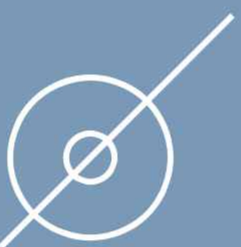
미국의 사이버 안보 동맹 전략



2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 17호
발간일: 2024년 8월 20일

정성철 (명지대학교)

Ⅰ. 들어가는 글

미국은 지리적 축복을 받은 나라이다 (팀 마샬 2016). 광활한 영토, 풍부한 자원, 안정적 국경이 잠재적 국력을 이룬다. 신생국 미국은 영토를 확장하며 팽창의 역사를 거듭하며 외형의 확장을 일구었다 (권용립 2010). 19세기 중후반 아메리카 대륙의 패권을 차지한 이후에는 자국의 지위 유지와 상승에 노력을 기울였다. 19세기 초 먼로 독트린으로 유럽 강대국의 아메리카 개입을 명확히 반대하였으며, 20세기 초 유럽 대륙의 전쟁에 연루되는 것을 꺼려했다. 아메리카의 패권국으로 다른 지역의 전쟁에 개입할 전략적 유인이 약했던 것이다. 유라시아 대륙의 강대국은 끊임없이 서로를 경계하고 적대하는 사이 대서양과 태평양으로 둘러싸인 미국은 자국의 본토를 침공하는 외부 세력을 마주할 일이 없었다.

하지만 2001년 9·11 테러는 미국이 더 이상 천연의 요새가 아님을 일깨워 주었다. 뉴욕과 워싱턴에서 발생한 비극적 사건은 이슬람 테러단체에 속수무책으로 당하는 미국의 현실을 생생히 보여주었다. 소련의 붕괴 이후 적수가 없다고 생각했던 미국은 테러와의 전쟁을 선포한 이후 아프가니스탄과 이라크를 침공하였고 자유주의 세계질서의 해외 이식을 한층 일방적으로 추진하기 시작하였다. 그러나 전쟁 승리 이후 이라크 건설에 실패하고 글로벌 금융위기를 맞이하자 소위 자유패권 대외전략에 대한 국내 비판이 강화되었다. 그 대신 미국 국익을 손상시키는 과도한 해외 개입을 자제하고 중요 지역의 세력균형만 유지하자는 역외세력균형론(offshore balancing)에 대한 관심과 지지가 증가하였다 (Mearsheimer and Walt 2016).

이러한 탈냉전기 미국 대외전략을 둘러싼 논쟁 속에서 미국의 사이버 취약성에 대한 우려와 경고는 꾸준히 증가하였다. 2012년 10월 리언 파네타 국방장관은 “사이버 진주만 공격”에 대해 경고하였다 (박현 2012). 경제제재에 대한 보복으로 이란이 미국에 대규모 사이버 공격을 감행하리라는 우려 속에 나온 발언이었다. 비록 미국이 최고의 사이버 역량을 갖추었다고 하더라도 자국을 보호해줄 거대한 바다를 사이버 공간에서 창조하지는 못한다. 이러한 문제의식 속에 미국은 사이버 억지와 통합 억지와 관련한 개념과 전략을 꾸준히 발전시켰다. 최근 바이든 행정부는 민간 기업 및 유사 국가와 더불어 디지털 생태계 전략을 발표하면서 사이버 질서를 구축할 의지와 계획을 선보였다.

향후 미국은 사이버 안보를 확보할 다양한 전략을 적극적으로 구사할 것이다. 글로벌 리더십과 해외 개입에 대한 비판 여론에도 불구하고 사이버 취약성을 방취할 경우 미국의 핵심 국익을 보호할 방안은 찾기 힘들기 때문이다. 이러한 상황 속에서 현재 한미 양국은 사이버 협력을 중심으로 글로벌·포괄적 동맹 변환을 추진 중이다. 물리적 공간과 사이버 공간을 연계하여 다영역

위협에 대처하는 복합 동맹의 필요성을 양국 정부가 공감한 결과이다. 사이버 안보는 국가 뿐 아니라 기업과 민간이 모두 참여해야 하며 민주국가 간 양자·소다자·다자 협력이 활성화되고 있다는 점을 고려할 때 한미 사이버 동맹은 아직 초기라고 평가할 수 있다. 디지털 시대의 도래에 따른 위기와 도전에 대한 종합적 이해를 바탕으로 한국 정부가 대외전략의 목표와 방안을 구체화하는 것이 중요한 시점이다.

