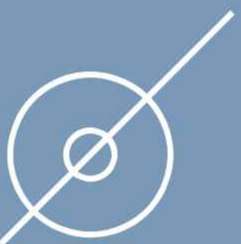
사이버 억지



2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 4호
발간일: 2023년 12월 27일

손한별 (국방대학교)

〈요 약〉

본 연구는 사이버 억지전략을 수립하기 위한 시론적 논의를 목적으로 한다. 사이버 공간은 이미 공격과 방어가 이루어지는 전장공간이지만 사이버 억지를 위한 이론적 논의는 크게 발전하지 못했다. 핵억지를 중심으로 발전해온 물리공간에서의 억지개념을 그대로 적용가능한 것인지, 사이버 공간만의 특수한 개념이 필요할 것인지에 대한 논쟁 수준을 벗어나 사이버 위협을 억지하기 위한 요건과 고려사항을 구체화할 필요가 있는 것이다. 이를 위해 본 연구는 사이버 공간의 전략적 특성, 공격과 방어의 수행방식, 사이버 억지의 개념과 발전과정, 사이버 억지의 대상, 내용, 방법 등에 대한 국내외의 다양한 논의를 다룬다. 본 연구는 먼저 사이버 공간에 대한 두 가지 관점이 있음을 전제하는데, “사이버 영역에서의 억지(in Cyber)”와 “사이버 영역을 통한 억지(through Cyber)”가 그것이다. 다음으로 사이버 억지의 핵심개념을 구체화하기 위해 누구로부터, 무엇을, 어떻게 억지할 것인가의 세 가지 질문을 제시한다. 첫째, 누구를 억지할 것인가에 대한 질문이다. 사이버 위협은 목적과 주체에 따라 구분할 수 있는데, 이는 위협 주체의 “귀속성”을 밝힐 수 있는지, 얼마나 신속하게 특정할 수 있는지의 질문으로 이어진다. 둘째, 무슨 행동을 억지할 것인가의 질문은 레드라인과 대응행동을 포함하는 억지 메시지로서 답할 수 있다. 상대에 대한 신뢰성있는 시그널링을 위해서는 대응행동의 “비례성”에 대한 검토를 요구한다. 셋째, 어떻게 억지할 것인가의 질문이 있다. 억지를 위한 다양한 개념과 방법들이 제시되었지만, 사이버 공격 전중후의 시간적 구분에 따라서 거부(Resistance), 응징(Retribution), 복원(Resilience)으로 억지 방법을 개념화할 수 있다. 그리고 억지를 위한 모든 방법과 수단은 “효과성”을 담보할 수 있어야 한다. 아울러 본 연구는 사이버 억지를 위한 정책제언으로, 사이버 억지를 위한 실질적인 능력 구비, 국가차원의 대응전략 수립, 국내 및 국제사회의 사이버안보 거버넌스의 정립을 제시하였다.

Ⅰ. 서론

상대로 하여금 내가 원하지 않는 행동을 하지 못하도록 하는 억지는 사실 “이상적” 개념이다. 전쟁에 대한 유인이 그대로 존재하는 가운데 잠재적인 공격자의 생각을 바꾸려는 노력이 성공할 수 있는지, 그것을 증명할 수 있는지에 대한 근본적인 회의가 있기 때문이다. 때문에 보푸르(Andre Beaufre 1965, 23)는 핵시기 이전의 억지는 단지 “승리할 수 있는 능력”을 갖추는 것을 의미했으며, 승리에 대한 기대치의 변증법에 의해서만 달성가능한 것이라고 말했다. 그리고 인류와 함께 시작된 전쟁의 오랜 역사 속에서 가공할 파괴력을 갖춘 핵무기가 등장한 최근에 이르러서야 비로소 “보복에 의한 억지(deterrence by retaliation)”가 실현가능해졌고, 억지는 국방안보의 중요한 의제로 등장했다.

핵무기의 등장 이후 강대국 간의 복잡한 억지 동학이 전략적 안정을 유지해온 냉전을 지나, 이제 사이버 공간(cyberspace)이 새로운 전략공간으로 등장했다. 단순히 정보를 저장하는 공간으로서 공격과 방어가 이루어지던 시기로부터 악성코드와 데이터, 조작된 정보가 지휘통제체계 전반에 혼란을 야기하며, 상대의 인식영역을 교란하고 변경하기에 이르렀다. 확대된 공간에서 새로운 주체가 새로운 수단과 방법을 적극적으로 활용하는 가운데, 국가안보 차원에서 사이버전 능력을 강화하며 전략적 우위를 달성하려는 노력이 지속되고 있다. 특히 미중의 신냉전, 핵무기의 확산과 고도화, 유럽과 아시아에서의 전통지정학의 부활과 함께 사이버전은 그 중요성을 더해가고 있으며, 사이버 공간은 전망가능한 모든 미래전 양상에서 핵심적인 위치를 점하고 있다.(김정기 2018, 254-267)

본 연구의 연구질문은 다음과 같다. 첫째, 사이버 공간은 새로운 전략공간인가, 어떠한 특성을 가지고 있는가? 공격우위의 공간인가? 둘째, 사이버 공간에서는 공격과 방어가 어떻게 이루어지는가? 사이버 안보전략은 어떠한 틀로 구성되어 있는가? 셋째, 사이버 공간에서의 억지란 무엇인가? 그 개념은 어떻게 발전해왔는가? 넷째, 사이버 억지의 핵심개념은 무엇인가? 누구로부터, 무엇을, 어떻게 억지한다는 것인가? 기존의 억지 개념들은 사이버 억지에서도 그대로 적용이 가능한가, 사이버 억지를 위한 새로운 개념이 존재하는가? 사이버 억지를 달성하기 위한 요건과 고려사항은 무엇인가?

위의 연구질문에 답하기 위해 본 연구의 구성은 다음과 같다. 2장에서는 사이버 공간에서의 공격과 방어를 다룬다. 기본적으로 공격과 방어를 결정하여 군사력의 사용방법을 선택하는 전략이 그대로 적용되는지 개념적으로 검토한 이후, 미국과 한국을 중심으로 사이버 안보전략이 어떻게 구성되어 있는지 확인한다. 3장에서는 억지 개념이 영역과 기능적으로 확대되고 있음을 살펴보고, 사이버 억지의 개념이 어떻게 발전해왔는지 보고자 한다. 4장에서는 사이버 공간의 특성을 고려한 사이버 억지의 특수성, 사이버 억지의 요건, 원칙, 방법, 개념 등을 종합적으로 검토하고, 5장은 결론을 대신하여 사이버 억지를 위한 몇 가지 제언을 제시한다.

Ⅱ. 사이버 공간에서의 공격과 방어

1. “공격우위”의 특수한 공간인가?

사이버 공간이 가지고 있는 특수한 환경은 기존의 공격과 방어에 대한 이론에 반론을 제기해 왔다. 인간이 만들어낸 사이버 공간은 자연공간과는 다를 것이라는 기대가 반영되기도 했다. 안보적 측면에서 사이버 공간은 다음과 같이 특성을 가진다. 첫째, 국가 외의 행위자가 공격과 방어를 위한 무력을 보유할 수 있다. 둘째, 첩보활동과 공격행위가 밀접하게 연계되어 있다. 셋째, 기본적으로 공격우위의 안보구조이다. 넷째, 의도와 관계없이 경로를 제공하며, 연루될 가능성이 있다.(장노순 2019, 7-10) 일부의 특성은 새로운 공간에 대한 이해와 적응이 부족하여 발생하는 과도적인 현상이기도 하지만, 네트워크와 정보신호로 구성된 사이버 공간이 가진 특수한 환경에서 비롯되는 것이다.(Dorothy Denning 2015)

특히 “불완전한 귀속(attribution) 문제”는 공격우위의 구조를 형성하는 가장 핵심적인 요인이다. 귀속 문제를 만드는 것은 다음의 세 가지 이유 때문이다. 첫째는 네트워크, 공급망, 사용자 등 사이버 공격에 다양한 수단이 사용될 수 있다, 둘째는 경로상 수없이 존재할 수 있는 가짜 깃발(false flags) 또는 우회기술 때문이다. 셋째, 정치안보적 이유로 인해 의도적으로 귀속을 밝히지 않을 수도 있다.(기세찬 2022, 193-195) 물론 기술이 발전하면서 귀속 문제는 점차 해소될 것으로 예상되지만,(Thomas Rid and Ben Buchanan 2015, 31) 사이버 공간의 특수한 환경이 주는 제약은 지속될 수밖에 없다.

