도들을 구축하고 있다. 대만 등은 사이버 안보법 제정 6년만인 올해 다양한 변화들을 반영한 수정안을 통과시키면서 사이버 안보법 2.0시대에 있다. 미국 의회의 경우 117대 회기 첫 해인 2021년에 제기된 사이버 안보 관련 법안이 총 150여개에 달했다. 또한 정보위 뿐만 아니라 상하원 국방위, 국토안보위, 상업과학교통위 등 다양한 상임위에 사이버 안보관련 소위를 두고 복합적 측면에서 사이버 안보를 다루고 있다.

한국의 사이버안보 전략은 사이버 방어와 공세적 사이버 등 전략의 범위가 확대되고 있으나, 법률 집행(law enforcement)과 민관협력의 생태계 구축 등 제도화된 실행력 강화가 보완되어야 한다. 진화하는 사이버 위협에 대응하기 위해 법적 제도적 기반을 강화하고, 민간기업, 학계, 시민사회, 개인을 포괄하는 전사회적 접근이 중요해 지는 현실 속에서 한국 사이버 안보의 실행력 강화를 위해 국회의 정치적 관심과 적극적 역할이 요구된다. 국회는 사이버 안보 관련 입법은 물론 예산 및 감독, 기술과 산업발전을 위한 지원 등 다양한 측면에서 사이버 안보의 중요한 행위자이다. 사이버 안보위협이 날로 진화하는 현실 속에서 사이버안보의 실행력 강화를 위한 제도화, 전사회적 접근이 무엇보다 중요한 시기라는 점에서 입법 등 필요한 조치와 제도화를 위한 국회의 적극적 관심과 논의의 필요성을 제기한다.

I 서 론

오늘날 경제와 사회 전반이 점점 더 디지털화 되어가고 상호연결성이 높아지고 있다. 한편으로 인공지능 등 기술의 급속한 발전은 사이버 공격의 용이성, 빈번성, 치명성을 더욱 높이고 있다. 특히, 생성형 인공지능의 발달은 악의적 활동을 하는 사이버 공격세력의 기술적 역량을 더욱 강화시키면서 방어가 어려워질 것이라는 우려가 부상하고 있다.[1] 사이버 위협의 증대는 단순히 정보통신 인프라 위협을 넘어 직접적인 경제적 손실부터 생명의 위협, 사회안정과 신뢰 위협, 나아가 우크라이나 전쟁에서 보듯 개인의 안전과 국가의 경제, 생존에 직적접 치명적 위협을 초래할 수 있는 요소가 되고 있다. 2024년 6월 런던에서는 의료기관에 대한 해킹으로 수천 건의 수술과 진료가 취소되기도 했고,[2] 인도에서는 은행 서버가 해킹되어 253억이 불법유출 되는 사건도 발생한 바 있다.[3] 2024년 사이버 범죄로 인한 비용이 9조 5000억달러(1경 2천651조원)에 달할 것으로 예측되기도 한다.[4] 이렇듯 초연결 디지털 사회에서 우리가 직면하고 있는 사이버 공격의 위험성은 그 다양성과 치명성을 예측하기 어렵다는 점에서 더 큰 불안을 낳고 있다.

이러한 위협의 진화 속에서 미중 경쟁의 심화라는 지정학적 변화는 사이버안보의 위기를 더욱 제고시키고 있으며, 우크라이나 전쟁은 사이버 공간의 안보가 어떻게 물리적 공간의 안보와 밀접히 연계되는지를 명확히 보여주고 있다. 사이버안보는 국가의 존속과 경제사회 안정, 국민의 안전에 있어 필수적인 요소로 자리 잡고 있다. 미국은 사이버공간 보호를 국가안보의 최우선 분야의 하나로 강조하고 있으며 영국도 사이버안보를 테러, 자연재해, 국제전쟁 위기와 같이 제1의 국가안보위기로 규정하고 있다. 대만은 사이버안보가 곧 국가안보라는 슬로건으로 사이버안보의 중요성을 강조하고 있다.

글로벌한 사이버 위협의 확대 속에서 한국은 사이버 공격이 가장 빈번한 대표적인 사이버 전장 중 하나이다. 마이크로소프트(Microsoft)의 2023 디지털 방어 보고서(Digital Defense Report)에 따르면, 2022년 사이버 공격을 받은 전 세계 120개국 중에서, 한국은 우크라이나, 이스라엘에 이어 세계에서 세 번째로 가장 많은 사이버 공격을 받은 국가로 나타났다.[5] 2022년 2월부터 전쟁 중에 있는 우크라이나를 제외하면 한국은 이스라엘에 이어 가장 많은 사이버공격을 받은 국가이다. 이러한

1) 세계경제포럼(WEF)의 조사결과 향후 2년간 생성인공지능이 공격자들에게 이로울 것이라는 응답(55.9%)이 방어자들에게 이로울 것이라는 응답(8.9%)보다 훨씬 높게 나타났다. World Economic Forum, "Global Cybersecurity Outlook 2024," Insight Report, 2024.01.
2) BBC, "Hospital cyber-attack hampers GP blood services," 2024.06.28.
3) India Today, "Cyber criminals hack into server of Noida bank, steal Rs 16.71 crore," 2024.07.16.
4) Cobalt, "Top Cybersecurity Statistics for 2024," 2023.12.08.
5) Jonathan Greig, "Ukraine, Israel, South Korea top list of most-targeted countries for cyberattacks," *The Record*, 2023.10.07.

환경 속에서 한국 정부도 2024년 사이버 국가안보전략, 국가사이버안보 기본계획을 발표하는 등 대응을 강화하고 있다.

미래 디지털 시대는 사이버안보가 곧 국가안보이고 국민안전이면서 경제안보라고 할 수 있다. 이에 본 연구는 사이버안보가 국가안보와 개인안전, 경제사회에 미치는 파괴력이 점점 더 커지는 현실 속에 주요국 사이버안보 전략의 변화와 방향을 살펴보고 한국 사이버안보전략에의 시사점과 국회의 역할을 논한다. 특히 기술의 발전과 지정학적 환경의 변화 속에서 사이버안보 개념의 확장과 사이버안보 전략의 진화를 키워드 분석, 키워드 네트워크 분석을 통해 고찰하고, 한국 사이버안보 전략과의 비교를 통해 향후 사이버안보전략의 발전방향과 국회의 역할을 제언한다.

본 보고서는 2장에서 2010년대, 2020년대 주요국 사이버안보 전략 키워드 분석과 키워드 네트워크 분석으로 사이버안보 개념의 변화를 분석한다. 이를 통해 사이버안보가 초기 정보보안, 통신네트워크 보안이라는 좁은 개념에서 경제, 사회 등을 포괄하는 방향으로 확장되고 있으며 전략적 방향 또한 회복력, 공급망, 민관협력, 기술과 생태계 등 인프라 보호뿐만 아니라 복합적인 경제, 사회의 역량과 회복력을 강화하는 방향으로 확대되고 있음을 보여준다.

사이버안보 개념의 확장이 기술의 발달과 함께 사회전반의 디지털화와 연계되고, 지정학 변화로 촉진되는 복합안보의 부상 속에서 전개되고 있다는 점에서 3장은 복합안보 시대 사이버안보의 중요성을 강조하고 이를 위한 국가의 역할, 정치와 의회의 역할을 논한다. 캐벌티(Cavelty)와 웽거(Wenger)는 사이버안보 문제를 기술적 문제로 보는 시각에서 안보정치적 과제로 보는 시각의 전환을 강조한다.[6] 그만큼 국민적 인식과 전정부적, 전사회적 협력이 중요하다는 점에서 이를 국가안보 의제화하고 광범위한 이해당사자를 관여시키는 정치가 필요하다는 것이다. 세계의 사이버안보 전략이 경제, 산업, 기술, 사회, 국방 등 복합적이고 체계적인 생태계 구축의 문제로 나아가고 있다는 점에서 한국의 사이버안보 전략 또한 정부 주도의, 기술적 문제를 넘어 포괄적 토대적 생태계 구축의 문제로 인식되고 전정부적 전사회적 대응이 필요하다는 점에서 적극적인 '사이버 안보정치'와 국회의 역할을 제언한다.

6) Myriam Dunn Cavelty, Andreas Wenger (2020), p.17.

Ⅱ 사이버안보 개념의 확장과 주요국의 사이버안보 전략 변화 분석

1. 사이버안보 개념의 확장

사이버안보는 얼마 전까지만 해도 소수의 전문가만이 주로 중요 통신 인프라 보호의 기술적 위험 문제를 중심으로 논의되었던 데 반해, 오늘날 사이버안보는 정부 최고위층이 국가안보 차원에서 다루는 핵심 어젠다로 부상하였다. 사이버안보 위협의 범위도 정치, 사회, 경제 등 많은 영역들이 디지털화되면서 그 영역이 급격히 확대되고 있다.[7] 2022년 미국 국가안보전략서는 사이버 공간을 기술, 무역, 경제와 함께 국제제도의 새로운 규칙이 요구되는 핵심 공간으로 강조한 바 있다.[8] 그만큼 사이버안보의 개념과 접근은 지속 확대되고 있으며, 단순히 정보보안이라는 기술적 개념을 넘어 경제와 산업, 외교 등의 다양한 측면에서 사이버안보 문제가 다뤄지고 있다.

사이버안보는 행위자에 따라 합의된 개념이 부재할 뿐만 아니라 용어의 의미가 시대에 따라 변해왔다. 초기의 사이버안보는 주로 정보시스템과 정보통신망을 보호하여 외부 침입과 침해를 방어하는 데 초점을 맞추었으며, 이는 전통적인 의미의 정보보안과 사이버보안에 해당한다. 이러한 접근은 상대적으로 제한적인 위협 환경에서 효과적이었으나, 기술의 발전과 더불어 사이버 공격의 수단과 방법이 고도화되고 다양한 신기술이 도입됨에 따라 기존의 위협 대응 중심의 접근에 한계가 드러났다. 또한, IoT, 클라우드 컴퓨팅, 가상현실, 디지털 트윈 등 새로운 기술의 확산으로 인해 사이버 공간과 물리적 세계의 경계가 점차 모호해지고 있다. 이에 따라 보호해야 할 대상의 범위가 확장되고, 공격의 영향이 단순한 정보 유출이나 시스템 장애를 넘어서 경제적 타격과 사회적 혼란까지 초래할 수 있다. 이제 디지털 공급망 보안은 사이버안보 뿐만 아니라 경제안보 차원에서도 중요한 요소로 인식되고 있다. 사이버안보의 개념은 인터넷 도입 초기의 정보보안 중심에서 디지털 사회 전반의 안전 유지로 개념이 확장되고 있다.