Ⅱ. 단극체제의 등장과 사이버 안보

냉전의 종식은 곧 미국의 승리이자 '역사의 종언'이라는 인식을 확산시켰다. 하지만 9-11테러는 미국이 맞설 새로운 현실을 일깨워졌다. 더 이상 지리적 이점에 안주할 수 없는 시대인 것이다. 당시 미국의 대응은 테러와의 전쟁이었다. 하지만 비국가 행위자를 적대하는 전쟁은 애당초 여러 문제를 안고 있었다. 영토와 국민이 없는 테러집단을 어디에서 찾을 수 있으며, 전쟁에서의 승리를 무엇으로 확정할 수 있는지, 테러리스트와 민간인을 어떻게 구별하며 차별할 수 있는지와 관련된 이슈가 줄기차게 제기되었다. 전통적 전쟁에서 발생한 규범과 원칙을 새로운 전쟁에서 적용할 수 있는지, 비정규전을 정의롭게 수행하고 종결할 기준과 방안이 무엇인지 다수의 국제윤리 전문가는 토론하기 시작하였다. 소련 붕괴 이후 초강대국 미국에 대항하는 강대국 연합이 부상할지를 둘러싼 논쟁은 자취를 감추었다.

하지만 비국가 행위자는 미국이 마주할 새로운 도전의 일부였다. 1990년대부터 시작된 인터넷은 빠른 속도로 가상 공간의 영향력을 강화시켰다. 사이버에서 물리적 거리는 무의미했다. 해양국가 미국이 오랫동안 누려온 지리적 이점을 사이버에서 찾아볼 수 없었다. 과학기술이 교통·통신 시설을 통해 강대국의 해외 투사력을 강화시켰다면, 가상공간은 지정학의 위상과 지리의 힘을 약화시켰다. 대서양과 태평양 덕분에 유럽·아시아 분쟁과 거리를 두기도 했던 미국에게 사이버는 낯설고 위험한 공간이었다. 9-11 테러 이후 미국은 비국가 행위자의 위협에 맞서서 국경감시와 통제를 강화하거나 (잠재적) 공격자들을 색출하고 제거하는 전략을 추진했다. 하지만 사이버 적대행위와 관련해서는 이러한 전략의 효율성은 떨어지기에 사이버 공간에 적절한 새로운 개념과 전략의 필요성이 꾸준히 제기되었다 (Craig and Valeriano 2018).

그동안 물리적 공간에서 (1) 세력균형·(2) 상호의존·(3) 수비우위는 무력 충돌을 억지하는 요인으로 주목받았다. 하지만 아래에서 서술하듯이 이들의 영향력은 사이버 공간에서 현저히 제한적이라고 평가받고 있다.

첫째, 사이버 공간에서 세력균형에 따른 상호 억지가 발생하기 어렵다. 사이버 공격을 받은 경우 그 공격자를 바로 파악하는 것이 어렵다. 국가가 해외 거점을 사용했다거나 민간단체에 의뢰하여 사이버 공격을 감행했다면 공격자 색출과 책임 추궁은 더욱 어려워진다. 따라서 사이버 보복이 두려워 사이버 공격을 자제하리라고 예상하는 이들이 많지 않다. 하지만 사이버 공격에 대해 물리적 공간에서 응징하거나 물리적 공격에 대해 사이버 공간에서 응수하는 사례는 늘어나고 있다. 미국 정부는 2014년 소니픽처스 해킹사건을 감행한 북한 해커를 기소하고 그와 그의 회사를 제재 명단에 포함시켰다 (강영두 2018). 이란은 미국이 자국의 혁명수비대 사령관을 제거하자 그에 대한 보복으로 미 연방정부기관 웹사이트에 대한 사이버 공격을 감행한 바 있다 (하채림 2020). 사이버의 등장은 물리적 공간의 세력균형마저 불안하게 만들고 있다.