하지만 아직까지는 ‘사이버 전쟁(cyber war)’으로 불릴만한 충돌이 없었던 것이 사실이기 때문에, 공격이 우위를 가진다고 단정짓기는 어렵다. 현재까지는 주제 측면에서 사이버범죄나 사이버테러, 유형 측면에서 사이버 첩보활동, 수준 측면에서 사이버 분쟁 수준에 머물고 있기 때문이다. 하이브리드전의 가장 최근 사례인 우크라이나-러시아 전쟁에서도 사이버전은 “전쟁개시 성격의 전초전”, “물리적 공격과의 협동작전”으로 나타났다.(송태은 2022, 222-225) 따라서 과연 “사이버 전쟁”이라고 명명할 수준의 공격과 방어가 사이버 공간에서 이루어질 것인지, 공격우위의 공간인지에 대한 평가는 아직 이르다,

그런 의미에서 전통적인 공격과 방어 이론이 사이버전에도 적용되는지는 논쟁적이다.[1] 사이버전이 정보전의 하위 요소로 인식되던 시기에도 네트워크 기술은 일정한 공간을 형성하는 기술로 인식되었고, 핵심 노드(node)에 대한 집중적인 공격과 방어가 정보전의 성패를 결정했다. 이러한 기술과 환경은 항공무기가 등장하면서 발전한 항공전의 양상과 유사하다.(마틴 반 크레벨드 2018, 174-182) 여전히 상대의 중심(重心)을 타격하는 것은 상대의 의지를 굴복시키는 전쟁의 목적을 달성하는 가장 유력한 수단이다. 또 기습의 효과는 일회적이며 방자는 이점을 활용하여 공세를 이전할 수 있다. 그러나 반면에 사이버 공간이 가지고 있는 엄청난 속도와 자동성, 질적 우위의 절대성, 파괴력보다는 정확성이 요구되는 특수성이 있으며, 사이버 공간이 기존의 물리적 공간에 대한 의존성을 낮추게 된다면 사이버 공간에 대한 완전히 새로운 이론을 요구하게 될 것이다.

2. 사이버 안보전략의 틀

1) 클라우제비츠가 일관되게 “방어가 공격보다 강한 형태의 전쟁”이라고 강조한 것은 전쟁의 시작으로부터 종결에 이르는 전 과정을 살펴보면 타당하지만,(박창희 2013, 148-152) 혁신적인 공격무기가 등장한 초기 전역에서는 분명히 공격이 우세했으며, 새로운 공격무기는 상대에게 충격과 손실을 강요했다. 또한 그 실질적 효과와 관계없이 정책결정자의 오판을 야기하기도 한다. 이른바 “공격의 신화” 시기가 존재한다는 것이다.(Stephen van Evera 1999, 194-198)

사이버 공간의 특수성에 대한 논쟁이 지속되고 있으나,[2] 각국의 사이버 안보전략은 여전히 새로운 공간적 특성에 적응 중이다. 여전히 사이버 전쟁보다는 사이버 테러 또는 분쟁에 대한 대응과 억지에 초점이 있기 때문이다. 하지만 각국은 2007년 에스토니아에 대한 공격 이후 사이버 위협의 존재를 분명히 인식하고 있는데, 다음과 같은 전제를 공유하고 있다. 첫째, 국가안보를 위협할 수준의 사이버 공격이 가능하며, 이는 국가의 안보와 경제에 막대한 피해를 입힐 수 있다. 둘째, 국가 주요기반시설이 사이버 공격에 매우 취약한 수준에 있다. 셋째, 사이버 범죄나 공격이 특정 국가의 후원 아래 이루어질 수 있으므로 국가 차원에서 포괄적으로 대응방안을 논의해야 한다.(임종인, 김근혜 2021, 168)

미국의 전략문제연구소(CSIS)는 글로벌 사이버 전략지수(Global Cyber Strategies Index)를 제공하고 있는데, 사이버 위협에 대한 국가적, 조정된 억지력 및 대응에 대한 포괄적 교리로서 국가전략을 발표한 국가는 현재까지 78개국에 이른다.[3] 이와 함께 군사, 컨텐츠, 프라이버시, 중요 인프라, 상업, 범죄 등으로 구분하여 각 기능별 사이버 전략을 보유하고 있는 국가들에 대한 데이터를 제공한다. 이들 국가들이 보유하고 있는 전략의 종류를 통해서도 관심사를 파악할 수 있지만, 각국은 사이버 위협환경, 지정학, 국내정치 및 사회, 인식 수준 등에 따라서 범위와 접근방식에 차이가 있다. 이러한 국가별 차이에도 불구하고 사이버 안보전략이 다루는 의제와 범위는 확대되고 있다.

임종인과 김근혜(2021, 172-177)는 지난 10년간 전세계 10개국이 발간한 국가 사이버안보 전략을 분석하여 국가별 전략이 가지고 있는 공통적인 핵심요소를 다음과 같이 제시하였다. 주요기반시설 보호, 사이버안보문화 촉진, 사이버 범죄 대응, 사이버 외교, 민-관 협력, R&D 촉진, 훈련 및 교육 프로그램, 사이버보안 비상태세 준비, 사이버보안 훈련, 국가 사이버 위기관리 및 사이버안보 긴급사태 계획, 사이버안보 거버넌스, 디지털 경제 육성, 사이버 군사 및 방첩활동 등이다. 한국 정부가 최초로 발간한 『국가사이버안보전략』에서는 국가 핵심인프라 안전성 제고, 사이버공격 대응역량 고도화, 신뢰와 협력 기반 거버넌스 정립, 사이버보안 산업 성장기반 구축, 사이버보안 문화 정착, 사이버안보 국제협력 선도 등 6개 전략과제를 제시하였다.(청와대 국가안보실 2019)

사이버전(cyber warfare)과 직접 관련된 일부 전략서의 내용을 살펴보자. 먼저 미국 의회 산하의 “솔라리움위원회”(US Cyberspace Solarium Commission)의 최종보고서에서는 “다층화된 사이버 억지(layered Cyber Deterrence)” 전략을 제시했는데, 행위 조성(Shape Behavior), 이익거부(Deny Benefits), 비용부과(Impose Costs)로 구성된다. 미국 국방부가 작성한 『사이버전략』도 분명한 목적을 제시했는데, 무력충돌 이하의 활동을 비롯하여 악의적인 행동을 교란 또는 중지시키는 전진 방어(defend forward), 미군의 이점에 기여하는 네트워크와 시스템의 보안과 복원력 강화, 상호이익 증진을 위한 기관, 산업계, 국제파트너와의 협력, 전시 사이버부대의 합동작전 수행, 공세적 사이버능력과 혁신적 개념의 발전을 제시했다.(Department of Defense 2018, 1) 한국의 『국가사이버안보전략』도 두 번째 전략과제인 “사이버공격 대응역량 고도화”에서 세 가지의 목표를 분명히 제시하고 있는데, 효율적 억지, 능동적 대응, 대응역량 확충이 그것이다.

각국의 특수성을 반영하고는 있지만 잠재적이지만, 분명하게 상대를 상정하고 의도적인 위협에 대한 억지와 대응을 전제하고 있음을 알 수 있다. 개인이나 해커 그룹이 주도하는 소규모

2) 일반적으로 거론되는 사이버 공간의 특성은 익명성(anonymity), 복잡성(complexity), 공개성(open access), 연결성(interconnectivity), 책임회피성(juristical diffusion) 등이다.(Alex Wilner 2022, 252)

3) https://csis-website-prod.s3.amazonaws.com/s3fs-public/220414_Cyber_Regulation_Index.pdf

범죄나 테러가 아니라 국가가 개입, 지원하는 상황에 대한 심각성을 인식하고, 적대적인 의도를 가진 국가가 군사적 이점을 잠식하고, 인프라를 위협하며, 경제적 번영을 감소시키는 장기적이고 전략적인 경쟁(competition)을 계속하고 있음을 전제하고 있다. 미국의 "경쟁 연속체(Competition Continuum)"에서 사이버전은 가장 먼저, 가장 빈번하게 활용되며,(US JCS 2019, 2-7) 중국의 "초한전"에서도 사이버전은 군사와 비군사 영역을 연결하는 "超군사" 영역에서 핵심적인 위치를 차지한다.(차오량, 왕상수이 2021, 139) 따라서 각국의 사이버안보전략은 사이버 공간의 특성 뿐만 아니라 사이버 위협이 발생하는 시기와 양상을 반영하여 전략을 수립하고 갱신하고 있다.

Ⅲ. 사이버 공간에서의 억지

실제 공격이 일어나기 전에 위협을 억지하려는 목표는 갈수록 중요성을 더하고 있다. 각국의 사이버안보전략을 다룬 문서들에서 "사이버 억지"는 최우선 과제로 제시된다. 다만 사이버 억지란 무엇인지, 어떻게 달성할 것인지에 대해서는 서로 다른 인식을 갖고 있다. 사이버 위협의 목적, 시기, 양상이 결코 사이버 공간 내에 한정되지 않는다는 점에서 사이버전은 사이버 공간에서의 공격과 방어 차원에 머무르지 않는다. 또한 전략과 기술의 발전에 따라 사이버 위협 대응의 목표와 방법도 달라진다. 상대보다 앞서, 유리한 지점을 확보하려는 경쟁은 새로운 전략공간인 사이버 영역에서 더욱 적극적으로 이루어지며, 사이버 공간에서의 위협적인 행동을 단념시키려는 사이버 억지의 중요성도 부각된다.

