사이버 억지의 새로운 개념화: '한미 사이버 안보 동맹론'의 성찰적 맥락에서

김상배 | 서울대학교 정치외교학부 교수

| 목차

| 주제어 사이버 안보, 동맹, 억지, 창발, 피드백, 한국, 미국; Cybersecurity, Alliance, Deterrence, Emergence, Feedback, South Korea, United States

이 글은 '한미 사이버 안보 동맹론'이 딛고 선 개념적 기반과 담론적 프레임을 성찰하는 차원에서 '사이버 억지'의 개념을 새롭게 세우는 시도를 벌였다. 최근 제기되고 있는 한미 사이버 안보 동맹론은 전통적인 억지 개념을 사이버 안보 분야에 적용하려는 발상을 바탕에 깔고 있다. 그러나 사이버 공간의 고유한 성격이나 진화하는 미국의 억지 전략, 한미관계 전반의 미래 등을 고려할 때 이러한 시도는 한계를 안고 있다. 향후 한미 사이버 안보협력이 원용할 사이버 억지의 개념은, 전통억지 개념을 적용하려는 단순계적 발상을 넘어서, 사이버 공간의 복잡계적 특성을 고려한 유연하고도 통합적인 시각을 원용해야 한다. 이러한 문제의식을 바탕으로 이 글은 기존의 미국 정책서클과 국제정치학계에서 수행된 개념적 응용의 작업을 바탕으로 하여 사이버 억지의 새로운 개념화를 시도하였다. 이러한 과정에서 이 글은 복잡계 이론에서 말하는 '창발과 피드백'의 입체적이고 동태적인 구도에서 사이버 억지의 개념을 볼 것을 제안하였으며, 기존의 사이버 억지 개념들을 아우르는 일종의 '메타 프레임'으로서 '창발에 대한 축적적 억지(cumulative deterrence against emergence)'의 개념을 제시하고, 이를 한미 사이버 안보협력의 향후 과제를 가늠하는 작업에 적용하였다.

국제정치논총 제63집 2호 (2023), 51-88.
https://doi.org/10.14731/kjir.2023.06.63.2.51

Ⅰ. 머리말

최근 양적·질적으로 진화하는 사이버 위협에 적극적으로 대응하는 다양한 방안들이 국내외적으로 모색되고 있다. 그중에서 크게 주목받는 것 중의 하나가 '한미 사이버 안보 동맹론'이다. 70년의 역사를 가진 한미동맹을 강화하는 차원에서 한미 상호방위조약의 관련 조항을 개정하여 현실 공간의 동맹 구도를 사이버 공간으로 확장하고 이를 바탕으로 북한의 사이버 위협에 대처하는 굳센 태세를 보여주자는 담론이다.[1] 여기에 일종의 '사이버 부국강병론'을 지향하는 기술·공학적 시각이 가세하여, 국내 사이버 역량을 강화하는 차원에서 더 많은 자원과 인력을 확보하고 이를 정책적으로 전폭 지원하는 도약의 계기를 한미 사이버 안보 동맹 체결을 통해서 찾자는 담론이 제기되고 있다.[2] 이 글은 국제정치학의 시각에서 한미 사이버 안보 동맹의 담론이 딛고 서 있는 개념적 기반은 무엇이고 과연 그것은 적절한지, 그리고 향후 한미 양국이 사이버 안보협력을 지속적으로 추진해 나간다면 한국은 어떠한 개념적 자원을 개발할 필요가 있는지 등의 문제를 살펴보고자 한다.

한미 사이버 안보 동맹론의 기저에는 '억지(deterrence)'[3] 개념, 그중에서도 특히

1 이러한 담론은 2023년 4월 26일 미국 워싱턴 DC에서 열린 한미 정상회담에서 양국 정상이 발표한 공동성명에서 극명하게 드러났다. 양국 정상은 한미동맹을 사이버 공간에까지 확장하기로 선언했으며, "전략적 사이버 안보 협력 프레임워크"라는 별도의 문서를 채택하고 향후 과제로 한미 상호방위조약을 사이버 안보에 적용할 논의를 시작한다는 문구를 담았다. 대통령실 뉴스룸, "한미 정상, 전략적 사이버 안보 협력 문서 채택." 『보도자료』 (2023년 4월 27일), https://www.president.go.kr/newsroom/press/TFsqADSy (검색일: 2023년 5월 6일).

2 임종인, "한·미 사이버동맹 걸맞은 사이버 역량 갖춰야." 『중앙일보』 (2023년 5월 1일), https://www.joongang.co.kr/article/25159152 (검색일: 2023년 5월 6일); 박춘식, "한미동맹을 사이버 안보까지 확장한 워싱턴 선언 '환영'." 『전자신문』, (2023년 5월 3일), https://www.etnews.com/20230503000172 (검색일: 2023년 5월 6일).

3 16세기 후반에 출현한 영어의 'deterrence'는 "공포로 단념시켜 중지시킨다(discourage and stop by fear)"라는 뜻의 라틴어 '*deterrere*'에 기원을 둔다. 'deterrence'의 번역어로 국내에서는 '억지(抑止)'와 함께 '억제(抑制)'가 사용되는데, 이 글에서는 라틴어 어원의 뜻을 살려 '억지'로 번역하였다. 다만 이미 고유명사가 된 '확장억제전략협의체(EDSCG)'에서는 '억제'를 사용하였다.

'확장억지(extended deterrence)'의 개념이 자리 잡고 있다. 대북 억지의 차원에서 미국의 재래식 능력과 핵 능력을 빌려 쓰듯이 사이버 능력을 빌려 쓰자는 논리이다. 이렇게 사이버를 확장억지에 포함하자는 논의는 2022년 5월 한미 정상회담에서 언급되었고, 그해 9월 개최된 한미 '확장억제전략협의체(EDSCG)' 회의에서 미국의 핵우산을 활용하는 대북 확장억지 방식과 더불어 논의되었으며, 그 이후 여러 공식 채널을 통해서 발전하고 있다. 이러한 '사이버 확장억지론'은 한미 양국이 사이버 안보 협력의 강화 필요성에 대한 인식을 공유한다는 점에서는 고무적이다. 그러나 한국 측에서 의도하고 있는 사이버 억지의 부과가 실제 효과를 보기 위해서는 현재 딛고 서 있는 개념적 논의보다는 좀 더 새롭고 정교한 프레임이 필요하다. 특히 사이버 분야의 고유한 성격이나 진화하는 미국의 억지 전략, 한미관계 전반의 미래 등을 고려할 때, 그것이 얼마나 타당한 문제 제기이고, 더 중요하게는 사이버 분야에서 얼마나 효과가 있을지에 대해서는 면밀한 검토가 필요하다.

오랫동안 진행해온 억지 개념에 대한 학계의 논의[4] 에 비추어 볼 때, 현재의 한미 사이버 안보 동맹론은 전통적인 '보복(punishment)에 의한 억지' 개념에 기반을 두고 있다. 이러한 전통억지 개념에 기반을 둔 이른바 '원점타격론'이나 '전쟁엄포론', '사이버 킬체인' 등의 주장은 결연한 의지의 표명이라는 상징적 효과는 있을 수 있겠지만, 사이버 안보 분야의 성격상 실제로 그 효과를 얼마나 거둘 수 있을 것이냐에 대해서는 의문이 제기된다. 보복억지 개념에 기대었던 초기 사이버 논의에 비해서, 최근 학계의 연구 경향은 오히려 사이버 억지의 '적용무용론'으로 기울어 왔다. 이러한 과정에서

4 사이버 억지 논쟁의 기본구도에 대한 소개로는 Erica Lonergan and Mark Montgomery, "What is the Future of Cyber Deterrence?" *SAIS Review of International Affairs* 41-2 (2021), pp. 61-73, DOI: https://doi.org/10.1353/sais.2021.0018; Aaron F. Brantly, "Entanglement in Cyberspace: Minding the Deterrence Gap." *Democracy and Security* 16-3 (2020). pp. 210-233, DOI: 10.1080/17419166.2020.1773807을 참조; 국내 연구로는 민병원, "사이버공격과 사이버억지의 국제정치: 규제와 새로운 패러다임을 중심으로." 『국가전략』 제21권 3호 (2015). pp. 37-62를 참조

‘거부(denial)에 의한 억지’ 개념이 주목받기도 했다. 특히 사이버 공간의 고유한 특성을 바탕으로 하는 디지털 인프라 및 역량의 비대칭성, 책임 귀속(attribution)의 복잡성, 공격 주체와 보복 대상의 다양성 등의 문제로 인해서, 공격자에 비용을 부과하는 것이 복잡할 뿐만 아니라 공격 자체를 원천적으로 거부하는 것이 제약되기 때문에, 전통억지 모델을 사이버 분야에 적용하기 힘들다는 것이었다.[5)]

이 글은 사이버 억지 개념의 논의가 기존의 ‘적용-무용의 이분법’ 구도에서 벗어나야 한다고 주장한다.[6)] 사이버 안보 분야에 억지 개념의 적용이 어려운 것은 맞지만, 그렇다고 사이버 억지 전략 자체가 무용한 것은 아니다. 오히려 필요한 것은 여러 유형의 사이버 억지 전략이 작동하는 방식과 조건 및 효과를 구체적으로 탐구하는 작업이다. 이러한 이분법적 발상이 지배했던 것은, 적의 공격을 원천 봉쇄해야 한다는 ‘절대적 억지’에 대한 미국 정책서클의 고전지정학적 강박감이 작용했기 때문일 수도 있다. 그러나 핵 공격과는 달리 사이버 공격의 경우에는 그것이 일정한 수위 이하에서 지속적으로 감행되는 것으로 전제하고, 그 공격의 빈도와 정도를 어떻게 제한하느냐를 고민하는 ‘상대적 억지’의 개념으로 다루어야 한다. 특히 억지 개념을 사이버 분야에 적용하는 것이 가능한지를 묻는 ‘단순계적 발상’을 넘어서, 사이버 공간의 특성을 고려한 유연하고도 통합적인 ‘복잡계적 시각’의 도입이 필요하다. 이러한 맥락에서 이 글은 사이버 안보의 ‘복합지정학(Complex Geopolitics)’에 대

5 사이버 억지의 ‘적용무용론’으로는 Michael P. Fischerkeller and Richard J. Harknett, “Deterrence is not a Credible Strategy for Cyberspace.” *Orbis* 61-3 (2017), pp. 381–393; Amir Lupovici, “The ‘Attribution Problem’ and the Social Construction of ‘Violence’: Taking Cyber Deterrence Literature a Step forward.” *International Studies Perspectives* 17-3 (2016), pp. 322–342; Eugenio Lilli, “Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence,” *Contemporary Security Policy* 42-2 (2021), pp. 163-188, DOI: 10.1080/13523260.2021.1882812을 참조.

6 사이버 억지론의 이분법 구도를 넘어서자는 유사한 문제제기로는 Uri Tor, “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence.” *Journal of Strategic Studies* 40-1/2 (2017), pp. 92–117, DOI: 10.1080/01402390.2015.1115975을 참조.

