사이버 억지 전략의 발전
: 미국의 거부, 복원력, 징벌의 사이버 작전

유인태 | 단국대학교

| 목차

미국의 사이버 억지 전략은 어떻게 발전했는가? 본 논문은 두 개의 억지 전략, 즉 거부에 의한 사이버 억지와 징벌에 의한 사이버 억지가 국가 사이버 전략 수립 초기부터 고려되었지만, 동시에 발전하기보다 순차적인 강조를 통해 상호보완의 형태로, 단번에 이루어진 것이 아니라 점진적으로 현실과 조응해 가며 발전해 왔다고 주장한다. 기존 연구들은 단편적 전략 개념이나 정부 문서를 중심으로 이루어져서, 통시적 발전 과정을 담아내지 못하고 있다. 사이버 공간의 특수성은 핵무기 기반의 억지 이론의 쇄신을 요구하였으며, 이에 미국은 우선적으로 거부에 의한 사이버 억지의 한 형태인 복원력의 사이버 억지를 발전시켰다. 다른 한편으로 2018년 이후 미국은 징벌적 사이버 억지를 위한 전략적, 정책적 수단들을 본격적으로 강화해 나갔다. 공개 귀속 시행, 금지선 설정, 보복을 동반하는 수세적 사이버 작전 그리고 공세적 사이버 작전이 포함되는 징벌 억지 수단의 보강 등과 관련된 문제들을 하나씩 풀어나가며, 아직 완벽하지는 않지만, 과거에는 불가능하거나 위험하다고 생각되었던 효과적 억지를 위한 장치들을 동맹국들과 함께 마련해 나가고 있다. 이와 같은 맥락에서 결론에서는 한국이 미국과 사이버 억지 전략 및 전술 차원에서의 협력 시 고려해야 할 사항들에 대해 제언하고, 향후 연구 어젠다를 제시한다.

| 주제어 신호 보내기, 복원력, 공개 귀속, 전진 방어하기, 공세적 사이버 작전, 금지선, 국제 사이버 규범

Ⅰ. 서론

미국의 사이버 억지 전략은 어떻게 발전해 왔는가? 일반적으로 억지 전략을 크게 '징벌에 의한 억지(deterrence by punishment)'와 '거부에 의한 억지(deterrence by denial)'로 나누어 보면, 미국의 사이버 억지 전략 또한 이러한 이론적 개념에 따라 이해할 수 있다. 초기 미국의 억지 전략은 사이버 공간의 특성 때문에 징벌적 억지 가능성에 회의적이었으며, 이 때문에 '거부에 의한 억지' 개념을 중심으로 전개되었다. 그 이후 '복원력(또는 회복탄력성, resilience)' 개념을 추가하며 '거부에 의한 사이버 억지'로서의 '복원력에 의한 사이버 억지(cyber deterrence by resilience)'로 발전했으며, 최근 들어 '징벌에 의한 사이버 억지' 개념으로의 발전을 거듭하고 있다. 초기에는 거의 불가능하다고 여겨졌던 '징벌에 의한 억지' 전략이 점차 사이버 작전(cyber operations)의 수행 내용이 되고 있으며, 더불어 공세적 사이버 역량(offensive cyber capabilities)의 중요성도 강조되고 있다.

본 논문의 주장을 뒷받침하기 위해 미국의 공식 문서들과 관련 담론 및 사건들을 제공한다. 이들 간의 관계가 유기적으로 연관되어 상호작용이 있는 것을 전제하지만(cf. Dunn Cavelty and Eglof 2019), 본 연구의 주목적은 그러한 상호작용에서의 인과기제 검증이 아닌 미국 사이버 억지 전략의 변화를 이해하는 것이다.[1] 억지 전략 쇄신의 계기가 되는 환경으로서 국제 정세, 주요 사건들,

1) 연구 질문에 대해 본 연구는 미국의 사이버 억지 전략의 변화를 추적하며 서술(description)하고자 한다. 서술의 학문적 가치 및 서술적 추론에 대해서는 게링(Gerring 2012), 킹 외(King et al. 1994)의 2장, 크루저(Kreuzer 2019)를 참조하라.

또는 정책형성 자들의 인식의 변화는 언급하나, 인과관계 연구에 앞서 더 중요한 것은 설명하려는 대상의 변화를 규명하는 것이기 때문에, 미국의 사이버 억지 전략의 미묘한 변화를 체계적으로 파악하고자 한다.

미국의 사이버 억지를 실현하기 위한 공적 제도의 변화는 전략, 법, 정책, 이니셔티브, 행정명령, 조직의 변화를 통해 이루어졌다. 이러한 변화는 한 번에 빅뱅과 같이 일어나서 그 후 고정되는 형태를 보이지 않았다. 오히려 이러한 과정은 역사적 제도주의에서 언급하는 '점진적 변화(gradual change)'에 가깝다(Mahoney et al. 2016, 77). 기존의 제도는 그다음 단계의 제도적 결과가 생기기 위한 필요조건을 제공할 뿐 아니라, 때로는 종국적 결과의 구체성을 좌우하는 충분조건에 가까운 원인이 되기도 한다. 사이버 초강대국으로서의 미국은 글로벌 사이버 억지 전략의 개척자이자 선도자였다. 냉전기 핵 억지 전략은 새로이 부상한 사이버 공간에서의 악의적 행위를 억지하기 위한 어느 정도의 토대를 제공하였지만, 사이버 공간의 특성은 기존 억지 전략 적용에 다수의 어려움을 제기했다. 이 때문에 거부에 의한 사이버 억지 전략이 먼저 선택되어 발전하게 되었다. 거부에 의한 억지 전략이 진행되는 한편, 정책형성 자들은 악의적 사이버 행위를 억지하기에 한계가 있음을 주요 사건들과 국제 정세를 통해 인식하고 차츰 징벌에 의한 사이버 억지를 수행하기 위한 제도적 장치들을 마련하게 되었다.

당연하게도, 미국의 사이버 억지 전략의 제도적 발전 과정을 다른 강대국뿐 아니라 중견국인 한국과 같은 나라에 그대로 적용할 수 없다. 따라서 한국 정책에의 함의는 결론에서 언급한다. 그럼에도 이 연구가 미국 사례에 주목하는 이유는, 미국이 동맹국과 파트너 국가들뿐 아니라 경쟁국들의 사이버안보 전략의 발전 양상에 상당한 영향을 주는 주요 행위자이기 때문이다. 파이브 아이즈(Five Eyes) 회원국들과 같은 첩보 동맹국들뿐 아니라 일본과 같은

군사 동맹국들의 사이버안보 전략은 미국의 사이버안보 전략과 유사한 방향으로 발전해 왔다.[2)]

사이버 억지에 관한 초기 연구들은 주로 핵무기 기반의 억지 이론을 가지고 사이버 억지의 가능성에 대해 추론하는 문헌들이 많았다(Buchanan 2016; Kugler 2009; Libicki 2009).[3)] 이러한 연구들은 사이버 공간에서 비용 부과뿐 아니라, 공세적 사이버 작전의 효과를 거두기 어렵다고 보았고, 따라서 억지는 어렵다고 생각했다(Arquilla and Ronfeldt 1993; Fischerkeller and Harknett 2017; Kello 2017). 그러나 그 이후의 연구들은 냉전기 핵 중심의 억지 이론에 기반한 판단에서 벗어나, 거부뿐 아니라 징벌에 의한 억지, 나아가 공세적 사이버 작전의 가능성에 대해 정책 제안을 하고 있는 (회색) 문헌들이 다수 나오고 있다(Borghard and Lonergan 2021; Gartzke and Lindsay 2019).[4)] 그러나 이러한 단편적 억지 관련 연구들은 사이버 억지 전략이 어떻게 발전해 왔는지를 종합적이고도 통시적으로 보이지 못하고 있다. 국내 문헌들은 대체로 본 논문에서 다루는 일부 정부 문서나 작전 개념을 중심으로 연구되었다. 그에 비해 본 논문은, 단발적이고 산재해 있던 미국의 사이버안보 전략에 관한 지식을 사이버 억지 이론을 통해 정리할 뿐 아니라, 사이버 억지 전략과 작전 개념들을 체계적으로 정리하여 연결하고 있다.

이 글은 다음의 구조를 갖는다. 다음 장에서는 일반적 억지와 사이버 억지의 특수성을 이론적 개념을 통해 기술한다. 사이버 공

2) 일본은 2022년에 채택된 국가안전보장전략서에서 '능동적 사이버 방위(active cyber defense)'를 처음으로 적시한다. 이는 국가 안보적 우려를 일으키는 사이버 공격의 가능성을 사전적으로 제거하기 위한 것이며, 그 개념은 후술할 미국의 '전진 방어하기(defend forward)' 작전 개념과 유사하다.

3) 같은 맥락에서 나이(Nye 2016) 또한 사이버 억지 논의가 핵 억지 이론의 첫 번째 물결과 같은 맥락이 지배적이라고 보았다.

4) 그 외 문헌들은 본문에서 인용한다.

간에서 억지를 작동시키는 것이 왜 그리고 어떻게 어려운 것인지를, 물리적 무기에 기반한 억지 이론을 사이버 공간에 적용할 시 직면하는 도전을 통해 이론적으로 살핀다. 이러한 이론적 논의는 이어지는 분석 장에서 미국의 사이버 억지 전략이 왜 그리고 어떻게 발전해 나가는지를 이해하는 데 중요하다. 분석은 크게 두 개의 소절로 구성된다. 전자는 거부에 의한 사이버 억지 전략의 발전을, 후자는 징벌에 의한 사이버 억지 전략의 발전을 다룬다. 분석적 목적을 위해 두 절로 나누었지만, 실제로는 이 두 개념이 학계와 실무자들 사이에서 사이버안보 국가전략 구상 초기부터 병존했으며, 대립보다는 보완적 전략적 개념으로 인식됐다. 다만, 징벌에 의한 사이버 억지를 시행하기 위한 도전들이 더 컸기 때문에, 미국은 이들을 점진적으로 극복해 가며 사이버 억지 전략을 발전시켜 왔다. 국제 정세 차원에서도 2018년 미·중 전략 경쟁으로의 전환과 러시아-우크라이나 전쟁 등의 지정(경)학적 긴장의 상승 등은, 악의적 사이버 행위가 지속되고 심해지는 경향성을 동반했으며, 이러한 배경은 미국 사이버 억지 전략의 전환을 위한 환경이 되었다. 마지막 절에서는 요약, 본 연구의 기여, 정책 제언, 향후 연구 방향 등을 논한다.