1. 억지 개념의 확대와 사이버 공간

핵무기의 대량사용을 억지하는 것으로부터 시작된 냉전기 억지 개념은 비교적 달성하기가 쉬웠다. 지역 국가간 분쟁도, 낮은 단계의 무력충돌도 핵무기가 사용되는 수준에 이르는 확전사다리(escalation ladder)를 상정하고 있었기 때문이다. "안정-불안정의 역설"은 낮은 단계의 전술적 충돌은 빈번할 수 있음을 전제하지만, 언제 어떻게 핵사용으로 비화될지 모른다는 불안감은 안정과 불안정 사이의 불분명한 공간을 넓히며 모든 종류의 충돌을 억지해왔다. 따라서 특정한 행동을 하지 못하도록 억지하고, 일단 발생한 공격을 확전되지 않도록 억지하는 것을 동시에 달성할 수 있었다.

상대를 강압하기 위한 것이든, 전쟁의 참화를 막아야 한다는 열망에 의한 것이든 억지에 대한 요구는 지속되었지만, 탈냉전과 함께 억지의 개념은 변화해왔다. 21세기 들어 안보환경의 몇 가지 중요한 변화에 기인하는데, 강대국 핵경쟁의 부활과 새로운 핵보유국으로의 확산, 다양한 형태의 테러리즘 등장, 사이버 공격의 증폭과 사이버전에 대한 전망, 새로운 무기기술의 증가와 확산 등이다.(Patrick Morgan 2019, 50) 이러한 복잡하고, 어려우며, 예측과 관리가 불가능한 안보환경의 변화는 완전히 새로운 억지 개념을 필요로 하기도 하지만, 냉전기 핵억지의 근간을 유지해온 보복억지의 압도적 논의에서 한발 물러나 있던 거부에 의한 억지(deterrence by denial)와 같이 개념들이 다시 강조되기도 했다.

일반적으로 상대의 비용-편익 계산에 영향을 미쳐야 하는 억지의 성공요소는 능력, 신뢰성, 전달로 정리하지만, 이를 정확히 측정하기는 어렵다. 억지는 "만약 네가 특정한 행동을 한다면, 이러한 결과를 맞게 될 것"이라는 메시지가 분명하고 신뢰성있게 전달되어야 하는데, 억지하고자

하는 대상은 누구이며, 어떤 행동을 억지하려는 것인지, 이를 위해 어떤 능력이 필요한지, 어떤 방법과 수단이 사용될 것인지, 또 어떻게 보복을 하겠다는 것인지를 분명히 하지 않다면, 단순히 상대가 예상되는 위해를 가하지 않았다고 해서 억지가 성공적으로 달성되었다고 보기 어렵다.[4)]

이러한 어려움은 억지의 대상, 방법과 수단이 각각 범위를 알 수 없는 스펙트럼을 가지게 된 데서 비롯된다. 억지는 네 번의 큰 물결을 거쳐 현재와 같이 크게 확대된 개념을 갖게 되었다.(Alex Wilner 2020, 250-251) 첫째, 억지해야 할 대상과 함께 억지를 위해 함께 행동할 수 있는 행위자가 동시에 확대되었다. 둘째는 억지해야 할 위협, 억지와 대응을 위해 사용할 수 있는 방법과 수단이 동시에 확대되었다. 셋째, 공격자와 억지자가 동시에 운신할 수 있는 공간이 크게 확대되었다. 억지를 위해서는, 누구를 억지할 것인가? 무슨 행동을 억지할 것인가? 어떻게 억지할 것인가?의 질문에 대답할 수 있어야 한다. 그러나 사이버 영역의 발전을 비롯하여 이러한 질문에 답하기가 더욱 어려워진 상황이 된 것이다.

그리고 억지를 가장 어렵게 하는 것은 사이버 능력이 사이버전 뿐만 아니라 전쟁의 모든 측면을 결정하게 되었기 때문이다. 사이버 능력은 새로운 공간에서 다양하게 활용할 수 있지만, 억지의 계산을 더욱 복잡하게 만든다. 항공기나 미사일 공격을 교란, 방어, 무력화할 수 있고, 상대의 정보작전을 교란하거나 방해하며, 정부 통치기능이나 사회 기반시설을 교란하여 전쟁지속능력에 타격을 줄 수도 있다. 또한 거의 즉각적으로 운용이 가능하다는 점에서 상대의 행동 이전에 예방공격이나 선제공격에 적극적으로 활용될 수도 있다. 결국 사이버 공간을 어떻게 활용하느냐에 따라 억지의 효과성이 결정된다.

2. 사이버 억지의 역사적 발전

사이버 공간에서 상대를 억지할 수 있을 것인지에 대한 질문은 많은 연구자들의 관심을 받아왔다. 위에서 살펴본 바와 같이 대부분 국가의 사이버안보전략이 사이버 억지를 핵심목표로 제시하고 있지만 모두 같은 의미를 담고 있는 것은 아니다. 주요 사건에 따라 사이버전의 시기를 구분하며, 사이버 억지는 이러한 사이버전의 변화에 따라 결정된다.(Omry Haizler 2017) 사이버 억지는 다른 영역보다 비교적 짧은 역사를 가지고 있지만 급격한 기술의 발전에 따라 사이버전과 함께 개념이 변해왔으며, 재래식 억지와는 차별성을 가지고 발전해왔다. 이는 무엇보다 “사이버”가 체계, 플랫폼, 영역, 또는 단순 형용사로 각기 다르게 사용되어 왔으며, 서로 다른 인식에서 비롯되기 때문이다.(Jacquelyn Schneider 2019, 96-100) 사이버 억지의 발전을 시기별로 개념화하면 아래와 같다.

• **연결성에 대한 공격과 보호 :** 초기의 사이버전은 정보전의 일환으로만 인식되었다. 유선 수단에 의해서만 통신이 이루어지던 시기에는 “사이버”라는 용어 자체가 빈번히 사용된 것은 아니었다. 1970년과 1980년대에는 상대의 통화를 도청하거나, 통화 상대를 몰래 바꾸거나, 전화벨을 계속 울리게 하여 통화 시도를 차단하는 등의 활동이 시도되었다. 이 시기의 사이버 억지는 공격자의 동기와 능력에 초점을 맞추어, 공격, 재활, 재범과 같은 범죄학의 개념들이 사용되었다.(Stefan Soesanto and Max Smeets 2021, 387) 네트워크를 안정적으로 보호하는 것이 무엇보다 중요했으며, 억지는 ‘잘 수행된 방어’의 다른 이름으로 사용되었고, 이는 연결성

4) 억지는 상대의 인식(perception)을 변화시키는 것이고, 따라서 상대의 신념과 예상에 영향을 끼치고, 충분한 보상과 보증을 통해 단념시키는 것도 포함된다.(Michael Mazarr 2018)

(connectivity)에 국한된 공격과 방어를 의미한다.

• **저장정보의 파괴와 교란 :** 이후 인터넷의 등장과 함께 사이버전의 개념도 확대되었는데, 이는 네트워크 자체 뿐만 아니라 저장된 정보에 접근할 수 있게 되었음을 의미한다. 당시 발전하고 있던 컴퓨터, 무선 및 유선통신 수단, 네트워크 장비는 모두 공격할 수 있는 지점으로 식별되었다고, 정보전을 통해 상대를 교란, 파괴, 조작할 수 있게 되면서 사이버전의 개념은 한 단계 발전하였다. 상대의 인식을 변화시키고, 국내 불안정을 야기하며, 국제사회의 여론을 결집하는 행동은 억지의 가능성에 대한 인식의 단초를 제공했다.(John Arquilla and David Ronfeldt 1993) 그러나 여전히 사이버 억지보다는 공격과 방어에 관심이 있었다.

• **사이버 공간의 군사화 :** 많은 연구들은 2007년 에스토니아에 대한 DDoS 공격이 사이버전 연구에 있어 중요한 기점이 되었다고 본다. 실제로 사이버 공격이 취해지는 “공간”으로서 인식되기 시작했고, 약자조차도 상대의 취약성을 공략하여 굴복시킬 수 있다는 것을 확인한 것이다. 진정한 의미에서 사이버전이 가능하다는 인식은 사이버 억지에 대한 관심을 이끌었다. 활발한 연구 사이에서 사이버 억지는 기존의 억지 개념으로 이해가 가능한지, 또는 특수한 개념이 필요하다는 논쟁이 있었다.(Dorothy Denning 2015, 11-12) 나아가서는 사이버 영역의 특수성을 강조하여 사이버 억지는 여전히 실현불가능한 개념이라는 주장도 존재했다.(Richard Harknett and Michael Fischerkeller 2017)

• **사이버 억지의 범위 확대 :** 이같은 논쟁은 사이버 억지의 범위에 대한 서로 다른 이해에서 비롯되는 것이기도 한데, 사이버 수단으로 모든 군사적 공격을 억지하는 것인지, 다른 모든 군사력을 활용하여 사이버 공격을 억지하는 것인지, 오직 사이버 수단에 의해 상대의 사이버 공격을 억지하는 것인지에 대한 이해가 다르기 때문이다. 이러한 논쟁 역시 사이버 수단에 의한 범죄행위나 사이버 수단을 하나의 군사수단으로 보던 것에서, 사이버 공간을 새로운 공간으로 보는 인식으로 확대되어 왔기 때문이다.(Dorothy Denning 2015, 11-12)

• **새로운 주제의 탐색 :** 향후 사이버 억지에 대한 논의를 다음의 네 가지로 분류한 소산토와 스미트(Soesanto and Smeets, 394-396)의 연구는 중요한 관점을 제공한다. 첫째는 사이버 억지를 보다 넓은 차원에서 다영역 또는 교차영역 억지의 일환으로 이해하는데, 포괄적 범위의 억지에서 디지털 기술의 역할에 주목하는 것이다. 둘째는 전체적인 공격과 방어에 기여하는 사이버 작전 자체를 바라본다. 셋째는 억지로부터 강제(compellence)로 관심을 전환하여, 사이버 능력은 상대의 행동을 저지하는 데 그치지 않고 보다 공세적인 목적을 갖고 특정한 행동을 하도록 압박할 수 있다는 것이다. 마지막으로 전략적 경쟁자와의 접촉을 지속하면서 사이버 영역에서 우세를 달성한다는 “지속적 개입(persistent engagement)”은 일회적인 억지가 아니라 장기적 경쟁의 관점에서 바라본다.