한 시각을 원용하여 실용적인 억지 전략의 마련을 뒷받침하는 사이버 억지의 새로운 개념화를 시도하고자 한다.[7)]

이전에도 사이버 억지의 개념을 변화하는 환경에 맞추어 응용하려는 시도는 다양한 경로를 통해서 진행되었다.[8)] 특히 미국의 억지 전략과 관련하여 진화해 온 개념들이 눈에 띈다. 예를 들어, 2018년 미 국방부의 사이버 전략은 '선제적 방어(defend forward)' 개념을 통해서 사이버 작전의 전략 비전을 정교화하는 시도를 펼쳤다.[9)] 2020년 3월에 발간된 '사이버 공간 솔라리움 위원회'의 보고서는 신흥기술로서 사이버 분야의 특성을 담아내기 위해서 전통적인 억지 개념으로부터의 탈피를 주장하며 '층위적 사이버 억지(layered cyber deterrence)'의 전략을 제안하였다.[10)] 2022년 미 국방부의 국방전략에서 제시한 '통합억지(integrated deterrence)'의 개념도 변화하는 미국 정책서클의 억지 개념을 잘 반영하는데, 여기서 제시된 '회복(resilience)에 의한 억지' 개념에 주목할 필요가 있다.[11)] 이러한 미국 정책담당자들의 문제의식은 2023년 3월에 발표된 미 백악관의 사이버 안보 전략에까지 이어진다.[12)]

학계에서도 이러한 개념응용의 문제의식을 바탕으로 전통적인 보복억지와 거부억지 개념의 이분법적 구도를 넘어서려는 시도들이 있었다. 종합적인 시각에서 사이버 억지의 개념을 정리한 조지프 나이(Joseph Nye)의 작업에서부터 여러 학자의 연구가 축적됐다.[13)] 이를 통해서 '연루(entanglement)에 의한 억지,' '규범과 금기(norms

7 '사이버 안보의 복합지정학'에 대해서는 김상배, 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 (파주: 한울, 2018) 특히 제2장을 참조.

8 이러한 개념적 응용에 대한 학계의 논의는 Lucas Kello, *The Virtual Weapon and International Order.* (New Haven: Yale University Press, 2017); Erik Gartzke and Jon R. Lindsay (eds.) *Cross-domain Deterrence: Strategy in an Era of Complexity.* (New York, NY: Oxford University Press, 2019)를 참조

9 U.S. Department of Defense, "2018 Department of Defense Cyber Strategies." (2018).

10 Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report* (2020).

11 U.S. Department of Defense, *National Defense Strategy of the United States* (October, 2022).

12 White House, *National Cybersecurity Strategy* (March 1, 2023).

and taboos)에 의한 억지,' '포괄적(comprehensive) 억지,' '축적적(cumulative) 억지,' '층위적(layered) 억지,' '횡영역적(cross-domain) 억지,' '집단(collective) 억지' 등의 개념이 사이버 안보 분야에서 다양하게 제시되었다. 이러한 작업의 연장선에서 보면, 현재 필요한 것은 이들 개념 중에서 단순히 어느 하나를 고르거나 이들을 대체하는 개념을 하나 더 추가하려는 시도보다는, 이들 개념을 아우르는 '메타 프레임(meta-frame)'을 개발하는 차원에서 새로운 개념화를 시도하는 데 있다.

이러한 문제의식을 바탕으로 이 글은 일종의 메타 프레임을 개발하는 차원에서 '창발에 대한 축적적 억지(cumulative deterrence against emergence)'의 개념을 제시하고, 이를 통해서 현재 거론되는 '한미 사이버 안보 동맹론'을 성찰하고 향후 방향을 짚어 보았다. 새로운 사이버 억지의 개념을 적용해서 보면, 향후 한미 사이버 안보협력은 현재 제기된 동맹담론의 수준을 넘어서 그 방향을 새롭게 설정할 필요가 있다. 특히 '창발에 대한 축적적 억지'의 시각에서 보면, 한미 사이버 안보협력은 저층위-중층위-고층위의 각 층위에 적합한 방안을 모색하는 차원에서 연루·규범억지를 통한 '행태형성,' 거부억지를 통한 '이익거부,' 보복억지를 통한 '비용부과' 등을 복합적으로 활용하는 유연한 전략을 펼쳐야 한다. 결국 사이버 안보위협의 창발에 대응하는 억지의 핵심은 여러 층위에 걸쳐서 입체적이고도 동태적인 피드백의

13 Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace." *International Security* 41-3 (2016), pp. 44-71, doi:10.1162/ISEC_a_00266; Jacquelyn G. Schneider. "Deterrence in and Through Cyberspace." in Erik Gartzke and Jon R. Lindsay (eds.) *Cross-Domain Deterrence: Strategy in an Era of Complexity* New York, NY: Oxford University Press, 2019, pp. 95-120; Jon Lindsay et al, "Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity," *Journal of Cybersecurity* 1-1 (2015), pp. 53-67,. DOI: 10.4324/9781315225623-2; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24-2 (2015), pp. 316-348; Erica D. Borghard and Shawn W. Lonergan. "Deterrence by Denial in Cyberspace." *Journal of Strategic Studies* (2021), DOI: 10.1080/01402390.2021.1944856; Mark Montgomery and Erica Borghard, "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence." *Joint Force Quarterly* 102 (2021), pp. 79-89.

메커니즘을 동원하는 데 있다.

이 글은 세 부분으로 구성되었다. 제2장은 억지의 개념에 비추어 한미 사이버 안보 동맹의 담론을 검토하였다. 특히 확장억지론과 통합억지론으로 대변되는 한미 담론의 차이를 지적함으로써 이 글이 모색한 개념화 작업의 필요성을 제기하였다. 제3장은 한미 사이버 안보 동맹론이 딛고 선 개념적 기반과 담론적 프레임을 체계적으로 성찰하는 차원에서, 기존 학계에서 연구된 다양한 사이버 억지의 개념을 소개하고 이들을 보는 분석틀을 마련하였다. 제4장은 복잡계 이론에서 말하는 '창발과 피드백'의 동태적 구도에서 사이버 억지의 개념을 새롭게 개념화하고, 이를 한미 사이버 안보협력의 사례에 적용하여 향후 과제를 가늠하는 토대로 삼았다. 끝으로, 맺음말에서는 이 글의 주장을 종합·요약하고 향후 한미 사이버 안보협력의 추진을 위해서 필요한 여타 과제를 간략히 짚어보았다.

Ⅱ. 억지 개념으로 보는 사이버 안보 동맹론

1. 한국의 '사이버 확장억지론'

기존의 한미 사이버 안보협력은 주로 정책논의를 중심으로 진행되었는데, 그 과정에서 한미 사이버 안보 동맹론은 한미 정상회담의 전개 과정을 통해서 제기되었다. 박근혜 정부 당시 한미 정상은 2013년과 2014년 두 차례의 정상회담에서 사이버 안보협력을 주요 어젠다로 상정했다. 구체적 논의를 발전시킨 것은 2015년 10월 워싱턴에서 열린 한미 정상회담인데, 사이버 안보 분야를 포함하여 양국의 포괄적 동맹관계를 공고하게 다지는 행보를 보였다. 문재인 정부 당시인 2021년 5월 한미 정상회담에서는 사이버·우주 등의 영역에서 협력을 심화하기로 했고, 이후 양국 간에 한미 랜섬웨어 워킹그룹을 구성하고 2021년 9월 첫 회의를 개최했다. 윤석열 정부 들어 2022년 5월 열린 한미 정상회담에서는 사이버 공간에서 적대세력 억지, 기반

시설 보호, 범죄 대응, 자금세탁과 가상화폐 등 여러 이슈의 공조가 포함되었다.[14)]

이밖에도 한미 사이버 안보협력은 다양한 협력지침과 양해각서, 워킹그룹 및 협의체, 정책포럼 등을 통해서 진행되었다. 한미 국방협력지침(2011)에서 사이버 공격 예방을 위한 상호 협력을 명시했으며, 한미 국방부 간 IA/CND(Information Assurance and Computer Network Defense) 양해각서 체결(2009), 한미 사이버사령부 간 양해각서 체결(2022) 등을 통해 협력의 기반을 마련했다. 한편, 한미 사이버워킹그룹(2021~), 한미 국방사이버정책실무협의회(2014~), 한미 사이버정책협의회(2012~) 등 사이버 안보 분야의 별도 협의체를 운영하고, 동시에 한미 안보협의회의(Security Consultative Meeting, SCM, 2012~), 한미 ICT정책포럼(2013~), 한미 정보통신기술(ICT)협력위원회(2021~), 북한 사이버 위협 대응 한미 실무그룹(2022~), 한미 국가안보위원회(NSC) 간 소통 채널 마련(2022) 등 여러 수준의 한미 협의체에서 사이버 안보 이슈를 논의해 왔다.

이러한 기류는 최근 확장억지의 맥락에서 제기된 사이버 억지론을 통해서 좀 더 구체화되는 양상이다. 2022년 5월 한미 정상은 재래식 능력뿐만 아니라 핵과 미사일 방어 능력을 포함하여 가용한 모든 범주의 방어역량을 사용하여 미국이 한국에 대한 확장억지를 제공한다고 확인하였다. 양 정상은 연합방위 태세 제고를 통해 억지를 더 강화할 것을 약속하고, 필요시 미군의 전략자산을 시의적절하고 조율된 방식으로 전개하여 대북 억지력 강화를 위한 조치를 모색하기로 확인하였다. 이러한 맥락에서 한미는 국가 배후의 사이버 공격을 포함한 다양한 사이버 위협에 대응하기 위한 협력을 대폭 확대해 나가기로 했다. 아울러 양 정상은 가장 이른 시일 내에 고위급의 '확장억제전략협의체(Extended Deterrence Strategy and Consultation Group, EDSCG)'를 재가동하기로 합의하였다.

14 김소정, "2022 한미정상회담과 사이버 안보: 억지력 강화를 위한 전략적 과제." 『국가안보전략연구원 Issue Brief』 제361호 (2022-05-31).

이에 의거하여 2022년 9월 열린 제3차 한미 '확장억제전략협의체' 회의에서는 미국의 핵우산을 활용하는 기존의 대북 확장억지 방식 외에도 사이버 안보를 포함하는 진전된 억지 방안이 논의됐다. 이 회의에서는 사이버, 우주, 전자기 등 진전된 비핵 능력을 통해 대북 억지를 강화하겠다는 사안이 새롭게 언급됐다. 공동선언문에서 양측은 동맹의 미사일 대응 역량과 태세는 물론 확대된 다영역 연습 참여 등 사이버·우주 영역에서의 지속적인 협력을 강화하고, 관련 공조를 증진해 나가기로 했다고 밝혔다. 한편, 2022년 11월 제54차 한미안보협의회의(SCM) 공동성명에서는 강력한 대북 억지 메시지의 반영 및 미국의 확장억지 공약의 범위 확대를 제시하면서, 한미 공약의 범위를 기존의 핵·재래식·미사일 방어로부터 더욱 진전시켜 사이버·우주·전자기 등과 같은 비핵 능력으로 확장할 것임을 밝혔다.

이러한 전개 과정에서 한국은 핵 억지 개념을 사이버 분야에 적용하자는 태도를 보였다. 대북 억지의 차원에서 '핵우산'처럼 '사이버 우산'도 빌려 쓰자는 기대 하에 사이버 안보 분야 한미동맹을 강화하자는 것이다. 이렇게 사이버 안보 분야에 핵 억지의 개념을 적용하려는 시도는 국내적으로는 최근 '한국형 3축 체계', 즉 킬체인 선제타격, 한국형 미사일방어체계, 대량응징 보복 등에 대한 논의의 연장선에서 제기된 확장억지론에 입각해 있다. 이렇게 확장억지라는 프레임에서 사이버 안보를 보는 경향은 2023년 1월 국방부 업무보고에서도 드러났다.[15] 확장억지는 일반적으로 미국이 한국에게 제공하는 것을 의미하는데, 거기에 사이버를 집어넣겠다고 말하는 것은 양방향적 발상이라기보다는, 미국이 더 높은 사이버 역량을 바탕으로 한국에게 무언가 제공해주기를 원하는 정책적 기대가 반영된 것이라고 할 수 있다. 이러한 흐름은 2023년 4월 미국 워싱턴 DC에서 열린 한미 정상회담에도 반영되어, 한미 양

15 국방부, "힘에 의한 평화 구현." 『2023년 주요 업무 추진계획』 (2023-01-11). https://www.korea.kr/docViewer/skin/doc.html?fn=3b343d5508949dce5cab8b86724ff5af&rs=/docViewer/result/2023.01/11/3b343d5508949dce5cab8b86724ff5af (검색일: 2023년 1월 28일)

국은 동맹을 사이버 공간에까지 확장하기로 선언했으며, 향후 한미 상호방위조약을 사이버 안보에 적용할 논의를 시작하기로 했다.

