신호이론으로 보는 국제위기 시 사이버 작전의 의도

최은아 (성균관대학교)

주제어

신호이론, 국가위기관리, 강압과 조정, 사이버 작전, 중국의 대만 사이버공격

국문요약

2022년 8월 미국 낸시 펠로시 하원의장의 대만 방문 행사 전후에 중국은 왜 대만에 사이버 공격을 가하였는가? 단순히 물리적으로 피해를 주기 위함이었을까? 아니면 특정 의도를 전달하고자 한 신호였을까? 본 연구는 신호이론(theory of signaling)을 적용하여 국제위기 상황에서 이해당사국 간 주고받는 사이버 작전의 의미를 분석하는 데 목적이 있다. 국제정치학에서 신호는 상대국가의 행동을 변화시키기 위해 수행하는 강압외교의 핵심 요소이다. 따라서 신호를 보내는 목적은 대개 강압외교의 행태로서 결의(resolve)로 풀이돼왔다. 하지만 최신 연구논의들은 국제위기관리 차원에서 위기의 확대방지를 위한 조정(accommodative) 신호에 주목하고 있다. 위기관리 차원에서 공격국가는 대외적으로 갈등이 고조되는 상황과 확전을 피하고 대내적으로 국내정치적 비용을 낮추는 지렛대로써 사이버 작전을 사용할 수 있다. 사이버 공격행위에 관한 신호이론의 적용은 국내 학계에서 거의 시도되지 않았다. 따라서 본 연구에서는 국외연구를 바탕으로 사이버 작전 신호의 요건과 종류, 기준 등을 정리하여 사이버 작전 신호를 구분하는 틀을 제시하였다. 그리고 이를 2022년 8월 중국-대만 국제위기 사례에 적용해 중국이 사이버 작전을 통해서 대만에 전달하려는 신호의 의미를 분석하였다. 강대국이든 약소국이든 분쟁을 겪는 상황에서 양보 혹은 타협을 위한 사이버 조정 신호를 보내 위기의 평화로운 해결을 유도할 수 있다. 이는 국가 사이버 안보전략의 이행과 국가위기관리 차원에의 정책 결정과 판단에 있어서 전략적 함의를 줄 수 있다.

Ⅰ. 서론

적의 행동에 영향을 주고 그로써 정치적 목적을 달성하기 위해 무력 또는 위협을 사용하는 영역으로 사이버공간이 부상하고 있다. 2000년대부터 국제사회에서 크고 작은 분쟁이 발생할 때마다 분쟁 당사국들은 사이버 작전을 부분적으로 동원하는 행태를 보여 왔다. 사이버 작전을 수행한 이후에 공격국가는 사이버공간의 익명성을 활용해 책임을 회피할 수 있으며, 반대로 정략적 판단하에 공격행위를 인정할 수 있다. 타겟국가 역시 기술적, 정략적 판단하에 공격국가를 향해 공개적으로 책임을 묻거나, 반대로 어떠한 입장도 취하지 않을 수 있다. 국제위기 상황에서 공격국가와 타겟국가 사이에 수행되는 사이버 작전은 어떠한 의도를 가지는가? 그리고 공격국가에 의해 수행된 사이버 작전을 두고 이후 공격국가는 어떠한 태도를 보일 수 있는가? 본 연구는 국제위기 시 이해당사국이 수행하는 사이버 작전의 의미를 분석하기 위해 시작되었다.

초기 국제정치학계에서 사이버전(Cyber Warfare)에 관한 논의들은 고전 전략이론을 적용하여 사이버 작전행위의 효용성을 평가하는 데 주목하였다. 즉, 사이버 전쟁이 기존 재래식 전쟁을 대체할 만한 정도인지와 그 영향력은 어느 정도인지를 평가하는 것이다.[1] 사이버전의 의미와 효용성에 대해서는 고평가 또는 저평가되는 등 아직까지 논의가 분분하다. 정보전의 일부로서 적에게 결정적 우위를 가져올 수 있는 수단이자 군사전략 전반에 변화를 일으킬 정보혁명(Information Revolution)이라는 주장이 있는 반면, 우리가 겪는 것은 사이버수단의 영향력 효과(Influence Effect)일 뿐이지, 사이버 전쟁은 아니라는 주장도 있다.[2]

이스라엘의 시리아 레이더 시설 마비 사태(2007), 미국·이스라엘의 이란 나탄즈 핵시설 스턱스넷(Stuxnet) 공격(2010) 등 사례를 볼 때 파괴적인 행태의 사이버 공격들이 이미 시작되었음을 들어 사이버전의 효용을 크게 평가할 수 있다. 그러나 실제 사이버 전쟁 수준으로까지 볼 만한 사이버전은 아직 단 한 차례도 발생하지 않아 사이버 공격과 위협을 과대포장하지 말아야 한다며 주의 환기를 요하기도 한다.[3] 쿠글러(Kugler)는 사이버 공격 자체가 목적이기 보다는 목적을 위한 '수단'으로 활용될 수 있으므로, 특정 아젠다에 대한 압력이나 강압의 일환으로 수행될 수 있다고 지적하였다.[4]

현대전으로서 사이버전의 효용을 둘러싸고 경험적 입증이 부족한 상황에서도 여전히 사이버 작전은 은밀히 혹은 공개적으로 이루어지고 있다. 국력이 강한 국가들은 압도적 우세에 따른 공격 이점이 있음에도 왜 사이버 작전을 통해 상대국에 파괴적인 피해를 주지 않는가? 작전의 성공 여부와 관계없이 국가가 수행하는 이러한 사이버 작전은 어떤 의도의 신호를 전달하기 위함이 아닐까? 사이버공간이라는 회색지대에서 전략과 전술, 작전상 의미를 두고 여러 분석

---

1) Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, "On Cyber Warfare," *A Chatham House Report* (London, UK: Chatham House 2010); Thomas G. Mahnken, "Cyberwar and Cyber Warfare," in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age (Vol. II)* (Washington, DC: Center for a New American Security, 2011), pp. 55-64; 손영동, 『iWar: '사이버 냉전시대' 국가는 어떻게 생존하는가?』 (서울: 황금부엉이, 2010).

2) John Arquilla and David Ronfeldt, *Cyberwar is Coming!* Rand Corporation, 1993; John Arquilla and David Ronfeldt, "In Athena's Camp Preparing for Conflict in the Information Age," *Comparative Strategy* Vol. 12, No. 2, Spring 1993, pp. 141-165; Thomas Rid, Cyber War Will Not Take Place, *Journal of Strategic Studies* 35(1), 5-32, 2012.

3) Thomas Rid(2012), *Ibid.*

4) Richard L. Kugler, "Deterrence of Cyber Attacks," In Kremer et al.(Eds.), *Cyberpower and national security* (Washington D.C.: National Defense University Press, 2009), pp. 309-310.

이 나오는 가운데, 우리는 사이버 작전이 물리적 피해 목적보다도 상대국가의 의사에 영향을 미치도록 하는 하나의 전략적 신호로 기능할 수 있다는 점에 주목해야 한다.

본 연구에서는 갈등과 협상이 오가는 위기 상황에서 사이버 작전을 주고받는 이해당사국 간 의도를 신호이론으로 해설하고자 했다. 신호이론은 국가 수준의 정보 비대칭 상황에서 국가 간 상호작용을 설명하는 이론이다.[5] 국제정치학에서 신호는 상대국가의 행동을 변화시키기 위해 수행하는 강압외교 전략의 핵심 요소이기도 하다. 사이버안보 연구자들은 국가가 사이버 작전을 통해 전달하려는 의미에 주목하여 신호이론을 사이버공간에서도 적용하기를 시도하였다.[6] 신호이론은 국가의 사이버 작전 사용에 관하여 다른 성격 차원에서 신호하는 바를 전달할 수 있다는 답을 제시하여 국제위기 현상에 대한 해석을 돕는다.

국내 학계에서는 사이버 작전 신호에 관하여 신호가 되기 위한 요건은 무엇인지, 신호의 종류에는 무엇이 있는지 등 신호이론에 기반한 기초논의들이 거의 진행되지 않았다. 이에 본 연구를 통해서 사이버 작전이 특정 신호로 기능할 수 있으며, 그 신호를 강압 신호와 조정 신호로 구분할 수 있음을 주장하였다. 그리고 구분 기준으로 1) 비용편익 계산, 2) 사이버 작전의 공개 여부, 3) 사이버 작전에 관한 의사전달 세 가지를 제시하였다. 사이버 작전 신호에 관한 분석틀이 부재한 상황에서 신호의 요건, 신호 종류를 구분하는 기준 등을 제시하였다는 것이 본 연구의 기여점이다.

사이버공간에서 신호이론 적용이 유용한 점은 다음과 같다. 첫째, 정보 비대칭이 극대화된 사이버공간의 특성을 반영하여 사이버 작전이 신호로서 전달되는 의도와 메커니즘을 더 잘 이해할 수 있다. 이 이론은 공격행위가 항상 상대방에게 위협을 가하여 전쟁 수준의 상황 악화를 초래할 목적이라는 관점만이 아니라, 자신에 관한 정보를 상대방에게 전달하여 갈등을 완화하기 위한 위기관리 차원에서 수행될 수 있다는 관점을 포괄한다. 둘째, 사이버 작전 수행 관련한 경험적 사례연구에서 나타나는 구조적 한계를 국내정치적 요인을 통해 보완할 수 있다. 신호이론은 상대방이 원하는 이익과 보내려는 신호를 정확히 이해하기 위해 국가체제와 제도를 고려하거나, 비용편익 계산에 있어서 청중 비용 등 여러 가지 변수를 고려한다.

본 연구에서는 올해 8월 미국 펠로시(Nancy Pelosi) 하원의장의 대만 방문 행사를 빌미로 중국이 대만을 상대로 구사한 사이버 공격 사례를 국가행위자의 신호보내기 차원에서 해석하였다. 이를 통해 중국이 보낸 사이버 작전 신호가 강압적 차원에서의 결의를 보여주는 것인지, 갈등 완화 차원에서의 조정을 보여주는 것인지 구분 짓고자 하였다. 1950년대 초반 발생한 1·2차 대만해협 위기와 1995년 3차 대만해협 위기에 이어, 펠로시 의장의 대만 방문으로 촉발된 이번 4차 위기는 긴장과 대치 속에서 중국이 빈번한 사이버 작전들을 수행하였다는 특징을 보였다. 따라서 물리적 군사작전 외에 수행한 사이버 작전이 대만에 어떠한 신호를 전달하기 위함이었는지 살펴보았다.

연구 질문을 검증하기 위해 국가별 발표한 사이버 작전 관련 공개자료와 사이버전 관련 학술 문헌들을 종합검토하여 질적 분석을 진행하였다. 제2장에서는 국제정치학에서 다뤄지는 신

---

5) 1990년대 미국 국제정치학계는 국가들이 전쟁으로 인한 피해를 미연에 방지할 수 있도록 사전 협상에 이르지 못하는 원인을 찾는 과정에서 신호이론을 도입하였다. 조동준, “신호이론으로 분석한 2013년 한반도 위기,”『평화학연구』 제19권 1호(2018), p. 127.

6) Mason Rice, Jonathan Butts and Sujeet Shenoi, “A signaling framework to deter aggression in cyberspace,” *International Journal of Critical Infrastructure Protection*, Vol. 4 No. 2 (2011), pp. 57-65; Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020); Erica D. Lonergan and Shawn W. Lonergan, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises,” *Security Studies*, 31(1) (Feb 17, 2022), pp. 32-64.

호이론의 논의배경과 사이버공간에서 이루어지는 신호 역학을 소개하였다. 그리고 기존 연구 논의를 바탕으로 신호의 요건과 종류, 구분 기준 등을 제시하였다. 제3장에서는 사례 분석을 통해 중국이 구사한 사이버 공격행위를 신호이론으로 해설하여 전개 과정과 결과를 분석하였다. 그리고 신호이론을 사이버공간에 적용함에 따라 나타나는 시사점과 한계를 도출하였다. 마지막 장에서는 사이버 영역에서 신호이론이 어느 정도 설득력을 갖추는지 평가하고, 정책적으로 수렴 가능한 방향과 후속연구를 제언하였다.

Ⅱ. 신호이론과 사이버공간에의 적용

본 장에서는 먼저, 국제정치학에서 논의되는 신호이론에 관한 국내외 연구들을 소개하여 국제위기 속 신호 역학의 이해를 돕고자 하였다. 다음으로, 신호이론을 사이버 영역에 적용한 국내외 연구들을 소개하였다. 기존연구들은 대전략 차원에서 사이버 강압에 주목하여 활발히 논의되어 온 것에 비해, 조정전략에 관한 연구는 최근에야 논의가 시작된 측면이 있다. 이에 국제위기 상황에서 이해당사국 간 확전과 위험 확대를 방지하는 조정의 의미에도 주목하여야 함을 주장하였다. 특히 국내 학계에서는 사이버 작전 신호에 관한 기초논의들도 거의 진행되지 않았다. 따라서 기존 논의 중심으로 사이버 작전 신호가 되기 위한 요건을 정리하였으며, 이를 바탕으로 사이버 작전 신호를 강압과 조정 신호로 구분하였다. 그리고 두 신호를 구별할 때 고려해야 할 세 가지 기준을 도출하였다.