둘째, 사이버 공간에서 상호의존에 따른 국제협력을 관찰하기 어렵다. 앞서 언급한 것처럼 수

많은 국가와 비국가 행위자가 활동하는 사이버에서 장기적 이익을 기대하며 상호 협력을 결정하는 메커니즘이 작동하기 어렵다. 다수의 해킹 그룹과 관련 조직은 자신의 정치적·경제적 목적을 달성하기 위해 불법 수단마저 적극적으로 활용한다. 이러한 행위자를 대상으로 일반 국가가 상대 이익이 아니라 절대 이익을 추구하며 안정적 협력관계를 구축하는 것은 사실상 불가능하다. 국가와 민간의 협력이 국제정치에서 빈번해지고 있지만 이는 민간이 속한 국가와 다른 국가 간 우호적 관계를 기초로 이루어지고 있다. 러시아가 우크라이나를 침공하자 미국의 주요 IT기업들이 우크라이나를 지원했던 최근의 사례를 대표적으로 생각해볼 수 있다. 아직까지 서로에 대한 의존관계를 바탕으로 장기적 관점에서 협력을 선호하는 행위는 사이버에서 일반적이지 않다.

셋째, 사이버에서 공격보다 수비 우위를 믿는 행위자는 찾기 어렵다. 사이버 공간에서 모든 행위자는 공격이 최선의 수비라고 믿는 경향이 강하다. 과학기술의 발달과 지정학 이점으로 수비가 손쉬운 행위자는 공격 감행을 자제한다. 누구도 정복할 수 없는 철옹성을 쌓은 군주, 엄청난 대양에 둘러싸인 해양 국가, 모든 미사일을 감지하고 요격하는 방어체제를 구축한 미래 국가 등이 바로 수비 우위를 누리는 행위자이다. 이들 사이에서 충돌과 전쟁은 제한적일 수밖에 없다. 그러나 사이버에서 자국 시스템과 인프라를 완벽히 보호할 수 없다는 생각이 정설이다. 따라서 대다수 국가는 '선제적' 대응을 강조하며 공격 우위의 현실에 적응한다. 미국이 내세우는 '선제적 방어'는 감시와 추적에 기반하여 즉각적이고 충분한 보복을 미리 준비한다는 점에서 전통적 의미의 방어와는 차별성을 지닌다.

위와 같은 사이버의 특징은 단극체제의 정점에 올라선 미국에게 새로운 도전을 야기했다. 압도적 군사력으로 상대를 억지할 수 없으며, 막대한 경제력으로 상대를 의존망에 유인할 수 없고, 공격 의사가 없음을 천명하며 상대를 안심시키는 전략도 무용하다. 과거에는 잠재적 위협으로부터 대서양과 태평양이 보호해 주었지만 사이버 공간에서 그러한 방패는 존재하지 않는다. 다수의 전문가가 9-11 테러를 비국가 행위자의 위협에 초점을 맞추었지만 그러한 행위자들이 가상 공간을 자유롭고 효율적으로 활용한다는 점이 새로운 도전의 핵심이었다. 사이버 공간은 그들에게 정보와 영향력을 제공하면서 물리적 공간의 영향력을 제한하면서 상이한 공간을 매개하는 역할을 감당하였다. 사이버의 등장은 공간 개념과 대외 전략의 변화를 불가피하게 만들었다.