이상에서 살펴본 '사이버 확장억지론'은, 사이버 안보의 성격이나 미국이 제시하는 통합억지의 개념과의 정합성 등을 염두에 두고 그 타당성과 효과성이 검토되어야 한다. 게다가 북한의 경우처럼 디지털 인프라가 제대로 구축되지 않은 상대에 대한 사이버 보복 공격의 실효성이 매우 낮은 상황에서 억지력 자체를 기대하기도 쉽지 않다. 만약에 물리적 전쟁으로의 확전을 감행할 생각이 있는 것이 아니라면, 북한은 사이버 공간에서 잃을 것이 그리 많지 않다는 것이 문제이다. 게다가 한국처럼 방어하는 쪽의 취약성이 비대칭적으로 높다면, 상대방에게 보복의지를 강하게 전달하기도 쉽지 않다. 따라서 단순히 '확장'하는 차원을 넘어서 여타 억지 수단과 적극 '연계'하는 접근이 병행되어야 한다.

한편, 일각에서 한미동맹의 사이버 억지 전략은 '지정학적 문턱 너머로 심각한 사이버 공격을 받는 상황'에만 초점을 맞춰야 한다는 주장이 제기되고 있는데,[16] 사이버 안보 분야의 특성상 딱히 그러한 상황을 특정하기도 쉽지 않다. 이러한 주장은 신흥안보(emerging security)의 성격을 갖고 창발하는 사이버 안보의 특성을 오해하고 사이버 억지를 단순한 전통 억지의 프레임에서 이해한 발상이라고 할 수 있다. 사이버 안보 분야의 특성상, 억지 개념이 효과적으로 작동하기 위해서는 그러한 지정학적 임계점을 넘어서 공격이 가해지기 전에 미리 대응하는 것이 오히려 더 중요할 수도 있다. 이 글이 한국이 제시하는 사이버 억지가 실효성을 보기 위해서는 좀 더 정교하고 새로운 프레임이 필요하다고 주장하는 이유이다.

16 James E. Platte, "Toward a Joint US-ROK Cyber Deterrence Strategy." *38 North Commentary* (2021) https://www.38north.org/2021/11/toward-a-joint-us-rok-cyber-deterrence-strategy/ (검색일: 2023년 1월 17일).

2. 미국 주도 사이버 안보 동맹과 통합억지론

한미 사이버 안보 동맹론은 최근 동맹국과의 연대를 강화하는 미국의 행보와 연관 지어 그 의미를 생각해 봐야 한다.[17] 미국은 유럽 및 인도·태평양 지역의 동맹국들과 높은 수준의 사이버 안보협력을 진행하고 있다. 2014년 러시아의 크림반도 병합 이후 나토(NATO)는 '웨일스 정상 선언(Wales Summit Declaration)'을 발표했는데, 사이버 공격에 대해서도 나토 조약 제5조의 집단안보 조항을 적용한다는 내용이었다. 이어서 2016년 6월 나토 회원국 국방장관들은 '사이버방어공약(Cyber Defence Pledge)' 채택을 통해서 동맹 차원에서 사이버 공격에 공동 대응하겠다는 의지를 다졌다. 또한 미국은 '쿼드 사이버 안보 파트너십(Quad Cybersecurity Partnership)'에서 제시된 의제를 통해서 회원국들과 함께 사이버 안보 분야의 취약성과 사이버 위협으로부터의 회복력을 강화하는 방안을 모색했다. 2021년 10월 미국은 유럽 및 아시아 30여 개국 장관들과 '국제 랜섬웨어 대응 이니셔티브(CRI, International Counter Ransomware Initiative)'를 발족시켜 각국의 핵심 인프라, 에너지 및 보건기관 등을 노린 랜섬웨어 공격을 규탄했다.

미국의 사이버 안보 동맹 행보를 보여주는 대표적인 사례는 미일 동맹이다. 미일은 2013년 '사이버방호정책워킹그룹'을 창설한 뒤 지속적으로 사이버 안보협력에 대한 논의를 진행했다. 2015년 미일 정상회담에서 합의한 '방위협력지침(U.S.-Japan Defense Guidelines)' 개정안에서는 사이버 안보협력을 포함시켰는데, 미국은 일본이 군사시설과 국가 기반시설에 대한 사이버 공격에 대응하도록 지원하기로 약속했다. 이러한 전개는 미국과의 협력을 통해 일본이 자체적으로 사이버 안보 분야의 역량

17 Sung Chul Jung, Jaehyon Lee, and Ji-Yong Lee, "The Indo-Pacific Strategy and U.S. Alliance Network Expandability: Asian Middle Powers' Positions on Sino-US Geostrategic Competition in Indo-Pacific Region." *Journal of Contemporary China* 30-127, (2021), pp. 53-68, DOI: 10.1080/10670564.2020.1766909

을 강화할 뿐만 아니라, 일본이 미국의 사이버 방위능력에 기대어 자국의 사이버 안보를 보장받는다는 점에서 미국의 '사이버 우산'에 일본이 편입됐다고 평가받기도 했다. 이는 2019년 '미일안보조약' 제5조 집단자위권에 사이버 공격이 포함되는 행보로 이어졌는데, 이는 미일 양국이 집단자위권을 사이버 공격에도 적용한다고 확인한 것을 의미한다. 2023년 1월 발표한 미일 공동성명에도 미일 양국은 합동태세를 강화하여 억지력을 확장할 것이라고 밝히면서 사이버 영역을 강조했으며, 같은 달에 열린 '미일 2+2회의'에서는 미일 안보조약의 적용 대상을 우주로 확장하는 방안에도 합의하였다.

미국은 여타 인도·태평양 지역 국가들과도 사이버 안보협력을 강화하고 있다. 2011년 미국·호주 양국은 앤저스(ANZUS) 협정이 사이버 공간에 적용됨을 공동 선언하며 상호방위의 기반을 마련했으며, 연례외교국방각료급회의(AUSMIN)를 통해 지속적으로 사이버 안보 이슈를 논의하고, 미·호 사이버사령부 간 공동가상훈련장 설립 등 여러 가지로 실질적 협력을 지속하고 있다. 한편 미국은 최근 오커스(AUKUS)에서도 호주, 영국 등과 인공지능, 양자기술, 사이버 안보 분야 협력을 논의하기 시작했다. 또한 미국은 2021년 8월 미국·싱가포르 사이버 협력 양해각서를 체결하여 양자 간 사이버 안보협력 관계를 제도화했는데, 이는 기존의 양국 국방협력을 사이버 방위 분야로 확대한 것을 의미한다. 이 양해각서 체결을 통해 미국과 싱가포르는 사이버 안보 분야에서 정보공유뿐만 아니라 합동 훈련에서의 협력을 강화하는 한편, 양국의 파트너십을 핵심 기술과 연구개발 분야로도 확대하였다.

이러한 미국의 행보는 최근 '통합억지'의 구도로 수렴하고 있다. 2022년 미 국방부의 국방전략에서 제시된 통합억지는 기존에 미국이 구상하는 동맹의 근본적인 구도를 변화시키겠다는 의도가 담긴 개념이다.[18] 인도·태평양 지역의 주로 양자관계에

18 U.S. Department of Defense (2022)

기초한 동맹을 '연맹해서(federated)' 전진 배치된 미국의 전략자산을 통합·사용함과 동시에 동맹국들을 연동해서 자산을 함께 사용하겠다는 것이다.[19] 이러한 미국의 계획이 성취된다면 미국 주도의 동맹은 큰 구조적 변화를 맞이하게 될 것이고, 미국이 동맹을 통해 제공하는 억지력도 향상될 것이라는 기대이다. 통합억지의 개념이 출현한 배경에는 '총체적(holistic)' 전략을 구사하는 중국에 '총체적으로' 맞대응하려는 미 국방부의 문제의식이 담겨있다. 과거 미 국방부의 억지 접근이 종종 우선순위의 혼란과 억지 대상에 대한 명확성의 결여 등으로 인해서 훼손됐다는 인식이다. 통합억지는 억지를 유지·강화하기 위한 미 국방부의 정책과 투자 및 활동을 정비하자는 문제 제기이며, 이를 통해서 구체적인 문제에 대한 맞춤형 전략을 개발하는 성격을 가진다.

2022년 미 국방부의 국방전략은 통합억지라는 틀에서 북한의 공격을 억지할 것이라고 적고 있다. 공중과 미사일 방어를 통합하고, 동맹국인 한국과의 긴밀한 조정과 상호운영, 핵 억지, 복원력 이니셔티브, 합동전력의 글로벌 전개로부터 나오는 직접적인 비용 부과를 추구한다는 것이다. 좀 더 구체적으로 미 국방부는 핵무기의 고유한 억지 효과와 함께 재래식, 사이버, 우주, 정보 역량을 맞춤형으로 결합한 억지 전략을 구사하겠다고 밝혔다. 이러한 맥락에서 보면 미국의 대북 사이버 억지는, 한국이 상정하는 '사이버 확장억지론'보다는 좀 더 포괄적 틀에서 설정되었다고 볼 수 있다. 미국이 한국보다 더 포괄적인 프레임에 입각해서 사이버 안보협력을 보고 있다는 증거는 2023년 미 백악관의 사이버 안보 전략에서도 나타났다.[20] 미국은 i) 디지털 생태계에 대한 위협에 대응하는 연대의 구축, ii) 국제 파트너 역량의 강화, ii) 동맹과 파트너를 지원하기 위한 미국의 역량 확장, iv) 책임있는 국가 행위를 위한

19 박원곤, "미국의 인도·태평양 전략과 한미동맹: 통합억제와 전 세계 대비태세." 『한국국가전략』 7-2 (2022), pp. 29-58.

20 White House (2023).

글로벌 규범 강화의 연대 구축, v) 정보, 커뮤니케이션, 운영기술 제품과 서비스 등의 글로벌 공급망 안전 확보 등을 전략목표로 제시하였다.

요컨대, 미국은 주로 중국발 사이버 위협을 염두에 두고, 한국을 비롯한 동맹국과 파트너 국가들을 미국 주도 동맹 네트워크에 참여시킨다는 통합억지 전략의 맥락에서 프레임을 짜고 있다. 이에 비해 한국은 북한발 사이버 위협에 초점을 맞추고 미국이 한국에 일방적으로 제공하는 확장억지를 확대·제도화하는 차원에서 사이버 안보 동맹을 강화하려는 프레임을 설정한다.[21] 여기서 관건은 미국이 제시하는 통합억지의 목표와 한국이 기대하는 확장억지 기반의 한미 사이버 안보 동맹론이 서로 얼마나 맞아떨어질 것이며, 더 나아가 얼마나 유기적으로 조율되느냐의 문제일 것이다. 이러한 맥락에서 볼 때, 한미 사이버 안보 동맹론은 한국과 미국이 설정하고 있는 '사이버 억지 프레임'의 차이를 제대로 인식하고, 그 차이를 해소하려는 노력에서 시작해야 할 것이다. 그런데 여기서 특히 더 주목할 점은, 최근 한국의 '한미 사이버 안보 동맹론'이 상정하고 있는 사이버 억지의 프레임이 미국이 제시하고 있는 프레임보다 협소하게 설정되었다는 사실이다. 특히 한국이 원용하는 프레임은 주로 전통억지의 개념에 입각하는 경향이 크다는 점이 문제다. 이러한 문제의식을 바탕으로, 이하에서는 한국이 제시하는 사이버 억지의 프레임에 문제를 제기하는 차원에서 기존의 사이버 억지 개념을 체계적으로 분석하고 이를 바탕으로 새로운 개념화를 시도하고자 한다.