위에서 살펴 본 사이버 억지 개념의 변화는 주로 미국 사이버 억지의 변화였다는 점에서, 알렉스 윌너(Alex Wilner 2020, 269-273)가 미국 사이버 억지의 변화로부터 도출한 몇가지 교훈은 일반론으로 확대가능할 것이다. 첫째, 거부에 의한 억지로부터 보복에 의한 억지로 초점을 전환해왔는데, 이는 기술발전에 따라 다양한 차원에서 보복공격이 가능해진 상황을 반영한다. 둘째, 하지만 거부와 보복은 상호보완적인 수단으로 작동해왔으며, 실제 전투의 현장에서는 명확하

게 구분되지도 않는다. 셋째, 공격의 귀속을 밝히는 것은 보복을 가능하게 함으로써 억지 효과를 높이는 방향으로 발전해왔다. 넷째, 사이버 억지는 군사적 강압보다는 유관부서와의 협력적 행동으로 역할해왔다. 다섯째, 사이버 억지는 군이나 정부 뿐만 아니라 민간 영역과 중첩하면서 국가 차원의 통합을 요구하게 되었다.

Ⅳ. 사이버 억지의 핵심개념

1. 사이버 공간에 대한 두 가지 관점

사이버 공간의 특수성 때문에 사이버 억지가 달성가능할 것이냐의 논쟁은 지속되었지만,[5] 사이버 기술과 전략개념의 발전에 따라 억지의 실효성에 대한 평가는 긍정적인 방향으로 전환되었다. 위협과 공격의 주체를 식별할 수 있는 기술이 발전하고 있고, 억지 실패 시에도 활용할 수 있는 다양한 공격 및 방어무기가 존재하며, 억지의 신뢰성이 경험적으로 검증되고, 보복 의지를 전달할 수 있는 수단이 충분하다는 점을 들 수 있다.(송운수 2022, 61-63) 핵무기와 같은 가공할 파괴력을 갖춘 무기처럼 직관적으로 억지를 달성하기는 어렵겠지만, 보다 정교한 방법과 수단에 의해서 억지를 달성할 수 있다는 것이다.

새로운 전략공간으로서만 인식되던 사이버 공간은 이제 다른 모든 영역과 연결된다. 사이버 공간을 보다 좁게 인식하느냐, 확장하여 인식하느냐에 따라 사이버 억지의 개념도 대별된다. 사이버 공간은 최초에는 별도의 공간으로 존재하다가 다른 영역과 연결되고 역할이 확장되었으며, 현재 미국이 추진하고 있는 "통합억지(Integrated Deterrence)"의 개념이 사이버 억지를 포함한다는 주장은 정책적으로 타당하다.[6] 다만 사이버를 별도의 공간과 기능으로 구분하는 것은 개념을 엄밀하게 이해하고 실효성있는 방법과 수단을 고안하는데 도움이 된다. 이러한 구분에 따라 억지의 대상이 사이버 공간 내부인지, 외부인지, 다른 한편으로 억지의 수단이 사이버인지 그 외의 것인지에 따라 4개의 억지 유형이 만들어질 수 있다.(Erica Lonergan and Mark Montgomery 2021, 64-67)

사이버 공간에 대한 관점을 두 가지로 보다 단순화해보면, 사이버 억지에 대한 두 가지 관점이 있다.(Jacquelyn Schneider 2019, 96-100) 첫째, "사이버 영역에서의 억지(in Cyber)"는 협의의 사이버 억지로, 즉 사이버 공격을 사이버 능력을 활용하여 억지하는 것을 의미한다. 사이버 공간의 특수성에 초점을 두어, 사이버 기술에 의존하여 특별한 개념을 발전시킬 것을 요구한다. 하나의 영역(domain)은 고유의 공유된 지식, 기술, 경험, 훈련, 능력, 목표 등을 가지고 있기 때문이다.(Patrick Morgan 2019, 50) 특히 사이버 공격은 높은 불확실성이라는 특징을 가지고 있는데, 비밀스러운 선제공격에 활용될 수 있고, 급격한 확전의 가능성은 낮으며, 정교하게 표적을 공략할 수 있기 때문에 "비밀 군사작전"과 그 특징을 같이 한다. 반대로 공격을 억지하는 입

5) 전통적으로 억지를 위해서는 분명한 물리적 충돌, 행위자의 합리적 계산, 분명한 책임귀속성, 충분한 보복, 능력의 분명한 현시, 보복에 대한 통제능력 등의 요건이 갖추어져야 하지만, 사이버 공간에서는 비물리적 작전, 다양한 행위자, 비용-편익분석의 어려움, 비대칭적-다자간의 상호작용, 지속적인 변동성, 모호성에 기반한 전략 등을 강조한데서 차이가 있다.(Mariarisaria Taddeo 2018, 340).

6) "사이버 진주만" 같은 사건이 아직 일어나지 않았고, 사이버 공간에서만 효과적으로 작동가능한 억지수단은 존재하지 않으며, 현재 시급한 위협에 대응하기 위해 사이버 능력이 절대적이라는 점에서 통합억지에 방점을 두어야 한다는 주장은 현재 미 국방부의 상황인식을 반영한다.(James Van de Velde 2023)

장에서도 특정 국가의 압도적 우세가 보장되지 않고, 이를 상대에게 인식시키는 것도 어렵기 때문에 사이버 영역에 국한된 특별한 개념이 필요하다는 것이다. 그러나 이론적 차원에서 사이버 공간을 기타 영역에서 분리할 수 있다고 하더라도, 실제 운용의 차원에서는 이를 분리할 수 없다는 비판이 있다.[7)]

둘째, "사이버 영역을 통한 억지(through Cyber)"는 광의의 사이버 억지로, 사이버 억지를 통해 다른 영역에서의 공격을 억지하는 것을 의미한다. 다른 한편으로는 사이버 영역에서의 능력과 의지만으로는 모든 사이버 위협을 억지할 수 없다는 인식도 포함한다. 데닝의 주장처럼 지상억지, 해상억지, 우주억지라는 말이 존재하지 않는 것처럼 사이버 억지라는 말은 합당하지 않을 수 있다. 사이버 공간 역시 일정한 지형과 영역, 연결지점 등을 가지고 있으며, 이를 통해 다른 영역들과 연결된다.(Dorothy Denning 2015, 11-12) 사이버는 국가와 사회의 다른 모든 영역을 연계하고 있으며, 이제 사이버 영역을 거치지 않고서는 어떠한 운용도 불가능하다. 이는 다른 영역과의 통합을 통해서만 효과적인 억지가 가능하다는 인식은 "교차영역억지(Cross-Domain Deterrence)"(Jon Lindsay and Erik Gartzke 2019) 또는 "복합억지(Complex Deterrence)"(T.V. Paul et al. 2009)의 논리를 제공한다. 미 국방부의 최근 『사이버전략』은 군사능력이 "국력의 다른 수단들과 통합하여 사용될 때 가장 효과적이며, 각 부분의 합보다 더 큰 억지력을 창출한다"는 것을 분명히 하고 있다.(DoD 2023, 2)

2. 사이버 억지를 위한 세 가지 질문

사이버 억지의 성공을 어떻게 판단할 것인가에 대한 일반적인 정의는 없지만, 소산토(Stefan Soesanto 2022, 20-24)는 공세적인 행동을 시도하지 않거나, 공격을 당했다고 하더라도 사이버 또는 그 외의 영역에서의 대응을 통해 즉각적으로 종결하도록 하거나, 혹여 잘못된 대응을 통해서라도 미래 상황에 대한 신뢰성있는 평판을 획득하거나, 기타 특정한 행위를 차단할 때 억지가 성공했다고 판단하였다. 아울러 제1격에 대해 자위권적 대응을 하지 못하거나, 먼저 선제공격을 취하거나, 전략적 시그널링이 붕괴하거나, 공격에 대한 비례적 대응이 이어져 확전하게 된다면 억지에 실패한 것이라고 규정하였다.