오랫동안 미국 대외전략을 둘러싼 논쟁은 현실주의와 자유주의 전통을 배경으로 진행되었다. 최근 수년 현실주의 학자들은 탈냉전기 미국대외전략에 대한 거센 비판을 제기하였다. 자유주의 "망상"으로 나토 팽창과 이라크 전쟁을 수행한 결과 미국은 쇠락을 맞이했다는 지적이다 (Mearsheimer 2018; Walt 2018). 이러한 현실주의 비판자들은 세력균형론에 입각한 자제(restraint)를 강조한다. 과도하고 무차별적 개입이 아니라 주요 지역에 대한 선별적 개입을 통해 국력 낭비를 막고 반미주의를 약화시킬 것을 제안한다. 그동안 유럽·중동·아시아 지역에 지속적으로 개입했다면, 이제 아시아에 집중하면서 유럽과 중동과 일정한 거리를 두면서 필요할 경우 해당 지역 동맹을 활용할 것을 제안한다. 세계를 미국화하겠다는 야심, 글로벌 패권국에 등극하겠다는 목표를 버릴 것을 역설한다.

그러나 이러한 현실주의 전략은 가상 공간이 몰고 온 새로운 도전에 눈을 가리고 있다. 더 이상 미국이 "대양의 억제력"(stopping power of war)을 활용해 아시아·유럽·중동의 분쟁과 거리를 둔 채 선별적 개입만 가능한 시대가 아니다 (Kaginele 2024.). 미국의 상당한 국부는 자국 빅테크 기업의 사이버 활동에서 창출되고 있으며, 미국의 핵심 인프라와 주요 시설에 대한 사이버 공격 위협은 증대했으며, 미국 주도 질서에 반기를 든 세력은 사이버 활동을 통하여 역량을 급속도로 강화하고 있다. 사이버의 등장으로 서반구 패권국으로 다른 지역의 세력균형을 도모하는 역외 균형자 전략의 실효성은 줄어들었다. 미국의 적대 세력이 사이버를 활용해 심리전과 국

내개입을 시도하는 현실 속에서 아시아와 유럽에서 무조건 발을 빼야한다는 주장에 동조하는 이들은 줄어들 수밖에 없다.

Ⅲ. 단극체제의 위기와 사이버 동맹

1. 강대국 경쟁과 사이버 분쟁

탈냉전기 사이버 공격의 증가에 대응하여 미국의 대외전략은 지속적으로 변화했다. 아래 [표1]에서 정리한 바와 같이, 클린턴 행정부 시기 사이버 공간이 부상하자 사이버 보안과 사이버 공격은 주요 이슈로 부상하면서 경각심을 불러 일으켰다. 부시 행정부에 들어서 최초의 사이버 전략이 문건으로 발표되자 사이버 안보는 국가안보의 핵심 의제로 자리 잡았다. 오바마 행정부는 사이버 문제를 둘러싼 국가와 민간, 국가와 국가 사이의 다양한 협력을 강조하기 시작했으며, 트럼프 행정부는 사이버 안보의 대상을 미국 전체로 확장하면서 사이버 공격이 미국인의 생활방식 자체를 위협한다는 인식을 확산시켰다. 2023년 바이든 행정부는 〈국가사이버안보전략〉을 발표하면서 주요기반시설에 대한 보호 및 신기술 도래에 대한 대응에 있어서 국제협력의 필요성을 강조하였다.

시기	핵심 문건	주요 특징
클린턴 행정부 1·2기 (1993.1-2001.1)	• 〈국가 정보기간시설 보호법〉(1996) • 대통령지시 63호(1998)	• 사이버공격에 대한 취약성 인지 • 사이버보안을 국가 중요 정책으로 규정
부시 행정부 1·2기 (2001.2-2009.1)	• 〈사이버공간의 안전을 위한 국가전략〉(2003)	• 사이버보안이 사이버안보라는 국가 안보문제로 격상 • 사이버억지 개념의 등장
오바마 행정부 1·2기 (2009.1-2017.1)	• 〈국가사이버안보종합이니셔티브〉(2009) • 〈사이버공간 국제전략〉(2011) • 〈국방사이버전략〉(2015)	• 정부와 민간의 정보공유 법적 근거 • 사이버안보 보호대상에 지적재산권 포함 • 사이버 관련 국제협력 중요성
트럼프 행정부 (2017.1-2021.1)	• 〈국가사이버전략〉(2018) • 〈사이버국방전략〉(2018)	• 사이버안보의 대상 확대(미국인, 미국 사회, 생활방식) • 사이버 위협에 대한 공격적 대응
바이든 행정부 (2021.1-현재)	• 〈국가사이버안보전략〉(2023)	• 주요기반시설 보호 체계 강화 • 위협국가에 대응하기 위한 국제협력 강조 • 신기술 도래에 따른 대응 마련