21 물론 양국의 프레임이 전제로 한 사이버 위협의 현실은 계속 변화하고 있다. 여태까지는 미국에 중국발 위협이 중요하고, 한국에는 북한발 위협이 중요했다면, 최근 그렇게 간단하게 볼 수 없는 상황이 발생하고 있다. 미국도 북핵 위협만큼이나 북한발 사이버 위협에 민감하게 반응하고 있으며, 중국발 사이버 위협에 대한 한국의 인식도 변화하고 있다.

Ⅲ. 기존 사이버 억지 개념의 이해

1. 사이버 억지의 네 가지 메커니즘

억지는 보통 "상대방으로 하여금 자신이 기대하는 이익보다 비용이 초과할 것이라고 믿게 함으로써 어떤 행동의 수행을 단념케 하는 것"으로 정의된다.[22] 이러한 억지의 작동 메커니즘은 기본적으로 인지적 합리성(cognitive rationality)에 기반을 두는데, 기존 연구에서 억지 개념을 구분하기 위해서 원용하는 잣대는 두 가지이다. 그 하나는 인지적으로 '비용-이익 계산'을 행하는 '기준(reference)'인데, 행동에 영향을 미치는 인지 과정에 '비용을 부과'하느냐, 아니면 '이익을 거부'하느냐의 문제이다. 다른 하나는 비용-이익 계산이 작동하는 '수준(level)'의 문제인데, 행위자들 간의 상호작용 수준이냐, 아니면 구조의 수준이냐의 문제이다. 이러한 두 가지 잣대로 보면 사이버 억지 개념은 〈그림-1〉에서 보는 바와 같이 네 가지 유형으로 나누어 이해할 수 있다.[23]

22 Nye (2016), p.5; 억지 개념에 대해서 더 살펴보고 싶으면, Glenn H. Snyder, *Deterrence and Defense* (Princeton, NJ: Princeton University Press, 1961); Robert J. Art, "To What Ends Military Power?" *International Security* 4 (1980): pp. 3–35; Robert Jervis, "Deterrence Theory Revisited." *World Politics* 31-2 (1979), pp. 289–324를 참조.

23 사이버 억지의 개념 유형의 구분에 대해서는 다양한 시도들이 있는데 최근의 문제제기로는 N. J. Ryan, "Five Kinds of Cyber Deterrence." *Philosophy and Technology* 31 (2018). pp. 331–338, DOI 10.1007/s13347-016-0251-1; Cyberspace Solarium Commission (2020); Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43-2 (2020), pp. 245-280, DOI: 10.1080/01402390.2018.1563779; Lonergan and Montgomery (2021); Lilli (2021); Stefan Soesanto. "Cyber Deterrence Revisited." *Perspectives on Cyber Power CPP-8.* Maxwell Air Force Base, Alabama: Air University Press, 2022를 참조

〈그림-1〉 억지의 유형 구분

	비용 부과	이익 거부
행위자 수준	보복에 의한 억지	거부에 의한 억지
구조적 수준	규범에 의한 억지	연루에 의한 억지

출처: 필자 작성

첫째, '보복에 의한 사이버 억지'인데, 이는 보복공격의 가능성이 상존하기 때문에 섣불리 먼저 공격을 감행하지 못하게 하자는 개념이다. 냉전기 미국의 핵전략은 이러한 억지 개념에 기반을 두고 있었는데, 최근에는 이러한 개념에 기반을 둔 사이버 안보의 대응 방안들이 등장하였다. 즉 사이버 공격을 하려고 해도 상대방의 보복이 두려워 공격하지 못하게 하는 억지책을 마련하자는 것이다. 2012년 10월 리언 패네타 미 국방장관이 '사이버 진주만'을 언급하며 이란의 사이버 공격에 대해서 제기한 '원점타격론,' 2021년 7월 조 바이든 미 대통령이 미 국가정보국(DNI)에서 러시아의 사이버 공격이 물리적 전쟁을 유발할 수도 있다고 경고한 '전쟁엄포론', 그리고 시스템 침투 전에 공격자가 수행하는 사전 작업을 세밀히 탐지하여 선제적으로 대응하자는 '사이버 킬체인'의 구상 등이 '사이버 보복억지 담론'의 사례들이다.

이러한 보복억지 개념은 공격받는 측의 결연한 의지의 표명이라는 상징적 효과를 볼 수는 있겠지만, 핵 억지의 개념이 전제로 한 단순계적 인과관계의 논리를 오늘날 복잡계 네트워크를 속성으로 하는 사이버 안보 분야에 그대로 적용하기 곤란하다는 점에서 한계가 있다. 특히 보복억지를 수행하는 데에는 보복의 대상을 설정하는 것이 중요한 문제인데, 사이버 안보 분야에서 보복의 대상을 확인하고 그 책임을 귀속하는 과정은 핵전쟁이나 재래식 전쟁의 경우에 비해서 좀 더 복잡하다는 점이 문제이다. 이외에도 공격주체의 다양성, '무고한 대리인'의 문제, '가짜 깃발(false flags)'의 문제, 수집한 정보의 대중공개 어려움 등을 이유로 사이버 공격을 사전에 탐지하거나 사후에 확인한다는 것은 쉬운 일이 아니다. 이러한 문제는 1990년 중후반 초기 사이버 억지 연구에서 상세하게 지적된 바 있다.[24)]

둘째, '거부에 의한 사이버 억지'인데, 이는 방어와 회복의 역량을 보여줌으로써 '공격해 봤자 헛수고'라는 메시지를 발신하여 공격자의 의지를 애초부터 꺾자는 개념이다. 아무리 날카로운 '창'으로 공격해도 뚫리지 않는 '방패'라는 '철옹성 이미지'를 각인시켜 사이버 공격 자체를 아예 단념시키자는 것이다. 예를 들어, 2015년에 최근 크라우드스트라이크(CrowdStrike)라는 미국의 민간 정보보안 업체가 허리케인 팬더(Hurricane Panda)라고 불리는 중국 해커 그룹의 공격을 최초로 저지했다고 주장했다. 이 업체에 의하면, 중국 해커 그룹이 자신들의 침입 비용이 커진다는 사실을 인지하고 이전의 공격 시도 때 자신들이 낭비한 시간과 비용을 고려해서 2015년 1월의 사이버 공격을 포기했다면서 "공격 가치가 없다고 공격을 포기하는 경우는 우리도 처음 봤다"라고 했다.[25]

거부억지의 작동 메커니즘에서는 공격자의 '비용-이익 계산'의 과정에 보내는 '시그널 효과'가 중요한 변수이다. 예를 들어, 시그널 효과의 작동과정에서는 견실한 기술 역량, 사이버 방어훈련 역량, 지속적인 개입의 의지, 위협정보의 공유체계 구비, 사이버 귀속의 정확성, 오류나 버그 탐지의 속도, 주의보 발령이나 패치 릴리스 등의 신속성, 실전 수준의 전술·전략 기술 시연, 강력한 선언적 정책 표방, 표준·법·규정의 정비 등을 보여주는 것이 중요하다. 그러나 사이버 기술이라는 관점에서 볼 때, 방어에 비해 공격이 압도적으로 유리하다는 사실이 여전히 거부억지 개념을 원용하는 데 있어 제약요인으로 작용한다. 게다가 사이버 위협과 사이버 무기의 급속한 발전, 그리고 인터넷의 개방환경을 통한 지식과 역량의 빠른 전파와 습득으로 인해서 사이버 안보 분야에서 거부억지가 작동할 입지는 점점 더 줄어들고 있다.[26]

셋째, '연루에 의한 사이버 억지'인데, 이는 사이버 공격이 공격 대상뿐만 아니라

24 John Arquilla and David Ronfeldt, *The Advent of Net War* Santa Monica, CA: RAND Corporation, 1996.
25 김상배 (2018), p. 207.
26 Tor (2017), p. 101

공격자 자신에게도 피해를 주는 상호의존의 환경에서 발생한다는 특성을 활용하자는 개념이다. 연루억지는 신자유주의 국제정치이론가인 조지프 나이에 의해서 제시된 개념이다.[27] 나이가 말하는 연루는 다름 아닌, '리스크의 공유'이다. 예를 들어, 공격과 피해의 양방은 호혜적인 경제 관계를 통해서 상호연결 및 상호의존하고, 특히 사이버 공간에서는 글로벌 연결성을 제공하는 기반 인프라와 네트워크를 공유하기 때문에, 어느 일방의 사이버 공격은 이러한 상호 연결성을 침해하고 상호 리스크를 증대시킨다는 것이다. 나이는 이러한 상황에 착안하여 연루의 전략이 공격자에게 스스로 비용을 부과하는 억지 전략으로 작동할 수 있다고 보았다. 상호 리스크를 줄임으로써 공격-방어 양방이 모두 이익을 얻을 것이라는 기대를 낳는다는 것이다.[28]

사이버 공간에서 연루 전략은, 견실한 방어를 구축하거나 보복 행동으로 위협하는 전략을 넘어서, 공격자의 '비용-이익 계산'에 영향을 미치는 대안적 방안을 제시한다. 기본적으로 연루 전략은 실질적인 비용을 치르지 않고서는 빠져나갈 수 없을 정도로 복잡한 상호작용의 구조를 창출하는 데서 비롯된다. 궁극적으로 연루 전략은 공격자의 판단 준거를 '비용 감수'에서 '이익 추구'로 이행시키는 목적으로 수행된다. 이런 점에서 연루억지는 보복억지와 거부억지의 두 개념이 채우지 못한 틈새를 메우는 의미가 있다.[29] 그럼에도 이러한 연루억지의 전략은 일정한 정도 이상의 상호의존 관계를 상정할 수 있는 국가들 사이에서나 원용할 수 있는 개념이라는 한계를 지닌다. 상호의존의 정도가 일정 수준 이하에 머물고 있는 국가들에는 적용하기 힘들다는 것이다. 또한 최근 '경제안보'의 맥락에서 거론되는, 이른바 '상호의존의 무기화' 현상은 연루의 메커니즘이 '억지'가 아닌 '무기'로 작동할 수도 있는 양면성을 보여준다는 점에서 연루억지 개념의 주장 자체를 무색케 하는 면도 없지 않다.[30]

27 Nye (2017), pp. 58-60.
28 Soesanto (2022), p. 13.
29 Brantly (2020), pp. 210-233.
30 Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global

끝으로, '규범에 의한 사이버 억지'인데, 이는 공격을 통해서 얻을 수 있는 이익을 넘어서 행위자의 평판을 해치는 비용을 부과하자는 개념이다. 연루억지 개념과 마찬가지로, 규범억지는 공격이 방어에 의해서 거부되지 않고 맞공격의 보복 위협이 없더라도 공격자에게 비용을 부과하는 '구조적 환경'을 배경으로 해서 작동하는 메커니즘이다. 그러나 연루억지와는 달리 규범억지의 작동에 있어서는 일정 정도의 책임귀속 역량이 뒷받침되어야 한다. 한편, 이러한 규범억지의 개념은 '금기(taboo)에 의한 억지' 또는 '공개적 망신 주기(naming and shaming)에 의한 억지'와도 밀접히 연관된다.[31] 예를 들어, 만약에 저강도 분쟁에서 어느 강대국이 핵무기를 사용하여 약소국을 제압하려 한다면, 이는 널리 공유된 핵무기 관련 규범을 위반하는 것으로 그 강대국의 평판을 해치는 비용을 발생시킬 것이다. 사이버 공간에서도 이러한 평판비용의 부과는 무력분쟁 이하에서 발생하는 사이버 범죄와 테러 행위를 단념시키는 효과를 낳는다.