그러면 사이버 억지의 성공을 위해서는 무엇이 필요할 것인가? 2017년 미국 하원 군사위원회에서 마틴 리비키(Martin C. Libicki 2017, 1-2)가 제시한 사이버 억지의 성공을 위한 네 가지 능력은 중요한 기준을 제공한다. 첫째, 정확하게 사이버 공격자의 귀속을 밝힐 수 있는 능력. 둘째, 효과적으로 레드라인을 전달할 수 있는 능력. 셋째, 상대가 레드라인을 넘었을 때의 신뢰성 있는 대응. 넷째, 성공적으로 보복할 수 있는 능력이다. 리비키의 기준을 바탕으로 아래의 질문에 차례로 대답함으로써 사이버 억지의 성공을 위한 핵심개념들을 살펴보자.

(1) 누구를 억지할 것인가?

7) 미국 국방부가 발표한 『Cyber Strategy 2023』은 사이버는 『국방전략서』가 도입한 "통합억지"를 위한 "Campaigning"의 중요한 도구 중 하나임을 분명히 하면서, 2015년 전략서의 사이버 억지, 2018년의 "전진방어" 개념을 포기한 것은 아니지만 도구적 의미를 명확히 했다. 이는 사이버 영역 내에서의 혁명적인 변화를 전망했던 데에서 벗어나 다른 영역과의 연계성이라는 현실을 인정했음을 의미한다. 전문가들은 "고립된 상태에서 비축된 사이버 역량은 억지 효과가 거의 없다"는 선언은 "더 이상 사이버를 위한 사이버는 없다(Cyber for Cyber's Sake)"는 것을 분명히 한 것이라고 강조한다.(Emerson Brooking and Erica Lonergan, 2023)

사이버 공간에서 발생하는 국가이익의 침해행위는 다양한 행위자에 의해서 이루어진다. 비국가 행위자에 의한 사이버 범죄나 테러는 전세계 위협평가에서 빠지지 않는다. 최근 미국 정보당국의 위협평가에서도 다국적 조직이 랜섬웨어 공격을 지속적으로 실시하여 자금을 탈취하고, 중요한 서비스를 중단하며, 중요한 데이터를 노출하고 있음을 명시하고 있다. 특히 2022년에는 기존의 데이터 암호화 방식으로부터 데이터 공개 위협을 통해 보상을 요구하는 비즈니스 모델을 발전시키고, 가상 시스템 저장장치와 같은 광범위한 대상에 영향을 미치는 멀웨어의 기능을 개선했다고 분석했다. 또한 이들은 정부 조치와 국민 관심에 따라 운용을 중단했다가도 조직명을 변경 또는 재구성을 통해 활동을 재개한다고 밝혔다.(DNI 2023, 31)

그러나 사이버전(cyber warfare)으로 명명했다는 사실은 사이버 위협이 개인이나 범죄집단이 아니라 특정 정부의 행동과 결부되어 있으며, 국가의 무장력을 수단으로 대응해야 함을 의미한다. 정부의 입장에서는 다른 정부에 의한 사이버 위협이 더욱 우려될 수 밖에 없는데, 이미 적대적 의도를 가지고 있고 위해를 끼칠만한 능력을 보유하고 있기 때문이다. 2007년 에스토니아에 대한 사이버 공격, 2008년 조지아에 대한 공격, 2010년 이란 핵시설에 대한 스턱스넷 공격, 2009년 북한의 DDoS 공격, 2014년 크름반도 합병시 하이브리드 공격 등은 모두 국가에 의해 실행된 사례이다.

사이버 위협은 목적과 주체에 따라서 구분할 수 있는데, 위협의 주체는 국가, 집단, 개인으로, 목표는 물리적 파괴, 시스템 교란, 자원의 획득 등이다. 이들을 조합하면 사이버 전쟁, 사이버 테러, 사이버 교란, 사이버 간첩, 사이버 범죄의 5가지 유형으로 구분할 수 있다.(김상배 2018, 122) 가장 중요한 것은 국가행위자가 정치적, 안보적 의도를 가지고 있는지가 사이버 갈등과 사이버 범죄를 구분하는 기준이 되지만, 이를 신뢰성있게 확인할 수 있느냐의 귀속성 문제는 여전히 남는다. 때문에 사이버 억지가 사이버 공간에서 벌어지는 모든 공격적 행위를 억지하기를 기대하는 것은 비현실적이라는 비판 역시 지속적으로 제기된다.

• **위협의 목적 :** 사이버 위협의 목적에는 군사적 공격, 외교적 강압, 첩보활동, 공급망 점유(장노순, 11-17) 등이 있고, 목표 수준에 따라서는 단기적 파괴와 교란, 이익과 자원의 획득, 장기적 우세 확보 등이 있을 수 있다. 국가 수준의 위협이라면 그것이 사이버 영역이든 아니든 분명한 “의도”에서 비롯된다. 따라서 억지를 위해서는 위협 주체의 상황인식과 의도가 무엇인지를 정확히 파악하고, 그것을 단념시키는 것이 중요하다.(Timothy M. McKenzie 9-10) 다만 위협의 주체와 목적 등을 공개하는 것은 불필요하게 국민을 불안하게 만들 수 있고, 공격과 방어 무기의 구분 불가능성 때문에 사이버 안보딜레마가 증폭될 수 있다.(Guy-Philippe Goldstein 2013, 126-127)

• **위협의 주체 :** 사이버 기술은 접근성이 높기 때문에 누구나 위협의 주체가 될 수 있다. 물론 아직은 레온 파네타(Leon Panetta)가 경고한 “사이버 진주만”, “사이버 9.11”, “사이버 아마겟돈”, 영화에서도 등장한 바 있는 “파이어세일” 등은 일어나지 않았지만 언제든지 재앙적인 결과를 가져올 수 있는 사이버 공격이 시작될 수 있다. 때문에 미국은 전략문서에서 지속적으로 러시아와 중국, 북한 등의 국가행위자 뿐만 아니라 사이버 공간에서의 개인과 집단 행위자의 위협 변화를 분석해왔다. 비국가 행위자를 억지하기 위한 강력한 수단은 존재하기 어려운 것은 사실이지만 완전히 불가능한 것은 아니다. 테러리스트와 같이 “스스로 기꺼이 목숨을 내어놓는다고 하더라도 헛된 공격 중에 죽고 싶지는 않을 것”이라는 분석은 비국가 행위자에 대한 억지가 불가능하지는 않음을 주장한다.(Paul Davis and Brian M. Jenkins 2002).

'누구를 억지할 것인가'의 질문은 자연스럽게 위협 주체의 "귀속성"을 밝힐 수 있는지, 얼마나 신속하게 특정할 수 있는지로 이어진다. "귀속의 딜레마"는 특히 사이버 억지에 있어서 가장 중요한 연구주제였다.(Nicholas Tsagourias 2012; Thomas Rid and Ben Buchanan 2015; Clement Guitton and and Elaine Korzak 2013) 명확한 근거에 의해 주체를 밝히는 것과 함께 신속성이 담보되지 않으면 억지는 달성되기 어렵다. 자신들의 정체가 드러나지 않는다고 믿는다면 보복 위협은 효과가 없기 때문이다. 물론 사이버 공간의 특징으로 제시되는 귀속의 문제는 사이버 영역에만 국한되는 것은 아니다. 오히려 기술의 발전은 사이버 영역에서도 지문을 남긴다. 사이버 포렌식(cyber forensics) 기술이 점차 발전하고 있다는 점에서 위협의 주체와 목적을 특정할 수 있는 가능성은 높아지고, 억지의 성공가능성도 높아진다.

(2) 무슨 행동을 억지할 것인가?

사이버 공간에서는 핵억지와 같은 절대적인 의미의 억지는 존재하기 어렵다. 핵무기를 보유했다는 사실은 상대의 핵위협 뿐만 아니라 다른 모든 위해 행위를 억지할 수 있는 잠재력을 가지고 있었다. 따라서 점차 사이버 수단을 통한 다른 영역에서의 억지가 가능해지겠지만 아직은 사이버 능력은 사이버 공격만을 억지하는데 활용된다. 미국의 경우 다양한 사이버 위협인식과 사이버 이외의 능력을 통한 대응을 보여주었다. 오바마 정부 시기에는 북한의 소니 픽쳐스 공격에 대한 제재를 부과했고, 트럼프 행정부는 화웨이 사태가 부각된바 있다. 바이든 행정부에서도 사이버안보에 대한 행정명령을 내리면서 중요성을 강조했다. 결국 중요한 것은 피해를 가져올 수 있는 위협 행위를 정확히 파악하고, 이를 경고하는데 있다.