Ⅱ. 전통적 억지 이론과 사이버 공간의 도전

이 장은 효과적 사이버 억지를 위한 이론적 요인들을 검토한다. 사이버 억지 전략은, 기존의 억지 전략과 다른 이론과 정책이 개발되고 발전하는 양상을 보이는데, 그러한 변화를 위해서는 기존 억지 이론의 사이버 공간에의 적용에 제기됐던 도전에 대한 이해가 필요하다. 사이버 공간의 특수성에 주목하고, 사이버 억지 전략

의 변화와 어떤 관계가 있는지를 논한다. 미국 사이버 억지 전략의 경우, 거부에 의한 억지, 복원력에 의한 억지, 그리고 징벌에 의한 억지를 차례대로 발전시켜 나갔다. 특히, 근래에 들어 징벌적 사이버 억지를 발전시키고 있는데, 이러한 과정을 이해하기 위해서는 사이버 공간의 속성이 제기하는 도전을 파악하고, 징벌적 억지와의 관계성을 이해할 필요가 있다.

억지를 단순하게 정의하자면, 상대에게 메시지를 보내어 상대가 본래 하려고 했던 행위를 그만두게 하는 것이라고 할 수 있다. 억지가 작동하기 위해서는, 상대방이 공격할 때보다 공격하지 않을 때의 기대 효용(expected utility)을 크게 만들어야 한다. 이에 따라 전통적 억지 전략은 크게 두 가지로 나뉘는데, 상대방의 공격 성공의 이득(benefits)을 없애는 '거부적 억지'와 공격에 대해 비용(costs) 또는 대가(consequences)를 부과하겠다고 위협하는 '징벌적 억지'이다. 전자에 따르면, 공격에 드는 비용이 공격으로 얻는 이익보다 크다고 생각될 때 억지가 작동하며, 후자에 따르면, 공격 성공의 이익보다 보복으로 인한 피해가 크다고 생각될 때 억지가 작동한다. 그런데 사이버 공간이 연루되면, 사이버 공간의 특수성 때문에 전통적 억지 이론이 그대로 작동하기 어렵게 하는 도전들이 부상한다.

첫 번째 도전은, 귀속(attribution)의 문제이다. 귀속을 행위의 원인 또는 인과관계를 특정하는 것이라고 정의했을 때, 사이버상에서는 익명성 때문에 귀속의 어려움이 있다고 논의되었다. 억지가 작동하기 위한 핵심 요소는 귀속의 가능성인데, 사이버상의 귀속 문제는 억지가 작동하기 어렵게 한다. 국가 행위자에 의한 핵무기 사용을 상정한 전통적 억지 이론에서는 크게 주목받지 않는 문제이다. 특히, 귀속은 징벌에 의한 억지에 필수적이었는데, 누가 공격하는지 알아야만 보복이 가능하며, 그 보복에 대한 두려움이 생성될 때 억지가 작동하기 때문이다. 그리고 귀속에 의해서 공격

자가 누구인지, 어디서부터 비롯되는지를 알 수 있으므로, 공격을 '거부'할 수 있는 대비가 더욱 효율적으로 된다. 무엇보다 전략적 관점에서 귀속이 중요한 이유는, 공격에 대해 책임지는 정치적 행위자가 누구인지 알아야 하기 때문이다. 그래야만 그들의 계산을 바꿀 수 있게 억지 정책을 구체적으로 세울 수 있다.

그러나 사이버상에서의 귀속 수행 역량은 발전하여 더 이상 종종 '할 수 있다, 없다'로 명백히 구분되는 이분법적 문제가 아닌, 정도의 문제이다.[5] 특정 사이버 공격이 어느 국가에서부터 비롯되는지 기술적으로 추적되더라도, 특정된 악의적 행위자가 그 나라 정부와 어떤 관련이 있는지, 무슨 목적을 가지고 행했는지는 쉽게 알 수 없으므로, 100퍼센트 완벽한 귀속은 어렵다.[6] 사이버 공격에는 비국가 행위자가 종종 연루되기 때문에(Maurer 2018), 장시간의 포렌식 조사를 통해서도, 해당 범죄자의 동기뿐 아니라 국가 행위자와의 관련성을 확정적으로 귀속하기는 쉽지 않다.[7] 그리고 귀속은 정치적 문제이기도 하다. 특히 공개 귀속(public attribution)의 경우가 그러한데, 가령 귀속 결과의 공개가 국제정치적 파란을 몰고 올 대상이라고 한다면, 귀속을 끝까지 추구하지 않거나, 공개적 귀속을 하지 않는다(Clark and Landau 2010; Rid and B

5) 사이버 UNGGE에서도 기술적(technical), 법적(legal), 정치적(political), 세 가지 분류의 귀속을 받아들이고 논의를 진행한 바 있다. 여기서 법적 귀속은 국내 사법절차에 의한 귀속 작업을 의미한다. 이 세 귀속은 유기적으로 연결되어 있다. 가령, 법적 귀속 과정에서 사법 당국자에 의한 악의적 공격자에 대한 기소와 판결 그리고 사실관계의 규명은, 정치적 귀속의 부담감을 덜어줄 수 있다.

6) 따라서 귀속의 정확도를 높이기 위해 휴민트(humint)의 조력이 수반되기도 한다. 이렇게 귀속에 있어 정보력이 중요하기 때문에, 미국에서는 군 사이버사령부의 사령관과 첩보기관인 NSA의 국장의 겸직이 가능했다.

7) 해당 나라의 수사 협조가 요구되는 사항이나, 모든 국가 간에 수사 공조가 원만하게 된다고 볼 수 없다. 2023년 한국의 사이버범죄협약(일명 부다페스트협약) 가입은 형사사법공조조약(MLAT)의 한계를 보완하고, 수사 공조의 원만화를 위한 노력이라고 볼 수 있다.

uchanan 2015). 섣불리 귀속의 결과를 공표하여 생길 분쟁의 확전(escalation)이나 국제정치적 긴장 상승을 고려하면, 설령 기술적 귀속이 가능하다고 해도 공개적 발표를 주저하게 된다.

귀속과 관련되어 사이버 공간의 특성에서 비롯되는 '타이밍(timing)' 문제 또한 징벌적 억지의 문제점을 크게 부각했다. 사실, 기술적 귀속은 이미 충분히 가능할 정도로 발전해 왔으나, 정치적 이유로 대응에 지연이 생길 수 있는데, 이는 전통적 억지 이론이 상정했던 것과는 다른 상황적 조건이다. 전통적 억지 전략에서는 대응의 즉각성이 중요했는데, 즉각적으로 반응이 가능할 수 있어야만 거부에 의한 억지가 작동하기 때문이다. 그리고 즉각적으로 보복해야만 특정 행위가 용납되지 않는다는 신호를 명확히 보낼 수 있기 때문이다.

이러한 사이버상의 특성 때문에, 오바마 정권에서 미 국방부와 미군의 사이버안보 대책 추진자이자, 국방부 부장관(Deputy Secretary of Defense)을 지낸 윌리엄 린(William J. Lynn III)도, 한 번의 클릭으로 0.3초 동안 지구를 두 바퀴 도는 속도로 공격이 이루어지는데, 공격 근원을 특정하는 조사는 수개월도 걸릴 수 있다며, 이러한 대응 속도로는 기존의 억지 전략은 파탄할 수밖에 없다고 언급한 바 있다(Lynn 2010b). 사이버 공간에서 귀속의 어려움 때문에 대응이 지연되면, 특정 사이버 공격에 대한 보복적 대응이 그 사이버 공격에 대한 보복인지 아닌지에 대한 명확한 신호로서 전달되기 어렵다. 따라서 사이버 공간의 특성은 특히 징벌적 억지 전략이 성립되기 어렵게 한다(Clarke and Knake 2010, 6장; Morgan 2010).

귀속의 문제와 관련한 사이버상의 조건들은 징벌에 의한 억지를 실현하기 어렵게 한다. 그에 반해 거부에 의한 억지는 상대적으로 귀속의 필요성과 타이밍에 제약을 덜 받을 수 있다. 따라서 사이버 억지와 관련하여, 거부에 의한 억지에 기반한 전략 개념들과

정책들이 먼저 고안되리라 생각할 수 있다. 그런데 거부에 의한 억지 전략에도 한계가 존재한다. 사회의 모든 것들이 인터넷에 연결되는 현대 사회에서는 방어해야 할 범위가 너무 광범위하며, 더욱 많은 것들이 인터넷에 연결됨에 따라 그 수비 비용이 기하급수적으로 증가할 수 있다. 그리고 민간이 대거 연루됨에 따라 공격자의 기대 효용에 영향을 미칠 수 있는 방어 수단의 배치에 제약이 생기고, 이 때문에 적국의 공격 행태를 형성할 수 있는 영향력에 한계가 있을 수밖에 없다. 따라서 보다 효과적인 억지를 위해서는 거부에 의한 사이버 억지뿐 아니라 징벌에 의한 사이버 억지 수단의 보완이 요구된다.

두 번째 도전은 메시지를 전달하는 의사소통(communication) 과정에 있다. 즉, 사이버 공간의 특수성 때문에 전통적 억지 이론이 그대로 작동하기가 어려운 또 다른 이유는 신호전달(signaling)의 어려움 때문이다. 물론 의사소통 과정 이전에 자국의 보복에의 전념(commitment to retaliate) 혹은 보복하겠다는 굳은 결심(resolved)이 전제되어야 하지만, 그것이 시행 능력과 함께 잘 신호전달 되어야 한다. 이렇게 '신뢰할 수 있는 위협(credible threat)'이 잘 신호전달 되어 잠재적 적대국이 이를 고려할 수 있어야 한다. 종합하자면, 억지될 적국이, 억지하고자 하는 국가의 의지(willingness)와 역량(capabilities)이 있다는 것을 알아야 한다.