규범억지의 전략은 사이버 공간에서 국제규범을 창출하려는 정부 차원의 노력을 통해서 드러나고 있다. 예를 들어, 유엔에서의 정부자문가그룹(GGE)과 개방형워킹그룹(OEWG)의 활동, 탈린 매뉴얼(Tallin Manual)의 마련 등과 같은 노력은 국제법·규범을 사이버 안보 분야에 적용하려는 시도들이었다. 이러한 규범적 모색은 사이버 공격을 제한하는 일반원칙을 창출함으로써 사이버 공간에서의 악성 행위에 대해 평판 비용을 부과하는 것을 목적으로 했다.[32] 이러한 노력 중에서 '상당한 주의(Due Diligence)'의 의무를 규범화하려는 시도에 주목할 필요가 있는데, 이는 지리적으로 사이버 공격이 시작된 국가에 책임을 물어 사이버 위법 행위를 자국의 국내법에 따라 처벌하고 통제하도록 유인하자는 구상으로서 규범억지의 취지와 맥이 닿

Economic Networks Shape State Coercion." *International Security* 44-1 (2019), pp. 42-79, https://doi.org/10.1162/ISEC_a_00351

31 Nye (2016), p. 60.

32 Soesanto (2022), p. 9.

는다. 이는 기본적으로 국제법적 검토의 문제이지만, 사이버 억지가 궁극적으로는 공격의 배후지가 되는 국가와 협력하는 외교적이고 규범적인 노력으로도 연계됨을 보여주고 있다.

2. 새로운 사이버 억지 개념의 시도들

오늘날 빠르게 변화하고 있는 사이버 위협의 총체성과 복잡성을 고려할 때, 이상에서 살펴본 사이버 억지의 네 가지 메커니즘 중에서 어느 하나도 사이버 억지의 전반적 효과를 끌어내는 유일한 해법이 될 수는 없다. 어느 하나의 개념에만 의존하여 시야를 좁게 설정해서 사이버 억지 전략을 채택한다면, 그 효과를 제대로 보기도 어려울 뿐만 아니라 오히려 더 많은 것을 놓칠 수도 있다. 따라서 이들 개념이 지니는 상호보완적 성격을 이해하고 이들을 모두 아우르는 '포괄적(comprehensive) 억지'[33] 개념을 고민하는 것이 필요하다. 이를 위해서 우선 필요한 것은 기존의 전통적 억지를 보는 것과는 다른 시각에서 사이버 억지의 개념을 이해하려는 새로운 마인드의 도입이다.

우선, 포괄적 사이버 억지 개념을 개발하기 위해서는 '단절적 모듈 마인드'가 아니라 '연속적 스펙트럼 마인드'가 필요하다. 핵 억지와 달리 사이버 억지는 '원천 봉쇄'를 지향하는 절대적 개념이 아니라 빈도와 정도를 '제한(restrictive)하는' 상대적 개념으로 이해해야 한다. 유리 토르(Uri Tor)가 제안한 '축적적(cumulative) 억지' 개

33 '포괄적 억지' 개념의 필요성에 대한 문제제기로는 Scott Jasper, "Deterring Malicious Behavior in Cyberspace." *Strategic Studies Quarterly* 9-1 (2015), pp. 60-85; Aaron F. Brantly, "The Cyber Deterrence Problem." in T. Minárik, R. Jakschis, L. and Lindström (eds.) *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. NATO CCDCOE Publications, Tallinn, 2018, pp.31-53; Lilli (2021), p. 166; Joe Burton, "Cyber Deterrence: A Comprehensive Approach?" NATO Cooperative Cyber Defence Centre of Excellence (2018) https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April 2018.pdf (검색일: 2023년 3월 24일)을 참조.

념은 사이버 위협의 지속적 성격과 이에 대응하는 사이버 억지의 스펙트럼 마인드를 강조하고 있다. 그는 지속적으로 분쟁에 휘말리고 있는 이스라엘의 사례에 대한 소개를 바탕으로 사이버 공격을 원천 봉쇄한다는 식의 비현실적인 목표설정을 넘어, 사이버 공격은 늘 반복적으로 발생하는 것이라고 당연시하는 전제 위에서 펼치는 새로운 억지 개념의 필요성을 제기하였다.[34)]

또한 사이버 억지 개념은 견실하고 안전한 인프라를 구축하고 이에 대한 공격을 완벽하게 막는다는 '방어 마인드'보다는, 공격받더라도 빠르게 원상으로 복구할 것이라는 '회복 마인드'를 바탕으로 개발되어야 한다. 2022년 미 국방부의 국방전략이 제시한 '회복(resilience)에 의한 억지' 개념은 바로 이러한 마인드를 강조하였다. 회복억지는 공격받아서 와해되더라도 '견뎌내고,' '싸워내고,' 그리고 '빠르게 회복하는' 역량을 보여주자는 개념인데, 이를 통해 사이버 공격이 누릴 이익을 거부한다는 점에서 거부억지의 개념과도 통하는 바가 크다. 사이버 공격이라는 것은 애초에 예방 자체가 어렵기 때문에 공격받은 후에 그것을 빨리 복구하는 것이 더 중요한 해법일 수 있다는 것이다.[35)]

이렇게 축적적이고 회복적 성격의 사이버 억지는 '다양성'의 개념을 바탕으로 전개되어야 실질적 효과를 볼 수 있다. 기존의 사이버 억지 연구는 세 가지 종류의 다양성을 강조하였다. 첫째는 '다층위성'인데, 미 의회의 위임을 받아 설치된 '사이버 공간 솔라리움 위원회'가 2020년에 펴낸 보고서는 다층위성에 기반을 둔 '층위적(layered) 사이버 억지'의 개념을 자세히 설명하고 있다. 이 보고서는 보복·거부·연루·규범 억지 등과 같이 기존에 제시되었던 사이버 억지 개념들을 입체적으로 결합했는데, 그 핵심 구상은 다층적인 억지 메커니즘을 가동하여, 미국의 시스템을 노리는 사이버 위협에 대해서 '동시적이고(concurrently), 지속적이며(continuously),

34 Tor (2017), p. 95.
35 U.S. Department of Defense (2022), p. 8

협업적으로(collaboratively)' 대응해야 한다고 제언하였다.[36]

둘째, 다층위 억지의 개념과 함께 '횡영역(cross-domain)' 또는 '다영역 억지'의 개념에도 주목해야 한다.[37] 사이버 억지를 포괄적으로 가동하기 위해서는 사이버 공간의 도구적 활용에만 국한될 것이 아니라, 육·해·공·우주·사이버 공간에서의 '다영역 작전(multi-domain operation)'을 통해서 외교, 정보, 군사, 경제, 금융, 첩보, 법 등과 관련된 국가역량 전반을 활용하는 접근법이 필요하다는 것이다.[38] 이러한 다영역 억지의 개념은 사이버 공간에서 발생한 위협일지라도 이에 대응하기 위해서는 사이버 영역의 외부로부터도 권력자원을 동원할 의사를 보여주어야 한다는 인식을 바탕에 깔고 있다. 필요에 따라서는 모든 영역을 아울러서, 국력을 총체적으로 동원해서라도 사이버 위협에 대응하겠다는 의지를 보여주자는 것이다.

끝으로, '다자적(multi-lateral) 억지'도 사이버 억지 개념의 다양성을 보여주는 중요한 개념이다. 2022년 미 국방전략의 통합억지 개념은 해당 국가뿐만 아니라 여러 나라가 함께 대응하는, '집단적(collective) 사이버 억지'의 중요성을 강조하였다. 이는 사이버 억지의 달성을 위해서는 미국이 혼자서 나설 수는 없으니, 동맹국이나 파트너 국가들과의 협력을 통해서 사이버 억지의 효과를 거두겠다는 의지를 표명한 것으로 볼 수 있다. 집단적 대응의 태세를 다양화하고 그 범위를 확장함으로써 공격자의 행위를 어렵게 할 수 있다는 것이다. 이러한 집단적 억지가 효과를 거두기 위해서는 사이버 공간에서의 적절한 '행위형성(shape behavior)'을 목표로 한 규범의 마련이 중요하다는 점도 강조하고 있다.[39]

요컨대, 효과적인 사이버 억지를 위해서는 여러 층위에 걸쳐서 감행되는 공격의

36 Cyberspace Solarium Commission (2020), p. 23
37 Jon Lindsay et al, (2015); Gartzke and Lindsay (eds.) (2019).
38 Antonio Missiroli, "The Dark Side of the Web: Cyber as a Threat." *European Foreign Affairs Review* 24-2 (2019), pp. 135-152.
39 U.S. Department of Defense (2022), p. 9, 14-15

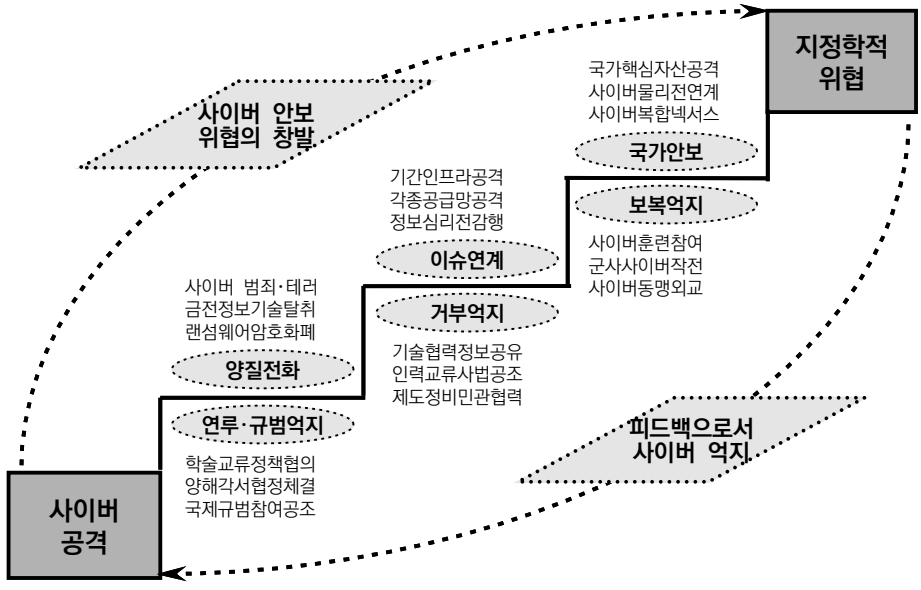
종류에 맞추어 '최적의 조합'을 추구하는 맞춤형 전략이 필요하다. 사이버 억지가 실제 효과를 보기 위해서는 보복, 거부, 연루, 규범의 각기 다른 메커니즘을 적재적소에 동원하는 것이 필요한데, 그 최적의 조합은 상황에 맞추어 유연하게 채택되어야 한다. 이를 위해서는 기존의 사이버 억지 개념뿐만 아니라, 앞서 살펴본 포괄적 억지 개념의 새로운 시도들, 즉 축적적 억지, 회복에 의한 억지, 다층위 억지, 다영역 억지, 다자적 억지 등을 통합적으로 활용할 필요가 있다. 이렇게 보면, 지금 우리에게 필요한 것은, 기존의 개념 중에서 어느 하나를 선택하는 작업이 아니라, 이들 개념을 전체적으로 아우르는 '메타 프레임'의 개발이라고 할 수 있다.