1. 국제정치학으로 보는 신호이론

신호이론에서 갈등과 협상은 상대방이 모르는 정보를 서로 전달하는 과정이다. 자신의 진정한 의지만 알고 있는 행위자들은 상대방의 진정한 의지가 무엇인지 알지 못한 채 상대방이 보여주는 행동들을 보고 상대방 의지의 강도를 유추해야 한다.[7] 갈등 상황에 있는 행위자들은 본인의 능력과 의지 등 정보를 상대방에게 보낸다. 정보를 전달하는데 드는 비용은 정보의 신뢰성을 좌우한다. 예를 들어, 수신자는 송신자가 위협에 얼마나 큰 비용을 부담하였는지, 해당 위협을 감수할 경우 발생하게 되는 위험은 어느 정도인지 비용 편익을 계산하게 된다. 그리고 만약 비용 부담이 적다면 그 신호를 값싼 신호(costly signals)로 취급하여 신뢰하지 않을 수 있다. 따라서 신뢰할 수 있는 신호(credible signals)이려면 해결되지 않은 상태를 단념시킬 수 있는 비용이나 위험이 수반되어야 한다. 마찬가지로 협상 상황에서도 전달하는 정보가 어느 정도 비용이 들거나 신호로 인하여 피해가 사후에 초래된다면 신뢰성을 높일 수 있다. 따라서 분쟁에서 위협하는 행동은 무조건 상황을 악화시키기보다는 자신에 관한 정보를 상대방에게 전달하여 분쟁을 폭력적 수단에 의하지 않고 해결하는 수단이 될 수 있다.[8]

국제정치에서 신호는 국제위기 상황에 놓인 이해당사국들 간의 상호작용 속에서 발견된다.

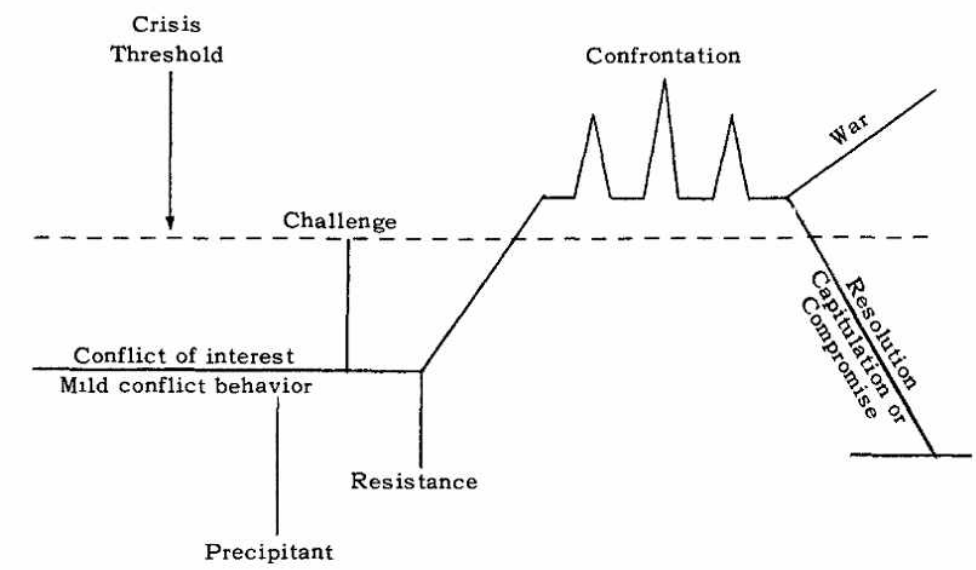
---

7) 김지용, “위기 시 청중비용의 효과에 관한 이론 논쟁 및 방법론 논쟁의 전개과정 고찰,”『국제정치논총』 제54집 4호(2014), p. 201.

8) 신호이론은 동물들의 상호작용을 연구하는 진화생물학 분야에서 발전한 이론으로서 진화생물학적 접근 방식은 다음 문헌에서 참고할 수 있다. 조동준(2018), *op. cit.*, pp. 126-128.

국제위기에 관한 합의된 개념 정의는 없지만, 국제위기란 둘 이상의 주권국가가 실제 전쟁은 아니더라도 확전 가능성이 위험할 정도로 높다는 인식을 수반하는 심한 갈등에서의 일련의 상호작용을 말한다. <그림 1>과 같이 위기의 정도를 단계별로 보면, 이익의 갈등(Conflict of Interest) → 도전(Challenge) → 자극적인 행위(Precipitant) → 가벼운 분쟁(Mild Conflict Behavior) → 저항(Resistance) → 대결(Confrontation) → 조건부 항복(Capitulation) 또는 타협(Compromise) 또는 전쟁(War) 순으로 전개된다. 위기는 언제나 심한 갈등을 포함하고, 위기의 첫 단계에서 당사자들 간에 심한 이익의 갈등이 발생하며 이때 위기관리가 실패하면 대결이나 전쟁으로 확대될 가능성이 높다.[9)]

<그림 1> 위기의 단계



출처: Glenn Herald Snyder and Paul Diesing, *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises* (Princeton, New Jersey: Princeton University Press, 1977), p. 15.

스나이더와 디싱(Snyder and Diesing)은 국가 간 위기 발생의 원인이 '이익의 갈등'에서 비롯된다고 본다. 국제위기관리 차원에서 타협 시 교섭자들은 자신이 얻을 수 있는 이익의 가치를 높이고 상대방의 이익의 가치를 줄이려고 하며, 상대방이 추구하는 이익이나 결의를 정확히 파악하는 것에 관심이 있다. 위기 시 협상에 앞서 상대가 중요시 하는 이익과 가치가 무엇인지를 파악하면 상대방을 효과적으로 위협할 수 있다. 여기서 이익과 가치는 '가치 구조(value structures)'를 통해 설명되는데, 위기 상황에서 당착한 이해관계는 세 가지 범주로 구분된다. 먼저, 분쟁 대상의 물질적 권력에서 파생된 전략적 이익(strategic interests), 둘째, 권력과 관련 있으나 자신의 결의, 유연성, 위신, 동맹의 신뢰성, 예측 가능성 등에 관한 다른 이들의 이미지로 인한 결과의 영향과 관련된 평판 이익(reputational interests), 셋째, 위 두 가지와 달리, 미래 권력과 협상 능력에 도움 되지 않는 자존심, 명성, 경제적 가치 등 자체를 위한 내재적 이익(intrinsic interests)이다.[10)]

---

9) 김법헌·김덕기, "중국의 대만해협 위기관리 교훈이 미국 대응전략과 군사력에 미친 함의 -진먼다오(金門島)·마주다오(馬祖島) 위기를 중심으로-," 『대한정치학회보』 제27권 2호(2019), p. 80.

신호는 국가가 상대방을 인식하고 궁극적으로 이익 극대화를 추구하는 행태를 보여주는 측면에서 위기 연구의 핵심 역학이다. 위기관리는 양국 간 또는 다자 국가 간의 국가이익이 상충하는 곳에서 발생하는 갈등과 분쟁상태가 전쟁으로 확대하느냐 아니면 평화상태로 회복하느냐를 결정하는 분수령이 된다.[11] 스나이더와 디싱은 국가들이 협상 과정에서 발휘할 수 있는 '교섭력(bargaining power)'[12]에 주목하였고, 협상에서 강압(coercion), 조정(accommodation), 설득(persuasion) 세 가지 전략과 전술 과정이 구분되어 나타난다고 했다.[13] 강압과 조정 과정은 상대방에게 위협과 양보를 통해 불러올 수 있는 결과의 선택지 중에서 택일하도록 하지만, 설득 과정은 상대방이 가치 구조와 예상결과에 대한 인식을 스스로 바꾸도록 영향을 미친다는 점에서 차이가 있다.[14]

강압 이론은 대체로 셸링(Thomas C. Schelling)의 연구를 기반으로 진행되어왔다.[15] 셸링에 따르면 강압이란 위협 또는 제한된 군사력을 사용하여 상대방의 행동에 궁극적으로 영향을 주는 것을 의미한다. 즉, '어떤 대상을 항복하게 하거나 순응하게 만들 수 있을 정도로 해를 입히거나 혹은 일어날 가능성이 큰 피해를 초래하는 위협'이다.[16] 강압은 실제 폭력이 행사되기 이전에 위협 그 상태를 유지하여 상대방으로 하여금 특정 행동과 결과를 취하도록 유도한다. 즉, 셸링이 지적하는 '폭력'이 상대에게 선택권이 없는 '전쟁'이라면, '강압'은 상대에게 선택지를 남기는 '외교 전략'이다.[17] 강압자와 적국의 분류는 상호 간 강압한다는 맥락에서 보면 임의적이기 때문에, 강압자는 상대적으로 강력한 국가 또는 적극적으로 현상 타파를 추구하는 국가로 분류된다.[18] 강압에 따르는 비언어적 소통이나 신호 보내기는 군사적 혹은 정치·외교적 행동으로 취해질 수 있으며, 종종 상황의 구조적 여건이나 전개 양상에 따라 그 위협이 강화되거나 약화 될 수 있다.[19]

국제정치에서 조정은 위기 상황에 있는 협상 당사자 중 일방이 요구, 양보, 타협과 같은 제안을 하면 상대방이 그것의 일부 또는 전부를 받아들이면서 합의로 수렴되어 가는 일련의 과정이다. 조정은 게임이론적 접근 중 하나의 전략으로도 잘 알려져 있다.[20] 국가는 긴장과 갈등

---

10) Glenn Herald Snyder and Paul Diesing(1977), *op. cit.*, pp. 183-184.

11) 김법헌·김덕기(2019), *op. cit.*, p. 80.

12) 교섭력은 양자 간에 보유하고 행사하는 정치 권력이라고 할 수 있다. 정치 권력에 대한 전형적인 정의는 A는 B에게 피해의 위협이나 보상의 약속을 함으로써 B가 원하지 않는 행동을 하도록 설득할 수 있을 정도로 B에 대한 권력을 갖는 것이다.

13) Glenn Herald Snyder and Paul Diesing(1977), *op. cit.*, p. 183.

14) *Ibid.*, p. 198. 세 가지 협상 전략과 전술 중에서도 강압과 조정에 관해서는 학술연구가 활발히 진행되어 왔지만, 설득에 관해서는 잘 다뤄지지 않았다. 따라서 본 연구 역시 이 점을 반영하여 서로 대척점에 있는 성격을 가진 강압과 조정 논의에만 초점을 두었다.

15) Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960); *Arms and Influence* (New Haven, CT: Yale University Press, 1996).

16) Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008), p. 3.

17) 정하연, "사이버 강압의 국제정치: 사이버 공격 사례를 통해 본 국가 간 갈등 연구," 이화여자대학교 정치외교학과 박사학위논문(2017.12), p. 43.

18) 강압시도의 사례로 강압자가 사용한 메커니즘과 성공 또는 실패에 따른 결과들을 소개하고 있는 연구는 다음을 참고하면 된다. 다니엘 바이먼(Daniel Byman), 매튜 왁스먼(Matthew C. Waxman) 지음, 이옥연 옮김, 『미국의 강압전략 : 이론, 실제, 전망』 (서울: 사회평론, 2004), pp. 73-76.

19) Alexander L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*, US Institute of Peace Press(1991), pp. 9-10.

20) 게임이론에서 조정은 서로 충돌하는 이익이 공통 이익과 관련이 클수록 상호 간에 얻을 수 있는 이득(gains)이 많다고 판단해 충돌보다는 합의에 도달하는 것에 관심을 두게 된다. 조정 전략은 양쪽이 공평하게 혜택을 배분할 수 있음이 보다 명확할 때 실행 확률이 높아진다. 경험적 증거는 부족하나, 주로 가치와 이익을 공유하고 있는 동맹국 사이에서 나타날 수 있다.

이 고조되는 상황을 피하고 확전을 방지하려는 위기관리 차원에서 조정을 시도한다. 대체로 약소국에서 더 큰 손해를 피하기 위해 시도하나, 강대국 역시 공격 비용을 최소화하여 일종의 양보를 보임으로써 국가이익을 극대화하는 동시에 확대위험을 방지할 수 있다. 국가 일방이 전쟁보다도 상대방의 항복이나 타협을 원할 경우에 서로의 대립은 세부 사항을 논의하는 해결 단계로 접어들게 되고, 이때 강압 전략보다는 조정 전략이 우세해진다. 스나이더와 디싱은 위기 상황에서 국가행위자의 비공개 의사전달 방식을 조정 전략으로, 공개 의사전달 방식을 강압 전략으로 일반화하였다.[21)]

한편, 이익과 가치 구조의 범주가 다양한 만큼 국가행위자의 의도를 파악하기 위해서는 미시적 접근에서 위기 시 의사결정을 하는 국가지도자의 동기, 배경, 인식 등에도 주목하여야 한다. 신호이론에 따르면 국가지도자의 의지는 국가의 정치제도와 국내 청중비용(audience cost)에 의해 영향을 받는다. 즉, 국가지도자는 국내정치적으로 집권한 정부에 부정적인 야당의 압박이 거세지거나, 국민의 정치적 선호도가 낮아지는 등 불안정한 권력 구도 상황이 올 위험을 예측하고 이를 피하고자 한다. 따라서 신호를 보내기에 앞서 위협 또는 경고가 이행되지 않을 때 자국민으로부터 받게 될 정치적 처벌과 같은 비용을 고려하게 된다.