이러한 국가사이버안보 개념의 확장은 전통적인 안보 이론의 패러다임 변화와 연계되어 있다. 기존의 안보 이론은 국가의 물리적 영토와 군사적 방어에 초점을 맞추었으나, 현대 안보 개념은 경제, 기술, 외교, 환경 등 다양한 영역으로 확장되면서 '복합안보'의 개념이 부상하고 있다. 사이버안보 또한 초기의 기술 중심, 네트워크 보호 중심의 방어 개념에서 출발하여, 시대적 변화와 기술 발전에 따라 보다 포괄적인 사회 안전과 유지를 강조하는 방향으로 진화하고 있다.

---

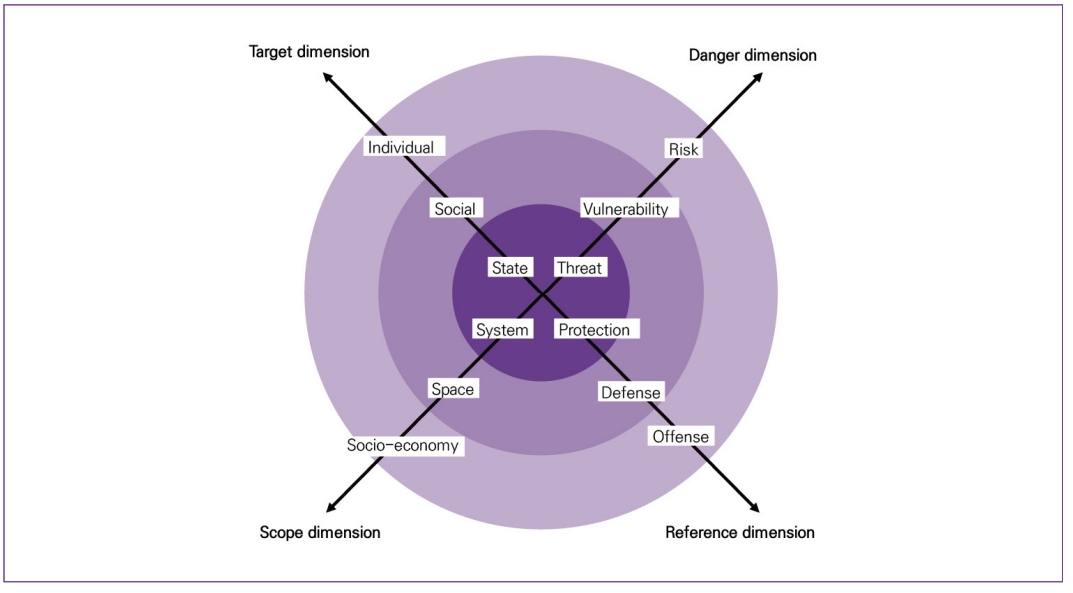
7) Myriam Dunn Cavelty, Andreas Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science," *Contemporary Security Policy*, 41-1 (2020), p. 7.
8) The White House (2022), "National Security Strategy," p.32.

[표 1] 전통적 안보와 기술적 사이버 보안 → 복합안보 패러다임과 포괄적 사이버안보

전통적 안보와 기술적 사이버 보안	복합안보 패러다임과 포괄적 사이버안보
- 군사적 방어와 물리적 영토보호 중점: 군사력과 방어체계 강화 - 정보시스템과 통신망 보호 중점 : 외부침입 차단과 사이버 공간 안정	- 경제, 사회, 정치, 기술, 환경 등 다양한 위협을 통합적으로 관리하고 대응 - 디지털 사회 전반의 안전 유지. 경제적, 사회적 안정 포함하는 포괄적 사이버안보

사이버안보 개념의 확장을 다면적 차원에서 고찰하면 [그림 1]과 같이 사이버안보의 범위가 시스템에서 사회경제로, 전략이 보호에서 공격으로, 보호의 대상이 국가에서 개인으로, 위험이 당면한 위협에서 취약성, 위험으로 확대되고 있음을 볼 수 있다.

[그림 1] 다면적 차원의 사이버안보 개념의 확장



2. 주요국 사이버안보 전략의 확장적 변화

이러한 다면적 차원에서 확장된 사이버안보 개념이 주요국의 사이버안보 전략에 어떻게 반영되었는지 그 실질적 변화 흐름을 살펴보기 위해 주요국에서 발표된 과거 국가사이버안보 전략서와 최근 국가 사이버안보전략서의 키워드 비교분석을 토대로 변화의 내용을 도출하였다. 우선 첫 번째 분석으로 미국, 영국, 일본, EU, 한국의 사이버안보 전략에서 이전과 현재의 키워드를 비교하였다.

분석 결과, 모든 국가가 사이버 위협에 대한 인식과 대응 방식을 더욱 포괄적이고 심화된 방향으로 확장하고 있음을 알 수 있다([표 2] 참조). 두 번째 키워드 네트워크 분석 또한 과거 위협과 정부 중심에서, 전략과 안보, 기업과 기술 등을 포괄하는 방향으로 변화하는 모습을 볼 수 있다.

국가별로 볼 때, 미국의 2018년 사이버안보전략 키워드는 '주정부(state government)', '사이버 활동(cyber activity)', '위험 관리(risk management)'로 내부 관리 및 조직적 대응에 중점을 두었다. 2023년 키워드는 '사이버안보(cybersecurity)', '안보활동(security practice)', '국가 안보(national security)'로 발전하면서, 주정부와 민간 부문이 함께 참여하는 보다 포괄적인 접근법을 채택하고 있다([표 2], [그림 2] 참조). 영국의 2016년 사이버안보 전략 주요 키워드는 '사이버안보(cyber security)', '법률 집행(law enforcement)', '공공 부문(public sector)' 등으로, 주로 국가적 차원의 방어에 초점을 맞추었다. 2021년은 '사이버 전략(cyber strategy)', '사이버 회복력(cyber resilience)', '기업(business organization)'으로 키워드가 이동하고 '사이버 생태계(cyber ecosystem)' '사이버 인력(cyber workforce)' 등 사이버 역량과 기술, 민간생태계가 강조되는 방향으로 변화했음을 보여준다([표 2], [그림 3] 참조).

일본의 2018년 사이버안보전략은 '사이버 공간(cyber space)', '공급망(supply chain)', '사이버 위협(cyber threat)'을 중심으로 인프라 보호와 국가적 대응을 주요 요소로 삼았다. 2022년은 '사회 전체 안보(societal security)', '디지털 전환 보안(dx security)', '협력 프레임워크(cooperation framework)'로 변화하였다.([표 2], [그림 4] 참조). EU의 2013년 사이버안보 전략은 '사이버 범죄(cyber crime)', '법률 집행(law enforcement)', '데이터 보호(data protection)' 등 주로 법적 대응과 규제에 초점을 맞추었던 반면, 2020년은 '디지털 시대의 사이버 전략(cybersecurity for the digital decade)', '법적 강화(legal reinforcement)', '대응 역량(response capability)' 등 보다 포괄적 협력적 대응을 강조하고 있다. 이는 EU가 회원국간 협력과 통합적 규범적 접근을 강조하고 있음을 보여준다([표 2], [그림 5] 참조).

한국의 경우 2019년 사이버안보 전략은 '사이버 위협(cyber threat)', '사이버 방어(cyber defense)', '정보 보안(information security)' 등 주로 군사적 방어와 정보 보호에 중점을 두었다면 2024년은 '공세적 사이버(offensive cyber)' '국제 협력(international cooperation)', '사이버 회복력(cyber resilience)' 등에 초점을 맞추고 있다([표 2], [그림 6] 참조).

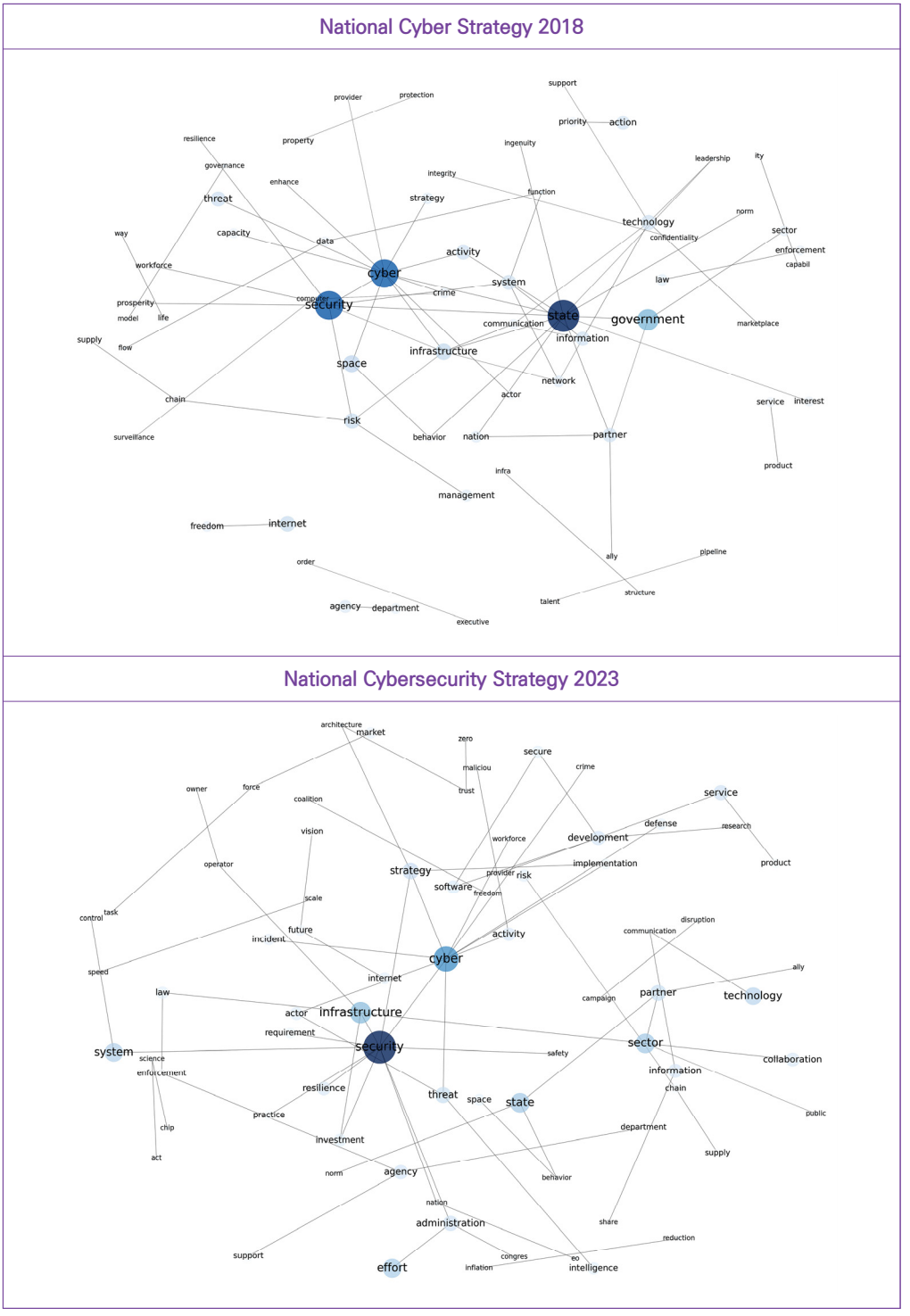
[표 2] 주요국 국가사이버안보전략 핵심 키워드 : 미국, 영국, 일본, EU, 한국 (*빈도수가 많을수록 위쪽에 있음)
(옆의 9쪽에서 계속)