그런데 신호전달 문제의 핵심은, 단순히 전달되는가 아닌가가 아니다. 구체적으로 무엇을 어떻게 전달하는가이다. 사이버 공간에는 이와 관련해 특별히 세 가지 어려움이 존재한다. 첫째, 우선 신호를 투명하게 보내는 것이 중요하지만, 신뢰할 수 있을 정도의 투명성 조절이 어렵다. 역량에 대한 정보를 밝힘으로써 위협의 신뢰성을 높일 수는 있다. 전통적인 무기의 경우, 억지 대상은 첩보, 감시, 정찰로 억지하고자 하는 국가의 의지와 역량을 어느 정도 확증할 수 있었겠지만, 사이버 역량은 그렇지 않다. 무기 특성상

상대방의 사이버 역량의 많은 부분이 베일에 싸여 있으며, 밝히기 전까지는 확인할 수 없는 바가 많다. 따라서 상대방의 행위를 억지할 수 있는 정도의 의지뿐 아니라 역량을 어느 정도 투명하게 밝히는 것은 억지로 이어질 수 있지만, 역으로 너무 많은 정보가 공개되면, 사이버 무기의 제로데이(zero-day) 취약성을 착취할 수 있는 능력을 잃게 되는 위험이 있다.

이 문제는 본 연구의 연구 대상인 미국과 같이 사이버 강대국으로 잘 알려졌으면 큰 문제가 아닐 수 있다. 미국의 사이버 역량에 대해서는 이미 전 세계가 스턱스넷(Stuxnet)과 같은 역사적 경험을 통해서 인지하고 있으며, 적대국인 러시아도 1990년대 말부터 국제 연합의 정부 전문가그룹에서의 사이버안보 규범 논의를 제기할 때 그 인식이 드러나고 있다. 하지만 신호보내기의 도전은 이하의 이유로 여전히 존재한다.

둘째, 신호를 공개적으로 보내는 것이 억지를 위해 효과적인 방법이지만, 반작용의 위험이 있다. 공개 선언이 효과적인 이유는, 정치적 지도자가 치러야 할 청중 비용(audience costs) 때문에라도, 위협의 신뢰성(credibility)을 더욱 증가시키기 때문이다(Fearon 1997, Morrow 1999).[8] 특정한 행동을 용납하지 않을 것이며, 만일 있을 때 그에 상응하는 조치를 취하겠다는 신호보내기의 차원으로 공개 선언을 했음에도 불구하고 지도자가 대응조치(countermeasures)를 취하지 않았을 경우, 자국의 국제적 명성에 손상이 갈 뿐 아니라, 국내 정치적으로도 수세에 몰릴 수 있기 때문이다. 그런데 공개 선언은, 상기한 귀속성 문제의 해결을 전제한다. 또한 섣불리 공개 귀속을 하게 되면 정치, 군사, 외교, 경제, 사회 등의 관계에 부정적 영향을 미치게 될 상황을 고려해야 한다. 공개 규탄에 대항해 적대국이 오히려 앙갚음하려 할 수도 있기 때문이다.

8) 공개적이기보다, 비밀리에 혹은 사적으로 '금지선'이 전달되는 것이 더 효과적이라는 주장도 있다(Nye 2021).

공개 귀속에 따르는 비용을 감수할 수 있다면, 그와 같은 신호 보내기는 억지를 위한 유용한 정책 수단이 된다. 비용을 감수할 수 있을 정도란, 여러 상황을 생각해 볼 수 있다. 이미 해당 국가와 공유하는 이익이 상당히 줄어들어 관계 악화로 인해 발생하는 추가적 한계 비용이 매우 적거나, 아니면 해당 국가의 사이버 공격이 자국의 국가 안보나(주요 인프라, 지식재산권, 민주주의 선거 절차와 같은) 전략적 이익을 심각하게 해치는 경우이다. 공개 귀속이 유용한 정책이 될 수 있는 이유는, 공개 귀속을 통해, 자국이 억지하고자 하는 의지를 명확히 할 수 있을 뿐 아니라, 귀속을 자신 있게 할 수 있을 정도의 사이버 역량을 표시할 수 있기 때문이다. 그리고 다른 징벌적 대응 행위에 정당성을 제공하며 자연스러운 가교가 될 수 있기 때문이다.

셋째, 신호보내기에서 특히 까다로운 문제는 어떤 내용의 메시지를 보내는가와 관련 있다. 특히 억지하고자 하는 '특정한' 공격 행위의 내용을 설정해야 하는데, 조작적 정의의 범위를 설정하기 어렵다. 이는 사이버 공간의 특성을 잘 반영하고 있는데, 인터넷이 우리 일상생활의 모든 영역에 들어와 있기 때문이고, 그 인터넷들이 서로 연결된 것과도 관련이 있다. 억지하고자 하는 악의적 행위를 특정하는 것이 어려운 것은 국가마다 핵심 이익이나 보호해야 할 대상이 다를 수 있기 때문이다. 이런 측면에서 보호되어야 할 대상에 대해 국가 간에 합의를 이루기 어렵다. 그리고 악의적 행위자들조차 그들의 행위의 피해 범위를 예측하지 못할 수 있다. 재래식 무기를 통한 물리적 공격은 그 피해 범위가 예상될 수 있지만, 모든 것이 연결된 사이버 공격에서는 부차적 피해(collateral damage)의 측정이 어렵다. 어떤 곳에서의 연결 차단이 다른 곳에서의 연결 지장으로 이어질 수 있으며, 특정한 타깃을 노린 사이버 무기가 예상치 못한 타깃, 예를 들어 인프라 시설에 공격을 행하여 민간의 피해가 발생할 수 있다. 이러한 사이버 공간의 특

성 때문에, 사이버 공격에 대한 '금지선'의 범위가 매우 포괄적이거나 모호할 수 있다. 특히, 민간이 네트워크 인프라를 제공할 경우, 군과 민간의 구분은 더욱 어려워진다.

이와 같은 이유로 국가 간에 '금지선(red line)'을 합의하는 것이 쉽지 않지만, 금지선의 설정은 보복에 의한 억지 전략의 핵심이다. 보복에 의한 억지는, 어떤 '특정한' 행동을 하게 될 경우, 즉, '금지선'을 넘는 행동을 할 경우, 상응 조치 또는 보복의 이유가 된다는 것을 상대방이 이해하고 납득할 수 있게 규정해야 한다. 너무 폭넓게 규정될 경우, 억지 대상은 자국의 이익에 저해된다고 보고 그러한 범위 설정이 부당하다고 생각할 수 있다. 또, 애매하게 설정될 경우 보복 조치의 시행이 정당한지부터 논란이 있을 수 있다. 사안이 더 복잡해질 수 있는 것은, 동맹국 간에 그러한 '금지선'에 대한 합의를 이루어야만, 공동의 위협에 대해 협력할 수 있게 되는 것이다. 억지를 위한 효과적인 금지선의 설정과 국제적 합의는 사이버 억지를 위한 도전으로 부상했으며, 실무자들과 학자들은 이를 해결해 나갈 필요가 제기되었다.

Ⅲ. 미국 사이버 억지 전략의 발전

이 장은 두 개의 절로 구성된다. 전반부는 거부 및 복원력에 의한 사이버 억지 전략, 후반부는 징벌에 의한 사이버 억지 전략의 발전을 보인다.

1. 전통적 억지 개념에서 거부에 의한 사이버 억지 전략으로의 쇄신

사이버 공간에 대해 그리고 사이버 공간으로부터의 위협이 점차 크게 인식되고, 방어자보다 공격자 우위의 논리가 지배적으로 되며, 사이버 공간의 불안정성은 더욱 주목받았다(Arquilla and Ronfeldt 1993).[9] 기존 전통적 억지 이론에 따르면, 공격이 방어에 비해 유리하다고 인식하는 것 자체가 행위자의 힘에 의한 현상 변화를 추구할 가능성을 높인다.[10] 이러한 불안정성에 대한 인식 증대는 억지 전략의 필요성으로 이어졌다. 사이버 공간이 2010년대부터 국가 행위자들에 의해 국가안보의 영역으로 본격적으로 인식되면서,[11] 사이버 공간에서 억지를 어떻게 작동시킬 것인가는 국

9) 이와 반대되는 견해는 Rid(2012), Gartzke(2013)을 참조할 수 있다.

10) 게다가 공격과 방어 무기 간의 구별이 되지 않으면, 안보딜레마가 발생하여, 힘에 의한 현상 변화 가능성은 더 커질 수 있다(Jervis 1978). 많은 사이버 무기가 이중용도 기술이라는 점을 감안한다면, 사이버 공간의, 사이버 공간을 통한 불안정성은 더 커질 수 있다.

11) 여러 국가들이 2010년대에 국가 사이버안보 전략서를 출간하지만, 미국 오바마(Obama) 정부는 그보다 앞서 2010년 3월에 (부시(Bush) 정부에서 작성 시작했던) '포괄적 국가 사이버안보이니셔티브(CNCI)'를 공표, 2010년 5월에는 '국가안전보장전략(NSS)' 및 '사이버 공간에서의 국제전략'을 내놓는다. 2010년 NSS에서는 디지털 인프라는 전략적 국가자산이며, 그것의 방어는 국가안전보장상의 우선 사항이라고 명시하고 있다.

가 안보 전략의 핵심 사안으로 부상하였다.

사이버 공간에서 억지가 작동하는가 아닌가에 대한 논의가 지속되면서, 점차 어떤 방식의 억지가 가능한가의 논의로 발전해 갔다. 사이버 공간에 대한 미국의 전략이 본격적으로 나오기 시작하는 2000년대 후반 이전에, 미국의 억지 전략은 크게 거부와 징벌에 의한 억지 분류를 따라 형성되어 있었다. 실례로, 미국 국방부는 '이익을 부정하는 억지(Deterrence by Denying Benefits),' '비용을 부과하는 억지(Deterrence by Imposing Costs),' 그리고 '적대국의 억제를 촉구하는 억지(Deterrence by Encouraging Adversary Restraint)'를 든다(Joint Chief of Staff 2006). 이 마지막 억지는, 공격을 하지 않는 것이 더 이익임을 적대국이 인식하게 하는 방식이며, 넓게 보면 '거부에 의한 억지'에 속한다.