Ⅳ. 사이버 억지의 새로운 개념화와 적용

1. 사이버 억지의 새로운 개념화

이러한 메타 프레임의 개발 차원에서 이 글은 〈그림-2〉에서 보는 바와 같이 복잡계 이론에서 말하는 '창발과 피드백'의 입체적이고 동태적인 프레임을 원용하여 개념화를 시도하였다. 사이버 안보위협이 '양질전화'와 '이슈연계' 및 '국가안보'의 임계점을 넘어서는 창발의 메커니즘을 따라가는 만큼, 이를 억지하려는 시도도 각 층위에 적합한 피드백의 메커니즘을 유연하게 적용하는 차원에서 진행하자는 것이다. 이러한 메타 프레임의 구도를 배경으로 도출한 사이버 억지의 개념을 굳이 명명하자면, '창발에 대한 억지(deterrence against emergence)'라고 부를 수 있을 것이다. '창발에 대한 억지'의 개념을 부연 설명하기 위해서 이 개념이 강조하는 핵심을 짚어보면 '입체성'과 '동태성'에서 찾아볼 수 있다. 먼저 입체성의 관점에서 보면, '창발에 대한 억지'는 양질전화-이슈연계-국가안보의 단계별로 '적합한(fit)' 억지의 옵션을 도입하는 과정에서 작동한다.

〈그림-2〉 '창발-피드백'의 프레임으로 보는 사이버 억지



출처: 필자 작성

첫째, 양질전화의 층위에서 볼 때, 일상생활 속에서 발생하는 사이버 범죄·테러, 금전·정보·기술 탈취와 절취, 랜섬웨어 및 암호화폐 공격 등에 대해서는 예방(prevention) 차원에서 연루억지나 규범억지의 개념을 적용해서 대응하는 것이 유용하다. 공동의 이익과 가치를 기반으로 마련한 사이버 규범의 집단적 집행은 공격자의 악의적 행동을 제약하고 책임있는 행동을 요구하는 '행태형성'의 효과를 기대케 한다. 이러한 접근이 국가 후원의 사이버 작전이나 사이버 범죄를 완벽히 제거하지는 못할지라도, 지속적인 비용부과와 이익보상을 통해서 악의적 행위를 수행할 인센티브를 잠식할 수는 있을 것이다.

둘째, 이슈연계의 층위에서 볼 때, 다양한 분야에 걸쳐서 발생하는 기간 인프라 공격, 각종 공급망 공격, 선거 시스템의 교란을 노린 정보심리전 감행 등에 대해서는 회복(resilience) 차원에서 거부억지의 개념을 적용해서 대응하는 것이 유용하다. 이러한 거부억지는 자원, 접근, 역량과 관련된 공격자의 선택지를 제한한다. 다시 말

해, 거부억지를 통한 취약성의 감소는 공격자가 원하는 결과를 달성하기 위해서는 더 많은 자원을 소모하고, 더 많은 접근법을 개발하고, 더 비싼 사이버 무기를 만들어야 할 필요를 초래하게 된다.

끝으로, 국가안보의 층위에서 볼 때, 지정학적 임계점을 넘어서 발생하는 국가 핵심자산 공격, 무력분쟁과 연계된 사이버전 수행, 기타 '사이버 안보 복합 넥서스'의 부상 등에 대해서는 엄포 차원에서 보복억지의 개념을 적용해서 대응하는 것이 유용하다. 사이버 억지는 실제로 공격자에게 비용을 부과할 수 있는 물적 역량을 바탕으로 해야 실질적 효과가 있다. 분쟁을 억지하고 악의적 공격행위를 무력분쟁 이하 수준으로 제한하고, 만약에 필요하다면 국력의 모든 옵션을 동원하여 공격을 제압하는 것이 필요할 수도 있다.

이렇게 입체적인 구도에서 이해한 '창발에 대한 억지' 개념은, 정태적인 성격의 것이 아니라, 창발과 피드백의 상호작용이라는 '동태성'을 바탕으로 한다. 이 글은 이러한 동태적 작동 메커니즘을 반영하는 용어로서, 앞서 살펴본 유리 토르의 '축적적 억지(cumulative deterrence)' 개념을 원용하고자 한다. '축적적 억지'의 개념은 연속적 스펙트럼 마인드에서 사이버 억지를 이해하려는 시도이다. 이러한 스펙트럼상에서 사이버 억지가 작동하는 핵심 메커니즘은 〈그림-2〉의 구도에서 보는 바와 같이, 미시적 수준으로부터 지속적으로 창발하는 사이버 위협의 수준에 맞추어, 한편으로 '하강(de-escalation)' 또는 '전진하거나(forward), 다른 한편으로 '상승(escalation)' 또는 '후진함으로써(backward)' 유연하게 대응하는 피드백의 작용을 통해서 드러난다.

이러한 과정을 축구 경기의 전술에 비유해 보면, 마치 상대방의 공격이 중앙선을 넘어오기 전부터 펼쳐지는 '전방 압박'의 수비 전술을 떠올려 볼 수 있다. 골이 들어갈 위험지역에 들어오기 전에 수비를 펼치듯이, 무력분쟁 이하의 수준에서 적의 악의적 행동을 막는 것이 목적이다. 이런 점에서 일종의 '전방 압박 억지'라고도 부를 수 있다. 그렇다고 축적적 억지의 개념이 저층위 수준으로 감행되는 모든 사이버 공격에 대해서 고층위 옵션을 동원해서 대응하는 것만을 설정하는 것은 아니다. 사이버 안보 분야의 특성상, 저층위나 중층위 공격에 대한 억지의 수단으로서 고층위 옵

션이 얼마나 효과적일지도 의문이다. 다만 억지 개념이 효과적으로 작동하기 위해서는, 지정학의 문턱을 넘어서는 공격만 막겠다는 발상으로는 안 되고, 좀 더 동태적으로 전후방을 넘나드는 발상이 필요하다는 것이다.

이러한 '축적적 억지'의 개념은, 미 국방부에서 제시한 '선제적 방어(defend forward)'의 개념과 유사하면서도 다르다. 미 국방부의 선제적 방어는 '선제대응(proactive)'의 성격이 강한 개념으로, "악의적 사이버 행위는 무력분쟁 이하의 수준에서 발생하더라도 그 근원을 찾아서 가능한 한 가까이 다가가서 와해하고 중지시키겠다는" 내용을 담고 있다.[40] 말로는 '방어'를 논하지만, 사실상 그 내용은 '공격'과 다름없다. 선제적 방어 개념과 마찬가지로 축적적 억지의 개념도 기간 인프라를 보호하고 네트워크 안보를 위해서 적의 공격이 목표에 도달하기 전에 그 위협을 중단시키는 방법을 찾는 데 중점을 둔다. 그런데 축적적 억지의 개념이 선제적 방어의 개념과 구별되는 차이점은, '전방'만 보는 게 아니라 창발의 관점에서 '전방'과 '후방'을 동시에, 그것도 유연하게 대응하는 피드백의 맥락에서 이해된 억지의 개념이라는 데 있다.

2. 새로운 사이버 억지 개념의 적용

이상에서 새롭게 개념화한 사이버 억지의 개념을 한미 사이버 안보협력의 사례에 적용해서 보면, 우선 향후 한미 사이버 안보협력은, 단순히 동맹이라는 고층위 협력에만 시야를 고정해서 추진하기보다는, 그 협력의 정도와 내용의 측면에서 사이버 안보협력과 관련된 여러 층위를 입체적이고도 동태적으로 아우르는 방식으로 시야를 넓혀서 진행해야 할 것이다. 이렇게 다층위로 협력 개념을 설정하는 것은, 〈그림-2〉에서 보는 바와 같이, 사이버 위협이 창발하는 동태적 구도와 연동하여 이에 대한

40 U.S. Department of Defense (2018).

'축적적 대응책'을 마련하는 접근이 지닌 유용성 때문이다. 다시 말해 사이버 위협의 성격에 따라서 저층위-중층위-고층위에 걸쳐서 각기 특화된 억지 개념을 바탕으로 협력 방안을 선택하고 이를 탄력적으로 조합할 수 있어야 할 것이다.

첫째, 저층위에서 발생하는 사이버 위협에 대해서는 연루억지나 규범억지를 통한 '행태형성' 목적의 협력을 모색해야 한다. 국제적 참여와 협력을 통해서 구축된 규범은 국가 및 비국가 행위자들의 책임있는 행태를 형성하고, 더 나아가 섣불리 상대의 이익을 침해하는 사이버 작전의 수행에 대해서 평판비용을 부과할 것이다. 규범·규칙 기반 질서를 지원하는 동지국가(同志國家, like-minded countries)나 파트너 국가들과의 연대 구축을 통해서 이러한 연루억지와 규범억지의 효과는 더욱 커질 것이다.

이러한 저층위 협력 방안으로는 대략 세 가지가 거론된다. i) 학술교류 차원에서 전문가 워킹그룹의 운영, 사이버 안보 및 규범 관련 워크숍 개최, 민간 부문과 학계의 연계 추진 등이 필요하다. ii) 사이버 안보 관련 양해각서나 협정의 체결은 정보공유, 정책연구, 모범관행 등과 관련된 합의를 이행하는 약속을 담고서 정책조율과 관련 제재조치에 공동보조를 취한다는 점에서 중요하다.[41] iii) 국내외적으로 진행되는 사이버 안보 규범 형성과정에 참여하여 공동보조를 맞추는 것도 중요하다.

둘째, 중층위에서 발생하는 사이버 위협에 대해서는 거부억지를 통해 '이익거부' 목적의 협력을 모색해야 한다. 이 층위에서는 회복력의 구비를 통해서 공격작전의 이익을 거부하고 공격자의 목적 달성 역량에 대한 확신을 감소시켜야 한다. 이러한 노력은 기술력 고도화를 바탕으로 해킹 세력의 추적·감시 역량을 확충하고 이를 기반으로 사이버 공격의 배후를 규명하는 태세의 완성도를 대외적으로 알리는 효과를 낳을 것이다.

41 2010년대 중반 무렵까지의 사이버 안보 관련 정보공유 협정에 대해서는, Theresa Hitchens and Nilsu Goren, "International Cybersecurity Information Sharing Agreements" Center for International and Security Studies, University of Maryland (2017). https://www.jstor.org/stable/resrep20426#metadata_info_tab_contents (검색일: 2023년 3월 24일)을 참조.

대략 다섯 가지 방안이 중층위 협력 과정에서 거론된다. i) 사이버 안보 분야의 핵심·신흥 기술 관련 연구개발 협력을 강화할 필요가 있다. ii) 사이버 공격과 관련된 위협정보의 공유도 중요하다. iii) 사이버 역량 강화를 위한 교육, 전문인력의 교류. 인력양성 프로그램 운영도 중요한 협력 사안이다. iv) 사이버 공격에 대응하는 정책과 태세를 조율하는 거버넌스 체계의 구체화도 필요한데, 여기에는 사이버 안보 관련 법·제도·조직의 정비, 사이버 범죄에 대응하는 사법공조 체계의 가동 등이 포함된다. v) 좀 더 넓은 의미에서 관·학·산·연의 정책 네트워크 구축도 필요하다.

끝으로, 고층위의 사이버 공격에 대해서는 보복억지를 통해 '비용부과' 목적의 협력을 모색해야 한다. 이 층위에서는 군사적 수단의 사용을 포함하여 무력분쟁 이하 수준에서 발생하는 여타 층위의 사이버 공격을 억지하는 모든 옵션을 동원할 수 있다. 이 과정에서 비용부과의 역량을 보여주는 차원에서 선언적 정책도 채택할 수 있다.