미국		영국		일본	
National Cyber Strategy 2018	National Cybersecurity Strategy 2023	National Cyber Security Strategy 2016	National Cyber Strategy 2021	Cybersecurity Strategy 2018	Cybersecurity Strategy : Cybersecurity for All 2022
state government	cyber security	cyber security	cyber strategy	cyber space	cyber space
cyber security	security resilience	cyber crime	cyber security	cyber security	supply chain
cyber activity	supply chain	cyber threat	law enforcement	supply chain	cyber security
risk management	law enforcement	law enforcement	cyber crime	infrastructure operator	security measure
law enforcement	cyber activity	cyber risk	cyber power	risk management	cyber attack
department agency	security practice	cyber capability	cyber capability	product service	government agency
security risk	security requirement	cyber space	cyber space	cyber crime	dx security
cyber crime	product service	government department	cyber resilience	cyber attack	cyber defense
cyber space	sector partner	cyber attack	cyber risk	security policy	government security
supply chain	infrastructure security	public sector	supply chain	information security	product service
cyber strategy	research development	product service	business organisation	iot system	security policy
priority action	cyber workforce	security sector	information system	information system	economy society
internet freedom	cyber threat	cyber defence	network information	security risk	information sharing
state partner	state behavior	computer network	security resilience	information sharing	security environment
cyber actor	software development	cyber activity	cyber threat	development security	risk management
security workforce	market force	business organisation	cyber force	incident response	information system
cyber threat	secure software	service government	cyber operation	information telecommunication	cyber crime
cyber capacity	cyber incident	internet thing	cyber ecosystem	management level	information security
behavior space	security safety	system data	cyber workforce	research development	chain risk
chain risk	collaboration sector	sector security	cyber attack	security incident	trustworthines supply

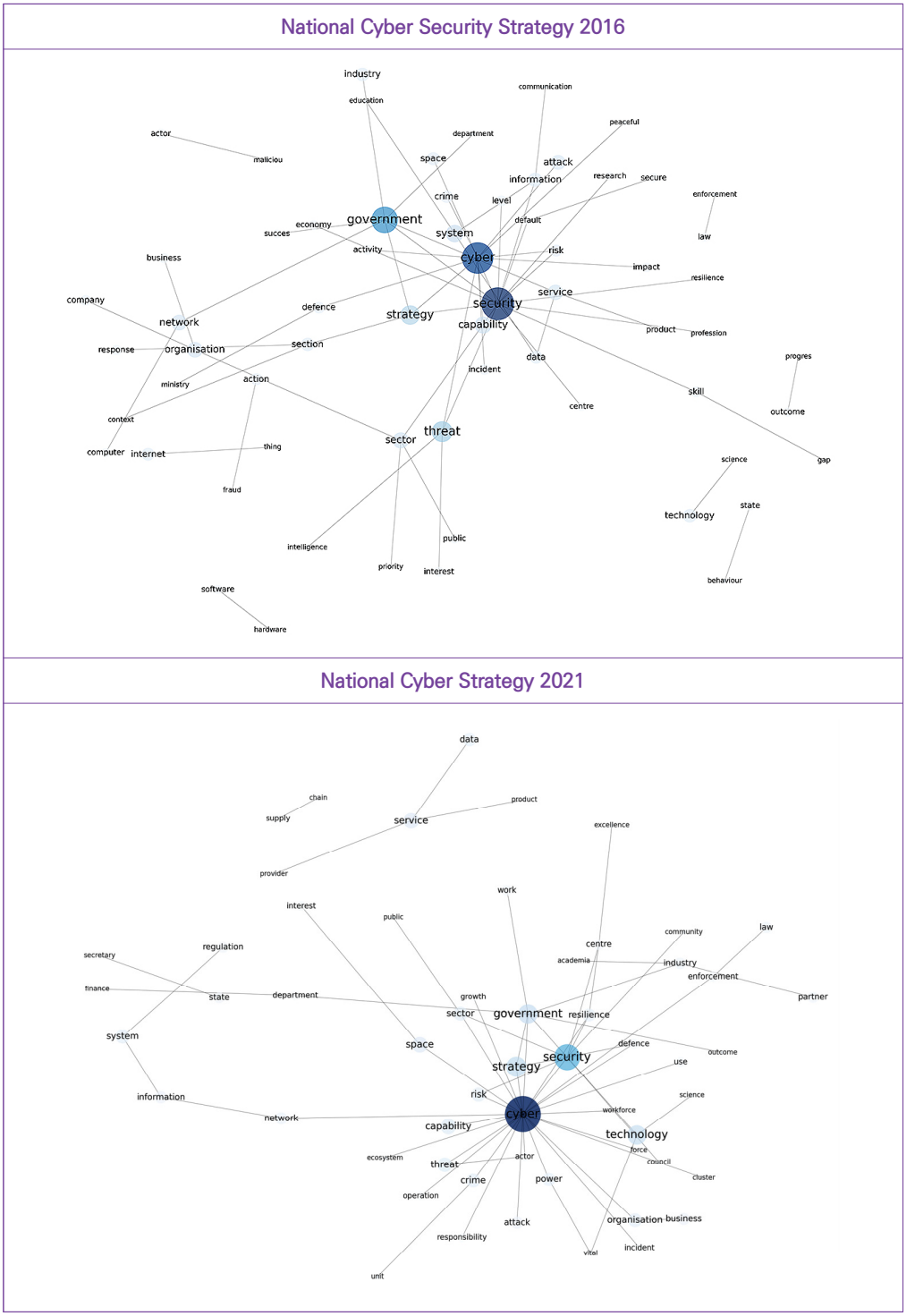
[표 2] 주요국 국가사이버안보전략 핵심 키워드 : 미국, 영국, 일본, EU, 한국 (*빈도수가 많을수록 위쪽에 있음)

EU		한국	
The EU's Cybersecurity strategy 2013	The EU's Cybersecurity strategy for the digital decade 2020	National Cybersecurity Strategy 2019	National Cybersecurity Strategy 2024
cyber crime	cyber security	cyber security	cyber security
law enforcement	cyber crime	cyber threat	national security
cyber space	supply chain	information communication	cyber threat
information system	cyber attack	cyber attack	cyber defense
data protection	law enforcement	cyber crime	security threat
cyber incident	cyber diplomacy	security industry	offensive cyber
information security	action plan	plan implementation	cyber resilience
cyber security	capacity building	cyber space	international community
information infrastructure	cyber unit	response capability	security principle
cyber defence	cyber threat	security threat	cyber cooperation
risk management	cyber defence	threat information	cooperation framework
information sharing	security defence	core infrastructure	response system
defence policy	cyber space	information security	supply chain
cyber resilience	security network	security activity	cyber space
security priority	cyber capacity	threat security	information collection
security standard	information system	trust cooperation	management system
publicprivate partnership	cyber activity	security environment	fundamental rights
product service	security incident	security system	security policy
information society	economy society	security technology	active participation
infrastructure protection	defence policy	devise measure	realm defense