그런데 사이버 공간의 특성은 상기한 바와 같이 전통적 억지 정책을 그대로 적용하기에는 여러 어려움을 내포했다. 이 때문에 미군의 사이버사령부(United States Cyber Command, CYBERCOM)의 초대 사령관이자 국가안전보장국장을 지낸 알렉산더 키스(B. Alexander Keith)도 CYBERCOM이 개시하기 직전 의회에서 사이버 분야에서의 억지는 냉전기와 달리 폭넓은 관점에서 억지를 쇄신할 수 있는 연구가 필요함을 호소했다.[12] 많은 연구자도 적어도 물리적 공간에 기반한 전통적 억지 전략, 특히 징벌에 의한 억지는 여러 한계가 있다는 점에 동의하고 있었다(Clarke and Knake 2010, 6장; Morgan 2010; Nye 2016).

12) Statement of Gen. Keith B. Alexander, Commander United States Cyber Command, Before the House Committee on Armed Service, September 23, 2010. CYBERCOM은 2010년에 형성된 혁신적인 새로운 군 조직이다. USCYBERCOM이 세워질 초기, 방어적 목적을 띠고 있었기 때문에, 가장 큰 우려 중 하나는 미국이 공세적 사이버 연구에 과도한 강조를 두고 있다는 것이었고(Singer and Friedman 2014), 이는 사이버 공간을 더욱 불안정하게 만들 수 있다고 생각했기 때문이다.

이런 흐름에서 미국의 사이버 억지 전략은, 후술하는 바와 같이 한편으로 징벌에 의한 억지 전략도 모색되었으나, 먼저 거부에 의한 억지 전략을 추구하게 된다. 이는 상기한 바와 같이 사이버 공간의 특성이 징벌적 사이버 억지의 실현에 더 큰 도전을 부과하고 있었기 때문이다. 이러한 인식은 린(Lynn) 국방부 부장관의 '새로운 영역에 대한 방어(Defending a New Domain: The Pentagon's Cyberstrategy)' 논문에도 잘 드러난다(Lynn 2010a). 유사한 시기에 발간된 정책문서도 위협과 취약성을 발견, 탐지, 분석하여 피해를 줄이게 하기 위한 실시간 능력을 의미하는 '능동적 사이버 방어(active cyber defense)' 개념을 채택한다(The Department of Defense 2011b).[13)]

이렇게 사이버 공간에서의 억지 전략의 방향성이 어느 정도 확립되어 가는 과정에서, 2014년부터의 논의에 '복원력'이라는 새로운 개념이 부상한다. 2014년 7월 국무부 내 국제안전보장 자문위원회가 내놓은 '국제 사이버 안정성에 관한 보고서'는 세 유형의 사이버 억지를 제시한다(International Security Advisory Board 2014). 잠재적 공격자에 대해 공격이 실패하거나 혹은 효용이 없다고 생각하도록 하는 거부적 억지, 보복 손해를 입을 것으로 생각하게 하는 징벌적 억지, 그리고 공격 대상의 아키텍처(architecture)가 공격당한 후라도 회복 탄력적이라고 생각하게 하는 '복원력'의 억지(deterrence by resilience)가 제시된다. 2015년에 4월에 나온 국방부 '사이버 전략'도 이를 답습하여, 억지의 핵심적 요소로 '거부,' '보복(반응, response),' '복원력'을 언급하고 있다(The Department of Defense 2015).

복원력이란 근래 들어 국제 안보나 경제 안보 등 여러 분야에서 사용되고 있는 개념인데, 거부에 의한 억지 논리를 공유하나 그

13) 더 상세한 학술적 논의는 재스퍼(Jasper 2017)를 참조하라.

작동 기제가 각각 다르다.[14] 복원력의 사이버 억지는 거부에 의한 억지와 유사한 논리로, 잠재적 적대자로 하여금 공격의 효용이 없다고 생각하게 만들어 하려던 행위를 멈추게 하는 것이다. 공격을 하더라도 쉽게 복원되기 때문에, 적대국에 공격의 이익보다 비용을 더 크게 인식시키기 때문이다. 복원력의 억지는 거부에 의한 억지와 작동 메커니즘이 다르다. 전자는 적대자에 의한 공격과 그로 인해 피해가 불가피한 것을 전제한다. 즉, 사이버 공격이, 과거 냉전기에 핵무기 사용이 일어나지 않았던 것과 같이, 전혀 없을 것이라고 기대할 수 있는 환경이 아니라고 본다. 따라서 복원력의 사이버 억지는 공격에 따른 피해가 발생하는 것을 상정하고, 그러한 상황에서도 원래 기능이 지속될 수 있고, 그 피해로부터 조기 복구할 수 있는 역량을 갖추는 것을 핵심으로 한다.

이러한 복원력의 억지 개념을 실현시키기 위한 사이버 전략은, 연방정부 차원에서뿐 아니라, 민간과의 연계 그리고 장기적인 시스템 개발의 필요를 제기한다(The Department of Defense 2015). 이 점에서 또한 기존의 재래식 무기에 기반한 거부에 의한 억지 전략과의 차이가 나타난다. 즉, 사이버 공간에 대한 방어가 더 이상 미군만으로는 불가능하다는 인식을 확실히 보이고 있다. 과거 정보기관과 군의 능력만으로 이루고자 한 거부에 의한 억지와 달리 민간과의 협업을 필요로 한다는 점에서,[15] 복원력의 억지는 새로운 사이버 공간의 부상에 대한 미국 억지 전략의 쇄신이었다.

민관의 협력을 기반으로 한 사이버 억지를 향한 노력은 '사이버 보안 인프라 보안청(Cybersecurity and Infrastructure Security

14) 미국은 복원력을 좀 더 넓은 전략 개념으로서 사용하고 있으며, 사이버 공간에의 적용이라고 볼 수 있다.

15) 같은 맥락에서 코스튜크(Kostyuk 2021)의 '공공 사이버제도(public cyberinstitutions)' 개념을 이해할 수 있다. 해당 용어는 정부의 사이버 억지 대책보다 더 넓은 민간의 사이버 역량도 포괄하는 정의를 제안하고 있지만, 구체적인 조작적 정의가 부족해 보인다.

Agency, CISA)'의 설립과 역할에 잘 드러난다. 예를 들어, CISA에서 발행하고 있는 '보안 권고문(cybersecurity advisory)'은 거부에 의한 억지 이론을 잘 구현하고 있다. 보안 권고문은 문제가 된 사이버 작전들에 대한 기술적 세부 사항들을 전술, 기술, 절차(tactics, techniques, and procedures, TTPs)에 따라 알리고, 대응과 완화를 위한 조치를 제시한다. 이러한 문서 발간의 일차적 목적은 문제와 대처 방식에 대한 신속한 정보 공유이다. 그뿐 아니라 특정 악의적 사이버 행위에 대한 정보 공유는, 해당 행위를 더 이상 유용하지 않게 만들어, 행위자가 새로운 TTPs를 개발하도록 강제함으로써 비용을 증가시킨다(NIST 2016, 4). 즉, 일차적으로는 정보 공유를 통해 공격의 이익을 감소시킬 뿐 아니라, 의도한 이익을 실현하게 하기 위한 공격자의 비용을 증가시킴으로써, 공격의 유인(incentives)을 줄여 해당 행위를 억지하기 위한 것이다. 사이버 작전의 비용이 재래식 무기에 비해 상대적으로 작기 때문에 방어자에 대한 공격자 우위의 의견이 있지만, 애초에 큰 효과를 낳을 수 있는 사이버 무기의 비용은 상당하며(Smeets 2018), 저렴한 사이버 무기에 의존하는 공격자들에게는 많은 시간과 인력이 필요한 새로운 TTPs 개발의 강제는 부담이 된다. 공격자 자신이 지급할 비용이 공격으로 인해 얻는 이익보다 커질 경우, 거부에 의한 억지는 작동한다.

복원력에 의한 사이버 억지를 잘 드러내고 있는 것이 2020년 3월에 발간된 솔라리움 보고서(Cyberspace Solarium Commission (CSC) Report)이다. '사이버공간 솔라리움 위원회'는 2019년 미국 의회가 통과시킨 국방수권법안을 통해 만들어졌다. 법안은 해당 위원회가 중대한 사이버 공격으로부터 미국을 방어하는 전략적 접근법에 대한 국가적 합의(consensus)를 만들어 내도록 주문하고 있다(NDAA 2019, Sec. 1652). 보고서는 '다층적 사이버 억지(layered cyber deterrence, LCD)'라는 새로운 전략 개념을 제시

하고 있기는 하다. 하지만 해당 억지 개념은 두 번째 요소에 특히 우선순위를 둔다고 하는데, 이는 적대적인 세력이 사이버 공격으로 이득을 얻지 못하게 하는 거부 전략을 의미한다(CSC 2020, 2). 즉, 민관협력에 기반한 방어를 통한 복원력의 사이버 억지를 강조한다. 여기서도 복원력에 의한 사이버 억지는 사이버 공간에서의 악의적 활동과 그에 의한 피해를 완전히 막을 수 없다는 인식을 보인다. 이는 기존 핵무기 기반의 억지와는 근본적으로 다른 인식이었다. 이런 상황에서 제일 나은 방법은 취약점을 최소화하고, 사이버 공격을 받더라도 그런 공격에 견디고, 기능을 유지하며, 피해를 짧은 시간 내에 복구할 수 있는 역량을 갖추고자 한다.