청중비용이론을 제시한 제임스 피어론(James Fearon)은 민주국가와 독재국가의 청중비용에 차이가 있다는 점을 강조한다. 예를 들어, 국내 청중이 어떠한 선호를 하고 있든지 간에 강경정책을 철회하는 민주국가의 지도자들은 청중비용을 감수해야 한다. 따라서 위기상황에서 강경정책을 추진함에 있어서 매우 조심스럽다. 하지만 강경정책을 고수할 때는 진정한 의지가 잘 전달되어 의지의 신빙성을 높이고 따라서 상대국이 유화정책을 취하도록 유도하여 전쟁이 회피될 수 있다.[22)] 독재국가에서는 독재자가 눈치를 보며 만족시켜야 하는 소수의 승리 연합(지배엘리트 내의 경합집단)이 국내청중으로 정의된다.[23)] 이들의 선호에 반하면 쿠데타, 숙청, 사형 등 회생 불가능한 처벌수준이 고려되므로 그에 따른 청중비용을 산출할 수 있게 된다.

국제위기 상황에서 상대방에 대한 믿음은 일시에 만들어지는 것이 아니라 갈등과 협상의 반복된 상호작용이라는 위기 역학을 통해 나타난다. 신호 분석은 국가를 합리적 행위자로 가정하더라도, 송신자 측면에서는 '정보를 왜곡하여 전달할 때 발생하는 이점에도 불구하고 신뢰성 있게 신호할 것인가?', 수신자 측면에서는 '과연 송신자가 보낸 신호를 정확하게 믿고 전략을 수정할 것인가?'와 같은 의문을 갖게 한다. 청중비용이론은 국가 행동이 비일관적일 때 그 이유를 국내 청중과 정치지도부 간의 상호작용으로 연결된 국내정치 요인에서 찾는다. 이는 국내정치 요인이 외교정책 결정인 '상위 정치(high politics)'에 일정 영향을 미칠 수 있음을 시사한다.

---

21) Glenn Herald Snyder and Paul Diesing(1977), *op. cit.*, pp. 251-252.

22) 그러나 질적 연구자들은 청중비용이 아닌 정책비용(policy cost)으로 설명되어야 한다고 주장한다. 즉, 강경정책이 국가에 엄청난 비용을 초래할 것으로 예상될 경우 국내청중은 강경정책의 철회를 결정한 지도자를 처벌하기보다 오히려 환영하고 보상한다는 것이다. 청중비용이론은 지도자가 국가이익보다 개인의 정치적 이익을 훨씬 더 많이 고려한다는 자유주의 가정에 기초해 있어 일정 한계를 보여준다. 김지용(2014), *op. cit.*, p. 224.

23) *Ibid.*, p. 213.

2. 사이버공간에서의 신호이론 적용

1) 기존연구

신호로서 사이버 작전은 주로 강압전략 차원에서 연구되어왔다. 연구자들은 사이버 강압전략을 어떻게 관찰하고 평가하는가? 초기 연구에서는 정량적 지표가 부족하여 사례 검증이 어렵다는 한계에 부딪혔다. 즉, 사이버전에 관한 체계적이고 경험적인 연구가 불가능하고, 사이버 작전을 비롯한 군사작전들이 대부분 비밀에 부쳐지기 때문에 군 관계자와의 인터뷰나 주요 작전 문서 등의 확보가 어렵다는 것이다. 그런데도, 사이버 공격에 관한 검증된 데이터가 쌓이면서 설문조사 방식을 병행해 정량적 분석을 시도함으로써 전쟁 시 사이버 강압수단의 효과성에 관해 연구가 이뤄지기도 했다.[24]

그밖에도 최근 논의들은 이론적 한계를 보완하기 위한 시도로서 실제로 발생한 사이버위협 사례들을 연구하여 적정한 일반화를 제공하고, 이론적 정립을 위해 더 체계적으로 이용할 수 있는 경험적 증거를 제시하고 있다.[25] 예를 들어, 러시아의 2007년 에스토니아에 대한 사이버 공격과 2008년 조지아에 대한 사이버 공격, 2014년 북한의 미국 소니픽쳐스(Sony Pictures Entertainment) 회사에 대한 사이버 공격 사건 등을 강압을 시도한 사례로 보고, 가설 검증 차원에서 사이버 위협이 강압을 위한 효과적인 수단인지 평가하는 것이다.[26] 이처럼 다양한 사이버 공격 사례에 관한 분석 연구들은 사이버 강압의 실패에 주목하며 강압수단으로서 사이버 작전의 효과를 대체로 낮게 평가하고 있다.

최신 연구들은 전략적 한계를 극복하기 위한 시도와 함께 사이버 공격이 주는 물리적 파괴력 외에 다른 영향력과 요소에도 주목하는 경향을 보인다. 일례로, 랜섬웨어 공격 직후 설문조사 데이터를 이용해 사이버 공격이 달성하고자 하는 주요 위협은 물리적 파괴가 아니라 정부를 향한 대중의 신뢰 감소 같은 사회적 위험이라는 주장을 검증하는 것이다.[27] 기존연구 논의가 국가의 사이버 작전 수준을 저강도-고강도로 분류하고 분석하거나, 군사적 위협과 사이버 작전이 연계 혹은 독립적 행위인지에 관해 분석하였다면, 새로운 논의들은 바뀐 전장 환경

---

24) Nadiya Kostyuk and Yuri M. Zhukov, “Invisible Digital Front: Can Cyber Attack Shape Battlefield Events?” *Journal of Conflict Resolution*, 63(2) (2019), pp. 317-347.

25) Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies*, 22(3) (2013), pp. 365-404; Brandon Valeriano and Ryan C. Maness, “The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11,” *Journal of Peace Research*, 51(3) (2014), pp. 347-360; Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies*, 38/1-2 (2015), pp. 4-37.

26) 장노순·김소정, “미국의 사이버전략 선택과 안보전략적 의미: 방어, 억지, 선제공격전략의 사례 비교 연구,” 『정치정보연구』 19(3), 2016.10, pp. 57-91; Travis Sharp, “Theorizing cyber coercion: The 2014 North Korean operation against Sony,” *Journal of Strategic Studies*, 40(7) (2017), pp. 898-926; 정하연, “사이버 강압의 국제정치: 사이버 공격 사례를 통해 본 국가 간 갈등 연구,” 이화여자대학교 정치외교학과 박사학위논문(2017.12); Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (2018; online edn, Oxford Academic, 24 May 2018).

27) Ryan Shandler and Miguel Alberto Gomez, “The hidden threat of cyber-attacks – undermining public confidence in government,” *Journal of Information Technology & Politics* (2022), pp. 1-16. 국가 차원의 사이버 공격에 대한 대중의 인지에 관한 유사 연구로는 다음이 있다. Marcelo Leal and Paul Musgrave, “Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks,” *Foreign Policy Analysis*, Vol. 18, Issue 2 (April 2022).

과 상황을 반영하여 국제위기를 관리하는 차원에서의 사이버 작전 사용에 주목하고 있다.

사이버공간에의 신호이론 적용을 시도하는 연구 흐름은 대전략 차원에서 주를 이루던 강압 연구가 실효성 측면에서 한계에 부딪히면서, 국내정치 변수를 고려하는 등 방식으로 자제(restraint) 혹은 조정 의미에 주목하는 논의로 확장되고 있다.[28] 즉, 사이버 작전이 위기 상황에서 전통적인 군사작전으로 확대되기보다는 긴장을 크게 높이지 않고 도발에 대응할 수 있는 수단을 제공하는 역할을 할 수 있다는 것이다. 발레리아노와 옌센(Brandon Valeriano and Benjamin Jensen)은 사이버 작전을 통해 자제의 신호를 보낼 수 있다고 주장하며 그 일례로 2015년 튀르키예의 러시아 전폭기 격추사건이 빌미가 된 국제위기를 꼽았다.[29] 이들 연구를 바탕으로 보가드와 로너건(Borghard and Lonergan)은 사이버 작전이 나아가 이해당사국 간에 위험의 확대를 방지하고 갈등을 완화하기 위한 조정 신호로 기능할 수 있음을 다섯 가지 국제위기 사례들을 분석하여 검증하기도 했다.[30]

사이버 작전이 자제나 조정의 의미를 담고 있는지에 관한 연구와 경험적 증거들은 아직 많지 않다. 사이버 작전은 실제 상대방에게 물리적 피해를 주는 공격이라는 점에서 위협이나 경고를 목적으로 한 강압전략과 어울려 보이기 때문이다. 그러나 과거와 달리 오늘날 국가들은 위기관리 차원에서 전쟁을 예방하고 확전의 위험을 최소화하여 국가이익을 극대화할 수 있는 방식을 추구하고 있다. 따라서 분쟁이나 국제위기를 겪고 있는 이해당사국 입장에서 사이버 작전은 국가 차원의 조정적 의도를 보여줄 수 있는 하나의 신호로 기능할 수 있다. 이는 실제 전쟁이 줄고 국제위기 발생 빈도가 증가하는 상황에서 국가행태에 대한 해석에 설득력을 높인다.

사이버 영역에서 나타나는 신호의 역학은 무엇일까? 신호보내기는 송신자와 수신자 간에 상호작용이 이루어지는 과정이다. 사이버공간에서 신호를 보내기 위해서는 먼저 상대국가의 사이버 환경의 특성과 능력을 긴밀히 파악해야 한다. 또한, 신호의 의도 및 목표와 관련된 모호성을 어떻게 해결할 것인지에 대해 정밀한 접근 방식이 필요하다. 일반적으로 수신자는 정치, 문화, 이념, 종교, 그리고 여타의 가치들이 상충하는 송신자와 대적할 가능성이 크다. 가치 차이로 인해 수신자의 신호를 받아들이는 송신자는 인식에 복잡성이 더해지고 이는 신호를 해석하는 데 많은 영향을 미친다. 따라서 상대방이 잘못 해석하거나 특정 의도가 간과되지 않도록 신호보내기의 선택과 모니터링에 신중해야 한다. 수신자 역시 오인식에 대한 가능성을 염두에 두고 맥락에 최적화된 적절한 메시지를 전달할 플레이를 선택해야 한다.[31]

---

28) 일부 연구자들은 분쟁 시 사이버 작전을 수행하더라도 그 자체로 위기가 고조되어 확전을 불러올 가능성에 대해 낮게 평가하고 있다. 이들은 오히려 사이버 작전이 위험 확대의 방지에 기여될 수 있다고 본다. 사이버 작전이 확전에 영향을 크게 미치지 않는다고 평가한 연구들은 다음과 같다. Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, 13(3) (Fall 2019), pp. 122-145; Brandon Valeriano and Benjamin Jensen, "The Myth of the Cyber Offense: The Case for Restraint," *CATO Institute: Policy Analysis 862* (15 January 2019), pp. 1-16; Jacquelyn Schneider, "Cyber and Crisis Escalation: Insights from Wargaming" (working paper, US Naval War College, Newport, RI, 2017).

29) 2015년 11월 24일 시리아 국경 인근에서 튀르키예 F-16 전투기가 러시아 Su-24 전폭기를 격추시켰다. 이후 러시아는 튀르키예 국영 은행과 정부 웹사이트를 대량 디도스 공격하여 대응에 나섰다. 러시아의 디도스 공격은 튀르키예의 군사 기지를 목표로 하는 장거리 미사일보다 튀르키예의 네트워크를 일시적으로 차단하도록 하는 것이 낫다는 판단하에 저강도 사이버 작전을 사용한 전략적 자제 사례에 해당한다.

30) Erica D. Lonergan and Shawn W. Lonergan(2022), *op. cit.*, pp. 32-64.

31) Mason Rice(2011), *op. cit.*, p. 62.