[그림 2] 미국 국가사이버안보전략 키워드 네트워크 분석

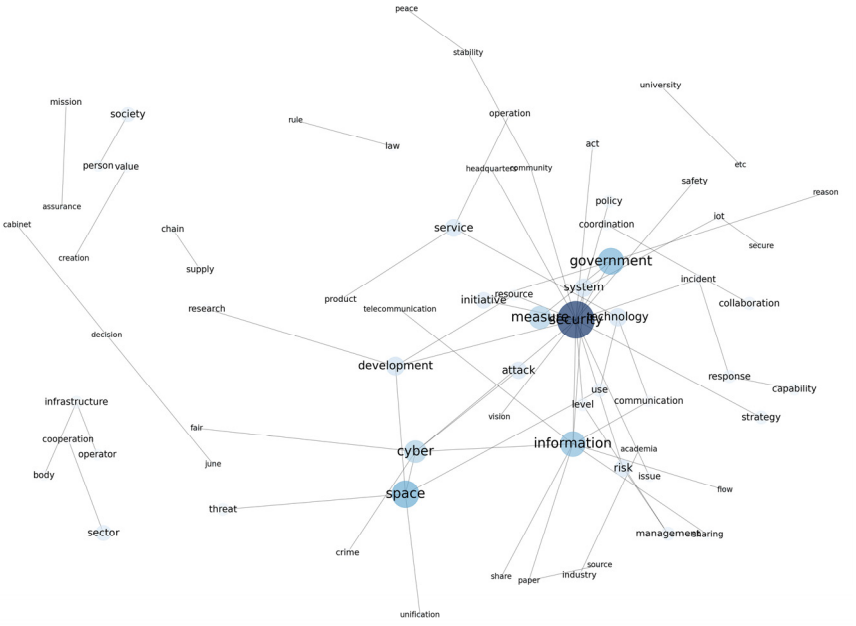


[그림 3] 영국 국가사이버안보전략 키워드 네트워크 분석

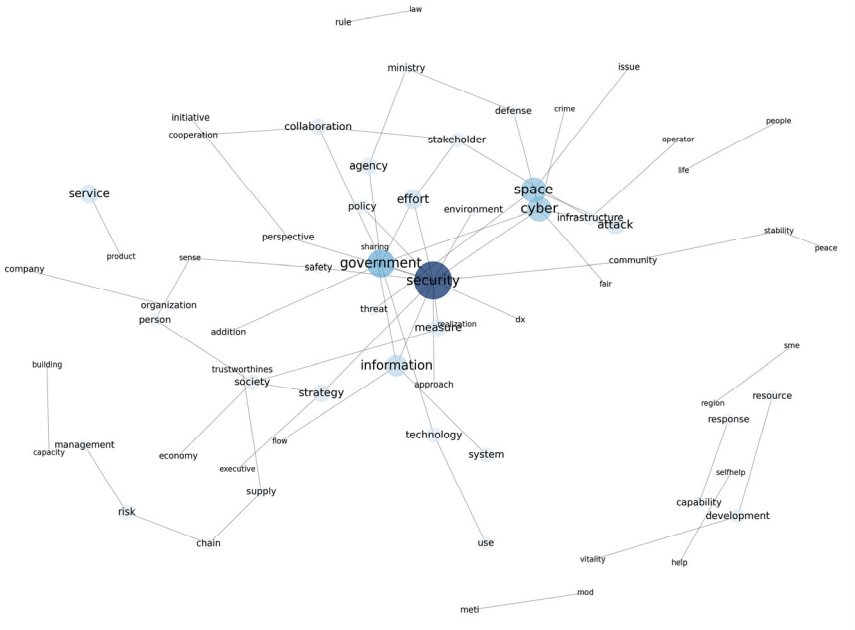


[그림 4] 일본 국가사이버안보전략 키워드 네트워크 분석

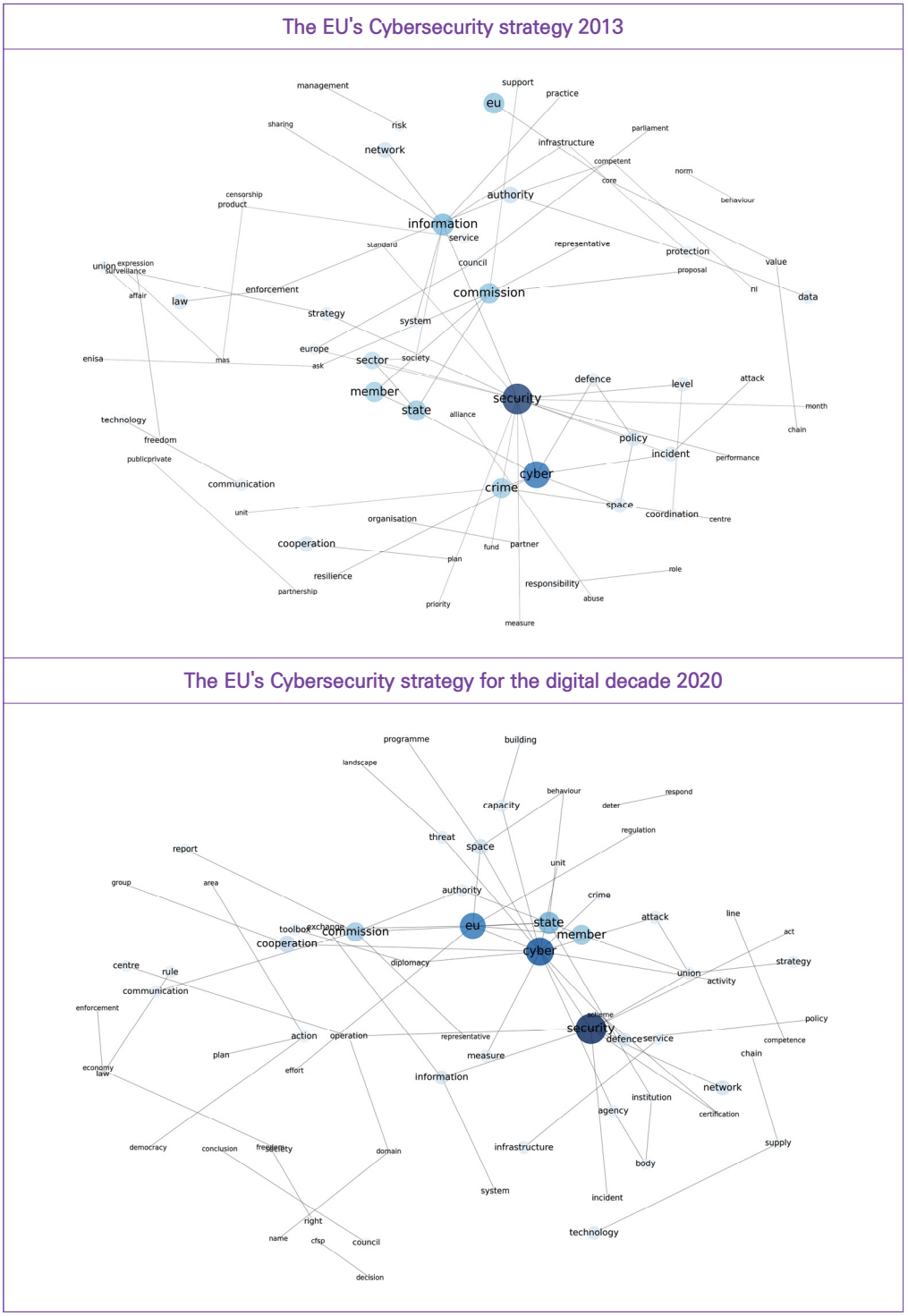
Cybersecurity Strategy 2018



Cybersecurity Strategy : Cybersecurity for All 2022

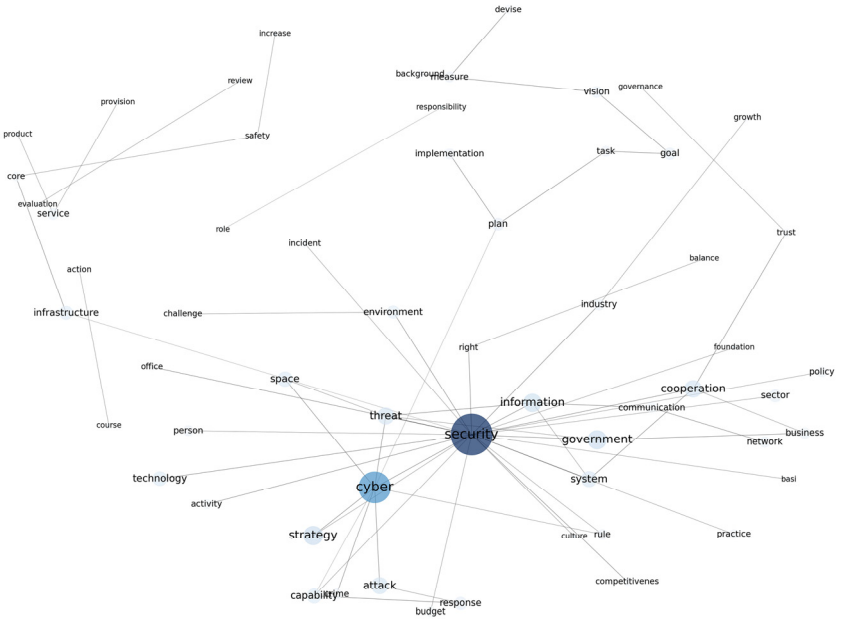


[그림 5] EU 국가사이버안보전략 키워드 네트워크 분석

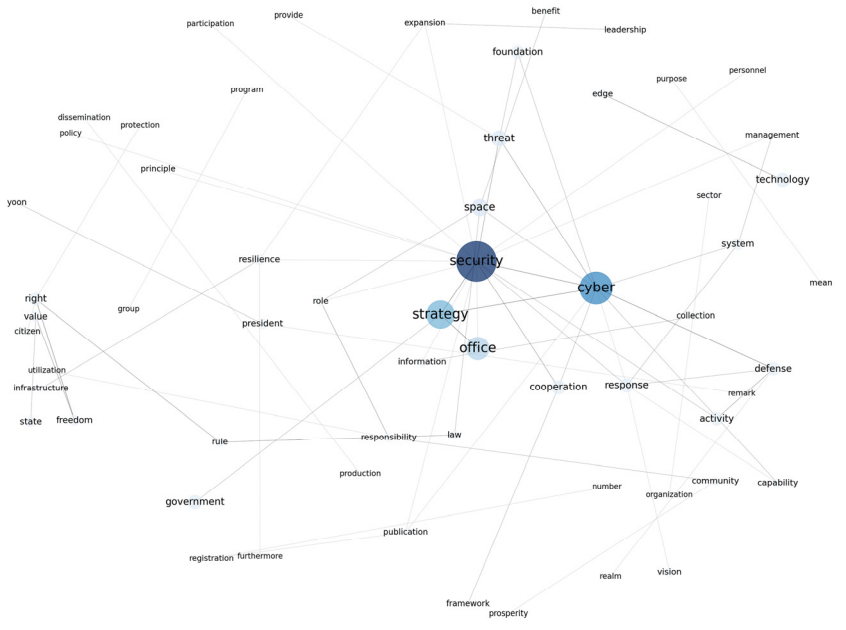


[그림 6] 한국 국가사이버안보전략 키워드 네트워크 분석

National Cybersecurity Strategy 2019



National Cybersecurity Strategy 2024



위의 키워드 네트워크 변화 분석은 사이버 위협 환경의 진화와 밀접히 연계되어 있다고 할 수 있다. 초기 정보보안과 네트워크 방어에 초점을 맞추었던 사이버안보전략이 2010년대에는 사이버 공격 양상과 위협의 다양화로 보다 포괄적인 사이버안보와 사이버 회복력 전략이 강조되고, 디지털화의 가속화, 미중 경쟁 심화와 전쟁, 그리고 사이버 공격의 확대 등 영향 속에서 최근에는 공급망과 역량강화, 생태계, 기업, 경제사회 등 그 포괄성이 더 높아지고 있다. 세계는 진화하는 기술과 변화하는 위협 환경에 대응하기 위해, '경제-기술-외교-사회' 전반의 사이버안보 생태계를 구축하는 방향으로 강화하고 있다.