한편, CSC 보고서는 '다층적 사이버 억지(LCD)' 전략 개념을 통해, 여러 사이버 억지 전략들의 발전과 통합을 위한 가교 역할을 하고 있다고도 볼 수 있다. LCD는 그때까지 발전해 온 거부(또는 복원력)에 의한 사이버 억지뿐 아니라, 지속적으로 발전 중이던 징벌에 의한 억지 전략을 포함하고 있다. 후자의 발전은 밑의 절에서 다룬다.

2. 징벌에 의한 사이버 억지의 발전

위에서 거부에 의한 억지 이론에 기반한 미국의 사이버 억지 전략의 발전을 보았다. 그렇다고 미국의 사이버 전략이 거부에 의한 억지만을 고집한 것은 아니고, 사이버 공간에 대한 국가전략 수립 초기부터 징벌적 사이버 억지에 대한 고려가 존재했다. 예를 들어, 2011년 11월에 나온 '국방부 사이버 공간 정책 보고서'는 이미 두 억지 전략을 고려하고 있다. 해당 보고서는 사이버 공간 또한 다른 영역과 마찬가지로 두 개의 억지 메커니즘이 존재하는데, 하나는 적의 목적을 부정하는 것이고, 다른 하나는 필요하다면 침공

하는 적대자에게 비용을 부과하는 것이라고 적시한다(The Department of Defense 2011a).

그런데 징벌적 사이버 억지의 이행을 위해서는 여러 어려움이 있었다. 밑에서 하나씩 차례대로 다루지만, 사이버 역량이 발전하고, 계기가 되는 사건들이 발생하며, 이러한 도전들에 대한 정책 형성자들과 전문가들의 인식과 담론이 변화되어 갔다. 그 과정에서 방어적 작전에 기반한 거부에 의한 억지 전략의 한계점도 점차 드러나게 되었다. 한편으론 복원력의 억지에 드는 비용이 증가하여 감당할 수 없는 수준에 이르게 된다는 비판이 제기되었으며, 다른 한편으론 복원력의 억지만으로는 중국과 러시아와 같은 국가들(혹은 그 내부의 비국가 행위자들)이 공격을 멈추지 않는다는 것이다. 즉, 거부에 의한 억지만으로는 적대 행위자들의 공격 행태를 형성해 나가기에 무리가 있다는 인식이 점증했다.

이러한 과정 중에 징벌에 의한 억지의 필요성을 제기하는 사건들이 일어나는데, 2014년의 북한에 의한 소니 픽쳐스에 대한 사이버 침해는 한 예였다.[16] 이 사건으로 인해 사회적으로 경각심이 높아진 상황에서, 알렉산더 키스에 이어 2015년에 CYBERCOM 사령관과 NSA 국장을 맡게 된 마이클 로저스(Michael S. Rogers)는 상원 군사위원회 청문회에서 순수하게 방어적이고 반응적인 전략만으로는 더 이상 억지가 작동하지 않으며, 공격 없는 방어를 위한 비용은 급상승할 것이기 때문에 공세적인 전략의 전개가 필요하다고 언급했다(Nakashima 2015).

미국의 사이버 억지 전략은 거부에 의한 억지를 중심으로 전개됐음을 위에서 보였다. 그러면서 다른 한편으론 징벌에 의한 억지의 필요성이 지속해서 제기되어 왔다. 그러다가 억지 전략의 무게

16) 미 백악관은 이 사건을 심각한 국가 안보 문제로 보고, 2015년 1월 북한 인민무력부 정찰국 소속의 인원들을 금융 제재의 대상으로 지정하였다. 이후로부터 외국발 사이버 공격에의 경제 제재 수단들은 빈번히 채택된다.

중심추의 이동이 2018년에 이르러 본격적으로 나타났다.

1) 공개 귀속(public attribution)의 활용

이론 장에서 논한 바와 같이, 보복으로서의 징벌을 하기 위해서는 우선 귀속이 가능해야 한다. 누가 공격했는지 알지 못하면, 징벌로서의 보복을 할 수 없기 때문이다. 따라서 귀속의 문제를 해결하기 위해 미국은 일찍부터 노력해 왔다. 2012년에 리온 파네타(Leon E. Panetta) 국방부 장관은 징벌적 억지를 복잡하게 하는 공격의 근원을 특정하는 문제를 해결하기 위해, 국방부가 지난 2년간 포렌식에 큰 투자를 해 왔고, 큰 진전을 지속해서 이루고 있는 과정이며 성과를 얻을 수 있었다고 언급한 바 있다(Panetta 2012). 그럼에도 귀속의 문제는 해결하기 쉽지 않았으며, 해당 문제를 해결하기 위한 역량과 경험이 축적되기까지의 시간이 필요했다. 시간이 지나면서, 귀속을 위한 기술적 수준도 점차 발전했으며, 법적 귀속을 위한 국내 법 제도적 측면들도 갖춰져 갔지만, 정치적 귀속에 대한 우려는 2018년까지 정책결정자들 사이에 여전히 강하게 남아 있었다. 이 때문에 징벌적 억지를 위한 핵심 조건인 정치적 귀속에 대한 의지가 난제로 존재했다. 그런데 2018년부터 그러한 분위기는 전환되었다.

미·중 전략 경쟁은, 소위 '무역 전쟁'의 발발을 서곡으로 하여, 중국, 러시아, 이란, 북한과 같은 나라들을 명백히 위협으로 지정하였다. 이런 구조적 변화는 정치적 귀속에 대한 우려를 급격히 줄이는 환경적 변화였다. 이러한 전환은 2018년의 '국가 사이버 전략(National Cyber Strategy)'에도 드러나는데, 3번째 필러(pillar)인 '힘을 통한 평화의 보전'은, 국제 구조적인 변화 속에서의 사이버 억지 전략의 변화를 나타냈다(The White House 2018). 미국은 악의적 행위자들에게 더욱 강력한 충격을 가하기 위해 신

속하고, 고비용이며, 투명한 '대가'를 부과하고, 동시에 강한 메시지를 전달할 것임을 천명하고 있다. 그리고 그러한 활동의 하나로 귀속을 포함한다.[17] 같은 맥락에서 2018년 미 국가정보국(Officie of Director of National Intelligence, ODNI)도 '사이버 귀속 지침(A Guide to Cyber Attribution)'을 발표했다.[18]

귀속은 세 측면에서 징벌에 의한 억지의 수단이 된다. 첫째, '이름 불러 망신 주기(naming and shaming)' 또는 '혐의 제기(accusation)' 과정을 통해 평판에 타격을 주고, 외교적 영향력을 약화할 수 있다(Finnemore and Hollis 2020). 다음으로, 국내/국제법을 통한 집행의 근거를 제공할 뿐 아니라 국제법이나 규범 생성의 환경을 조성한다(Egloff 2020). 마지막으로, 보복으로서의 대응조치(countermeasures)에 정당성을 더한다. 2018년 국가 사이버 전략은 공개 귀속 활용을 적시하고 있는데, 미국이 이전에는 공개 귀속을 하지 않았다는 것을 뜻하는 것이 아니라, 이제부터는 귀속을 징벌 차원으로써 인식하고 적극 활용하겠다는 것을 의미했다.

2) 징벌(punishment)적 작전의 강조

2018년에 이르러 미국의 사이버 억지 전략의 전환을 단적으로 드러낸 것이 국방부가 발간한 9월의 사이버 전략에 포함된 '지속적 관여(persistent engagement)'와 '전진 방어하기(defend forward)'이다.[19] 특히, 후자는 '무력 갈등(armed conflict)'에 이르지

17) 그리고 이러한 효과를 더 크게 하기 위해 동지국가연합과 함께 할 계획임을 밝히고 있다. 해당 전략서는 이를 '사이버 억지 이니셔티브(a Cyber Deterrence Initiative)'로 명명하고 있다.

18) 이러한 흐름을 반영하여 2019년 9월에 발표된 한국의 '국가 사이버안보 기본계획'에도 최종 공격원점 규명을 사이버공격 억지 수단으로 활용할 것을 언급하고 있다.

19) 일부는 '선제적 방어'로 번역한다. 그런데 '선제적'이라는 단어는 preemptive

않는 수위의 악의적 사이버 행위라도, 근원에서부터 훼방하고 멈추게 하는 것을 의미한다(Department of Defense, 2018).[20] 그리고 사이버 공간에 국한되지 않고 모든 가용한 수단을 써 '비용'을 부과하겠다고 한 점에서, 징벌에 의한 사이버 억지를 내비치고 있다. 즉, 방어를 통해 상대방에게 이득이 생기는 것을 거부하는 사이버 억지 전략을 넘어, 사이버 공간에서 적극적으로 징벌하여 상대방에게 비용이 부과됨을 예상케 하는 방식으로 억지하는 것을 의미한다.

'전진 방어하기' 개념은 확실히 복원력에 의한 억지 전략을 벗어나고 있지만, 여전히 그 자체만으로는 반응적(reactive)이며, 본질상 수세적 사이버 작전이라는 비판을 받기도 한다(Pendino et al. 2022, 2).[21] 설령 사이버 작전이 국경을 넘어 상대방의 시스템에 지장을 초래하는 보복적 방식을 취하더라도, 적대적 행위에 대응

의 번역어로 쓰기 때문에 혼동을 초래할 수 있다. 해당 전략서에서 'defend forward'는 재래식 전쟁에서의 preemptive strike와는 다른 의미로 사용된다. 오히려 냉전기에 사용되었던 개념인 'Forward Defense'의 사이버 공간에 응용한 것에 가깝다. Forward Defense는 위협 원천에, 즉 소련의 근처에 군사력을 배치하는 개념이었다. 따라서 'defend forward' 미국 본토의 네트워크에 이르기 전에 사이버 위협의 근원에서 맞서서 대처한다는 뜻이지, 반드시 선제적(preemptively)으로 대응한다는 뜻은 아니다.

20) 중국, 러시아, 이란, 북한과 같은 국가들이 점차 군사적 대응을 야기하는 결정적 구실을 제공하지 않는 방법으로 사이버 공간에서 작전을 펼치고 있다. 비폭력적이지만 전략적 손실을 입힐 수 있는 방법들, 예를 들어 허위조작정보(disinformation) 유포나 사이버첩보행위(cyber espionage)와 같은 '회색지대 갈등(grayzone conflict)'의 활용이다.