억지해야 하는 행위를 사이버작전의 스펙트럼으로 보자면, 물리적 피해를 입히는 사이버 공격, 정보의 흐름이나 기능을 마비시키는 사이버 교란, 디지털 정보에 대한 접근작전으로 크게 구분할 수 있다.(Timothy M. McKenzie 2017, 3-5) 그리고 제4차와 6차 UNGGE에서 채택된 11개 자발적 규범 중 '금지' 규범은 무슨 행동을 억지할 것인가에 대한 중요한 기준을 제기한다. "국가는 ICT를 이용하는 국제위법행위에 자신의 영토가 이용되는 것을 알면서 허용해서는 안된다." "국가는 주요기반시설에 의도적으로 피해를 입히거나 손상을 입히는 ICT 활동을 알면서 지원해서는 안된다." "긴급대응팀의 정보시스템에 피해를 입히거나, 악의적 국제활동을 위해 긴급대응팀을 이용해서는 안된다" 등이다.(박주희 2022, 3-4)

그리고 무슨 행동을 억지할 것인가는 분명한 억지 메시지로 드러나는데, 억지 메시지는 "레드라인(Redline)"과 "대응행동"을 포함한다. 사실 사이버 억지의 레드라인을 설정하는 것은 신뢰성의 문제를 내포하고 있기 때문에 쉽지 않다. 어느 수준의 위협 행위를 억지할 것인지의 기준을 정하는 것은 실질적인 대응행동을 전제하고 있다는 점에서 외교적 차원의 강압 메시지와는 다르다. 모든 위해 행위를 억지하면 좋겠지만, 대응행동에 나설 수 없다면 오히려 억지의 신뢰성을 낮추는 결과를 가져온다. 분명히 선언하지 않으면 억지할 수 있는 범위는 넓어질 수 있지만 신뢰성은 낮아지고, 선명성을 높이면 신뢰성은 높아지지만 억지의 범위는 좁아진다.

• **레드라인 설정 :** 억지를 위한 신뢰성을 담보하기 위해서는 분명한 레드라인을 설정해야 한다. 그러나 레드라인의 설정이 어려운 것은 사이버 위협의 수준이 천차만별이기 때문이기도 하고, 무력충돌과 첩보활동 사이의 회색지대에서 운용되기 때문이다.(Erica Lonergan and Mark Montgomery 2021, 69-70) 코스트윅 등(Nadiya Kostyuk et al. 2018, 123-134)은 사이버

전의 확전 사다리를 7개 단계로 구분했는데, 준비-경미한 괴롭힘-중대한 괴롭힘-경미한 공격-중대한 공격-치명적 공격-실존적 공격 등이다. 여기에 단순히 사이버 네트워크를 활용하는 것(Cyber Network Exploitation, CNE)과 사이버 공격은 구별해야 한다는 어려움도 존재한다.(Jacquelyn Schneider, 108-109) 사이버 공간에서의 주도권 확보, 자유로운 운용과 운신 수준의 위협은 장기적으로 피해를 끼칠 수 있지만 당장의 물리적인 피해는 초래하지 않을 것이고, 따라서 레드라인은 분명한 피해를 가져오는 행위로 제한될 수 밖에 없을 것이다.

• **신뢰성있는 시그널링(signalling) :** 레드라인이 제시되었다면, 대응행동이 시그널링을 통해서 제시되어야 한다. 위협 주체에게 어떤 비용을 부과할 것인가를 선언해야 하는 것이다. 신속하게, 대가를 치르는 결과를 부과할 것이라는 공개된 선언정책은 효과적이고 또 수용가능해야 한다. 따라서 선언정책은 선명성과 구체성, 엄중성을 갖추어야 한다. 이를 위해서는 상대의 사이버 공간에 침투할 수 있는 공격능력과 확전우세 확보가 필요하다. 여기에는 목표대상, 효과 유형, 지속시간 등에 대한 객관적인 자기평가가 필요하다.(Stephanie Pendino et al. 2022, 5) 주의해야 할 것은 이러한 선언정책이 국가의 평판에 영향을 주고, 차후의 억지 메시지의 신뢰성을 훼손할 가능성이 있다는 점이다. 즉 충분한 거부 및 보복 역량이 갖추어져 있지 않으면 시그널과 억지의 신뢰성은 담보되지 않는다.

'무슨 행동을 억지할 것인가'의 질문은 "비례성"의 문제로 귀결된다. 불필요한 확전을 방지하기 위해서는 보복의 수준을 통제할 필요가 있다. 민간인의 심각한 피해를 방지하고 무력충돌의 확전으로 이어질 가능성을 낮추기 위해서는 비례적인 보복을 해야 하는데, 적절한 상응 수단을 찾기가 쉽지 않다.(장노순, 6) 또 사이버 영역 내에서의 비례적인 보복은 사실 효과가 없을 수 있다. 공격자가 이미 충분한 방어능력을 갖추고 있을 가능성이 있고, 공개하지 않은 보복행위가 상대에게 인식되지 않을 가능성도 있기 때문이다. 또한 의도하지 않은 피해를 줄 수 있고, 상대가 추가 반격하거나 확전될 위험이 항상 존재한다.(Mariarisaria Taddeo 2018, 349-351) 따라서 공격수준에 따른 대응수단과 범위, 대응조건과 시간, 예상결과와 피해평가, 정치적 비용 등을 사전에 충분히 검토해야 한다.(Emilio Iasiello 2014, 60)

(3) 어떻게 억지할 것인가?

억지를 위한 다양한 개념과 방법들이 제시되었다. 위에서 본 바와 같이 초기에는 핵억지의 논리를 그대로 차용하였다. 따라서 핵억지로부터 이어온 "거부에 의한 억지", "보복에 의한 억지"가 큰 축을 이루고 있고, 사이버 억지의 특수성을 고려하여 "규범과 금기에 의한 억지"를 추가로 제기한다.(기세찬, 197-198) 이와 유사한 개념으로 "비정당화(delegitimization)에 의한 억지"가 있고,(Soesanto and Smeets, 392-394) 상호의존적 공간의 특성을 활용한 "얽힘(entanglement)에 의한 억지", 정치-사회-기술의 다층적 연계를 활용한 "연대(association)에 의한 억지"도 있다.(N. J. Ryan 2018, 334-335) 거부억지를 제외한 나머지는 무엇으로 불리든 공격 이후에 사이버 또는 다른 능력을 활용하여 공격자에 대한 보복을 위협함으로써 억지한다는 점에서 보복억지의 다른 이름으로 볼 수 있다.

본 연구에서는 사이버 공간의 특성을 고려하여, 두운(頭韻)을 맞추어 거부(resistance), 응징(retribution), 복원(resilience)을 세 개의 축으로 제시한 앤 햄머 등(Ann Hammer et al.

2020)의 연구를 중심으로 논의를 전개한다. 이들은 사이버 공격 발생 전후로 어디에 중점을 둘 것인지의 우선성을 고려하여 시간 프레임을 제시하고 있다. 즉 공격 발생 전에는 거부억지, 지속 개입, 전진방어, 다양한 방어수단이 요구되며, 공격 발생 직후에는 신속하고 충분한 보복, 국제사회의 개입과 지지, 결속에 의한 응징, 공격 이후에는 피해로부터 회복 및 복구할 수 있는 국가 능력을 통한 억지로 세분화했다. 이러한 세 개의 방법으로서의 개념은 억지를 위한 수단을 각각 포함하고 있다.[8)]

• **거부(Resistance) :** 거부는 상대가 얻을 수 있는 '이익을 거부'하는 억지 개념과 직접 연결되는데, 상대가 신속하게 승리하는 것을 차단하고 비용/편익 계산을 복잡하게 만드는 것을 의미한다.(Michael Gerson 2009) 여기에는 사이버 조직, 인력, 무기체계, 기반 인프라, 선제적, 공세적 수단이 필요하다. 거부억지의 핵심은 정치적 의지보다는 기술적 능력에 있다는 것이다. 또한 물리적 분리와 정보보안체계도 중요한 요건이 된다. 이러한 사이버 방첩활동은 공격 활동을 사전에 탐지하는데 있어 핵심적인 위치를 차지하는데, 국내외의 적대세력의 사이버 공격 의도와 위협을 파악함으로써 선제적으로 방어하고 피해를 약화시킬 수 있다는 것이다. 물론 상대의 이익을 거부하고 비용을 부과하는 것에 일국의 대응만으로는 충분하지 않을 수 있고 네트워크가 글로벌화되어 있다는 점을 볼 때, 방첩활동의 범위 역시 글로벌화되어 있어야 한다. 이는 국가의 능력과 기술의 통합을 가능하게 하고 구체성있는 대응행동의 기회를 확대하는 결과를 가져온다.