한국의 사이버안보 전략은 사이버 방어와 공세적 사이버 등 그 범위가 확대되고 있으나, 키워드 분석 결과 실행력과 관련된 내용이 상대적으로 보이지 않는다. 미국은 '법률 집행(law enforcement)', '보안실행(security practice)', 영국은 '법률 집행(law enforcement)', '사이버 생태계(cyber eco-system)', 일본은 '보안 조치(security measure)', '위험 관리(risk management)', EU는 '법률 집행(law enforcement)', '위험 관리(risk management)' 등 실행과 관련한 키워드들이 눈에 띄나, 한국의 사이버안보전략은 공세적, 확장적 개념의 도입에도 불구하고 법 집행 등 실행력 측면의 보완이 중요할 것으로 보인다.

Ⅲ 한국 사이버안보전략과 의회에의 제언

1. 파괴적 기술혁신과 지정학 위기의 시대, '사이버안보 정치(cybersecurity politics)'

초연결의 디지털 시대, 인공지능 등 '파괴적 기술(disruptive technologies)'의 부상, 그리고 지정학적 위기는 사이버 위협의 양상과 영향을 더욱 광범위하게, 복잡하게, 치명적으로 변화시키고 있다. 파괴적 기술을 정의하는 데 중요한 것은 "무엇이 기술을 '파괴적'으로 만드는가, 무엇이 파괴되는가"의 문제이다.[9] 인공지능이 초래할 사이버 공격 발전의 속도를 방어 기술, 그리고 제도가 따라가지 못하면서 디지털 사회, 초연결 사회의 경제, 공동체와 개인의 삶을 더욱 용이하게 심각하게 파괴할 수 있다는 점에서 미래사회 안전의 '불확실성'은 더 높아지고 있다.

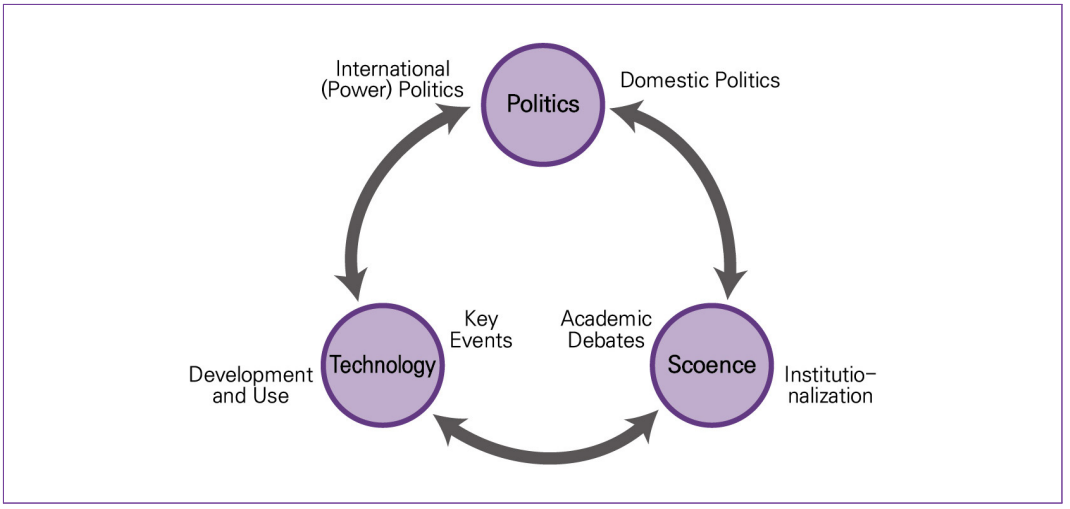
사이버안보 개념의 확장과 전략의 복합성은 효과적인 사이버안보 전략과 정책이 정부, 경제, 사회의 행위자들을 모두 포괄하여야 함을 보여주고 있다. 그러나, 역사적으로 정부, 경제, 사회가 어떻게 상호작용하여 왔는지 국가별로 차이가 존재하고 그러한 다양한 차이는 사이버안보에 있어 정부 역할의 가능성과 제약, 그리고 이들을 둘러싼 정치적 논쟁에 영향을 미치게 된다.[10] 또한 사이버안보를 위한 국가주도의 노력은 이념적 반대입장, 상호불신, 이해관계의 차이 등으로 인해 어려움을 겪으면서 상당수 비정부 단체들뿐만 아니라 기업들이 관여하기도 한다.[11] 사이버안보 위협의 증대와 고도화 속에서 사이버안보의 성공은 국가에 배태되어 있는 '정부-경제-사회'의 관계 속에서, 사이버안보 문제의 중대성을 인지하고 의제화하는 정치적 의지, 그리고 민간기업, 시민사회, 개인 등 다양한 행위자들의 협력을 견인하면서 전사회적 차원의 사이버안보역량을 강화하고, 다면적 사이버안보의 생태계를 구축하기 위한 정치과정이 중요하다.

'사이버안보가 곧 국가안보'라는 인식을 공유하고 필요한 조치들을 단행해 하기 위해서는 이러한 동력과 실행력을 추동해 가는 사이버안보 정치의 필요성이 제기된다. 사이버안보 정치는 사이버안보를 '국가 대전략'의 중요한 일부로 인식하고, 국가가 평시와 전시에 경제, 군사, 외교, 사회, 정보 등 모든 자원을 배치하여 국가, 사회, 경제가 안전하게 유지되도록 노력해야 할 필요성을 상기하는 것이다. 사이버안보 전략과 정책은 국제환경과 국내정치의 상호작용 속에서 정부가 사이버안보 위협을 어떻게 해석하고, 이해하고, 규정하고 정책문제의 우선순위를 결정하느냐 하는 사이버안보정치의 과정

9) Jonathan Lewallen, "Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity," *Regulation & Governance* 15-4 (October 2021), p. 1035
10) Myriam Dunn Cavelty, Florian J. Egloff (2019), "The politics of cybersecurity: Balancing different roles of the state," *Antony's International Review*, 15 (1). p. 52.
11) Myriam Dunn Cavelty, Andreas Wenger (2020), p. 17.

속에서 수립된다. 위협의 규정과 전략의 수립이라는 사이버안보 정치의 구성요소는 아래와 같이 국제정치, 국내정치, 기술발전과 활용, 계기(사건), 학문적 토론, 제도화라는 6가지 요소이다.

[그림 7] 사이버안보 정치(cybersecurity politics)를 추동하는 6가지 요소[12)]



위의 그림과 같이 사이버안보 전략은 "기술-정치-과학(제도)"의 상호작용 속에서 형성되고 이행되는 것이다. 기술의 발전과 활용, 핵심 계기, 그리고 국제관계와 국내정치가 상호작용하는 속에서 어떻게 학문적 지적 토론이 전개되고 제도화의 과정이 나타나느냐가 사이버안보 정치의 형성에 중요한 구조라고 할 수 있다. 우선 기술발전 속도는 과거보다 훨씬 더 광범위하고 빠르게 진행되면서 그 속도는 안보를 책임지는 정부와 조직, 시민사회의 역량을 넘어서고 있다. 사이버안보 전문가들은 생성 AI가 향후 2년간의 사이버안보에 가장 큰 영향을 미칠 것이라고 전망하고 있다.[13)] 기술의 발전과 함께 이벤트(사건)들은 사이버안보 위협 인식과 전략에 중대한 영향을 미친다. 또한 지정학적 환경 변화라는 국제정치 변화와 국내정치, 그리고 사이버안보를 토론하고 연구하는 학계의 논의와 관련 법과 조직들이 생성되는 제도화는 사이버안보 정치의 중요한 요소이다.

한국의 사이버안보 정치는 기술의 발전과 다양한 중요 계기(북한의 사이버 해킹, 딥페이크 문제 등), 그리고 지정학적 위기들이 작동하면서 정부의 사이버안보전략을 강화시키고 있다. 그럼에도 불구하고 제도화를 위한 다양한 융합적 학계의 토론과 논의, 입법과 체계구축 등 제도적 측면의 취약성,

12) Myriam Dunn Cavelty, Andreas Wenger (2020), p. 9.
13) World Economic Forum, "Global Cybersecurity Outlook 2024," Insight Report, 2024.01. p.14.

더욱이 국내정치적 관심과 적극적 역할이 상대적으로 약해 왔다는 점에서 이 6가지 요소의 불균형적 동학이 사이버안보전략의 제도화와 실행력을 강화할 수 있는 사이버안보정치를 작동시키지 못해왔다고 할 수 있다.

캐벌티(Cavelty)와 에글로프(Egloff)는 자유민주주의 국가에서 사이버안보에 대한 국가의 역할은 정치적으로 논쟁적인 주제라고 강조한다. 사이버안보 정책을 둘러싼 정부, 경제, 사회 간의 긴장이 있고 다양한 이해관계자들의 연결이 정부의 역할을 뒷받침하기도 하고 저해하기도 한다는 것이다.[14] 사이버안보의 문제는 국가가 국내 시민사회의 의무를 통제할 수 있는 추가 수단을 부여하게 되기도 한다. 일례로 미국 사이버인프라보호국(Cybersecurity and Infrastructure Security Agency)은 '주요기반시설 사이버사고 보고법(CIRCIA, Cyber Incident Reporting for Critical Infrastructure Act)'을 공표하고 화학, 의료, 식량, 상하수도시스템 등 16개 주요기반시설 부분의 소규모이상 기업들은 사이버 공격을 받은 경우 72시간 내에 보고하도록 규정하고 있다. 이러한 조치 이외에도 사이버 위협에 대한 효과적 대응을 위해 세계는 민관협력의 중요성을 강조하고 제도화된 협력체계를 구축하고 있다. 사이버안보 개념의 확장과 위협의 포괄성은 점점 더 이러한 전사회적 협력의 필요성을 높이고 정부의 안보적 역할공간을 허용하고 있다.