이러한 고층위 협력 방안으로는 주로 세 가지가 거론된다. i) 사이버스톰(Cyber Storm)이나 사이버플래그(Cyber Flag) 등과 같은 공동 사이버 훈련에의 참여를 확대할 필요가 있다. ii) 사이버 위협에 대응하는 연합 군사작전의 수행 역량을 강화하고, 지능화·고도화된 사이버 전력 구축을 위한 협력 및 사이버 작전의 여건 보장을 위한 제도 및 인프라를 확충할 필요가 있다. iii) 사이버 외교무대에서의 협력과 공조뿐만 아니라 사이버 위협에 대응하는 차원에서 경제제재, 수출통제, 외교적 조치 등에서 전략적으로 보조를 맞출 필요가 있다.

이러한 맥락에서 볼 때 2023년 4월 한미 정상회담에서 채택한 문서인 "전략적 사이버안보 협력 프레임워크"를 통해서 다층위 접근의 필요성을 지적한 것에 주목할 필요가 있다. '협력의 범위'에 대한 논의에서, 한미협력을 사이버 공간까지 확장하고, 사이버 위협 정보의 공유를 포함한 사이버 안보 기술, 정책, 전략에서 협력을 증진하며 신뢰를 구축하기로 하였는데, i) 사이버 공간에서 악의적인 행위자들의 활동을 차단·억지하기 위해 다양한 종류의 대응수단을 개발·실행하고, ii) 사이버 공간에서 파괴적이고 불법적인 행위에 관여하는 국가에게 책임을 물을 수 있도록 협력하며, iii) 사이버 훈련, 핵심 기반 시설 보호 연구·개발, 인재양성, 사이버 위협정보 실시간 공

유, 사이버 복원력 확보를 위한 민·관·학 협력 네트워크 구축 등 현재의 협력을 보다 굳건히 발전시켜 나갈 것이라 강조하였다.[42)]

이렇게 사이버 억지의 개념을 다층위적이고 입체적으로 설정하는 노력과 더불어, 사이버 억지의 동태적 운용이라는 관점에서 한미 사이버 안보협력을 저층위 또는 중층위 협력으로 유지하는 것이 맞을지, 아니면 고층위 협력의 차원에까지 격상하는 것이 맞을지에 대한 고민이 필요하다. 이러한 동태적 접근은 한미 사이버 안보협력을 저층위 협력에서 시작해서 중층위 협력을 거쳐서 고층위 협력으로 발전시키자는 '기능주의적 접근'과는 그 성격이 다르다. 기능주의적 접근은 이른바 '연성안보' 분야의 협력에서 시작해서 '경성안보' 분야의 협력으로 발전시켜 나가자는 발상을 바탕에 깔고 있다.

또한 이러한 사이버 억지의 개념은 미 국방부에서 제시한 '선제적 방어'와도 다르다. 선제적 방어는 무력분쟁 수준 이하에서 발생하는 사이버 공격이라도, 피해가 발생하기 전에 그 근원을 찾아서 중지시키겠다는 의지를 바탕으로 한다. 이에 비해, 이 글에서 제시하는 사이버 억지의 개념은, 앞서 제시한 '창발에 대한 축적적 억지'의 맥락에서 이해해야 한다. 사이버 안보 분야의 협력은 저층위에서 중층위를 거쳐서 고층위로 '상승'하는 일방향 모델이 아니다. 만약에 이러한 '상승' 구도의 실천이 가능하더라도 무작정 고층위 모델에 해당하는 정치군사 동맹 수준의 협력으로 격상하는 것이 능사가 아니다. 오히려 층위별로 다양한 협력 방안을 마련하고 이를 유연하게 조합해서 활용해야 한다.

이렇게 개념화한 사이버 억지의 개념은 최근 사이버 안보 분야에서 공격과 방어가 엄밀하게 구분되지 않는 가운데 복잡화되고 있는 현상을 적절하게 반영한다. 예를 들어, 사이버 안보 업무의 실무기관인 국가정보원 국가사이버안보센터(NCSC)는 각

42 대통령실 뉴스룸 (2023)

종 사이버 공격에 체계적으로 대응하기 위해 그 파급영향과 피해규모 등을 고려하여 사이버위기경보를 발령하고 있는데, 이는 '창발에 대한 축적적 억지'의 일례를 보여준다. 실제로 사이버위기경보는 「사이버안보업무규정」 제15조에 의거하여 사이버 공격의 수준에 따라 정상 단계로부터 관심·주의·경계·심각의 단계가 발령된다.[43] (문단 통합함) i) 정상 단계: 국내 민간 분야 인터넷 소통 및 사용에 지장이 없는 단계로서 위험도가 낮은 국지성의 이상 트래픽의 발생 가능성은 존재한다. 웜·바이러스 등 악성코드의 출현을 탐지하고 신규 보안 취약점 또는 해킹 기법 등을 발표한다. ii) 관심 단계: 위험도가 높은 웜·바이러스, 취약점 및 해킹 기법 출현으로 인해 피해 발생 가능성이 증가한 단계이다. 해외 사이버 공격 피해가 확산되어 국내 유입이 우려되고, 침해사고가 일부 기관에서 발생하며 국내외 정치·군사적 위기상황의 조성 등 사이버 안보에 대한 위해 가능성이 증가할 경우 발령된다. iii) 경보 단계: 일부 정보통신망 및 정보시스템의 장애가 발생하는 단계이다. 침해사고가 다수기관으로 확산될 가능성 증가하고 국내외 정치·군사적 위기 발생 등 사이버 안보에 대한 위해 가능성이 고조될 경우 발령된다. iv) 경계 단계: 복수 정보통신서비스제공자(ISP) 망·기간통신망에 장애 또는 마비가 발생하는 단계이다. 침해사고가 다수 기관에서 발생했거나 대규모 피해로 확대될 가능성이 증가할 경우 발령된다. v) 심각 단계: 국가 차원의 주요 정보통신망 및 정보시스템 장애 또는 마비가 발생한 단계이다. 침해사고가 전국적으로 발생했거나 피해 범위가 대규모인 사고가 발생할 경우 발령된다. 사이버 위협의 정도와 성격이 변함에 따라 사이버위기경보가 상향 및 하향 조정을 거듭하게 되는 것이다.

43 법제처 국가법령센터, "사이버안보업무규정" https://www.law.go.kr/법령/사이버안보업무규정/(31356,20201231) (검색일: 2023년 5월 7일).

V. 맺음말

이 글은 '한미 사이버 안보 동맹론'의 바탕이 되는 개념적 기반과 담론적 프레임에 문제를 제기하고 이를 넘어서는 새로운 개념화의 작업을 시도하였다. 최근 제기된 한미 사이버 안보 동맹론은 한미 상호방위조약의 개정 과정에 사이버 안보 관련 조항을 포함하여 미국의 '사이버 우산' 제공의 약속을 받아내고, 국내적으로도 사이버 역량 강화를 위한 계기를 마련하자는 담론이다. 이러한 담론은 사이버 안보 분야에서 한미협력을 강화하기 위해서 노력한다는 점에서 의미를 찾을 수는 있겠지만. 사이버 공간의 고유한 성격이나 진화하는 미국의 억지 전략, 한미관계 전반의 미래 등을 고려할 때 한계가 있는 것이 사실이다. 향후 한미 사이버 안보협력은 전통적인 동맹과 억지의 발상을 넘어서 사이버 공간의 복잡계적 특성을 고려한 유연하고도 통합적인 시각을 바탕으로 추진되어야 한다. 이러한 문제의식을 바탕으로 이 글은 한미 사이버 안보 동맹론이 딛고 선 이론적 기반이라고 할 수 있는 전통억지 개념을 비판적으로 검토하고 이를 보완·대체하는 새로운 개념화를 시도하였다.

기존에 통용되고 있는 사이버 억지의 네 가지 메커니즘, 즉 보복억지, 거부억지, 연루억지, 규범억지의 개념 중에서 사이버 위협에 완벽하게 대응하는 데 활용할 수 있는 단일 해법을 찾기는 어렵다는 것이 이 글의 인식이다. 각 개념이 모두 특정한 사이버 안보의 맥락에서 제한적 유용성만을 지니고 있기 때문이다. 따라서 오늘날 사이버 위협의 총체성과 다양성을 설명하기 위해서는 이들 개념을 포괄적으로 묶어서 이해하려는 노력이 필요하다. 이러한 문제의식을 바탕으로 이 글은 기존의 미국 정책서클과 국제정치학계에서 제시된 다양한 사이버 억지의 응용개념들을 검토하고, 이들을 아우르는 '메타 프레임'을 마련하는 차원에서 '창발에 대한 축적적 억지'의 개념을 제시하였다. 이는 향후 한미 사이버 안보협력의 방향을 모색하는 데 길잡이 역할을 할 것으로 기대된다.

이러한 시각에서 볼 때, 향후 한미 사이버 안보협력은 사이버 안보 각 층위의 특성을 고려한 다층위적이고 입체적인 접근을 통해서 추진되어야 한다. 한미 사이버 안

보 동맹의 체결이라는 고층위 협력에만 시야를 고정하기보다는, 사이버 위협의 성격에 따라서 그 협력의 내용을 차별화하고 이를 유연하게 조합하여 최적의 방안을 찾는 접근이 필요하다. 다시 말해, 양국이 당면한 사이버 위협의 성격에 맞추어 저층위 협력이나 중층위 협력을 채택하는 것이 맞을지, 아니면 고층위 협력의 차원에까지 격상시키는 것이 맞을지를 고민하여 실용적인 협력 방안을 모색하자는 것이다. 무력분쟁 수준의 이하에서 발생하는 사이버 위협에 대해서 무작정 고층위 대응을 하는 것은 바람직하지 않고 실질적인 효과도 얻기 어렵다. 게다가 사이버 안보 분야의 협력은 저층위에서 중층위와 고층위로 나아가는 일방향 모델을 설정할 성질의 것도 아니다. 오히려 이 글에서 제시한 '창발에 대한 억지'의 개념을 원용하여 동태적으로 풀어가야 할 문제이다.

이 글에서 제시한 축적적 억지의 개념은 '창발과 피드백'의 상호작용이라는 구도에서 본 사이버 억지의 동태성을 담아내려는 시도이다. 미시적 수준으로부터 지속적으로 창발하는 사이버 위협의 수준에 맞추어 유연하게 피드백을 실행하자는 것이다. 사이버 억지의 개념이 효과적으로 작동하기 위해서는, 지정학의 문턱을 넘어서는 공격만 막겠다는 전통적 발상으로는 안 되고, 좀 더 동태적으로 전후방을 넘나드는 발상이 필요하다는 것이다. 그렇지만 축적적 억지의 개념이 저층위 수준으로 감행되는 모든 사이버 공격에 대해서 고층위 옵션을 동원해서 대응하는 것이 아님도 명심해야 한다. 이러한 점에서 축적적 억지의 개념은, 악의적 사이버 행위는 무력분쟁 이하의 수준에서 발생하더라도 그 근원에 가까이 다가가서 중지시키겠다는 '선제적 방어'의 개념과 구별된다. 다시 말해, '전방'만 보는 게 아니라 창발의 관점에서 '전방'과 '후방'을 동시에 보자는 것이다.