• **응징(Retribution) :** 사이버 공격 이후에 보복을 가할 것을 선언 및 실행함으로써 억지를 달성한다. 응징의 효과성을 높이기 위해서는, 정확하게 위해 행위의 귀속을 판단하고,(Thomas Rid and Ben Buchanan 2014) 얼마나 빠르고 자신있게 보복할 수 있는지를 선언정책에 담아야 한다. 다만 응징의 수단은 사이버 공간에 국한되지는 않는다. 응징에 대한 나이의 주장은 너무나 유명한데, "지배계급의 통장을 비운다든지, 당황스러운 정보를 공개하거나, 네트워크를 교란하는 등의 표적화된 보복(targeted retaliation)을 준비"해야 한다고 말했다.(Joseph Nye 2021) 한편 응징에도 국제사회의 지지와 협력이 필요하다. 최소한 "공격을 실시한 주체를 명명하고 망신주기(naming and shaming)" 위해서는 국제규범의 제정, 국제법 하의 수단 마련도 필요하지만, 위협을 식별하고 대응하기 위한 최대한 많은 국가의 전력체계와 핵심기술이 확보되어야 한다. 중요한 것은 사이버 공격과 응징은 일회적이지 않다는 것이다. 일회성 보복이 충분한 억지효과를 가져올 수 없다는 비판에 대한 대안으로 "선택적 누적억지(selective cumulative deterrence)" 개념이 제시되기도 했다. 이는 모든 사이버 위협을 억지하는 것을 목표로 삼지 않으며, 경쟁의 장기적 속성을 고려하여 누적적인 효과를 유도한다는 것이다. 물론 스스로 경계하는 것처럼 누적억지는 "확전"의 위험을 높인다.(Stephanie Pendino et al., 2-6) 다른 한편 충분한 보복 효과를 달성하기 위해 "네트워크 마비전략"을 대안으로 제시하는 연구도 있다.(송운수 2022)

• **복원(Resilence) :** 사이버 영역에서는 완벽한 방어나 억지는 불가능하다. 그런 의미에서 복원력은 상대의 공격에 의한 피해를 최소화하고, 공격 이후에도 작전을 유지하도록 하며, 새로운 조건에 대한 적응과 복원을 통해 사이버 억지에 기여하는 중요한 능력이 된다.[9)] 위협 주체를 특

8) 억지를 위한 핵심능력과 수단은 일부 중첩되지만, 제시가능한 수단을 나열해보면 다음과 같다. 증강된 능동방어체계, 복원과 재건, 선언정책과 대응, 감시정찰 및 귀속판단, 보복계획, 공개 및 낙인(stigma), 국내법 적용, 국제협력과 제재, 사이버대응 과시, 물리적 대응, 조약과 군축 등(DA Donnelly et al. 2019, 56-62)

정하기 어렵고, 대응해야 할 위협이 너무나 다양하며, 의도하지 않았던 결과로 이어질 수 있는 위험(risk)이 존재하여 예측이 어려운 사이버 공간에서 복원력은 더욱 중요해진다. 또한 추가적인 공격을 억지함으로써 확전우세 달성에도 기여할 수 있다.(Will Goodman 2010, 127) 일반적으로 복원력은 다양성, 중복성, 무결성, 격리/분할/봉쇄, 감지/감시, 분산과 이동,(Paul Rosenzweig, 2014) 중복성, 다양성, 적응성이나, 유연성, 가시성, 민첩성으로 구분하기도 한다. 어떤 개념을 선택하든 간에 사이버 공격에 대한 복원은 세 가지 중요한 원칙을 가지고 있는데, 공격을 견디는 능력을 갖추고, 공격 중에도 작동하며, 신속하게 기능을 복구할 수 있어야 한다. 이는 공격으로 얻을 수 있는 이익을 불충분하게 만들고 비용을 높임으로써 억지에 실질적으로 기여할 수 있다.

'어떻게 억지할 것인가'의 질문은 "효과성"에 대한 논쟁으로 이어진다. 대표적인 논쟁이 있는데, 첫째는 미약한 사이버 인프라를 보유한 상대와의 억지게임에서 "취약성의 딜레마(vulnerability dilemma)" 상황은 오히려 억지의 효과를 반감시킨다. 미약한 사이버 인프라를 가진 상대를 억지하기 위해서는 물리적 수단을 포함한 추가적인 수단을 활용할 수밖에 없고, 이는 다른 영역에서의 억지 실패를 유발할 수 있기 때문이다.(Jon Linday 2013) 둘째는 공격우세의 공간인 사이버 영역에서 거부에 의한 억지가 성공하기 어렵다는 논쟁이다. 물리적 공간에서는 완충지역을 확장하고 보복능력의 회복탄력성을 갖추면 방어우세의 환경이 만들어지지만 사이버 공간에서는 여전히 기습공격의 유인이 존재한다는 점이다.[10] 게다가 공격이 실패하는 경우에도 치러야할 비용이 미약하다면 보복 및 거부에 의해서 억지되지 않을 것이라는 우려도 있다.

Ⅴ. 결론

사이버 공간은 더이상 국가 행위자가 독점하는 공간이 아니다. 지상, 해상, 공중의 영역처럼 군사적인 목적에서 먼저 사용되거나 공간에 접근할 수 있는 특정 국가에 의해 독점적으로 사용되었지만, 점차 모든 국가와 민간 영역에 개방되어 왔다. 하지만 다른 한편으로 사이버 위협이 갈수록 조직화되고 국가안보의 차원에서 활용되고 있다. 미국과 러시아, 중국 등 강대국 뿐만 아니라 인도와 파키스탄, 한국과 북한 등 국가간 적대적 경쟁이 장기화되는 가운데 사이버 공간은 전략적 공간으로서의 그 중요성이 부각되고 있다.

그런 의미에서 사이버 억지는 독립된 사이버 공간 내에만 적용되지 않는다. 그렇다고 해서 사이버 억지가 다른 영역과의 연결되어서만 작동하는 것은 아니며, 다른 영역을 연계하는 핵심공간으로서 사이버 억지의 중요성은 더욱 커지고 있다. 사이버 공간의 특수성은 기존 억지개념의 변

9) 2017년 국방과학위원회(DSB)의 "사이버억지TF"는 결과보고서에서, 맞춤형 억지 캠페인의 기획과 실행, 핵심무기체계에 대한 사이버 복원력 창출, 기반 능력의 증강을 세 가지의 핵심우선순위로 제시하였다. 이는 취약성을 감소시킴으로써 거부에 의한 억지를 달성하기도 하지만, 공격자에 대한 미국의 비용부과 위협의 신뢰성을 강화하는 것이기도 하기 때문이다.(DoD Defene Science Board 2017)

10) 사이버 공간이 "공격 우세(offense-dominant)의 환경"이 아니라 "공격 지속(offence-persistent)의 환경"이라는 주장은 눈여겨 볼만하다. 방자는 항상 공격에 대해 긴장하지만 압도적인 것이 아니며, 공자가 기습을 통해서 항상 전략적 이익을 취하거나 성공으로 이어지는 것은 아니기 때문이다. 임계점 이하의 공격으로부터 모든 스펙트럼의 공격이 지속될 수 있다는 것으로 공방이 일회적이지 않다는 주장은 자연스럽게 위에서 언급한 "누적적 억지" 개념으로 연결된다.(Mariarisaria Taddeo 2018, 346) 물론 그렇다고 해서 기습의 유인이 사라지는 것은 아니기 때문에 거부억지의 효과성에 대한 우려는 여전히 남는다.

화를 요구한다. 거부억지, 신뢰성, 자력구제와 같은 억지 개념은 지속되거나 오히려 강조되지만, 확장억제, 합리성, 상호확증파괴, 대등성, 응징보복과 같은 개념은 수정이나 파기를 요구한다. 사이버 억지의 성공에 대한 기대는 커지고 있다. 사이버 공간의 특수성을 고려하면 이론적으로는 억지가 어려운 것이 사실이나, 실제 억지의 실패 사례들로부터도 교훈을 얻을 수 있기 때문이다.(Will Goodman 2010)

위에서 제시된 사이버 억지의 개념과 조건 등을 고려하여, 사이버 억지 증진을 위한 다음의 몇 가지 정책제언으로 결론을 대신하고자 한다. 첫째, 가장 우선적으로는 억지를 위한 실질적 능력을 요구한다. 위협주체와 행위를 특정할 수 있는 감시정찰, 보안, 포렌식 능력, 거부와 응징 뿐만 아니라 신속한 복구와 복원을 위한 능력도 필요하다. 특히 강조되는 능력은 공격능력인데, 방어만으로는 특히 사이버 공격은 완전히 막을 수 없으며 사이버 공간에서 회색지대가 훨씬 크기 때문이다. 사이버 공격능력은 맞춤형의, 상호적 방어수단과 병행될 때 억지 효과가 극대화된다.

두 번째는 사이버 공격을 억지하기 위한 국가 차원의 대응전략이 필요하다. 외교, 정보, 군사, 경제 등 다양한 기능별 전략에서 사이버 위협과 대응이 중요한 과제이지만, 총체적인 차원에서 사이버 안보전략을 구체화하고 범정부적 노력을 결집하는 것도 중요하다. “통합억지”는 미국만이 추구할 수 있는 것은 아니다. 각각의 이슈가 사이버 영역을 중심으로 연계되어 있으며, 영역을 교차하면서 발전하고 있는 의도적 위협과 확산가능한 위험을 모두 고려해야 한다. 따라서『국가사이버안보전략』을 중심으로 통합성과 연계성을 유지하되, 부처별로 일관된 기조 하에 사이버전략을 작성하여 전략적 과제와 구체적인 내용을 제시할 필요가 있다.