결국 사이버안보의 성공은 시민사회와 민간경제사회분야와의 협력이 관건이라는 점에서 국가안보와 시민의 권리와 자유, 기업의 이익와 자유의 균형을 어떻게 조화하고 '사이버안보 생태계' 구축을 위한 협력의 체계를 구축할 수 있는지가 중요한 과제이다. 또한 사이버안보를 위해 수직적 차원(국가-지역-지방)과 수평적 차원(군-민간, 공공-민간)에서 협력해야 하는 행위자의 이질성은 추가적인 조정 및 협력 문제를 야기한다.[15] 부처간, 민간과 정부간의 벽이 존재하는 환경 속에서, 그리고 정부의 안보적 역할에 대한 시민사회의 신뢰가 필요하다는 점에서, 또한 사이버안보의 실행력 강화를 위한 제도화 과정에서 국내적 조정과 통합이 무엇보다 중요한 시기라는 점에서 입법 등 필요한 조치와 제도화를 위한 적극적 정치가 요구된다.

한국의 사이버안보 전략이 '사이버안보법' 등 제도화를 통해 구체적인 실행력을 갖추기 위해서는 사이버안보정치의 6가지 축 중에서 상대적으로 동력을 갖지 못했던 지적 토론(academic debates)과 제도화(institutionalization), 국내정치(domestic politics)의 작동이 그 어느 때보다 필요한 시점이다. 이에 본 연구는 '사이버안보가 곧 국가안보'라는 슬로건을 넘어 '사이버안보가 곧

14) Myriam Dunn Cavelty, Florian J. Egloff (2019), "The politics of cybersecurity: Balancing different roles of the state," *Antony's International Review*, 15 (1). p. 37.
15) *ibid*

국가안보이고 미래사회와 개인의 안보'라는 점에서 등 사이버안보의 실행력과 사이버 회복력 강화를 위한 생태계 구축에 있어 국회 역할의 중요성과 과제를 제언한다.

2. 국가안보와 국민안전을 위한 사이버안보 '정치'와 의회의 역할

1) '중장기 안보 대전략, 미래 복합안보'의 관점에서 사이버안보의 중대성 인식 필요

'사이버안보가 곧 국가안보(cybersecurity is national security)'라는 인식과 강조는 기술의 발전과 사이버 공간 위협의 치명성, 전면성으로 인한 글로벌 추세이다. 사이버안보는 경제적 안보, 환경 안보, 군사안보, 사회안전, 물리적 안전, 정체성 안보, 감정 안보 등 많은 다양한 안보들[16]과 직접 연결되어 있다. 기술의 발전과 디지털 연결성의 지속적 증대는 사이버 공간의 안보가 국가와 개인의 경제, 생활, 자아와 정서, 나아가 생명까지도 위협할 수 있는 다양한 위험들을 동시에 증대시키고 있다.

디지털 경제, 디지털 사회 전환 속도가 가속화되는 현실 속에서 사이버안보는 국가안보를 넘어 국가발전과도 밀접히 연계되고 있다. 2022년 사이버안보 경제성장 속도는 세계경제성장속도의 2배에 달했고, 2023년은 4배에 달했다.[17] 사이버 공간과 연계된 당면한 위협과 미래의 위험이 증가하고 복잡해지면서, 사이버안보를 강화하기 위해 정부부처간 협력과 통합이라는 '전정부적 접근(a whole of government approach)', 그리고 정부와 민간이 모두 함께 협력해야 한다는 민관협력(PPP, public-private partnership), 전사회적 접근(a whole of society approach)이 강조되고 있다. 또한 세계 국가들은 사이버안보를 위한 법 정비, 거버넌스 구축, 기술과 산업 촉진 지원, 민관협력 강화, 사이버 협력외교 확대 등 다양한 정책적 노력과 제도적 뒷받침을 통해 사이버안보를 강화하고 있다.

사이버안보는 민간분야의 역할과 산업 발전의 중요성이 점점 더 높아지는 추세에 있다. 사이버안보가 곧 국가안보라는 슬로건으로 사이버안보를 강화하고 있는 대만의 경우 국가안보의 핵심으로 사이버안보 문제가 다뤄지면서 공공부문과 민간부문의 사이버안보 산업 역량이 모두 강화되었다고 평가하고 있다. 또한 민관협력이 사이버안보 산업 거버넌스 향상에 기여하고 산업 공급망 안보를 제고하면서 민관협력의 사이버안보생태계가 강화되고 있다. 대만의 경우 시민사회가 허위정보에 대항하는 다양한 팩트체크 비영리 단체들의 활동이 기술적 사회적 역량과 글로벌 네트워크 모두에 적극적으로 역할하고 있다.[18] 한국의 사이버안보 또한 민간기업, 학계, 시민사회, 개인을

16) 안보의 다양한 유형에 대한 내용은 David A. Baldwin (1999), "The Concept of Security," *Review of International Studies* 23, pp.22-23. 참고
17) World Economic Forum, "Global Cybersecurity Outlook 2024," Insight Report, 2024.01. p.9.

포괄하는 전사회적 접근이 중요해지고 이는 사이버안보의 중요성에 대한 국민적 인식의 제고와, 민간기업 시민사회 등 다양한 행위주체들을 포괄하는 민관 협력 거버넌스의 구축을 위한 사이버안보정치의 필요성을 제기한다.

2) 미래 안보의 핵심인 복합적 사이버안보 강화를 위한 '정치' : 국회의 적극적 토론과 역할 필요

주요국 사이버안보 전략 개념의 확장과 진화는 한국 사이버안보 전략에 주요한 시사점을 제시하고 있다. 세계 주요국의회는 사이버안보법 등 다양한 입법과 전문가, 기업 공청회 등을 통해 사이버안보 생태계(cybersecurity ecosystem) 구축과 실행력을 담보할 구체적인 조치들을 추진해 가고 있다. 사이버 위협에 대해 수시로 보고를 받는 것은 물론 사이버안보 강화를 위한 예산과 입법, 정부조직 신설, 나아가 이러한 제도들이 효과적으로 투명하게 시행되고 있는지에 대한 감독에 이르기까지 다양한 역할로 국가의 사이버안보 강화를 뒷받침하고 있다. 미국 연방의회 117대 회기 첫 해(2021년)에 제기된 사이버안보 관련된 법안은 하원 96개, 상원 61개로 총 157개에 달했다.[19] CSIS가 분석한 사이버안보법안 목록에 따르면 아래표와 같이 잠재적인 사이버안보 취약성을 분석하고, 이해관계자에게 보고서와 브리핑을 하도록 하는 등 위험평가 관련된 법안이 102개로 가장 많았고, 사이버안보 역량 강화와 관련된 법안이 76개, 부처간 정보공유 등 정부조직을 업데이트하거나 사이버 관련 기관이나 프로그램을 설립하는 등의 조직관련 법안이 65개, 재정지원과 배분에 관련된 법안이 58개, 사이버안보 인력강화를 위한 법안이 41개에 달했다.

[표 3] 미국 연방의회 117대 회기(2021년도) 사이버안보 관련 법안에 제기된 내용[20]

	위험평가(risk assessment)	역량(capacity building)	조직 (organization)	재정지원 (funding)	인력 (workforce)
하원	61	47	35	34	27
상원	41	29	30	24	14
총합	102	76	65	58	41

반면 한국 국회 21대(2020.6-2024.5)에서 '사이버' 키워드로 검색되는 법안은 4개에 불과하고, 그 또한 임기만료로 폐기되었다.[21] 물론 법안발의 수로 관심과 정책적 비중을 명확히 평가하기는

18) 대만의 사이버안보전략과 사례 논의는 대만방위연구소 우종한(Wu Tsung-Han) 박사의 자문원고 "The Evolution of Cybersecurity Strategy: Taiwanese Case"에 근거하여 서술됨.
19) Georgia Wood, "Cybersecurity Legislation in the 117th Congress," CSIS, 2021.12.
20) 위 CSIS 보고서의 내용을 토대로 저자 작성.
21) 의안정보로 검색된 21대 국회 '사이버' 키워드의 법안은 '사이버안보 기본법안(조태용의원 등), 국가사이버안보법안(김병기의원 등), 사이버보안 기본법안(윤영찬의원 등), 유럽 사이버범죄 방지 협약 가입 촉구 결의안(박주민의원 등) 등 4개임. 해킹 등으로 관련 검색어의 법안도 '지능형 홈네트워크 해킹 방지 및 필수 장비 설치 확인을 위한 전수조사 촉구 결의안(김정

수 있으나 그만큼 국회에서 사이버안보의 중요성에 대한 정책적 관심과 토론이 활성화되지 않았음을 볼 수 있다. 사이버안보가 곧 국가안보라는 세계 주요국들의 담론이 말해주듯 사이버안보는 국가안보는 물론 미래 개인의 생명과 경제, 공동체의 안전을 위한 핵심요소라는 점에서, 그 중요성이 점점 더 높아질 것이라는 점에서, 정치적 관심과 토론, 입법 등 국회의 사이버안보 정치가 요구된다.

3) 사이버안보법은 '사이버안보에 대한 정치적 관심과 토론, 지적 논의, 제도화'라는 사이버안보정치의 출발

앞선 논의에서 한국의 사이버안보 전략은 사이버안보 정치를 구성하는 6가지 요소 중 기술발전과 계기, 국제정치가 이끌어가는 사이버안보 정치는 강하나, 국내정치와 지적논의(academic debates), 제도화의 요소는 상대적으로 취약하다고 한 바 있다. 또한 키워드 네트워크 분석을 통해 세계 주요국들의 사이버안보 전략이 '법률 집행(law enforcement)'과 '보안 조치(security measure)' '사이버 생태계(cyber ecosystem)' 등 구속력과 실행력을 강화하기 위한 제도들을 강조하는 것과 달리 한국은 사이버안보 전략개념의 확장과 공세성에도 불구하고 실행력과 관련된 구체성이 상대적으로 취약함을 보여준 바 있다.