<표 1> 기본적인 신호보내기의 예시

종류	내용
Offensive	**Null signal:** Show goodwill by not attacking; conduct secret invasive surveillance.(공격하지 않음으로써 선의를 보여줌; 비밀리 침투해 감시 수행) **Simple signal (reflexive):** Launch an attack when an imminent threat is detected.(임박한 위협이 탐지되면 공격 개시) **Simple signal (random):** Sever communication links to degrade the adversary's ability to communicate while giving the appearance that the cause was accidental.(원인이 우발적인 것처럼 보이도록 하면서 적의 의사소통 능력을 저하시키기 위해 통신 연결을 끊음) **Simple signal (other):** Actively probe the adversary's assets; launch a tit-for-tat and/or mirror image attack; deny service; disrupt the adversary's operations; destroy the adversary's data.(적의 자산을 적극적으로 조사; 흉내내기(tit-for-tat) 및/또는 미러 이미지 공격 개시; 서비스 거부; 적의 작전 방해; 적의 데이터 파괴)
Defensive	**Null signal:** Show goodwill or ignorance by not assuming a defensive posture; conduct passive surveillance; conduct secret active surveillance; sacrifice a less important system in an effort to study the adversary's attack methods.(방어적인 자세를 취하지 않음으로써 선의 또는 무시를 보여줌; 수동적 감시 수행; 비밀리 능동적 감시 수행; 적의 공격 수단을 연구하기 위해 덜 중요한 시스템을 희생함) **Simple signal (reflexive):** Sever Internet connections when an attack is imminent or underway; change the National Threat Advisory status and/or INFOCON status.(공격이 임박하거나 진행 중인 경우 인터넷 연결 차단; 국가 위협 주의보 상태 및/또는 인포콘 상태 변경) **Simple signal (random):** Deploy blue teams to identify and eliminate vulnerabilities; deploy open sensors; re-route traffic.(취약성을 식별하고 제거하기 위해 블루팀 배치; 개방형 센서 배치; 트래픽 경로 재설정) **Simple signal (other):** Announce the deployment of open and secret sensors.(공개 및 비밀 센서의 배포 발표)
Offensive-Defensive	**Null signal:** Display obliviousness or goodwill by not acting.(행동하지 않음으로써 의식하지 못함 또는 선의를 보여줌) **Simple signal (reflexive):** Change the DEFCON status.(데프콘 상태 변경) **Simple signal (random):** Announce that cyber operations forces are spread throughout the world and attacks may not be launched from within the geographical boundaries of the defender; threaten severe penalties to an adversary who conducts cyber operations on the defender; conduct a show of force to display capabilities; conduct a random security audit.(사이버 작전부대가 전 세계에 퍼져 있으며 방어자의 지리적 경계 내에서 공격이 시작될 수 없음을 알림; 방어자에 대해 사이버 작전을 수행하는 적에게 엄중한 처벌을 가하겠다고 위협함; 능력을 과시하기 위해 무력행사; 무작위 보안 감사 수행) **Simple signal (other):** Threaten an adversary with military and/or economic force; offer incentives for restraint; bluff an adversary with capabilities that are not yet weaponized.(군사 및/또는 경제적 힘으로 적을 위협; 자제(restraint)에 대한 인센티브 제공; 아직 무기화되지 않은 능력으로 적에게 허세부림)
Neutral	**Null signal:** Maintain the status quo by not acting.(행동하지 않음으로써 현상 유지)

	Simple signal (reflexive): “Growl” by actively pinging border routers worldwide.(전 세계의 경계 라우터에 적극적으로 인터넷 접속 확인(ping)을 보내 “으르렁(도발)”함) **Simple signal (random):** Create a mystery (e.g., slow communication links or drop a large number of packets); conduct a show of force.(미스터리 생성(느린 통신 연결 또는 많은 수의 패킷 삭제 등); 힘의 과시) **Simple signal (other):** Launch an attack on oneself using a known adversary capability; signal the discovery of an event that did not occur; offer assistance to the adversary (e.g., blue team services); perform benign tagging; send friendly alert messages by pinging the adversary's assets.(알려진 적의 능력을 사용해 자신에게 공격 개시; 발생하지 않은 사건의 발견을 알림; 적에게 도움 제공(블루팀 서비스 등); 자비로운 태깅 수행; 적의 자산을 인터넷 접속 확인(ping)을 보내 친근한 경고 메시지를 보냄)

출처: Mason Rice, Jonathan Butts and Sujeet Shenoi, “A signaling framework to deter aggression in cyberspace,” *International Journal of Critical Infrastructure Protection* Vol. 4 No. 2 (2011), p. 62.

사이버공간에서 신호보내기는 <표 1>과 같이 언어적 또는 비언어적 방식으로 전달될 수 있다. 예를 들어, 상대방의 네트워크 통신 연결을 차단하거나 서비스 거부, 데이터 파괴 공격을 하는 것은 비언어적 방식의 신호에 해당하며, 상대방의 공격에 대해 처벌 의사를 공개적 또는 비밀리에 전하는 것은 언어적 방식의 신호에 해당한다. 신호는 그 내용에 따라서 공격적, 방어적, 공격-방어 결합적, 중립적 성격으로 구분할 수 있다. 상대방에게 물리적 타격을 입히는 것은 능동적이자 공격적 성격에 가까우며, 취약성을 식별·제거하거나 국가 방호태세를 변경하는 것은 수동적이자 방어적 성격에 가깝다. 그밖에 공격과 방어가 결합한 성격의 신호를 보내거나, 중립적 성격의 신호를 보낼 수도 있다.

국가가 수행하는 사이버 작전 종류에는 사이버 영역에 걸쳐 발생하는 다양한 범주의 활동들이 포함될 수 있다. 네트워크를 통해서 또는 데이터가 저장된 시스템 자체에서 데이터 송수신을 방해, 저하, 파괴 또는 조작하는 사이버 공격, 기밀 정보를 탈취하기 위한 목적에서 컴퓨터 네트워크에 접근하는 사이버 첩보전, 청중의 인식에 영향을 주기 위해 민감한 개인 정보를 무기화하는 방식이 수반된 정보전 등이다. 이들 중에서도 신호로 분류되려면 강압적이라고 간주할 만한 것이어야 한다. 사이버 첩보전이나 정보전은 네트워크에 접근하여 데이터를 수집하는 것 자체에 목적이 있어 설상 강압 목적을 위한 사전 공격으로 수행된다고 하더라도 그 자체로는 신호로 보기 어렵다. 따라서 강압을 위한 사이버 신호는 컴퓨터와 네트워크, 시스템 자체에 있는 데이터를 교란, 거부, 저하, 파괴할 목적으로 하고 실제 그 피해가 일정 정도 드러나는 공격이어야 한다.[32]

위 사항들을 종합해보면, 사이버 작전이 신호가 되기 위해서는 두 가지 요건이 충족되어야 한다. 먼저, 수신자가 관측할 수 있어야 한다. 신호는 송신자가 타겟이 수신하도록 의도한 것이기 때문에 공개적이거나 비공개적인지 여부와 상관없이 수신자가 알 수 있도록 신호가 전달되어야 한다. 둘째, 어떤 방식으로든 신호를 신호하는 국가와 연결 지을 수 있어야 한다. 예를 들어, 첩보전 같은 스파이 활동에서는 비밀이 유지되어야 하므로 사이버 공격들이 제3국의 네

32) Erica D. Borghard and Shawn W. Lonergan, “The Logic of Coercion in Cyberspace,” *Security Studies*, 26(3) (2017), p. 459.

트워크를 경유하는 등 방식으로 우회하는 경우가 대부분이다. 이러한 사이버 작전 형태는 의도를 전달하기 위한 신호가 아니라고 봐야 할 것이다.

한편, 사이버공간에서의 신호이론 적용은 다음과 같은 비판에 놓일 수 있다. 개인 또는 해커조직과 같은 비국가행위자가 국가행위자 상대로 사이버 공격을 가했을지 모를 행위에 대한 책임을 국가에 귀속할 수 있는가? 즉, 주요 장애 요인으로 꼽히는 공격자의 귀속 문제를 어떻게 해결할 것이냐에 관한 연구가 꾸준히 논의되어왔다. 트레비스 샤프(Travis Sharp)는 귀속 문제를 해결하기 위해 강압의 행위자만이 아니라 갈등 관계에 놓인 타겟 대상의 행위까지 폭넓게 고려해야 하며, 사이버 공격행위의 범위를 징후 또는 탐지 수준에서도 인정해야 한다고 보았다.[33]

특히 사이버 강압에서 익명성에 기한 귀속 문제가 과장된 측면이 있다고 본 블래그덴(Blagden)은 공격자의 정체성이 모호하더라도 공격자가 원하는 이익이 드러나는 점에 주목하여야 하며, 강압자는 자신이 원하는 행동 변화를 지정하고 최소한 암묵적으로 이해관계를 식별해 선호도를 드러내기 때문에 귀속이 가능한 메커니즘을 보인다고 설명하였다.[34] 또 다른 연구에서는 공격국가가 자발적으로 사이버 작전에 대한 책임을 인정하여 신뢰, 위신, 강압 등 얻고자 하는 이익이 있음에 주목하거나[35], 나아가 이러한 공개 귀속(public attribution)이 전략적으로 성공하기 위한 국가 차원의 프레임워크를 제안하기도 했다.[36]

국제위기 상황에서 강압 또는 조정전략은 특정 이슈를 둘러싸고 갈등 관계에 놓인 국가들의 맥락 속에서 발생한 사이버 공격이 강압이나 조정 목적에서 수행되었다는 데에 초점을 둔다. 피해를 입은 국가는 정밀한 기술적 분석에 기반한 증거와, 이슈를 둘러싸고 갈등이 가시화된 정치적 상황 등을 종합하여 위협을 가한 국가를 추정할 수 있다. 그리고 입은 피해에 대해 공격국가에게 공식성명, 언론 보도 등을 통해 공개적으로 혹은 비공식 외교채널을 통해 비밀리에 경고할 수 있다. 이러한 점에서 사이버 영역 특성으로 인한 공격주체의 귀속 가능성은 더 이상 큰 난제는 아니라고 봐야 할 것이다.

2) 구분 기준

사이버 강압 신호와 조정 신호를 구분하는 기준에 대해 살펴보도록 한다. 먼저, 사이버 강압전략을 시행하기 위해 고려할 수 있는 요소들은 다양하다. 사이버공간은 시스템 및 네트워크에 접근하여 정보를 변경, 훼손, 파괴 또는 도용함으로써 타겟으로 삼은 청중에게 영향을 미치도록 설계된 종류의 강압적 작전에 무수한 가능성을 제공한다.[37] 보가드와 로너건은 사이

33) 사이버 강압에 관해 제시한 새로운 기준을 살펴보면, 강압의 행위자를 국가행위자에게만 한정하지 않고 국제정치적으로 비중이 높아지고 있는 비국가행위자까지 포함하였다. 또한, 강압자의 정체성과 관련해서. 구두 상으로 확립된 경우만이 아니라 타겟 대상에 의해 어느 정도 '알려진' 것도 해당한다고 보았다. 이는 강압자가 사이버 강압 시 책임회피가 가능한 문제를 고려하여 잠정적으로 특정된 강압자도 포괄하기 위함이다. 또한, 강압자의 위협을 군사행동을 통해 구두 또는 잠정적으로 알려진 범위에서 나아가 사이버 작전의 제한적 사용과 훈련까지 포함하였다. Travis Sharp(2017), *op. cit.*, p. 905.

34) David Blagden, "Deterring Cyber Coercion The Exaggerated Problem of Attribution," *Survival Global Politics and Strategy*, Vol. 62 Issue 1 (2020), pp. 131-148.

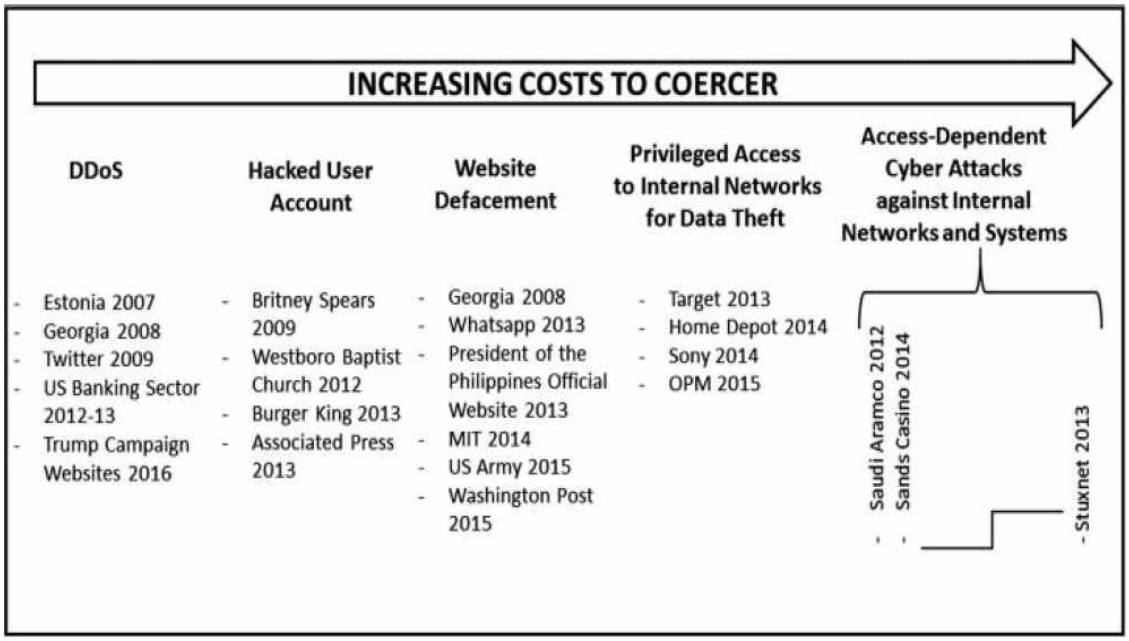
35) Michael Poznansky and Evan Perkoski, "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution," *Journal of Global Security Studies*, 3(4) (2018), pp. 402-416.

36) Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies* (2021), pp. 1-30.

37) Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," 2016 8th International Conference on Cyber

버 영역에서 선호되는 강압 외교 네 가지를 첫째, 명확히 전달되는 위협(clearly communicated threats), 둘째, 비용편익 계산(a cost-benefit calculus), 셋째, 신뢰성(credibility), 넷째, 재보장(reassurance)으로 정리하였다.[38]

<그림 2> 강압적인 사이버 작전의 스펙트럼[39]



출처: Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace, *Security Studies* 26(3) (2017), p. 467.

사이버 작전이 해당 국가의 신뢰할 만한 결의를 보여주는 신호이기 위해서는 그에 따른 비용 고려가 수반되어야 한다. 강압을 목적으로 보내는 사이버 신호이더라도 그 신호의 생성에 드는 비용과 노력이 많지 않다면 수신자는 전달된 신호를 강압으로 판단하지 않을 수 있다. 즉, 어떤 사이버 공격을 선택하느냐에 따라 신호하는 국가의 신뢰성 차원에의 비용이 달라진다. 위 분류에 따르면 사이버 강압 신호에 드는 비용은 디도스(DDoS), 사용자 계정 해킹, 홈페이지 변조, 데이터 탈취를 위한 네트워크의 기밀 접근, 네트워크와 시스템 내부로의 접근제어 공격 순으로 많이 든다고 개념화할 수 있다. 디도스 공격의 경우 대부분 저비용에 정교하지 않은 특성상 강압보다도 조정을 보내기 위한 공격으로 분류할 수 있을 것이다.

조정을 위한 신호에 드는 비용 계산으로 고려해야 할 청중에는 정부에 적대적인 야권과 국내 유권자가 있다.[40] 위기 상황에서 대치 중인 이해당사국들은 쌍방이 모두 확전을 원하지 않더라도, 정부가 더욱 공격적인 태도를 보여야 한다는 국내정치적 압력을 받을 수 있다. 이때 지도자들은 사이버 작전의 그럴듯한 부인 가능성을 이용해 확전 위험을 불러올 수 있는 강력

Conflict, p. 114.

38) Erica D. Borghard and Shawn W. Lonergan(2017), *op. cit.*, pp. 454-455.

39) 필자들은 국가 간 사이버 강압 신호를 분류하였더라도 제시된 사이버 작전 사례에는 비국가행위자에 의해 수행된 강압적이지 않은 공격까지 포함하고 있으며, 이는 독자들에게 공연히 알려진 사이버 작전들을 포함하여 개념화에 대한 이해를 돕기 위함이라고 밝혔다.

40) Erica D. Lonergan and Shawn W. Lonergan(2022), *op. cit.*, p. 37.

한 행동을 피하면서도 적절히 대응함으로써 국내 강경파 지지층을 달랠 수 있다. 더욱이, 국가 책임 수준을 둘러싸고 여전히 기준이 모호한 상황이어서 지도자들은 특정 행동이나 결정 전에 상대방과 서로의 상황을 관찰할 수 있다. 이를 통해 정부에 책임을 부여하지 않으려는 상대방의 의지를 평가하고, 따라서 국내 민족주의 정서를 더 자극하지 않도록 조절할 수 있다.

국가는 전략적 비밀유지(Strategic secrecy)를 고려해 전달하려는 신호를 판단한다. 먼저, 사이버 작전 신호의 공개성에 관한 것이다. 만약 국가가 공개적으로 사이버 작전을 수행했다면 상대방에게 보내는 위협에 대한 신뢰성이 강화될 수 있다. 동시에 그 위협은 상호 공개적으로 약속되고 위신을 보이는 것이므로 강압의 목적이 미이행될 경우 긴장 고조를 불러올 수 있다. 반대로, 국가가 비밀리에 사이버 작전을 수행했다면 추후 사이버 작전에 관한 그럴듯한 부인 가능성을 이용해 책임회피가 가능하다. 예를 들어, 정부가 연관성을 부인하기 위해 정부 지원을 받는 국가 배후 해커조직에 공격을 대리하는 경우이다. 이는 위협에 대한 신뢰성 저하로 이어지게 되며, 양국은 최소한 갈등이 유지되는 상황이나 긴장 완화로 전환을 꾀할 수 있다.

<표 2> 전략적 비밀유지와 조정 신호

의사전달		공격국가	
		책임을 인정함	**책임을 인정하지 않음**
타겟국가	**귀속함**	양국 간 양보를 제안하기 어려운 상황. 긴장 완화 가능성이 가장 낮음.	공격국가에 대한 국내정치적 비용 발생. 나중에 양보를 제안하기 어려워짐.
	귀속하지 않음	스스로 책임을 인정하여 귀속국가에 대한 국내정치적 비용 발생. 나중에 양보를 제안하기 어려워짐.	그럴듯한 부인 가능성을 유지하면서 위기 확대를 방지하고 긴장 완화 분위기를 조성할 수 있음.

출처: Erica D. Lonergan and Shawn W. Lonergan, “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises,” *Security Studies* 31(1) (Feb 17, 2022), pp. 43.

이해당사국의 정부 간 의사전달 방식에서도 마찬가지로 국가의 전략적 판단이 드러난다. 공격국가는 사이버 작전을 수행한 이후 해당 신호에 대해 정부 차원에서 책임을 인정하거나 인정하지 않을 수 있다. 예를 들어, A 국가는 B 국가를 상대로 사이버 작전을 수행한 이후 그 공격 사실을 인정하면서 추가 위협도 불사하지 않겠다는 강경 입장을 표할 수 있다. 하지만 공격국가가 사이버 작전에 관한 책임을 스스로 인정한다면 타겟국가에 대한 국내정치적 비용이 발생하기 때문에 추후 양보를 제안하기 어렵게 된다. 이때 타겟국가가 공개적으로 공격국가를 귀속한다면 양국은 대치상태에서 양보를 제안하기 어려운 상황을 지속하고 이후 갈등이 고조될 가능성이 커진다.

조정 신호로서 협상이나 양보 등을 통해 위기를 평화롭게 마무리하길 원하는 국가 행동은 공격국가와 타겟국가 모두 공개적인 의사전달 방식보다 비공개적인 의사전달 방식을 선택할 때이다. 공격국가는 사이버 작전에 관한 책임을 부인하고 갈등 봉합과 위기 완화에 적극적인 입장으로 나설 수 있다. 이때 타겟국가는 자국이 받은 위협에 대한 소행을 상대국가에 공개적으로 귀속하거나 귀속하지 않을 수 있다. 그러나 공개적으로 귀속할 경우 공격국가에 대한 국내정치적 비용이 발생하고 이 역시 나중에 양보를 제안하기 어렵도록 만든다. 따라서 양 국가

모두 사이버 작전에 관한 책임과 귀속에 있어서 비공개적으로 의사전달을 할 경우, 상호 간에 그럴듯한 부인 가능성을 유지하는 가운데 사적으로는 사이버 작전에 관한 귀속을 하더라도 위기 완화 분위기를 조성할 수 있다.

<표 3> 강압 신호와 조정 신호의 구분

기준	강압		조정
비용편익 계산	고비용	⟷	저비용
사이버 작전의 공개 여부	공개적	⟷	비공개적
사이버 작전에 관한 의사전달	공개적	⟷	비공개적

정리해보면, 국가가 사이버 작전 신호를 보내는 목적에는 첫째, 강압 차원에서 결의를 보여주기 위해 보내는 신호, 둘째, 조정 차원에서 타협 또는 양보를 나타내기 위해 보내는 신호가 있다. 강압 신호는 송신자가 전쟁이 발생할지 모를 일촉즉발의 위험이 닥치더라도 그 상황을 기꺼이 감수하여 승리를 쟁취하겠다는 의지가 강하다. 하지만 조정 신호를 보내는 송신자는 확전의 위험성이 커지는 것을 방지하고 갈등을 완화하여 위기를 평화롭게 해결하는 데에 목적이 있다. 사이버 작전 사용에 있어서 그것이 강압 신호인지 조정 신호인지 구별하는 기준으로는 먼저, 신호에 드는 비용과 청중비용 등 비용편익을 비교해 신호의 신뢰성을 판단할 수 있다. 다음으로, 사이버 작전이 공개적으로 수행되었는지 또는 비공개적으로 수행되었는지에 따라 구분할 수 있다. 마지막으로, 사이버 작전을 수행한 이후 해당 국가 정부의 의사전달 방식을 고려할 수 있다.

Ⅲ. 2022년 중국-대만 국제위기 사례 분석

1. 질문과 검증방법

본 연구는 사이버 작전 신호가 의미하는 바를 분석하기 위해서 국제위기 사례를 검증하고자 하였다. 앞선 보가드와 로너건(2022)의 연구에서는 2012년 중국-일본 센카쿠 분쟁과 2015년 러시아-터키 분쟁에서 나타난 사이버 작전이 조정 신호로 기능했음을 검증하였다. 두 분쟁의 공통점은 국가 배후에 있는 해커조직 혹은 핵티비스트 그룹들에 의해 저비용으로 수행된 사이버 작전이었다는 점, 그리고 국가지도자가 위기를 고조시키는 행동을 피하면서도 국내 유권자들의 반발을 사지 않도록 하는 레버리지로 사이버 작전을 사용했다는 점이다.

중국은 배후에서 지원하는 민영조직을 통해 공격 지시를 내리는 방식을 보여 왔으며, 당국 차원에서 수행하는 일련의 대외 사이버 공격에 관해서 언급을 삼가거나 관련 없다는 태도로 일관해왔다. 중국의 사이버 영역에서의 공격 행태는 군사작전이나 다른 공격수단과 달리 강압적이라고 단정할 수만은 없는 부분이 있다. 이러한 점에 주목하여 2022년 8월 펠로시 하원의장 방문 행사 기간에 중국이 대만에 수행한 사이버 작전이 강압보다는 조정 의미의 신호를 전달하려고 한 것이었는지 살펴보고자 하였다. 내용을 바탕으로 2022년 중국-대만 국제위기 사례를 통해 사이버 작전이 조정 신호로 기능했는지 검증하고자 하였다.

먼저, 중국이 대만에 수행하는 사이버 공격행위의 전반적 흐름을 살펴보고, 중국-대만 국제위기가 촉발된 배경과 중국의 일련의 사이버 공격행위들을 신호의 구분 기준에 따라 정리한다. 이를 통해 중국이 대만에 보낸 사이버 작전 신호의 의미를 판단하고자 하였다. 분석의 대상이 되는 신호로서 사이버 작전은 컴퓨터 네트워크와 시스템에 직접적인 영향을 미치는 물리적 공격만을 의미하며, 그밖에 심리전이나 인지전, 정보전을 배제하였다. 그리고 익명성과 부인 가능성으로 수행 주체에 대한 명확한 귀속이 어려운 점 등 연구 한계를 고려하여 국가 배후에서 조직적으로 활동하는 해커집단의 공격행위까지 포함하여 국가행위자를 대상으로 설정하였다.

2. 사례 분석

1) 중국의 대만 사이버 공격

대만해협을 둘러싼 미국과의 갈등 상황에서 중국은 강압 외교 등 수세적 전략을 펼치지만, 대만에 대해선 공갈과 소모전략 등 공세적 수단을 활용한다. 단, 그 기저에는 대화와 협상을 통한 위기의 평화적 해결이라는 기본원칙이 자리하고 있다.[41] 중국은 미국과 군사력을 다투며 해양패권을 둘러싸고 대만 해역에서 영향력을 높이고 있다. 최근 들어 중국이 대만 주변과 센카쿠 주변에 쳐진 대만과 일본의 방공식별구역(ADIZ)을 빈번히 침범하여 이를 무력화시키려고 시도하고 주변 해역에서 해상훈련을 빈번히 실시하는 것은 중국의 대만 합병과 미국-서방의 봉쇄선 돌파 노력의 일환이다. 중국은 국방백서에서 대만을 반드시 통일하겠다고 밝히고 있으

41) 한용준, “지정학적 위기에 대한 중국의 위기관리 전략 위기 협상을 중심으로,”『국제정치연구』제25집 3호(2022), p. 184.

며 2019년 최신예 스텔스 전투기 J-20을 이 지역에 배치했다.[42]

중국은 올해 하반기 대만 지방선거(2022년 11월 26일)와 2024년 대만 총통 선거를 앞두고 대만을 무력, 심리적으로 압박하며 전방위 공세를 이어오고 있다. 중국의 사이버 공격은 2016년 취임한 차이잉원(蔡英文) 대만 총통이 일국양제(一國兩制·한 국가 두 체제)를 거부하면서 정부와 독립적 성향의 집권 민진당의 기반을 흔들기 위해 더욱 빈번해졌다. 디도스 공격과 계정 해킹을 통한 첩보 활동에 그치지 않고, 최근 들어서는 대만 고위공직자와 기업인, 시민사회 내부에 친중 인식을 퍼뜨리기 위한 영향 공작에도 심혈을 기울이고 있다.