향후 한미 사이버 안보협력의 성공적 추진을 위해서는 사이버 억지의 새로운 개념화 작업을 넘어서 고려해야 할 과제도 많다. 예를 들어, 향후 한미 사이버 안보협력은 다영역 복합동맹으로 전개되고 있는 한미동맹의 포괄적 성격을 고려해서 추진되어야 한다. 최근 한미관계 자체가 정치군사 동맹의 단순한 성격을 넘어서 다양한 이슈들을 포함하는 복합적 관계로 발전하고 있다. 또한 사이버 안보 이슈의 외연과 내

포도 확장 및 심화하고 있다. 이에 따라 분야별로 양국의 역할분담 모델도 과거와 같이 한국의 일방의존 구도가 아니라 한미 상호의존의 구도로 변화하면서 한국이 일정한 역할을 담당해야 한다는 요구가 커지고 있다. 이렇듯 한미관계가 복합적으로 진화하고 있는 상황에서 단순히 '사이버 우산'을 빌려 쓴다는 수동적인 관점에서는 사이버 안보 분야에서 한미간의 협력 모델을 설정하기는 점점 어려워질 것이다. 이런 시각에서 보면 사이버 안보협력에서 한국이 미국에 기대할 것은 확장억지와 같은 '거시적 약속'이 아니라 다영역 억지의 개념에 입각해서 실용적인 협력 방안을 도출하는 '미시적 약속'일지도 모른다.

또한 한국이 사이버 안보협력을 추진함에 있어서 한미동맹이라는 양자관계에만 초점을 맞춰 논의를 협소화하기보다는 다자적 프레임에서 문제를 확장해서 보려는 노력이 필요하다. 한미 양자관계에만 매달리는 인상을 넘어서, 미국 이외의 다른 국가들과의 협력관계 설정도 적극적으로 고려하는, 즉 좀 더 넓은 의미의 '네트워크' 관점에서 사이버 안보협력의 문제를 볼 필요가 있다. 특히 최근 협력관계가 확대되고 있는 인도·태평양 지역 국가들과의 관계를 염두에 두면, 북한의 사이버 안보위협에 대응하기 위해서 한미동맹의 '링크'만을 강화하겠다는 발상은 다소 협소한 프레임 설정이라고 할 수 있다. 사이버 공격의 성격과 주체가 다변화되고 있는 최근의 양상을 제대로 이해하기 위해서는 다자적 억지의 개념을 적극 활용하여 사이버 안보협력의 구도를 넓혀서 볼 필요가 있다. 이러한 연장선에서 볼 때, 인태 지역뿐만 아니라 글로벌 차원의 국제기구 장에서 중견국으로서 한국의 사이버 안보 규범외교를 추진하는 것도 향후 큰 과제로 제기된다.

요컨대, 향후 한미 사이버 안보협력은 4차 산업혁명 시대의 한미관계를 새롭게 열어나간다는 미래지향적 시각에서 그 방향을 설정해야 할 것이다. 이러한 문제의식을 바탕으로 향후 한미관계의 연구는 기술·산업 분야에서는 반도체, 차세대 인프라, 인공지능, 양자기술, 원자력, 배터리, 그린테크, 바이오·제약 기술 등의 분야로 그 범위를 확장해야 할 것이다. 또한 우주 안보나 민군겸용기술, 자율무기체계 등과 관련된 첨단 군사기술 분야의 한미협력에도 주의를 기울여야 할 것이다. 이와 더불어 데이

터 및 플랫폼 경제 시대의 산업과 서비스, 그리고 미디어와 콘텐츠 분야의 한미관계에 관한 연구도 필요하다. 이러한 연구주제들을 탐구해 나가는 과정에서 전통적인 동맹국으로서 미국과의 관계를 어떻게 설정하고 발전시켜 나갈지의 문제는 중견국으로서 한국이 풀어야 할 제일 큰 외교안보적 숙제임이 분명하다.

참고문헌

1차 자료

국방부. "힘에 의한 평화 구현." 『2023년 주요 업무 추진계획』 (2023-01-11). https://www.korea.kr/docViewer/skin/doc.html?fn=3b343d5508949dce5cab8b86724ff5af&rs=/docViewer/result/2023.01/11/3b343d5508949dce5cab8b86724ff5af (검색일: 2023년 1월 28일)

대통령실 뉴스룸. "한미 정상, 전략적 사이버안보 협력 문서 채택." 『보도자료』 (2023년 4월 27일), https://www.president.go.kr/newsroom/press/TFsqADSy (검색일: 2023년 5월 6일).

법제처 국가법령센터. "사이버안보업무규정" https://www.law.go.kr/법령/사이버안보업무규정/(31356,20201231) (검색일: 2023년 5월 7일).

저서

김상배. 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 파주: 한울, 2018.

Arquilla, John and David Ronfeldt. *The Advent of Net War.* Santa Monica. CA: RAND Corporation, 1996.

Gartzke. Erik and Jon R. Lindsay (eds.) *Cross-domain Deterrence: Strategy in an Era of Complexity.* New York, NY: Oxford University Press, 2019.

Kello, Lucas. *The Virtual Weapon and International Order.* New Haven: Yale University Press, 2017.

Schneider, Jacquelyn G. "Deterrence in and Through Cyberspace." in Erik Gartzke and Jon R. Lindsay (eds.) *Cross-Domain Deterrence: Strategy in an Era of Complexity.* New York, NY: Oxford University Press, 2019.

Snyder, Glenn H. *Deterrence and Defense.* Princeton, NJ: Princeton University Press, 1961.

논문

민병원. "사이버공격과 사이버억지의 국제정치: 규제와 새로운 패러다임을 중심으로." 『국가전략』 제21권 3호 (2015).

박원곤. "미국의 인도·태평양 전략과 한미동맹: 통합억제와 전 세계 대비태세." 『한국국가전략』 제7권 2호 (2022).

Art, Robert J. "To What Ends Military Power?" *International Security* 4 (1980).

Borghard, Erica D. and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace." *Journal of Strategic Studies* (2021), DOI: 10.1080/01402390.2021.1944856

Brantly, Aaron F. "Entanglement in Cyberspace: Minding the Deterrence Gap." *Democracy and Security* 16-3 (2020). DOI: 10.1080/17419166.2020.1773807

Brantly, Aaron F. "The Cyber Deterrence Problem." in T. Minárik, R. Jakschis, L. and Lindström (eds.) *10th International Conference on Cyber Conflict CyCon X: Maximising Effects.* (Tallinn, NATO CCDCOE Publications, 2018).

Burton, Joe. "Cyber Deterrence: A Comprehensive Approach?" NATO Cooperative Cyber Defence Centre of Excellence (2018). https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf (검색일: 2023년 3월 24일).

Farrell, Henry and Abraham L. Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44-1 (2019). https://doi.org/10.1162/ISEC_a_00351

Fischerkeller, Michael P. and Richard J. Harknett. "Deterrence is not a Credible Strategy for Cyberspace." *Orbis* 61-3 (2017).

Gartzke, Erik and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24-2 (2015).

Hitchens, Theresa and Nilsu Goren. "International Cybersecurity Information Sharing Agreements" Center for International and Security Studies, University of Maryland (2017). https://www.jstor.org/stable/resrep20426#metadata_info_tab_contents (검색일: 2023년 3월 24일).

Jasper, Scott. "Deterring Malicious Behavior in Cyberspace." *Strategic Studies Quarterly* 9-1 (2015).

Jervis, Robert. "Deterrence Theory Revisited." *World Politics* 31-2 (1979).

Jung, Sung Chul, Jaehyon Lee, and Ji-Yong Lee. "The Indo-Pacific Strategy and U.S. Alliance Network Expandability: Asian Middle Powers' Positions on Sino-US Geostrategic Competition in Indo-Pacific Region." *Journal of Contemporary China* 30-127 (2021). DOI: 10.1080/10670564.2020.1766909

Lilli, Eugenio. "Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence." *Contemporary Security Policy* 42-2 (2021). DOI: 10.1080/13523260.2021.1882812

Lindsay, Jon et al, "Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity." *Journal of Cybersecurity* 1-1 (2015). DOI: 10.4324/978 1315225623-2

Lonergan, Erica and Mark Montgomery. "What is the Future of Cyber Deterrence?" *SAIS Review of International Affairs* 41-2 (2021). DOI: https://doi.org/ 10.1353/sais.2021.0018

Lupovici, Amir. "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives* 17-3 (2016).

Missiroli, Antonio. "The Dark Side of the Web: Cyber as a Threat." *European Foreign Affairs Review* 24-2 (2019).

Montgomery, Mark and Erica Borghard. "Cyber Threats and Vulnerabilities to Conventional and Strategic Deterrence." *Joint Force Quarterly* 102 (2021).

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace," *International Security* 41-3 (2016). doi:10.1162/ISEC_a_00266

Platte, James E. "Toward a Joint US-ROK Cyber Deterrence Strategy." *38 North Commentary* (2021) https://www.38north.org/2021/11/toward-a-joint-us-rok-cyber-deterrence-strategy/ (검색일: 2023년 1월 17일).

Ryan, N. J. "Five Kinds of Cyber Deterrence." *Philosophy and Technology* 31 (2018). DOI 10.1007/s13347-016-0251-1

Tor, Uri. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40-1/2 (2017). DOI: 10.1080/01402390.2015. 1115975

Wilner, Alex S. "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43-2 (2020). DOI: 10.1080/01402390.2018.1563779

보고서·미디어

김소정. "2022 한미정상회담과 사이버 안보: 억지력 강화를 위한 전략적 과제." 『국가안보전략연구원 Issue Brief』 제361호 (2022-05-31).

박춘식. "한미동맹을 사이버 안보까지 확장한 워싱턴 선언 '환영'." 『전자신문』, (2023년 05월 03일), https://www.etnews.com/20230503000172 (검색일: 2023년 05월 06일).

임종인. "한·미 사이버동맹 걸맞은 사이버 역량 갖춰야." 『중앙일보』 (2023년 05월 01일), https://www.joongang.co.kr/article/25159152 (검색일: 2023년 05월 06일)

Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report* (2020).

Soesanto, Stefan. "Cyber Deterrence Revisited." *Perspectives on Cyber Power* CPP-8. Maxwell Air Force Base, (Alabama: Air University Press, 2022).

U.S. Department of Defense, *2018 Department of Defense Cyber Strategies.* (2018)

U.S. Department of Defense, *National Defense Strategy of the United States* (October. 2022).

White House. *National Cybersecurity Strategy* (March 1, 2023).

A New Conceptualization of Cyber Deterrence: In the Reflective Context on the ROK-U.S. Cybersecurity Alliance Discourse

Sangbae Kim | Professor of Dept. Political Science and International Relations, Seoul National University

This paper attempts to refine the concept of "cyber deterrence" in the context of reflecting on the concept of deterrence on which the discourses on the ROK-U.S. Cybersecurity Alliance are based. The recent discourses on the ROK-US cybersecurity alliance is based on the idea of applying the traditional concept of deterrence to the cybersecurity field. However, considering the unique nature of cyberspace, the evolving U.S. deterrence strategies, and the future of ROK-U.S. relations as a whole, these attempts have limitations. The concept of cyber deterrence, which will be used by ROK-U.S. cybersecurity cooperation in the future, should go beyond the simple- system idea of applying the concept of traditional deterrence and use a flexible and integrated perspective considering the complex-system characteristics of cyberspace. Based on this awareness of the problem, this paper attempts a new conceptualization of cyber deterrence based on the conceptual work carried out in the existing U.S. policy circle and International Relations. In this process, this paper proposes to understand the concept of cyber deterrence in the dynamic composition of "emergence and feedback" that complex system theories have provided, and presents the concept of "cumulative deterrence against emergence" as a kind of "meta-frame" that encompasses existing concepts of cyber deterrence.

투고일: 2023년 03월 28일 | 심사일: 2023년 04월 18일 | 심사완료일: 2023년 05월 17일