21) 미국 사이버 사령부는 '지속적 관여(persistent engagement)'라는 전략을 위해, '전진 방어하기'라는 작전 개념과 '전진 추적 작전(hunt forward operations)'을 함께 제시한다. 후자는, 파트너 국가의 네트워크 내부에 존재하는 악의적 사이버 활동과 취약성을 함께 찾아가는 작전을 의미한다. 이는 "파트너 국가의 요구에 의한 엄격하게 방어적 작전"임을 밝히고 있다(https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/).

하는 작전이기 때문이다. 전략적 목적을 달성하기 위한 공세적 사이버 작전(offensive cyber operations)의 적극적 주창과는 거리가 있다. 이러한 비판에도 불구하고, 방어에만 전념하는 수세적 사이버 작전이 아닌, 보복을 동반하는 수세적 사이버 작전(defense cyber operations with retaliation)을 통해 대가를 치르게 한다는 점에서, (비록 엄격하게는 공세적 사이버 작전에 이르지 못하지만)[22] 징벌적 사이버 억지로의 전환을 명확히 보인다.[23]

징벌에 의한 사이버 억지로의 전환은, 악의적 사이버 행위에 대한 보복으로서 사이버 영역에 제한되지 않는 다양한 대응 수단(countermeasures)을 활용할 것이라고 천명하는 것에서도 볼 수 있다. 미국 국방전략서(National Defense Strategy)의 '통합 억지(integrated deterrence)' 개념은 이를 단적으로 보인다.[24] 통합된 억지는 육해공, 우주, 사이버의 모든 영역을 포함하며, 외교, 정보,

22) 공세적 사이버 작전은 수세적 작전에 기반한 보복 행위보다 훨씬 더 긴장상승/확전의 위험이 높다. 이 때문에 공세적 사이버 작전의 천명은 신중하게 이루어질 필요가 있다. 비록 명시적 선언을 하지 않았을지라도, 실제로는 공세적 사이버 작전이 (비)공개적으로 수행될 수 있으며, 보복을 동반하는 수세적 작전과의 경계성은 종종 모호할 수 있다.

23) 물론, '전진 방어하기'의 제시가 미국이 이전에 대응조치를 하지 않았다는 것을 의미하지 않는다. 미국은 악의적 사이버 행위에 대해 법적 기소나 경제 제재를 포함한 여러 조치들을 취해 왔다. 예를 들어, 미국은 2014년 북한의 소니픽처스 해킹 사건에 대해 경제 제재뿐 아니라, 비록 정부는 공식적으로 인정하지 않았지만, 북한의 인터넷망을 마비시키는 등의 대응조치를 취했다고 보도된 바 있다(Miller 2015).

24) 미국은 '통합 억지' 개념 이전에, '동등함(equivalence)'의 전략을 논의해 왔다. 해당 개념은 미군이 사이버 공간에서 싸우고 이길 계획을 가지고 있으나, 만일 사이버 공간이 바라는 결과를 낳기에 적절하지 않다면, 다른 영역에서의 '동등한' 공격도 불사하겠음을 의미한다. 이는 사이버 공간에서의 불리함을 사이버 공간 밖에서의 우세한 힘으로 치환하겠다는 것으로, '확전 지배(escalation dominance)'라는 개념과 맞닿아 있다(Mahnken 2011). 다른 영역으로의 확전 여부를 결정할 수 있는 것은 결국 전통적 강대국이며, 사이버 공간의 억지도 전통적 또는 물리적 역량을 가지고 달성할 수 있다는 뜻을 내포한다.

군사 그리고 경제적 모든 도구를 사용하여, 동맹국과 파트너 국가들과의 조율 협력하는 것을 포함한다(Garamone 2021).[25] 이 개념은 보복에 의한 사이버 억지를 이행하는 데 다음과 같은 이유로 중요하다.

첫째, 사이버 징벌 수단의 제한 때문이다. 모든 나라들이 미국 사회와 같은 정도로 인터넷에 기반에 의존하고 있지 않다. 예를 들어, 북한과 같은 나라는 인터넷 접속이 심하게 제한되어 있다. 사이버 공격의 대상이 많으며, 사이버 공격의 피해가 광범위할 수 있는 미국과 같은 나라에, 사이버 공간은 비대칭 영역이다. 인터넷 접속이 제한된 국가에 사이버 보복은 효과적인 징벌적 수단이 되지 않을 수 있다.

둘째, '타이밍(timing)'의 문제 때문이다. 복원력에 의한 억지의 경우, 얼마나 적절한 시기 내에 사이버 공간의 기능을 회복해 낼 수 있는가가 중요했다. 그런데 타이밍은 징벌적 억지를 위해서도 매우 중요하다. 10억분의 1초 사이에 가해지는 사이버 공격에 비해, 확전을 방지하기 위한 정확한 귀속과 사이버 보복 수단에 대한 효과의 추정에는 시간이 오래 걸릴 수 있다. 재래식 무기의 경우, 그 파괴 효과의 범위에 대해 비교적 잘 알고 있기 때문에, '통합 억지'는 보복에 걸리는 시간이나, 징벌을 행할 수 있는 유효 기간에 얽매일 필요가 없게 된다.

셋째, '신호전달'을 명확히 할 수 있다. 만일 상대방이 미사일로 공격했는데 맬웨어로 보복한다면, 해외뿐 아니라 국내 청중에게도 제대로 된 신호전달이 안 될 수 있다. 즉, 다양한 보복 수단 가운

25) 이런 가용한 모든 정책적 도구를 동원하는 종합적(comprehensive) 접근은 징벌, 거부, 연루, 그리고 규범의 차원에서 사이버 억지와 단념을 주장한 나이(Nye 2016)의 주장과 유사하다. 그러나 그는 귀속의 문제 때문에, 징벌에 의한 사이버 억지는 어렵다고 보았다는 점에서 징벌적 사이버 억지 전략의 발전을 고려하지 못했다.

데 신호전달을 극대화할 적절한 선택이 중요하며, 이 중에는 재래식 무기뿐 아니라, 대단히 소란스러운 사이버 무기부터 매우 은밀한 사이버 무기도 포함된다. 타깃으로 하는 청중에 따라 다양한 수단을 가용하게 되면 더욱 효과적인 신호전달을 할 수 있다.

이러한 유용성에도 불구하고, '통합 억지' 개념은 자칫 확전될 수 있는 위험을 내포한다. 특히, 자국에 가해진 사이버 공격으로 인한 피해라든가, 적국에 가해질 사이버 공격 피해의 규모와 범위에 논란이 있으면, 전쟁법의 비례성의 원칙에 따라 보복의 정당성이 결여될 수 있다. 이 때문에라도 사이버 침해의 피해를 평가할 수 있는 '위협침해 평가' 지수의 마련이 중요하게 된다. 그리고 그 상위 개념인 '금지선(redline),' 즉 넘어서는 안 되는, 혹은 넘게 되면 대응조치를 취하게 되는 전략적 사이버 인계철선(strategic cyber tripwire)이 필요하게 된다.

3) 금지선 설정

징벌적 억지를 위한 마지막 필수 요소는 '금지선' 설정이다. 상기한 바와 같이, 사이버 공격은 냉전기 핵무기와 달리 완전히 억지 될 수 있는 것이 아니다. 크고 작은 사이버 공격은 늘 있었으며, 앞으로도 계속될 것이기 때문에, 징벌적 사이버 억지의 핵심은 오히려 적의 사이버 공격 행태에 영향을 미치는 노력으로 이해해야 한다. '금지선'은 특정 악의적 사이버 행위를 하지 못하도록 '신호전달'의 역할을 함과 동시에, 적으로 하여금 금지선을 넘는 행위를 하기 전에 한 번 더 고민하게 만들 수 있다. 이런 맥락에서 '축적적 사이버 억지(cumulative cyber deterrence)'가 제안되기도 한다(Pendino et al. 2022; Tor 2017). 상호작용을 통해 특정 행위에 반응하는 금지선에 대한 학습효과가 쌍방 간에 축적되며, 특정 공격 유형에 대한 억지가 생성된다는 것이다.

징벌적 억지를 위해 적절한 '금지선'의 설정은 중요하다. 그런데 금지선을 어떻게 설정하는가는 징벌적 사이버 억지를 위한 큰 도전이 된다. 이런 맥락에서 2015년 4차 UN 사이버 GGE에서 합의된 11개의 규범은 유용하다. 글로벌 다자주의 회의에서 합의된 바이기 때문에, 해당 규범에 근거하여 금지선이 작성된다면, 정당성의 확보가 용이하다. 미국은 합의된 규범을 금지선의 근거로써 활용해 왔다.

하지만 국제 사회에서 받아들여질 수 있는 적절한 '금지선'의 설정은 쉽지 않다. 합의가 되더라도 이행은 더욱 어렵다. 특히, 적대적 국가 간에는 더욱 어려운데, 단적인 예가 2021년에 있었던 미국 바이든 대통령과 러시아 푸틴 대통령과의 회동에서 보인다. 바이든 대통령은 '사이버보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency, CISA)'에서 지정한 16개의 주요 인프라 영역들을 푸틴 대통령에게 제시하며, 공격의 대상이 되지 못함을 요구했다. 미 대통령이 러시아 대통령에게, 미국이 상당한 사이버 역량을 가지고 있으며, 기본적 규범을 위반할 때 사이버 역량으로 반응할 것이라는 경고를 한 것이다. 이는 사이버 억지 차원에서 의미가 있을 수 있지만, 결과적으로 푸틴 대통령은 이러한 '금지선'을 받아들이길 거부했다(Yoo 2022). 통신, 금융서비스, 정보 기술 등 16개의 주요 인프라가 너무 폭넓게 정의되었던 탓으로 볼 수 있다. 마찬가지로 중국에 대해 자국 기업을 지원하기 위한 사이버 첩보 행위에 대한 금지를 논의해 왔지만, 2015년 미·중 간에 합의된 바는 준수되지 않고 있다. 해당 사이버 첩보 행위가 너무 광범위하게 이루어지고 있으므로, 적절한 범위가 규정되지 않고서는 규범이 '금지선'으로 작동하기에는 무리가 있다.