사이버안보의 법적 기본토대가 될 '사이버안보법'은 17대 국회부터 법안 상정과 임기만료폐기의 과정을 반복해 왔다. 반면, 미국, 중국, 일본, 독일, 대만 등 주요국들은 2010년대 사이버안보법을 제정한 바 있고, 최근 기술발전과 사이버안보 위협 진화, 정부조직 개편 등 다양한 필요에 따라 법의 보완과 수정을 토론하고 있다. 사이버안보법 2.0시대를 준비하고 있는 것이다. 대만은 사이버안보법 신설 6년 만에 정부와 민간분야 모두의 수정요구를 반영하여 2024년 7월초 행정원 사이버안보법 수정안이 통과되어 입법원 심사를 진행중이다. 새 법안은 부처간 명확한 업무분장으로 책임을 명확히하고, 규제대상국의 사이버 감사 범위확대 및 관리 강화, 전담사이버안보인력 고용 촉구, 비정부기관의 주요 사이버안보 사고 조사 권한 부여 등을 포함하여 사이버안보 체계와 구속력을 강화하고 있다.

한국 사이버안보법은 국회의 관심과 집중적인 토론없이는 22대 국회에서도 쉽지 않을 수 있다. 사이버안보 정치의 취약성 속에서 기술발전은 전례없이 빠르게 진행되고 있고 사이버 공격 피해의 양상과 규모는 지속 확대되고 있다. 사이버안보의 중대성과 시급성을 고려할 때, 세계 주요국 사례의 분석과 사이버안보 위협평가 등을 토대로 사이버안보법을 집중 토론하고, 정치적 숙의(정치적 의지를 가진 집중적이고 광범위한 깊이있는 논의)의 과정을 거쳐 제정해 가는 노력이 필요하다.

호의원 등)' 등 소수에 불과

4) 디지털 시대 국가안보와 자유의 균형을 위한 국회의 역할[22]

한국 사이버안보법을 둘러싼 논쟁 중 하나는 국가의 감시 통제와 권한 강화의 문제였다. 세계 주요국들의 사이버안보 강화의 방향은 앞서 살펴보았듯 법적 구속력(law enforcement) 강화의 문제와 위협평가, 민관 협력의 생태계 구축이다. 대만은 2017년 사이버안보법을 제정, 정부기관부터 주요기반시설 제공자, 국영기업. 정부지원재단 등 비정부 기관을 포함하여 사이버안보 보호조치와 사고보고절차 등의 근거를 마련했다. 미국도 최근 '주요기반시설 사이버사고 보고법(CIRCIA)'을 통해 중요 인프라 부분의 소규모이상 기업들에게 사이버 사고 보고의무를 부과했다. '자유와 안보'라는 상충되는 원칙의 균형을 어떻게 조절할 것인지, 그리고 그 균형을 맞추는 방법에 대해 어떻게 광범위한 정치적 합의를 도출할 수 있을지에 대한 것은 항상 민주주의에서 존재해왔던 질문이다. 그러나, 디지털 기술의 발전과 사이버 공간 위협의 심화 속에서 '자유와 안보 사이의 균형' 논의는 그 어느 때보다 특별한 시기, 중요한 시기에 있다. 점점 더 상호연결되는 세상에서 사이버 공간의 안전 위협이 글로벌화하고 있으며, 유해한 기술적 접근이 용이해 지면서, 국가와 국민을 보호하기 위한 정부 주도의 개입에 점점 더 의존하게 되고 있다.

인터넷이 개인에 미치는 영향이 커지고, 테러리스트와 범죄자, 그리고 그들을 추적하는 정부당국 모두 기술적으로 점점 더 정교해지고 있다. 인터넷을 이해하고 인터넷을 이용해 위해를 가하려는 주체들을 이해하고, 그들을 식별하고 추적할 수 있는 역량을 갖춘 기관의 필요성, 그리고 체계적 대응을 위한 제도적 거버넌스의 필요성이 그 어느 때보다도 요구되고 있다. 사이버안보 임무와 정보기관을 포함한 담당 부처의 역할에 대한 논쟁은 선과 악이라는 이분법적 논쟁을 넘어서야 한다. '자유, 민주주의, 시민의 힘' 대 '대량의 정보수집 우려와 연결된 감시국가,통제국가' 사이의 이분법적 논쟁을 넘어, 우리 민주주의의 강점과 디지털 시대 정보를 다루는 국가기관과의 상호 작용에 대한 토론이 필요하다.[23]

한편, 사이버안보담당 기관이 개인 정보 보호와 국가 안보 간의 올바른 균형을 정확하게 이행한다고 주장하는 것만으로도 충분하지 않다. 그러한 균형을 확보하고 있는지 지속 확인되어야 하고 이는 강력한 엄격한 제3자 감독을 의미한다. 기관의 전문성에 근거한 임무를 수행하는 것에 대한 인정과 '정보 보안과 국가안보간의 균형'을 확보하기 위한 감독의 제도화를 조화하기 위한 깊이있는,[24] 광범위한 연구와 집중적 토론의 과정을 통해 사이버안보의 실행력과 생태계 구축을 강화할 수 있는 입법들을 제도화하는 국회의 역할이 필요하다. 국가안보와 자유의 올바른 균형을 확보하기 위한

22) 본 4항은 2014년 영국 부총리가 도감청 및 사이버안보 담당 정보기관인 정보통신본부(GCHQ)를 둘러싼 논쟁에 대해 "인터넷 시대 안보와 프라이버시"를 주제로 한 연설을 일부 인용하여 서술함. 디지털 시대 '국가안보와 개인정보보호' 사이의 균형, 정부의 역할을 논하는데 주요한 참고. Deputy Prime Minister, Nick Clegg, "Security and privacy in the internet age," 2014.03.04

23) Deputy Prime Minister, Nick Clegg, "Security and privacy in the internet age," 2014.03.04

24) Deputy Prime Minister, Nick Clegg, "Security and privacy in the internet age,"

정치가 필요하고,[25] 사이버안보법은 이러한 안보와 자유의 균형, 즉 '법에 의한 안보'의 토대가 될 수 있다는 점에서 정치적 숙의가 출발해야 하는 지점이라고 할 수 있다.

5) 사이버안보 개념의 확장과 포괄성에 기반한 다면적, 복합적 접근과 논의 필요

류알랜(Lewallen 2021)은 정부가 신흥기술의 불확실성을 어떻게 해석하고, 이해하고, 규정하고, 정책 우선순위를 결정하느냐에 따라 그 정책결정을 책임질 기관이 결정된다고 강조한 바 있다.[26] 사이버안보 또한 신흥기술의 부상을 어떻게 바라보고 어떻게 규정하며 무엇을 우선순위로 할 것인가에 대한 논의가 전략 방향과 거버넌스 구축의 중요한 요소가 될 수 있다. 디지털 전환이 가속화되는 오늘날 사이버안보 문제는 단순히 정보안보를 넘어 경제, 기술, 사회, 외교 등 다양한 분야의 안정과 발전에 핵심이 되고 있다. 세계는 사이버안보 산업 육성과 기술발전을 통해 글로벌 역량 우위를 추구하면서 한편으로 사이버안보외교를 통해 글로벌 협력네트워크 강화를 추구하고 있다. 특히 우크라이나 전쟁은 스타링크의 역할 등 외국정부는 물론 해외 기술기업들과의 협력의 중요성을 보여주었다. 최근 대만의 디지털장관이 영국을 방문하여 OneWeb 등과 긴급 위성통신 네트워크 구축 협력을 논의한 것은 사이버안보를 위한 기술협력 외교의 사례를 보여주는 것이다.

국회는 사이버안보법 제정은 물론 정부조직 업데이트, 예산 및 감독, 기술과 산업발전을 위한 지원 등 다양한 측면에서 사이버안보의 중요한 행위자이다. 입법을 통한 법적 근거 마련, 청문회와 감사 등을 통해 행정부의 사이버안보정책 수행, 법적 기준을 준수하는 지 등을 감독할 수 있고, 예결산을 통해 정부활동 지원을 강화하거나 통제할 수 있다. 제도적 건설자 역할은 물론 이행과정의 충실성과 적법성을 감독하고. 사이버안보기술 육성 및 산업발전을 촉진하기 위한 제도적, 재정적 뒷받침을 하는 등 다양한 역할을 수행할 수 있다. 또한, 전문가들의 의견과 이해당사자들의 의견청취 등을 통해 다양한 측면을 반영하고 토론하는 '정책 숙의'과정을 주도할 수 있다.

우선 첫째, 사이버안보의 중요성에 대한 초당적 인식과 이에 기반한 사이버안보 의원연구단체 구성 등을 통해 국회차원의 연구와 토론을 활성화하는 것을 검토할 수 있다. 미국은 2016년 상원의원이면서 정보위원회 위원장인 워너(Mark Warner) 의원 등이 주도하여 '사이버안보 코커스(Cybersecurity Caucus)'를 창립했다. 본 코커스는 사이버안보가 단순히 정보보안 차원을 넘어 건강, 경제적 번영, 국가안보, 민주적 제도 등에 영향을 미치는 복합적 이슈라는 점을 인식하고, 상원의회가 사이버안보 정책 이슈를 더 효과적으로 대응하는 것을 돕기 위해 초당적 교육 공간으로 창립되었다. 미국 상원

25) Deputy Prime Minister, Nick Clegg, "Security and privacy in the internet age,"
26) Jonathan Lewallen, "Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity," *Regulation & Governance* 15-4 (October 2021), p. 1035

사이버안보 코커스는 사이버안보분야의 공공 정책대화를 제고하고, 의원들과 보좌진들에게 정보안보 기술 전반에 대한 점증하는 위협에 대해 교육하는 것을 목적으로 하고 있다.[27] 한국 국회도 사이버안보 연구포럼 등 의원연구단체 설립을 통해, 사이버안보법 뿐만 아니라 사이버안보 강화를 위한 상시적 토론과 감독의 역할을 위한 전문가 공청회, 기업인 등 관련 이해당사자가 참여하는 토론회 등 민관협력과 소통의 사이버안보 생태계 구축에 기여할 수 있다.