중국은 군사력과 병행하거나 독립적으로 대만을 향한 사이버 작전을 꾸준히 사용해왔다. 중국의 일명 '해커 전쟁'은 1996년부터 2004년까지 대만 총선을 계기로 대만을 향해서, 1999년 베오그라드 주재 중국 대사관 폭파사건과 2001년 EP-3 정찰기 충돌 이후 미국을 향해서, 그리고 지난 10년간 야스쿠니 신사와 센카쿠/댜오위다오 열도 관련 논쟁으로 일본을 향해서 치러져 왔다.[43] 시진핑 주석이 권력을 잡은 이후 군사와 정보기관의 재편을 시작했으며, 사이버 전쟁을 우선순위로 정하고 중국의 사이버 역량을 증진하기 위하여 군사와 민간단체의 '결합'에 착수했다.[44]

특히 중국의 민족주의 해커들은 중국 정부의 암묵적 동의나 유도 하에 외국 웹사이트를 훼손하고 디도스 공격을 하는 등 중국 정부의 대리인 역할을 자처하면서 '애국적 핵티비스트'로서 항의의 상징으로 자리하고 있다. 중국의 국가 배후 해커조직에는 훙커/레드 해커(Honker Union/Red Hacker), 차이나 이글(China Eagle Union), 녹색군단(the Green Army), 홍객연맹(the Red Hacker Alliance) 등이 있다.[45] 이밖에도 APT41, 레드알파(Redalpha), 무스탕 팬더(Mustang Panda), 스캐럽(Scarab) 등 다양한 해커들이 민간단체 조직으로 국가지원을 받고 활동해왔으며, 민족주의 성향이 강한 자발적 해커들도 대만 사이버 공격을 빈번히 수행하고 있다.[46]

서방 국가와 글로벌 보안 기업들은 중국의 해커들이 탈취 형태의 단순한 해킹을 넘어서 이제 통제 강화 전략, 거액의 투자, 전 세계 다른 정부에 해킹 기술을 공급하는 인프라로 인해 능력이 세계 최고 수준에 도달해 있다고 평가한다.[47] 중국발로 추정되는 사이버 공격에 대해

---

42) 윤민우, "미국-서방과 러시아-중국의 글로벌 전략게임: 글로벌 패권충돌의 전쟁과 평화," 『평화학연구』 제23권 2호(2022), p. 26.

43) Jon R. Lindsay, "The Impact of China on Cybersecurity," *International Security* 39(3) (2014), pp. 32-33.

44) Patrick Howell O'Neill, "중국은 어떻게 유례없는 사이버 첩보 조직을 만들어냈는가," 『MIT Technology Review』 2022.03.12. https://www.technologyreview.kr/%EC%A4%91%EA%B5%AD%EC%9D%80-%EC%96%B4%EB%96%BB%EA%B2%8C-%EC%9C%A0%EB%A1%80%EC%97%86%EB%8A%94-%EC%82%AC%EC%9D%B4%EB%B2%84-%EC%B2%A9%EB%B3%B4-%EC%A1%B0%EC%A7%81%EC%9D%84-%EB%A7%8C%EB%93%A4%EC%96%B4/ (검색일: 2022.11.20).

45) Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies," *FPRI* (May 7, 2016), p. 408.

46) 글로벌 사이버 보안 업체마다 공격 단체를 지칭하는 방식이 다르다. 예를 들어 보안업체 '클라우드스트라이크(CrowdStrike)'나 '사이버엑스(CyberX)' 등은 지역을 대표하는 동물들의 이름을 해킹 그룹에 붙이는 경향이 있다. 그래서 중국과 관련된 해커들에는 '판다'라는 이름표를 붙인다. 반대로 '파이어아이(FireEye)' 같은 경우는 'APT'라는 공격 단체의 유형 뒤에 숫자를 붙여나간다. 문가용, "[주말판] 해킹 그룹의 기묘한 이름들, 누가 누가 붙이나," 『보안뉴스』 2019.02.09. https://www.boannews.com/media/view.asp?idx=76772 (검색일: 2022.11.05).

47) Patrick Howell O'Neill(2022), *op. cit.*; 중국 사이버안보의 전략과 체계는 다음을 참고할 수 있다. 김진형, "중국 사이버안보의 전략과 체계," 『CSF 전문가 오피니언』 2022.05.13. https://csf.kiep.go.kr/issueInfoView.es?article_id=46175&mid=a20200000000&board_id=4 (검색일:

서 서방 국가들은 적극적으로 중국에 비난 성명을 발표하고, 서구 언론은 분석 보고서를 통해 중국 정부의 소행이라고 추정해왔다. 이에 중국은 공산당 기관지인 인민일보나 자매지인 환구시보 등을 통해, 제기된 주장이 터무니없다며 비판하거나 아무런 반응을 하지 않음으로써 해당 사이버 공격과 무관하다는 태도를 보여왔다.[48)]

2) 2022년 중국-대만 국제위기

4차 대만해협 위기라 불리는 중국-대만 국제위기는 2022년 8월 미국 하원의장인 낸시 펠로시가 대만을 방문하는 행사로 인해 촉발되었다. 사이버 공격행위들은 펠로시 하원의장의 방문 직전과 직후 며칠 사이에 걸쳐 수행되었다. 대략 한 달간 긴장 국면에 있던 국제위기 속 중국의 사이버 공격행위에 관하여 신호의 구분 기준에 따라 내용을 살펴본다.

비용편익 계산 측면에서 중국은 저비용, 저강도의 디도스 공격을 사용하였다. 대만 중앙통신사에 따르면 어우장안(歐江安) 대만 외교부 대변인은 "펠로시 의장이 대만에 도착한 2일 밤 중국과 러시아 등지의 인터넷프로토콜(IP)을 통한 과도한 접속 시도가 있었고, 이에 따라 외교부 홈페이지가 일시적으로 마비되는 현상이 있었다"고 밝혔다. 어우장안 대변인은 "당시 중국, 러시아 및 기타 지역의 다수 IP에서 분당 최대 850만 회에 이르는 접속 시도가 이뤄지는 비정상적인 정황이 포착됐다"며 "이는 분명 (외교부) 홈페이지의 운영을 고의로 마비시키려는 의도였다"고 주장했다.[49)] 외교부뿐만 아니라 다른 대만 정부 기관의 웹사이트들과 전산시스템도 마찬가지로 디도스 공격을 받았다. 대만 총통부 홈페이지도 펠로시 하원의장이 대만에 도착하기 불과 몇 시간 전 디도스 공격으로 약 20분간 접속이 제한됐었다. 대만의 TVBS 기자는 트위터에 "이번 공격 트래픽은 정상 대비 200배에 달했다"고 설명했다.[50)] 대만 국방부는 3일 오후 11시 4분부터 국방부 서버가 디도스 공격을 받았고, 11시 27분에는 과도한 트래픽이 유입되면서 홈페이지가 마비됐다고 발표했다.[51)]

한편, 대만이 피해를 복구하기까지 오랜 시간이 걸리지 않았다는 점에서 사이버 공격이 저강도로 이루어졌음을 알 수 있다. 공격받은 웹사이트와 전산시스템은 일시적으로 운영에 차질을 빚었으나 대만당국의 조치로 곧 정상화됐다. 탕펑(唐鳳·오드리 탕) 대만 행정원 디지털 담당 정무위원은 다수의 정부 기관 웹사이트 트래픽이 평소보다 23배가량 치솟았다면서 관련 사이버 공격에 대해 적절한 조치가 취해졌다고 밝혔다.[52)] 대만 국방부는 마비된 홈페이지 서버를 1시간 뒤에 정상 복구했다고 밝혔다. 사이버 공격은 장기간에 걸쳐 정교하게 수행된 것이 아닌 일시적으로, 무작위 대상으로 이루어졌다는 특징을 보인다. 앞선 주요 정부 기관 대상의 공격 외에도 타오위안 국제공항, 대만 철로관리국, 대만 전력공사의 웹사이트 또는 전산

2022.11.20).

48) 국가행위자가 아닌 비국가행위자에 의해 사이버 작전이 수행된 경우, 당국의 소행이라고 재단할 수 없는 점은 분석상 한계로 남는다. 그러나 사이버공간에서 공격 주체의 부인 가능성이 큰 공격 이점으로 작용하는 근본적 특성을 참작할 때 여전히 국가행위자를 귀속할 여지를 남겨두어야 한다.

49) 정혜인, ""분당 850만회…中·러 사이버공격에 대만 정부 홈피 마비"," 『머니투데이』 2022.08.04. https://news.mt.co.kr/mtview.php?no=2022080416261562481 (검색일: 2022.10.15).

50) *Ibid.*

51) 류정엽, "[속보] 대만 총통부, 국방부, 외교부 홈페이지 해킹공격..범인은 누구?," 『nownews』 2022.08.04. https://nownews.seoul.co.kr/news/newsView.php?id=20220804601013 (검색일: 2022.10.15).

52) 장지현, "대만 사이버 공격에 中 소프트웨어 연루," 『시사저널』 2022.08.05. https://www.sisajournal.com/news/articleView.html?idxno=243734 (검색일: 2022.10.15).

시스템이 전방위적으로 사이버 공격을 받았다. 그리고 대만 편의점인 세븐일레븐(7-11)과 철도역의 전광판을 대상으로도 사이버 공격이 이루어졌다.

공격은 물리적 피해와 함께 심리전 전개 양상도 띠었다.[53] 8월 3일 일부 세븐일레븐에 설치된 TV 화면에 '전쟁 장수 펠로시는 대만을 떠나라'는 자막이 뜨는 일이 발생했는데, 대만의 국가통신위원회(NCC) 조사 결과, 중국의 소프트웨어가 이용된 것으로 파악됐다. 대만의 일부 철도역 전광판에도 펠로시 하원의장의 대만 방문을 반대하는 자막이 떴다. 7일에는 국립 대만대 교무처와 연구개발처 홈페이지에 빨간색 바탕에 금색과 흰색으로 쓰인 '세계에는 오직 하나의 중국만 있다'는 메시지가 올라왔다. 대학 측은 이 문구가 대만에서 사용하는 번체자(繁體字)가 아닌 중국에서 사용하는 간체자(簡體字)로 쓰였다는 점에서 중국발 해킹 가능성을 의심하고 있다.[54]

중국은 공산당 일당 체제라는 국가체제에서 야당과 유권자의 반발 가능성이 낮기 때문에 청중비용이 크지 않았다. 하지만 국제 이슈화되는 내부 여론을 관리해야 할 필요가 있었다. 펠로시 하원의장의 방문 직후 중국의 모든 민주당에서 공동성명서를 제출하여 해당 이슈를 비난하였고, 전중국대만동포연맹도 즉각 성명을 발표하여 대만을 향한 불만과 적대 의식을 표출하는 등 대만에 대한 부정적 여론이 확산하는 상황이었다.[55] 인민일보의 한 논평가는 "조국통일을 실현하려는 중국정부와 중국인민의 결심은 바위처럼 확고하며 그 누구도, 그 어떤 세력도, 그 어떤 나라도 바꾸지 않을 것"과 "우리는 외부의 간섭과 "대만 독립" 분리주의를 단호히 반대하며 어떠한 형태의 "대만 독립" 세력도 용납하지 않을 것"이라 말하여 대만과 미국을 향한 분노를 강하게 드러냈다.[56] 해외주재 총영사들은 페이스북과 트위터, 포토월 등 소셜 계정에 서명을 게시해 중국의 확고한 의지를 표명하였다. 이러한 행위들로 중국 시민들의 대만을 향한 비난 여론이 결집되는 효과가 있었을 것이며 중국당국은 민족주의자들의 적개심과 기대에 어느 정도 부응해야 할 부담을 가졌을 것으로 보인다.

사이버 작전의 공개성 측면에서는 사이버 공격이 중국 해커들에 의해 수행된 것으로 추정되므로 비공개적이라 볼 수 있다. 사이버안보 조사기관인 SANS 연구소 요하네스 울리히 연구부장은 "공격들은 중국 해커들이 자신들의 메세지를 전달하기 위한 비체계적·무작위적·비도덕적 공격"이라며 "중국 정부 해커들의 일반적 방법과는 일치하지 않는다"고 말했다. 전략국제연구센터(CSIS)의 제임스 루이스 전략기술국장도 중국 정부 소행은 아닌 것으로 보인다며 "아마추어 중국 해커들이 불쾌감을 표시한 것"이라고 전했다.[57] 중국당국의 작전 지시 여부가 불명확하나, 중국당국을 배후로 본 국제 해커집단 어나니머스는 대만대 홈페이지에 사이버 공격

---

53) 사이버 작전 신호에 포함되지 않으나, 중국은 대만 사회에 공포를 불러일으키고 대만 통일론을 정당화하려는 의도로 사이버 심리전도 빈번히 수행하였다. 대만 국방부는 중국 공산당이 8일간 대만에서 가짜뉴스를 퍼뜨리려는 시도를 272회 적발했다고 밝혔는데, 낸시 펠로시 하원의장의 대만 도착을 앞두고 포착되기 시작한 가짜뉴스는 펠로시 의장이 떠나고 중국군의 대만을 겨냥한 실탄 훈련이 시작한 4일 이후 본격화됐다. 코닷, "중국의 심리전…사이버공격·가짜뉴스로 대만 민심 흔들기," 『코람데오닷컴』 2022.08.09. https://www.kscoramdeo.com/news/articleView.html?idxno=23402 (검색일: 2022.11.01).