세 번째는 국내 및 국제사회의 사이버 안보 거버넌스의 정립이다. 먼저는 다양한 국내 제약과 도전을 해소하기 위한 국민과의 대화이다. 사이버 보안 법안의 제정과 개선에 대한 논의로부터 시작하여 정책적 관점에 기반한 국회의 인식 제고, 국민적 공감대 형성으로 나아갈 필요가 있다. 이를 통해 불필요한 국민의 우려나 논란을 차단하고 보다 효과적인 사이버 안보 시스템을 마련할 수 있다. 다른 한편으로 국제 거버넌스에의 적극적인 참여가 필요하며, 특히 동맹을 기반으로 협력을 강화해야 한다. 새로운 안보환경에서 새롭게 제기되는 통합억지, 정보동맹 등의 개념을 동맹 차원에서 발전시킬 필요가 있다. 나아가서는 방어우세의 사이버 환경을 위해 사이버 국제레짐을 주도해가야 할 것이다.

〈참고문헌〉

기세찬. 2022. “사이버 억제에 관한 연구,”『국방연구』, 제65권 3호.

김상배 편. 2018.『사이버안보의 국제정치학적 지평』. 서울: 사회평론아카데미.

김정기. 2018. “미래의 전쟁,” 군사학연구회 편,『전쟁론』. 서울: 플래닛미디어.

마틴 반 크레벨드. 2018.『다시 쓰는 전쟁론』. 강창부 역. 파주: 한울아카데미.

박주희. 2022. “UNGGE의 자발적 규범과 국내 사이버안보 법제,” Global Legal Brief, Vol.1. 한국법제연구원. .

송운수. 2022.『사이버 군사전략 개관』. 인천: 진영사.

송태은. 2022. “현대 전면전에서의 사이버전의 역할과 전개양상,”『국방연구』, 제65권 3호.

임종인, 김근혜. 2021. “국가사이버안보전략의 미래와 AI 융합보안,” 홍규덕 편.『초연결사회 국가보안의 위기. 왜 융합보안인가?』. 서울: 국가보안학회.

장노순. 2019. “사이버안보 위협, 대응 전략 그리고 한국적 함의,”『국가안보와 전략』, 제19권 2호.

차오량, 왕상수이. 2021.『초한전: 세계화 시대의 전쟁과 전법』, 이정곤 역. 서울: 교우미디어.

청와대 국가안보실. 2019.『국가 사이버안보 전략』. 서울: 청와대 국가안보실.

Arquilla, John and David Ronfeldt. 1993. “Cyberwar is Coming!” Comparative Strategy, No.12.

Beaufre, André. 1965. Introduction to Strategy. New York: Praeger.

Brooking, Emerson and Erica Lonergan. 2023. "Welcome to Cyber Realism: Parsing the 2023 Department of Defense Cyber Strategy," War on the Rock. 2023/9/25.

Davis, Paul and Brian M. Jenkins. 2002. Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda. Santa Monica: RAND Corporation.

De Velde, James Van. 2023. "Cyber Deterrence Is Dead! Long Live 'Integrated Deterrence," Joint Forces Quarterly 109.

Denning, Dorothy E. 2015. “Rethinking the Cyber Domain and Deterrence,” Joint Forces Quarterly 77.

Department of Defense. 2018. Department of Defense Cyber Strategy 2018-Summary. Washington DC: Department of Defense.

Department of Defense. 2023. 2023 Cyber Strategy of Department of Defense-Summary. Washington DC: Department of Defense.

DoD Defense Science Board. 2017. Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence. Washington DC: Defense Science Board, Feb.

Donnelly, DA, SL Clements, RA Weise, and R. Goychayev. 2019. "A Technical and Policy Toolkit for Cyber Deterrence and Stability," Journal of Information Warfare, Vo.18, No.4.

Gerson, Michael. 2009. “Conventional Deterrence in the Second Nuclear Age,” Parameters, Vol.39, No.3.

Goldstein, Guy-Philippe. 2013. “Cyber Weapons and International Stability,” Military and Strategic Affairs, Vol.5, No.2.

Goodman, Wil. 2010. "Cyber Deterrence: Tougher i Thoery than in Practice?" Strategic

Studies Quarterly, Fall.
Guitton, Clement and Elaine Korzak. 2013. "The Sophistication Criterion for Attribution," RUSI Journal, Vol.158, No.4.
Haizler, Omry. 2017. “The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking,” Cyber, Intelligence, and Security, Vol.1, No.1.
Hammer, Ann, Trisha Miller, and Eva Uribe. 2020. “Cyber Resilience as a Deterrence Strategy,” Sandia Report, SAND2020-5016. Sadia National Laboratories.
Harknett, Richard and Michael Fischerkeller. 2017. “Deterrence is Not a Credible Strategy for Cyberspace,” Orbis. Vol.61, No.3.
Hennessey, Susan. 2017. “Deterring Cyberattacks: How to Reduce Vulnerability,” Foreign Affairs, November/December.
Hynes, William. 2019. “Resilience Strategies and Approaches to Contain Systemic Threats,” OECD SG/NAEX. 2019.9.17.-18.
Iasiello, Emilio. 2014. "Is Cyber Deterrence an Illusory Course of Action?" Journal of Strategic Security, Vol.7, No.1.
Joinf Chiefs of Staff. 2019. Joint Doctrine Note 1-19, Competition Continuum. Washington DC: Joint Chiefs of Staff. 3 June.
Kostyuk, Nadiya, Scott Powell, and Matt Skach. 2018. “Determinants of the Cyber Escalation Ladder,” The Cyber Defense Review, Vol.3, No.1.
Libicki, Martin C. 2009. Cyberdeterrence and Cyberwar. Santa Monica: RAND.
Libicki, Martin C. 2017. "It Takes More Than Offensive Capabilities to Have an Effective Cyber Deterrence Posture," CT-465. Testimony presented before the House Armed Services Committee. Santa Monica: RAND Corporation.
Lindsay, Jon. 2013. "Stuxnet and the Limits of Cyber Warfare," Security Studies, Vol.22, No.3.
Lonergan, Erica and Mark Montgomery. 2021. "What is the Future of Cyber Deterrence?" SAIS Review, Summer-Fall.
McKenzie, Timothy M. 2017. "Is Cyber Deterrence Possible?" Air Force Research Institute Papers, CPP-4. Maxwell Air Force Base: Air University Press.
Morgan, Patrick. 2019. “The Past and Future of Deterrence Theory,” in Jon Lindsay and Erik Gartzke eds. Cross-Domain Deterrence: Strategy in the Era of Complexity. New York: Oxford University Press.
Nye, Joseph S. 2021. “Will Biden’s Red Lines Change Russia’s Behaviour in Cyberspace?” Austrailian Strategic Policy Institute. The Strategist, 8 July.
Office of the Director of National Intelligence. 2023. Annual Threat Assessment of the U.S. Intelligence Community. 6 February.
Paul, T.V., Patrick Morgan, and James Wirtz eds. 2009. Complex Deterrence: Strategy in the Global Age. Chicago: The University of Chicago Press.
Pendino, Stephanie. 2022. “U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light,” Campaigning: The Journal of the Joint Forces Staff College. 7

September.
Rid, Thomas and Ben Buchanan. 2015. "Attributing Cyber Attacks," Journal of Strategic Studies, Vol.38, No.1-2.
Rid, Tomans and Ben Buchanan. 2014. “Attributing Cyber Attacks,” Journal of Strategic Studies, Vol.38, No.1-2.
Rosenzweig, Paul. 2014. Cyber Warfare: How Conflicts in Cyberspace are challenging America and Changing the World, 정찬기, 이수진 역. 논산: 국가안보문제연구소.
Ryan, N. J. 2018. "Five Kinds of Cyber Deterrence," Philos. Technol. No.31.
Schneider, Jacquelyn. 2019. “Deterrence in and through Cyberspace,” in Jon Lindsay and Erik Gartzke eds. Cross-Domain Deterrence: Strategy in the Era of Complexity. New York: Oxford University Press.
Soesanto, Stefan and Max Smeets. 2021. “Cyber Deterrence: The Past, Present, and Future,” in Frans Osinga and Tim Sweijs eds. NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice. The Hague: T.M.C. Asser Press.
Soesanto, Stefan. 2022. “Cyber Deterrence Revisited.” Perspectives on Cyber Power, CPP-8. Maxwell Air Force Base: Air University Press.
Taddeo, Mariarisaria. 2018. "The Limits of Deterrence Theiry in Cyberspace," Philos. Thechnol. No.31.
Tsagourias, Nicholas. 2012. "Cyber Attacks, Self-Defence and the Problem of Attribution," Journal of Conflict & Security Law.
US Cyberspace Solarium Commission. 2020. U.S. Cyberspace Solarium Commission Final Report. Washington DC: Solarium Commission.
Van Evera, Stephen. 1999. Causes of War. Ithaca: Cornell University Press.
Wilner, Alex S. 2020. "US Cyber Deterrence: Practice Guiding Theory," The Joural of Strategic Studies, Vol.43, No.2.
Global Cyber Strategies Index, https://csis-website-prod.s3.amazonaws.com/s3fs-public/220414_Cyber_Regulation_Index.pdf

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.