금지선에 대한 합의가 동맹국들 또는 파트너 국가들과는 상대적으로 용이할 수 있지만, 그들 간의 협력 또한 전략적, 전술적 층위

에서 풀어야 할 여러 도전이 여전히 산적해 있다. 전략적 차원에서는, 그것이 방어적 대응이든 공세적 작전이든 간에, 과연 작전을 수행할 것인가, 그리고 한다면 어떻게 하는가에 대한 이해가 공유되어야 한다. 작전의 적절한 범위와 경계선을 정의해야 하는데, 이는 각 국가가 내리는 사이버 공간의 정의에 따라 다를 수 있기 때문이다.

전술적 차원에선, 공동 군사 작전 수행을 위해 어느 정도 첩보를 공유할 것인가의 문제가 있다. 첩보 행위는 국가별로, 혹은 파이브 아이즈와 같이 매우 소수의 국가 단위에서 이루어지는데(Gold 2020), 동맹은 두 국가 간 협력이나 나토(NATO)와 같은 좀 더 넓은 범위로 맺어져 있다(Jacobsen 2021; Platte 2023). 그리고 공세적 사이버 작전뿐 아니라, '지속적 관여'를 기반으로 한 '전진방어하기'의 경우도, 상대방에게 타격을 가하는 시점에만 첩보가 필요한 것이 아니라, 잠재적 적에 대한 상시적 첩보를 갖추고 있어야 수행이 가능하다. 그런데 이러한 매우 민감한 첩보가 국가 간에 공유될 수 있는가의 문제가 있다. 일국의 첩보 수집 방식은 동맹에 대한 첩보 수집을 포함하는 경우가 많기 때문이다. 첩보 수집과 군사 작전 수행 중에 어느 것에 우선순위를 두는가의 문제도 포함해서, 동맹국 간의 신호 첩보 수집 관련 협력의 제도화에는 이 밖에도 여러 난제가 존재한다(Lonergan and Montgomery 2022). 미국은 금지선의 투명성 증진과 동맹과의 조율을 진행 중이다.

Ⅳ. 결론

본 논문은 미국의 사이버 억지 전략의 발전 과정을 명확히 추적하는 것을 목적으로 하여, 크게 나누어 거부에 의한 억지와 징벌에 의한 억지 이론에 따라 서술하였다. 기존 연구들은 통시적인 사이버 억지 전략의 발전을 보지 못하고, 몇몇 개념에 국한하는 경향이 있었다. 그리고 거부와 징벌적 사이버 억지 전략과 수세적 그리고 공세적 사이버 작전 개념들과의 관계가 불명확했다. 공세적 사이버 작전이 무엇인지, 어떻게 징벌적 사이버 억지 전략과 연결되는지에 대한 논리도 명확하지 않았다. 이 논문은 미국 사이버 억지 전략의 발전 과정을 통해 이러한 연구 간극을 메우고 있다(<표 1> 참조).

<표 1> 사이버 억지 전략

억지 전략	영역 특화된 억지 전략	사이버 작전
거부에 의한 억지	(거부에 의한 사이버 억지)	정보기관·군 중심의 수세적 작전
	복원력에 의한 사이버 억지	민관협력의 수세적 작전
징벌에 의한 억지	(징벌에 의한 사이버 억지)	보복이 동반되는 수세적 작전 (예: '전진 방어 하기')
	축적에 의한 사이버 억지	공세적 작전 (예: 공개 귀속, 통합 억지 수단, 금지선 설정 기반의 사이버 공간 공격)

출처: 저자 작성

미국에서는 초기 사이버안보 국가전략 구상 시에 징벌에 의한 사이버 억지보다 거부에 의한 억지가 더 현실적인 전략으로 인식되었다. 사이버 공간의 특성은 특히 징벌에 의한 사이버 억지에 큰 도전을 제기하였는데, 크게는 귀속(타이밍)의 문제, 신호전달의

문제뿐 아니라, 구체적으로는 공개 귀속, 사이버 작전에 의한 긴장 상승 및 확전의 가능성, 사이버 무기 역량의 투명성 그리고 금지선의 설정 등이 있었다.

이 때문에 미국은 거부에 의한 사이버 억지를 바탕으로, 복원력에 의한 사이버 억지 전략을 우선 수립해 나갔다. 기존 핵무기 기반의 억지 전략과는 다른 사이버 공간의 특수성에 대한 인식을 두고, 사이버 공격의 불가피성을 전제하고 쇄신한 억지 전략이었다. 2020년 사이버 솔라리움 보고서에서도 강조되었던 사이버 억지로서의 다양한 이해당사자들 간, 특히 민관의 협력은, 정보기관과 군 중심의 전통적 억지와는 달랐다.

한편으로 거부에 의한 사이버 억지 전략을 발전시키지만, 다른 한편으로는 거부에 의한 사이버 억지의 한계를 경험하던 미국은, 결정적으로 2018년을 기점으로 사이버 억지 전략에 징벌적 요소들을 적극적으로 도입하기 시작했다. 귀속에 대해 기존에 제기되었던 문제들에 대해 기술적, 법적, 정치적 측면들에서 어떻게 해결하겠다는 지침을 마련하였고, 공개 귀속이라는 징벌을 통해 억지 효과를 노렸다(Egloff 2020). '통합 억지(integrated deterrence)' 또는 '영역 간 억지'(Gartzke and Lindsay 2019)를 통해서 악의적 행위자들이 대가를 치르게 하려고 수단을 가리지 않을 것을 표명했으며, '전진 방어하기(defend forward)'를 통해서 악의적 공격에 대한 보복적 대응을 서슴지 않겠다는 의지를 내비쳤다. 이와 같은 개념들은 모두, 기존에 인식되었던 사이버 공간의 도전을 극복하겠다는 미국의 의지를 뚜렷이 나타냈다. 그리고 신호전달의 효과를 높이기 위해 적대국의 '전략적 사이버 공격'이나 미국의 '전략적 이익'이라는 용어를 통해, 국가 안보, 주요 인프라, 지식재산권, 민주주의 선거 등을 '금지선'으로 설정하는 노력을 지속해서 하고 있다(The Department of Defense 2023).

미국은 현재 (보복을 동반한 수세적 그리고 공세적 사이버 작전을 포함하는) 징벌적 사이버 억지 작전의 동맹 간 협력을 추진하고 있다. 이런 맥락에서 본문에서 제기한 도전들 외에도, 한국과 같은 중견국이 동맹국과의 사이버안보 협력에 있어 고려해야 할 사항들이 있다. 첫째, 공세적 사이버 작전 수행의 상충점(trade-offs)을 인식해야 한다. 효과적인 사이버 작전의 수행과 사이버 무기 개발에는 막대한 비용이 드는데, 강대국에 비해 자원과 인력이 더 제한된 중견국은 총과 버터 사이에서 적절한 선택을 내려야 한다(Powell 1993). 제한된 자원만이 허락되기 때문에, 공세적 사이버 역량의 개발과 작전 대상도 신중히 제한해서 선택해야 한다. 한국은 공세적 사이버 작전을 (동맹국과 함께) 취할 필요가 있는지, 그리고 한다면 어느 국가(하부 행위자)를 대상으로 할 것인지 신중히 따져봐야 할 것이다. 중견국의 제한된 자원으로는, 방어적 사이버 작전에 기반한 최소한의 그러나 효과적인 공세적 사이버 작전이 적절할 것이다.

둘째, 사이버 작전은 고도의 기관 간 협조를 요한다. 사이버 작전과 관련해서는, 여러 유관 기관 중에서도, 특히 정보기관(의 첩보 수집)과 군 기관(의 무장) 간의 자원투입을 위한 우선순위 설정과 기관 간 조율을 위한 제도가 필요하다(Arena and Wolford 2012). 한국은 이와 같은 커다란 방향성에 대한 고민도 필요하지만, 실무적으로도 정부 기관 간뿐 아니라 민관 사이에도 데이터 이동 및 정보 공유를 원활히 협력하고 조율하기 위한 법과 조직체계의 제도 수립이 시급하다.

셋째, 지정학적 갈등에 전면적 참여 또는 헷징(hedging)과 같은 총체적 국가전략을 염두에 두고 규범 형성 노력에 적극적으로 참여해야 한다. 상기한 바와 같이, 국제 규범은 외교적 차원뿐 아니라 사이버 작전 차원에서도 핵심적 요소이다. 한국이 어떠한 가치와 대상을 수호하길 원하는지 규범을 통해 금지선을 명확히 하는

것은, 적대국에 억지 효과를 발휘할 수 있다. 그리고 우발적 확전을 방지하는 것이기도 하다. 특히, 사이버 작전의 수행을 동맹국과 협력하여 진행하게 될 경우를 대비하여, 한국의 상황과 이익이 반영되는 국제 규범 형성에 노력해야 할 것이다. 이는, 전략적, 전술적 층위에서 어느 정도로 정보와 역량을 공유하고, 임무와 책임을 분담할 것인지 등의 실무적 차원의 결정과도 연관된다. 한국의 대내적, 환경적 특수성을 잘 반영해야 할 것이다.

마지막으로, 2024년 2월 1일 한국은 '국가 사이버안보 전략'을 개정하며, 위협 주체, 국제협력 방안, 대내적 사이버안보 거버넌스 수립 방향성을 구체화했다(국가안보실 2024). 전략 이행을 위한 수많은 과제가 예상되지만, 전략서가 가장 처음으로 내세우는 '공세적 사이버 활동'에 대한 투명한 개념 정립이 무엇보다 필요하다. 이 논문에서 보이듯이, 어떤 활동이 공세적 사이버 작전을 이루는 것인지, 어떤 사이버 공격이 공세적 사이버 작전을 촉발하는지 금지선을 밝히고, 현상 유지를 위한 억지 차원의 공세적 작전임을 명확히 하는 것이 중요하다. 이러한 투명성 증진은 '공세적'이라는 표현으로 인한 불필요한 긴장 관계의 고조와 확전으로 이어지지 않고 억지의 실효성을 증진할 것이다.