둘째, 상임위 산하에 '사이버안보 소위' 설치 등으로 사이버안보 관련 입법, 예산, 정부역할과 관련한 회의는 물론 전문가공청회, 정부위협평가 보고 청취 등 필요한 토론을 전개할 수 있다. 미국 등 주요국 의회는 사이버안보 상설 소위원회 등을 통해 국가차원의 사이버안보전략과 정부전략, 정책, 예산, 입법 등에 대한 토론과 리뷰 역할을 수행하고 있다. 미국은 상하원 모두에 국방위 정보위 등 다양한 상임위에서 '사이버안보 소위'를 두고 안보는 물론 기술발전, 산업보호, 인재육성 등 다양한 차원에서 사이버안보를 접근하고 있다. 상원 국방위 사이버안보 소위는 △정보기술 연구개발, 사이버안보 역량 강화 위한 획득, 사이버 관련 훈련 및 장비 프로그램 등 다양한 사이버안보 예산 검토 △국방부 사이버 부대 등 감독의 역할을 하고,[28] 하원 정보위 사이버안보 소위는 정보기관들의 사이버정보활동 관련 입법, 예산, 프로그램 등을 관장하며,[29] 하원 국토안보위 사이버안보 인프라보호 소위는 국가안보와 경제를 뒷받침하는 주요기반시설 담당자, 정부와 비정부책임자간의 협력 향상, 정부네트워크 보호 등에 목적을 두고 사이버안보와 인프라안보국(CISA), 국토안보부의 사이버안보 임무 감독을 수행하고,[30] 하원 감독책임위원회(Committee on Oversight and Accountability)도 사이버안보, 정보기술, 정부혁신 소위를 두고 있다.[31]

[표 4] 미국 상하원 의회 상임위별 사이버안보 관련 소위[32]

상임위 (상·하원)	사이버안보 관련 소위
상원 국방위	subcommittee on Cybersecurity
상원 상업과학교통위	subcommittee on Consumer Protection, Product Safety, and Data Security
하원 국방위	subcommittee on Cyber, Innovative Technologies, and Information Systems
하원 정보위	subcommittee on National Security Agency & Cyber
하원 국토안보위	subcommittee on Cybersecurity and Infrastructure Protection
하원 감독책임위	subcommittee on Cybersecurity, Information Technology, and Government Innovation

27) Mark R. Warner, "Cybersecurity Caucus,"
28) US Senate Committee on Armed Services, Subcommittee on Cybersecurity
29) US House Permanent Select Committee on Intelligence, "National Security Agency & Cyber"
30) US House Homeland Security Committee, "Subcommittee on Cybersecurity and Infrastructure Protection"
31) US House Committee on Oversight and Accountability, "Subcommittee on Cybersecurity, Information Technology, and Government Innovation,"
32) 키워드 검색을 통해 나타난 사이버안보 관련 소위를 취합한 것으로 일부 누락과 오류가 있을 수 있음

한국 국회 또한 사이버안보의 '중대성과 시급성'을 인식하고 이를 둘러싼 복잡성과 다면성 속에서 사이버안보 강화의 제도화를 위한 '집중적 토론과 숙의'의 공간으로 역할할 필요가 있다. 사이버안보 위협의 중대성과 확장성에도 불구하고, 사이버안보문제에 대한 국회차원의 관심과 논의가 취약한 현실 속에서 사이버안보 역량 강화와 민관협력의 사이버안보 생태계 구축, 디지털 시대 미래 안보의 제도적 기반 구축 등의 측면에서 국가안보와 국민안전 모두를 위한 사이버안보의 포괄성을 이해하고, 다면적 역량강화를 위한 제도적 기술적 지원, 법적 제도화를 뒷받침할 정치적 의지와 토론이 필요한 때이다.

참고문헌

Alexander, D. (2013). "Resilience and Cyber Security: Moving Towards a Network Resilient Society." Computers & Security.

Baldwin, David A. (1999). "The Concept of Security," Review of International Studies 23.

Ballin, E.H., & Dijstelbloem, H., & Goede, P. (2020) "The Extension of the Concept of Security." SpringerLink.

Buzan, B., Waever, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.

Cavelty, Myriam Dunn and Andreas Wenger. (2020). "Cyber security meets security politics: Complex technology, fragmented politics, and networked science." Contemporary Security Policy, 41 (1).

Cavelty, Myriam Dunn and Florian J. Egloff. (2019). "The politics of cybersecurity: Balancing different roles of the state," Antony's International Review, 15 (1).

Daase, C. (2013). Von der nationalen zur menschlichen Sicherheit: politische und rechtliche Konsequenzen des erweiterten Sicherheidsbegriff. In A. Fischer- Lescano & P. Mayer (Eds.), (2010) Recht und Politik globaler Sicherheit. Bestandaufnahme und Erklärungsansätze (pp. 11-42). Campus Verlag: Frankfurt/New York.

European Commission. (2009). "Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security, and resilience." https://ec.europa.eu/

European Commission. (2013). "The EU's cybersecurity strategy: An open, safe and secure cyberspace." https://ec.europa.eu/

European Commission. (2020). "The EU's cybersecurity strategy for the digital decade." https://ec.europa.eu/

European Parliament and Council of the European Union. (2018). "General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)." https://eur-lex.europa.eu/

Government of Canada. (2023). "Canadian cybersecurity resilience plan." Public Safety Canada. https://www.publicsafety.gc.ca/

Government of Japan. (2018). "Cybersecurity strategy of Japan. National Center of Incident Readiness and Strategy for Cybersecurity." https://www.nisc.go.jp/

Government of Japan. (2018). "Cybersecurity strategy." https://www.nisc.go.jp/

Government of Japan. (2022). "Cybersecurity strategy: Cybersecurity for all."

https://www.nisc.go.jp/

HM Government. (2016). “National cyber security strategy 2016-2021.” https://www.gov.uk/

HM Government. (2021). “National cyber strategy 2022.” https://www.gov.uk/

HM Government. (2024). “Active cyber defense strategy.” https://www.gov.uk/

Krause, K., & Williams, M. C. (1997). “Broadening the Agenda of Security Studies: Politics and Methods.” Mershon International Studies Review.

Lewallen, Jonathan. (2021). “Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity,” Regulation & Governance 15 (4).

National Cyber Security Centre. (2016). “National cyber security strategy 2016-2021: Making the UK secure and resilient in cyberspace.” https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

National Security Council. (2018). “National cyber strategy of the United States of America.” The White House. https://www.whitehouse.gov/

National Security Council. (2023). “National cybersecurity strategy 2023.” The White House. https://www.whitehouse.gov/

Rid, T. (2013). Cyber War Will Not Take Place. Oxford University Press.

Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton & Company.

Sen, A. (1999). Development as Freedom. New York: Alfred A. Knopf.

The White House. (2008). “The comprehensive national cybersecurity initiative.” https://georgewbush-whitehouse.archives.gov/

United Nations Development Programme (UNDP). (1994). Human Development Report 1994. Oxford University Press. https://hdr.undp.org/en/reports/global/hdr1994

Wu, Tsung-Han. (2024). “The Evolution of Cybersecurity Strategy: Taiwanese Case” 국회미래연구원 자문보고서

대한민국 청와대. (2019). “국가 사이버안보 전략.” https://www.president.go.kr/

대한민국 청와대. (2024). “국가 사이버안보 전략.” https://www.president.go.kr/

BBC, “Hospital cyber-attack hampers GP blood services,” 2024.06.28. https://www.bbc.com/news/articles/clwwyp4330yo

Cobalt, “Top Cybersecurity Statistics for 2024,” 2023.12.08. https://www.cobalt.io/blog/cybersecurity-statistics-2024

Deputy Prime Minister, Nick Clegg, “Security and privacy in the internet age,” 2014.03.04

https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age

Greig, Jonathan. "Ukraine, Israel, South Korea top list of most-targeted countries for cyberattacks," The Record, 2023.10.07.
https://therecord.media/microsoft-2023-report-countries-most-targeted-cyberattacks

India Today, "Cyber criminals hack into server of Noida bank, steal Rs 16.71 crore," 2024.07.16.
https://www.indiatoday.in/technology/news/story/cyber-criminals-hack-into-server-of-noida-bank-steal-rs-671-crore-2567541-2024-07-16

Mark R. Warner 웹페이지. "Cybersecurity Caucus,"
https://www.warner.senate.gov/public/index.cfm/cybersecurity-caucus

The White House. (2022). "National Security Strategy."

US Senate Committee on Armed Services, Subcommittee on Cybersecurity
https://www.armed-services.senate.gov/subcommittees

US House Permanent Select Committee on Intelligence, "National Security Agency & Cyber"
https://intelligence.house.gov/subcommittees/national-security-agency-and-cyber-subcommittee.htm

US House Homeland Security Committee, "Subcommittee on Cybersecurity and Infrastructure Protection"
https://homeland.house.gov/cybersecurity-infrastructure-protection-and-innovation/

US House Committee on Oversight and Accountability, "Subcommittee on Cybersecurity, Information Technology, and Government Innovation,"
https://oversight.house.gov/subcommittee/cybersecurity-information-technology-government-innovation

World Economic Forum. "Global Cybersecurity Outlook 2024," Insight Report, 2024.01.
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf?_gl=1*1kh3xcz*_up*MQ..&gclid=EAIaIQobChMI37fQwo6tiAMVC2sPAh1qfzWFEAAYASAAEgK95fD_BwE

Wood, Georgia. "Cybersecurity Legislation in the 117th Congress."" CSIS, 2021.12.
https://www.csis.org/blogs/strategic-technologies-blog/cybersecurity-legislation-117th-congress

사이버안보 개념의 확장과 주요국의 사이버안보 전략 변화 : 한국 사이버안보에의 함의와 의회에의 제언

인 쇄 2024년 9월 13일
발 행 2024년 9월 13일
발 행 처 국회미래연구원
주 소 서울시 영등포구 의사당대로 1
전 화 02)786-2190
팩 스 02)786-3977
홈페이지 www.nafi.re.kr
인 쇄 처 ㈜명진씨앤피(02-2164-3000)

ISSN 2983-4392

국민을 지키는 미래로 나아가는 국회

ISSN 2983-4392

이 자료는 국회미래연구원 홈페이지(www.nafi.re.kr) 및
열린국회정보(open.assembly.go.kr)에서 확인하실 수 있습니다.

국회미래연구원
NATIONAL ASSEMBLY FUTURES INSTITUTE