54) "중국의 심리전…사이버공격·가짜뉴스로 대만 민심 흔들기," 『매일경제』 2022.08.09. https://www.mk.co.kr/news/world/view/2022/08/701673/ (검색일: 2022.10.15).

55) 위키피디아, "2022年南希·佩洛西窜访台湾事件," 『Baidu』 https://baike.baidu.com/item/2022%E5%B9%B4%E5%8D%97%E5%B8%8C%C2%B7%E4%BD%A9%E6%B4%9B%E8%A5%BF%E7%AA%9C%E8%AE%BF%E5%8F%B0%E6%B9%BE%E4%BA%8B%E4%BB%B6/61814472#3_2 (검색일: 2022.11.15).

56) "人民日报评论员：中国政府和中国人民实现祖国统一的决心坚如磐石," 『人民日报』 2022.08.03. https://wap.peopleapp.com/article/6823852/6691745 (검색일: 2022.11.15).

57) 박기현, "펠로시 방문하자 대만 정부 홈페이지들 디도스 공격 당해..中소행?," 『뉴스1』 2022.08.03. https://v.daum.net/v/20220803112420336 (검색일: 2022.10.31).

이 발생한 데 대한 보복으로 중국의 부동산회사 웹사이트를 해킹하였다.[58]

사이버 작전에 관한 의사전달 방식에 있어서 중국당국은 대만에서 발생한 사이버 공격들에 대해 공개적인 언급을 하지 않았다. 다만, 펠로시 하원의장의 방문 이슈에 대해 중국 국무원은 즉각 공식성명을 발표해 중국의 주권과 영토 보전을 도발하고 침해한 행위라고 규정하면서 강력규탄할 것이라는 강압에 가까운 의사전달 방식을 보였다. 펠로시 하원의장이 대만을 방문한 직후 국방부 보도대변인과 전인대 상무위원회 대변인이 무단 방문을 규탄하고 반대한다는 담화를 발표하였으며, 중국 공산당 중앙위원회 대만사무판공실과 중국인민정치협상회의 전국위원회에서도 중국에 대한 중대한 정치적 도발이라고 규정하는 등 내정 간섭을 반대하는 성명을 발표하였다.[59]

3. 소결

사이버 작전 신호의 구분 기준에 따르면, 중국은 펠로시 하원의장의 대만 방문에 대한 불만을 공식적으로 표출하기 위해 저강도 사이버 작전인 디도스 공격을 사용하였다. 대만의 여러 주요 정부기관 사이트와 사회기반시설을 향한 디도스 공격은 저비용 측면에서 일시적으로 이루어졌다. 따라서 대만에 일정 피해를 주었다고 하더라도 결의를 전하려는 신호로써 신뢰성은 다소 떨어진다고 볼 수 있다. 그리고 해당 사이버 작전은 중국당국이 공개적으로 수행하지 않고 중국 배후가 의심되는 해커들에 의해 우회적으로 수행되었다. 이후 사이버 공격 사실에 관하여 중국당국은 언급하지 않음으로써 책임을 부인하였다. 이는 그럴듯한 부인 가능성을 이용해 책임을 회피하는 방식을 택하여 국내정치적 비용 발생을 최소화하고 갈등이 확대되는 것을 막으려는 의도로 풀이할 수 있다.

<표 4> 중국의 사이버 작전 신호 요약

기준	중국의 사이버 공격행위
비용편익 계산	- 일시적이고 정교하지 않은 저비용, 저강도의 디도스 공격 - 일당체제 하에 청중비용은 낮으나 민족주의 여론 관리 필요
사이버 작전의 공개 여부	- 비국가행위자인 해커들 소행으로 추정되는 비공개적 공격
사이버 작전에 관한 의사전달	- 언급하지 않음으로써 책임을 인정하지 않음

58) 서희원, “어나니머스, 中 기업 해킹…대만대 사이버공격 보복,” 2022.08.24. https://www.etnews.com/20220824000241 (검색일: 2022.11.02).

59) “중국 전인대 상무위원회 대변인, 펠로시 미 하원의장 중국 대만지역 무단 방문 관련 담화 발표,”『신화망』 2022.08.03. https://kr.news.cn/20220803/15d4eefe7b774cb28c22d4958ae270fc/c.html (검색일: 2022.11.14). ; “펠로시 대만 무단 방문,중공중앙 대만사무판공실 성명 발표,”『신화망』 2022.08.03. https://kr.news.cn/20220803/9ff30b4e73d343ec93be2df80b82d437/c.html (검색일: 2022.11.14); “오겸 국방부 보도대변인, 펠로시 미 하원의장의 대만 무단 방문 관련 담화 발표,”『신화망』2022.08.03. https://kr.news.cn/20220803/af04d44334ef45afb024f3493e8b43cd/c.html (검색일: 2022.11.14); “펠로시 미 하원의장의 대만지역 무단 방문에 관한 전국정협 외사위원회 성명,”『신화망』 2022.08.03. https://kr.news.cn/20220803/248b2e71fb4b44c881d1470a787402e1/c.html (검색일: 2022.11.14).

신호이론을 통해 본다면 중국이 대만을 상대로 수행한 사이버 작전은 조정 의미에 가깝다. 강압 의미에 더 가까우려면 사이버 작전이 장기간에 걸쳐 정교하게 수행되어야 한다. 또한, 실제 물리적으로 파괴적인 효과를 불러왔어야 한다. 그러나 실제 대만을 향한 공격은 강압의 방식과는 거리가 있었다. 사이버 작전 역시 비밀리에 또는 중국 해커들에 의해 간접적으로 수행되어 조정에 가까웠다. 만약 중국이 직접 공개적으로 사이버 작전을 사용했다면 대만을 향한 강한 결의를 보여주었다고 볼 수 있었을 것이나 그렇지 않았다. 사이버 공격행위 직후와 이후에도 중국당국은 해당 공격들에 관한 공개입장이나 의사를 표명하지 않고 있다. 중국의 소극적, 수동적 행동은 사이버 공격을 통해 물리적 피해를 줄 목적보다도 적절히 한계를 보이고 책임을 부인할 수 있다는 이점을 활용하여 불필요한 긴장 고조를 피하는 일종의 양보를 택한 것으로 볼 수 있을 것이다.

보가드와 로너건(2022)의 분석과 비교해볼 때도 중국의 사이버 작전을 조정 신호로 풀이할 수 있는 두 가지 공통점이 있다. 첫째, 국가 배후 해커조직에 의한 저비용, 저강도의 정교하지 못한 사이버 공격으로 추정되는 점, 둘째, 청중비용으로 국내 민족주의자들에 대한 고려가 존재한다는 점이다. 즉, 중국당국은 미국 정치인의 대만 방문 예정으로 대만을 향한 분노가 강하던 국내정치적 상황을 관리해야 할 필요가 있었다. 이에 국내여론을 달래면서도 제한적인 효과를 보이는 지렛대로 사이버 작전 신호를 적절히 활용한 것이다. 한편, 두 사례의 차이점으로는 러시아-터키 사례에서 군사작전 대신 사이버 작전을 사용한 러시아와 달리, 중국은 대만을 상대로 군사작전과 그 외 다른 수단들도 병행하였다는 점이다. 이는 사이버 작전 신호에 관한 의미를 도출할 때 다른 공격행위들의 성격까지 종합적으로 고려해야 하는 측면에서 이론적 적용에 대한 설득력을 낮춘다.

특히 본 사례를 전체적으로 조망하였을 때 과연 중국당국이 대만을 상대로 조정을 시도한 것인지에 대해 의구심이 들 수 있다. 사이버 작전과 별개로, 중국당국은 조정보다는 결의의 의도가 짙은 공격들을 수행했기 때문이다. 중국은 대만 인근에서 4일부터 10일까지 군사훈련을 실시하였고 경제보복도 감행해 위기를 고조시키려는 모습을 보였다. 그러나 일각에서는 이러한 공격적인 군사행동에 대해서도 다른 견해를 보였다. CIA 분석가 존 컬버(John Culver)는 “중국 측이 자제한 것으로 볼 수 있지만, 다음에는 훨씬 더 큰 위협을 보여주기 위해 유보한 것이기도 하다”고 했으며, 담강대학교(淡江大学) 국제문제 및 전략연구소의 린잉유(Ying-yu Lin·林穎佑) 박사는 중국의 군사훈련이 펠로시 의장의 방문과 관계없이 이루어졌을 것이라는 입장을 밝히기도 했다.[60]

국제사회에서 중국이 대외적으로 비친 이미지와 외교적 수사(修辭) 역시 중국이 대만을 향한 공격 수위를 조절할 수밖에 없음을 가늠케 한다. 중국은 대만을 상대로 대화와 협상을 통한 위기의 평화적 해결이라는 기본원칙을 고수해왔다. 대만에 공세적인 수단을 사용하더라도 갈등이 커지거나 확전 위험을 불러오는 행위를 지속할 경우 국제사회에서 쏟아지는 비난을 감수해야 한다. 따라서 상대적으로 제한적인 수단을 통해 공격하여 대만에 위협을 주면서도 동시에 자제나 조정을 유도하여 위기를 관리하는 방식을 추구했을 가능성이 크다. 이러한 점에서 자제나 조정 신호로서 사이버 작전 사용은 여전히 의미 있다고 보아야 할 것이다.

60) “[이슈트렌드] 중국의 타이완 인근 군사훈련, 뉴노멀 되나,” 『CSF』 2022.08.18. https://csf.kiep.go.kr/issueInfoView.es?article_id=47228&mid=a20200000000&board_id=2 (검색일: 2022.11.16).

Ⅳ. 결론

탈냉전 시대가 도래하면서 전쟁보다는 크고 작은 무력 충돌을 관리하여 국가이익을 극대화하기 위한 전략을 세우는 것이 중요해졌다. 본 연구는 국가의 국제위기관리 차원에서 사이버 작전을 통해 국가가 전략적 의도를 전달할 수 있는지 확인하기 위한 시도에서 비롯되었다. 먼저, 국제정치학에서 신호이론에 관한 주요 논의들을 정리하고, 이론을 사이버 영역에 적용하여 사이버 작전이 신호가 되기 위한 요건들을 도출하였다. 사이버 작전은 언어적 또는 비언어적 방식으로 전달될 수 있으며, 다양한 사이버 작전 가운데 실제 수신하는 국가가 관측할 수 있는 위협 종류이어야 한다. 그리고 전달되는 신호는 신호를 보내는 국가와 반드시 연결되어 있어야 한다.

사이버 작전은 첫째, 강압 차원에서 결의를 보여주기 위해 보내는 신호, 둘째, 조정 차원에서 타협이나 양보를 나타내기 위해 보내는 신호 두 가지로 구분된다. 두 신호에 대한 구분 기준은 첫째, 발생하는 비용편익 계산, 둘째, 사이버 작전의 공개 여부, 셋째, 사이버 작전 이후 정부의 의사전달 방식이다. 공격에 드는 비용이 고비용에서 저비용으로 갈수록 강압이 아닌 조정 신호에 가깝다. 특히 국가지도자는 정부에 적대적인 야권과 국내 유권자에 관한 청중비용이 클수록 강압보다 조정을 고려하게 된다. 그리고 사이버 작전을 비공개적으로 은밀히 수행할 때보다 공개적으로 수행할 때 강압 신호에 더 가까우며, 작전 이후 정부가 공개적으로 책임을 인정하였을 때가 비공개적으로 인정하거나 부인할 때보다 강압 신호에 가깝다고 볼 수 있다.

본 연구는 2022년 8월 중국-대만 국제위기 사례에의 적용을 통해 사이버 작전상 의미 구분에 대한 검증을 시도하였다. 중국이 수행한 일련의 사이버 공격행위들은 세 가지 기준에서 모두 강압보다는 조정에 가까운 신호였다. 이를 통해 중국이 사이버 작전을 통해 대만에 전달하고자 한 의도가 조정에 있음을 확인할 수 있었다. 사이버 공격행위만을 놓고 본다면, 중국당국의 소극적, 수동적 행동은 사이버 공격의 특성상 물리적 피해에 적절한 한계를 주고 책임을 부인할 수 있다는 이점을 활용하여 불필요한 긴장 고조를 피하는 일종의 양보를 택한 것으로 볼 수 있을 것이다. 다만, 중국이 사이버 작전 외에도 군사작전과 경제보복 등 대만을 향해 다양한 수단으로 대응에 나섰기 때문에, 중국당국의 전체적인 입장이 조정 전략으로 수렴되었다고 보긴 어렵다는 분석상 한계를 도출하였다.