본 연구는 미국의 사례를 중심으로 사이버 억지 전략의 발전을 분석했다. 국제정치적 영향력과 사이버 공간에서 미국의 위상을 감안했을 때, 미국 사례의 분석은 억지 전략의 발전을 이해하는 데 중요하지 않을 수 없다. 그러나 모든 국가들이 미국과 같은 역량을 가진 것도 아니며, 놓인 환경도 각기 다르게 인식할 수 있다. 따라서 향후에는 다양한 중견국들의 사이버 억지 전략 및 작전에 대한 연구를 통해, 한국의 학계와 실무자들에게 또 다른 영감을 줄 수 있다. 인과관계 규명을 수반한 실증적 분석도 한 방법이다. 또 다른 향후 연구 방향은 사이버 작전의 동맹 간 혹은 동지 국가 간 협력에 대한 것이다. 구체적으로 어떻게 협력해야 할지에 관한

연구뿐 아니라, 어떤 협력 형태가 국가 간 분쟁의 해소, 혹은 확전으로 이어질지에 대해서 규명해 나갈 필요가 있다. 사이버 억지의 실제와 이론은 앞으로도 지속적인 상호작용을 통해 흥미롭게 전개되어 나갈 것이다.

〈참고문헌〉

국가안보실. 2024. 『국가 사이버안보 전략』. 서울: 대통령실 국가안보실.

Arena, Philip, and Scott Wolford. 2012. “Arms, Intelligence, and War.” *International Studies Quarterly* 56(2): 351–65.

Arquilla, John, and David F. Ronfeldt. 1993. “Cyberwar Is Coming!” *Comparative Strategy* 12(2): 141–65.

Borghard, Erica D., and Shawn W. Lonergan. 2021. “Deterrence by Denial in Cyberspace.” *Journal of Strategic Studies* 46(3): 534–69.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford University Press.

Clark, David D., and Susan Landau. 2010. “Untangling Attribution.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options of U.S. Policy*, 39. Washington DC: The National Academies Press.

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: The next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers.

Dunn Cavelty, Myriam, and Florian Egloff. 2019. “The Politics of Cybersecurity: Balancing Different Roles of the States.” *St Antony’s International*

Review 15(1): 37-57.

Egloff, Florian J. 2020. "Public Attribution of Cyber Intrusions." *Journal of Cybesecurity* 6(1): 1-22.

Fearon, James D. 1997. "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs." *Journal of Conflict Resolution* 41(1): 68-90.

Finnemore, Martha, and Duncan B. Hollis. 2020. "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity." *European Journal of International Law* 31(3): 969-1003.

Fischerkeller, Michael P., and Richard J. Harknett. 2017. "Deterrence Is Not a Credible Strategy for Cyberspace." *Orbis* 61(3): 381-393.

Garamone, Jim. 2021. "Concept of Integrated Deterrence Will Be Key to National Defense Strategy, DOD Official Says." U.S. Department of Defense(December 8). https://www.defense.gov/News/NewsStories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/.

Gartzke, Erik. 2013. "The Myth of Cyberwar." *International Security* 38(2): 41-73.

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

Gerring, John. 2012. "Mere Description." *British Journal of Political Science* 42(4): 721-46.

Gold, Josh. 2020. *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

International Security Advisory Board, United States Department of State. 2014. "Report on A Framework for International Cyber Stability." United States Department of State(July 2), 10-11.

Jacobsen, Jeppe T. 2021. "Cyber Offense in NATO: Challenges and Opportunities." *International Affairs* 97(3): 703-20.

Jasper, Scott. 2017. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. Lanham, MD: Rowman & Littlefield.

Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30: 167-214.

Joint Chief of Staff, Department of Defense. 2006. "Deterrence Operations Joint Operating Concept. Version 2.0." 24-28.

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

King, Gary, Robert O. Keohane, and Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press.

Kostyuk, Nadiya. 2021. "Deterrence in the Cyber Realm:

Public versus Private Cyber Capacity." *International Studies Quarterly* 65(4): 1151-62.

Kreuzer, Marcus. 2019. "The Structure of Description: Evaluating Descriptive Inferences and Conceptualizations." *Perspectives on Politics* 17(1): 122-39.

Kugler, Richard L. 2009. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, D.C.: National Defense University Press.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: The RAND Corporation.

Lonergan, Erica D., and Mark Montgomery. 2022. "The Promise and Perils of Allied Offensive Cyber Operations." 14th International Conference on Cyber Conflict: Keep Moving! (CyCon) 79-92.

Lynn, William J. III. 2010a. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89(5): 97-108.

Lynn, William J. III, Deputy Secretary of Defense. 2010b. Remarks at STRATCOM Cyber Symposium(May 26), Omaha, Nebraska.

Mahoney, James, Khairunnisa Mohamedali, and Christoph Nguyen. 2016. "Causality and Time in Historical Institutionalism." In *The Oxford Handbook of Historical Institutionalism*, edited by Orfeo

Fioretos, Tulia G. Falleti, and Adam Sheingate, 71-88. New York: Oxford University Press.

Mahnken, Thomas G. "Cyberwar and Cyber Warfare." In *America's Cyber Future: Security and Prosperity in the Information Age*, vol. 2, edited by Kristin M. Lord and Travis Shard. Washington, DC: Center for a New American Security.

Maurer, Tim. 2018. *Cyber Mercenaries: The State, Hackers, and Power*. New York: Cambridge University Press.

Miller, Zeke J. 2015. "U.S. Sanctions North Korea Over Sony Hack." *Time*(January 2).

Morgan, Patrick M. 2010. "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm." *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington D.C.: The National Academies Press.

Morrow, James. 1999. "The Strategic Setting of Choices: Signaling, Commitment, and Negotiation in International Politics." In *Strategic Choice and International Relations*, edited by David Lake and Robert Powell, 77-114. Princeton, NJ: Princeton University Press.

Nakashima, Ellen. 2015. "Cyber Chief: Effort to Deter

Attacks Against the U.S. Are Not Working." *The Washington Post*(March 19).

National Institute of Standards and Technology (NIST). 2016. "Guide to Cyber Threat Information Sharing." *NIST Special Publication* 800-150.

Nye, Joseph S. Jr. 2016. "Deterrence and Dissuasion in Cyberspace." *International Security* 41(3): 44-71.

Nye, Joseph S. Jr. 2021. "Will Biden's Red Lines Change Russia's Behaviour in Cyberspace?" *Australian Strategic Policy Institute: The Strategist*(July 8). https://www.aspistrategist.org.au/will-bidens-red-lineschange-russias-behaviour-in-cyberspace/.

Panetta, Leon E., Secretary of Defense. 2012. Remarks on Cybersecurity to the Business Executives for National Security(October 11), New York City.

Pendino, Stephanie, Robert K. Jahn Sr., and Kirk Pedersen. 2022. "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light." *Campaigning: Journal of the Joint Forces Staff College*(Sep 7): 1-10.

Platte, James E. 2023. "Bilateral Alliances in an Interconnected Cyber World: Cyber Deterrence and Operational Control in the US Indo-Pacific Strategy." *Asian Perspective* 47(1): 75-99.

Powell, Robert. 1993. "Guns, Butter, and Anarchy." *American Political Science Review* 87(1): 115-

32.
Rid, Thomas. 2012. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35(1): 5-32.
Rid, Thomas, and Ben Buchanan. 2015. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38(1-2): 4-37.
Singer, P. W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone needs to Know*. New York: Oxford University Press.
Smeets, Max. 2018. “A Manner of Time: On the Transitory Nature of Cyberweapons.” *Journal of Strategic Studies* 41(1-2): 6-32.
The Congress of the United States. 2018. John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019).
The Cyberspace Solarium Commission (CSC). 2020. CSC Report.
The Department of Defense. 2011a. Department of Defense Cyberspace Policy Report.
The Department of Defense. 2011b. Department of Defense Strategy for Operating in Cyberspace.
The Department of Defense. 2015. The DoD Cyber Strategy.
The Department of Defense. 2018. Department of Defense Cyber Strategy.
The Department of Defense. 2023. Summary: 2023 Cyber Strategy.

The White House. 2018. National Cyber Strategy. Washington D.C.: The White House.

Tor, Uri. 2017. "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence." *Journal of Strategic Studies* 40(1-2): 92-117.

Yoo, In Tae. 2022. "Bilateral Cyber Confidence Building Measures in Northeast Asia." *Korean Journal of Defense Analysis* 34(4): 633-656.

논문접수일 : 2024년 1월 25일
논문심사일 : 2024년 2월 6일
게재확정일 : 2024년 2월 19일

Evolving Cyber Deterrence Strategy of the United States
: Cyber Operations of Denial, Resilience and Punishment

| In Tae Yoo Dankook University

| Abstract

How has the U.S. cyber deterrence strategy evolved? The literature on U.S. cyber deterrence is often characterized with limited scopes, dealing with one or a few cyber deterrence strategies and concepts. This research, however, descriptively analyzes the development of U.S. cyber deterrence strategy, arguing that U.S. cyber deterrence strategy has gradually evolved in two, yet complementary, fashions, deterrence by denial and by punishment, in different time lines. This argument is in contrast to the idea that institutions are created as a "big bang" theory and evolve along the monotonic singular path. In the U.S., although strategies both on deterrence by denial and deterrence by punishment were considered in the early stages of developing U.S. national cybersecurity strategy, it first has focused on cyber deterrence strategy by denial and later gradually developed deterrence by punishment in cyberspace as it successfully dealt with challenges stemming from the unique attributes of cyberspace, which are different from those of the physical environment. The United States has now actively incorporated public attribution, retaliatory defensive and offensive cyber operations, and setting redlines as policy tools of deterrence by punishment. And these tools are still in development, especially in light of cooperation with allies. The conclusion makes policy suggestions to South Korean policymakers who are concerned with US-Korea cybersecurity cooperation and adds academic contributions by highlighting future research agendas.

| Keyword signaling, resilience, public attribution, defend forward, offensive cyber operations, redline, international cyber norms