사이버공간에서 신호이론의 적용은 사이버 작전을 사용하는 국가가 공격행위를 통해 전달하고자 하는 의미를 성공적으로 예측하려 할 때 하나의 실마리를 제공한다는 점에서 유용하다. 기존에 사이버 작전은 피해를 줄 목적이나 강압을 위한 위협 차원에서 사용한다는 시각이 일반적이었다. 하지만 국가는 상대적인 국력 격차를 극복하고 위기관리를 통해 국익을 극대화하고자 적극적으로 타협과 양보에 나설 수 있다. 조정 신호는 사이버 작전이 상대적으로 제한된 영향력을 발휘하며, 전략적 비밀유지를 가능하게 하여 국가 간 해결 분위기로 수렴되도록 협상 공간을 넓힌다는 점에서 그 효과가 발휘된다.

본 연구의 기여점은 사이버 작전 신호를 강압과 조정 신호로 구분하고 구분 기준을 제시하였다는 점이다. 이를 통해 국가 지도부는 사이버 안보전략 이행에 있어서 사이버 작전의 활용도를 높일 수 있다. 특히 강대국이든 약소국이든 전략적 이익을 추구하는 이해당사국은 국제위기관리 차원에서 자제나 조정을 위해 사이버 작전을 사용할 수 있다. 국가지도자는 사이버 조정 신호를 보내 국내정치적으로 발생하는 청중비용을 최소화할 수 있으며, 대외적으로는 확전을 방지하고 갈등을 평화롭게 해결하고자 하는 목표를 유도할 수 있다.

사이버 작전 사례에 관해서는 경험적 증거들이 더 뒷받침되어야 할 것으로 보인다. 반례로, 공격국가가 신호 목적으로 송신하더라도 타겟국가는 그것을 신호가 아니라고 오인할 수 있다. 반대로 공격국가는 신호를 의도하지 않고 손해를 입힐 목적 자체로 사이버 작전을 수행하였는데 타겟국가는 그것을 하나의 신호로 받아들일 수도 있다. 따라서 국가가 다른 이유보다도 신호로서 사이버 작전을 선택하여 얻는 효과성에 관해서는 연구가 보완되어야 할 것이다. 특히 강압에 관하여는 기존연구들이 다수 정리되어 있으나, 조정에 관하여는 실제 사례에 기반한 연구나 이론적 정립이 더딘 실정이다. 따라서 사례 중심으로 조정 신호의 효과성을 도출하는 후속연구가 진행되어야 할 것이다.

<참고문헌>

국내문헌

김법헌·김덕기. “중국의 대만해협 위기관리 교훈이 미국 대응전략과 군사력에 미친 함의 -진먼다오(金門島)、마주다오(馬祖島) 위기를 중심으로-.”『대한정치학회보』제27권 2호 (2019).

김지용. “위기 시 청중비용의 효과에 관한 이론 논쟁 및 방법론 논쟁의 전개과정 고찰.”『국제정치논총』제54집 4호 (2014).

김진형. “중국 사이버안보의 전략과 체계.”『CSF 전문가 오피니언』2022.05.13.

손영동.『iWar: ‘사이버 냉전시대’ 국가는 어떻게 생존하는가?』서울: 황금부엉이, 2010.

윤민우. “미국-서방과 러시아-중국의 글로벌 전략게임: 글로벌 패권충돌의 전쟁과 평화.”『평화학연구』제23권 2호 (2022).

장노순·김소정. “미국의 사이버전략 선택과 안보전략적 의미: 방어, 억지, 선제공격전략의 사례 비교 연구.”『정치정보연구』19(3) (2016).

정하연. “사이버 강압의 국제정치: 사이버 공격 사례를 통해 본 국가 간 갈등 연구.” *이화여자대학교 정치외교학과 박사학위논문* (2017.12).

조동준. “신호이론으로 분석한 2013년 한반도 위기.”『평화학연구』제19권 1호 (2018).

한용준. “지정학적 위기에 대한 중국의 위기관리 전략 위기 협상을 중심으로.”『국제정치연구』제25집 3호 (2022).

Byman, Daniel and Waxman, Matthew C. 이옥연 옮김.『미국의 강압전략 : 이론, 실제, 전망』서울: 사회평론, 2004.

국외문헌

Arquilla, John and Ronfeldt, David. *Cyberwar is Coming!* Rand Corporation. 1993.

_____. “In Athena’s Camp Preparing for Conflict in the Information Age.” *Comparative Strategy* Vol. 12. No. 2. Spring 1993.

Blagden, David. “Deterring Cyber Coercion The Exaggerated Problem of Attribution.” *Survival Global Politics and Strategy* Vol. 62 Issue 1 (2020).

Borghard, Erica D. and Lonergan, Shawn W. “Can States Calculate the Risks of Using Cyber Proxies.” *FPRI* (May 7, 2016).

_____. “The Logic of Coercion in Cyberspace.” *Security Studies* 26(3) (2017).

_____. “Cyber Operations as Imperfect Tools of Escalation.” *Strategic Studies Quarterly* 13(3) (Fall 2019).

_____. “Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises.” *Security Studies* 31(1) (Feb 17, 2022).

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020.

Brandon, Valeriano, Jensen, Benjamin and Maness, Ryan C. *Cyber Strategy: The Evolving Character of Power and Coercion* (2018; online edn, Oxford Academic, 24 May 2018).

Brangetto, Pascal and Veenendaal, Matthijs A. “Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations.” 2016 8th International Conference on Cyber Conflict.

Cornish, Paul, Livingstone, David, Clemente, Dave and Yorke, Claire. “On Cyber Warfare.” *A Chatham House Report*. London, UK: Chatham House 2010.

Egloff, Florian J. and Smeets, Max. “Publicly Attributing Cyber Attacks: A Framework.” *Journal of Strategic Studies* (2021).

George, Alexander L. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. US Institute of Peace Press (1991).
Kostyuk, Nadiya and Zhukov, Yuri M. "Invisible Digital Front: Can Cyber Attack Shape Battlefield Events?" *Journal of Conflict Resolution* 63(2) (2019).
Kugler, Richard L. "Deterrence of Cyber Attacks." In Kremer et al.(Eds.). *Cyberpower and national security.* Washington D.C.: National Defense University Press, 2009.
Leal, Marcelo and Musgrave, Paul. "Cheerleading in Cyberspace: How the American Public Judges Attribution Claims for Cyberattacks." *Foreign Policy Analysis* Vol. 18. Issue. 2 (April, 2022).
Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22(3) (2013).
_____. "The Impact of China on Cybersecurity." *International Security* 39(3) (2014).
Mahnken, Thomas G. "Cyberwar and Cyber Warfare." in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age (Vol.Ⅱ).* Washington, DC: Center for a New American Security, 2011.
Poznansky, Michael and Perkoski, Evan. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3(4) (2018).
Rice, Mason, Butts, Jonathan and Shenoi, Sujeet. "A signaling framework to deter aggression in cyberspace." *International Journal of Critical Infrastructure Protection* Vol. 4 No. 2 (2011).
Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35(1). 2012.
Rid, Thomas and Buchanan, Ben. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38/1-2 (2015).
Schelling, Thomas C. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.
_____. *Arms and Influence*. New Haven, CT: Yale University Press, 1996.
_____. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.
Schneider, Jacquelyn. "Cyber and Crisis Escalation: Insights from Wargaming." Working Paper. US Naval War College. Newport. RI. (2017).
Sharp, Travis. "Theorizing cyber coercion: The 2014 North Korean operation against Sony." *Journal of Strategic Studies* 40(7) (2017).
Shandler, Ryan and Gomez, Miguel Alberto. "The hidden threat of cyber-attacks – undermining public confidence in government." *Journal of Information Technology & Politics* (2022).
Snyder, Glenn Herald and Diesing, Paul. *Conflict Among Nations: Bargaining, Decision Making, and System Structure in International Crises.* Princeton, New Jersey: Princeton University Press, 1977.
Valeriano, Brandon and Jensen, Benjamin. "The Myth of the Cyber Offense: The Case for Restraint." *CATO Institute: Policy Analysis 862* (15 January 2019).
Valeriano, Brandon and Maness, Ryan C. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11." *Journal of Peace Research* 51(3) (2014).

보도기사

류정엽. "[속보] 대만 총통부, 국방부, 외교부 홈페이지 해킹공격..범인은 누구?"『nownews』

2022.08.04. https://nownews.seoul.co.kr/news/newsView.php?id=20220804601013 (검색일: 2022.10.15).
문가용. “[주말판] 해킹 그룹의 기묘한 이름들, 누가 누가 붙이나.”『보안뉴스』2019.02.09. https://www.boannews.com/media/view.asp?idx=76772 (검색일: 2022.11.05).
박기현. “펠로시 방문하자 대만 정부 홈페이지들 디도스 공격 당해..中소행?”『뉴스1』2022.08.03. https://v.daum.net/v/20220803112420336 (검색일: 2022.10.31).
서희원. “어나니머스, 中 기업 해킹…대만대 사이버공격 보복.” 2022.08.24. https://www.etnews.com/20220824000241 (검색일: 2022.11.02).
장지현. “대만 사이버 공격에 中 소프트웨어 연루.”『시사저널』2022.08.05. https://www.sisajournal.com/news/articleView.html?idxno=243734 (검색일: 2022.10.15).
정혜인. “"분당 850만회…中·러 사이버공격에 대만 정부 홈피 마비".”『머니투데이』2022.08.04. https://news.mt.co.kr/mtview.php?no=2022080416261562481 (검색일: 2022.10.15).
코닷. “중국의 심리전…사이버공격·가짜뉴스로 대만 민심 흔들기.”『코람데오닷컴』2022.08.09. https://www.kscoramdeo.com/news/articleView.html?idxno=23402 (검색일: 2022.11.01).
“[이슈트렌드] 중국의 타이완 인근 군사훈련, 뉴노멀 되나.”『CSF』2022.08.18. https://csf.kiep.go.kr/issueInfoView.es?article_id=47228&mid=a20200000000&board_id=2 (검색일: 2022.11.16.).
“오겸 국방부 보도대변인, 펠로시 미 하원의장의 대만 무단 방문 관련 담화 발표.”『신화망』2022.08.03. https://kr.news.cn/20220803/af04d44334ef45afb024f3493e8b43cd/c.html (검색일: 2022.11.14).
“중국의 심리전…사이버공격·가짜뉴스로 대만 민심 흔들기.”『매일경제』2022.08.09. https://www.mk.co.kr/news/world/view/2022/08/701673/ (검색일: 2022.10.15.).
“중국 전인대 상무위원회 대변인, 펠로시 미 하원의장 중국 대만지역 무단 방문 관련 담화 발표.”『신화망』2022.08.03. https://kr.news.cn/20220803/15d4eefe7b774cb28c22d4958ae270fc/c.html (검색일: 2022.11.14.).
“펠로시 대만 무단 방문,중공중앙 대만사무판공실 성명 발표.”『신화망』2022.08.03. https://kr.news.cn/20220803/9ff30b4e73d343ec93be2df80b82d437/c.html (검색일: 2022.11.14).
“펠로시 미 하원의장의 대만지역 무단 방문에 관한 전국정협 외사위원회 성명.”『신화망』2022.08.03. https://kr.news.cn/20220803/248b2e71fb4b44c881d1470a787402e1/c.html (검색일: 2022.11.14).
O’Neill, Patrick Howell. “중국은 어떻게 유례없는 사이버 첩보 조직을 만들어냈는가.”『MIT Technology Review』2022.03.12. https://www.technologyreview.kr/%EC%A4%91%EA%B5%AD%EC%9D%80-%EC%96%B4%EB%96%BB%EA%B2%8C-%EC%9C%A0%EB%A1%80%EC%97%86%EB%8A%94-%EC%82%AC%EC%9D%B4%EB%B2%84-%EC%B2%A9%EB%B3%B4-%EC%A1%B0%EC%A7%81%EC%9D%84-%EB%A7%8C%EB%93%A4%EC%96%B4/ (검색일: 2022.11.20.).
“人民日报评论员：中国政府和中国人民实现祖国统一的决心坚如磐石.”『人民日报』2022.08.03. https://wap.peopleapp.com/article/6823852/6691745 (검색일: 2022.11.15.).

기타 자료

위키피디아. “2022年南希·佩洛西窜访台湾事件.”『Baidu』 https://baike.baidu.com/item/2022%E5%B9%B4%E5%8D%97%E5%B8%8C%C2%B7%E4%BD%A9%E6%B4%9B%E8%A5%BF%E7%AA%9C%E8%AE%BF%E5%8F%B0%E6%B9%BE%E4%BA%8B%E4%BB%B6/61814472#3_2 (검색일: 2022.11.15).