[표1] 탈냉전기 미국의 사이버안보 전략

출처: 오일석·조은정 (2022: 15[표1]); 변진석 (2022: 45-55); 김소정 (2023)

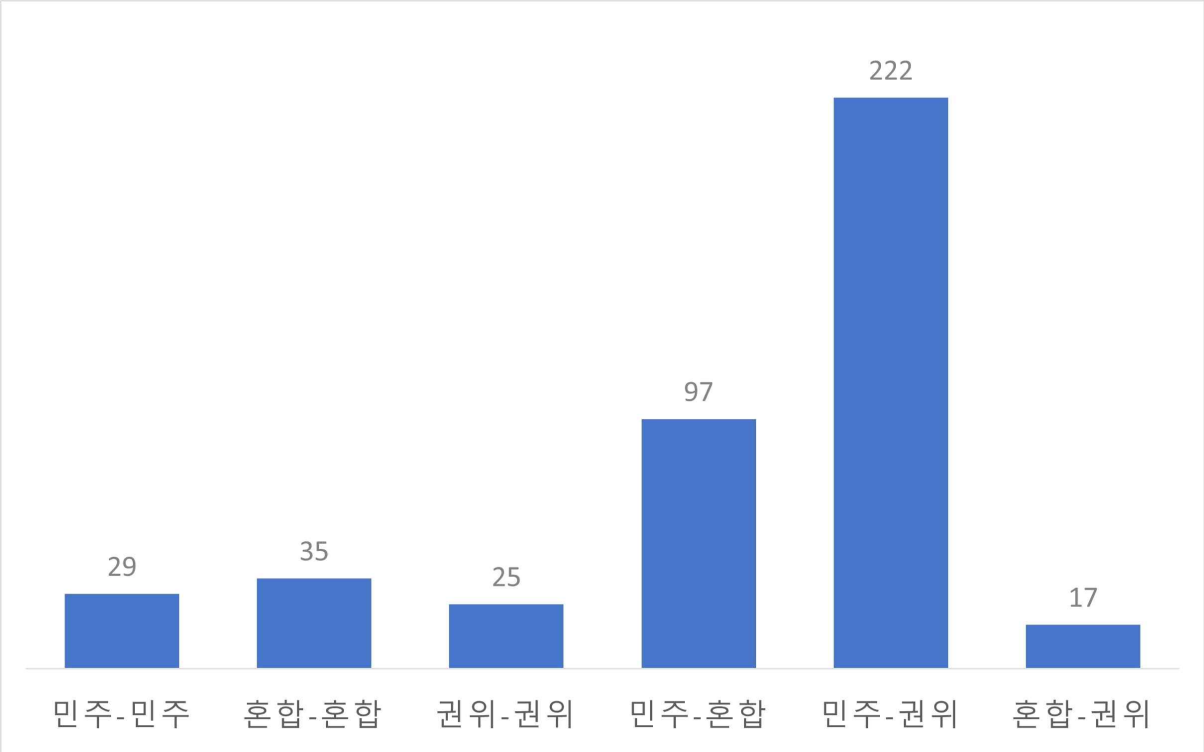
이러한 미국의 사이버 안보전략은 육·해·공·우주 물리적 공간을 연계하는 사이버의 특성을 반영한다. 상이한 물리적 공간을 매개하는 사이버는 독립 공간이자 연결 통로의 기능을 담당한다. 사이버 공격은 사이버 시설을 마비시키거나 주요 정보를 훔치는 것을 목표로 할 뿐 아니라 물리적 공간에서의 피해와 비용을 초래하고자 자주 감행된다. 대표적으로 2010년 미국과 이스라엘이 스턱스넷(Stuxnet) 바이러스 침투를 통해 이란의 핵시설을 공격한 사례가 있다. 과거 이스라엘은 이라크의 핵개발을 저지하기 위해 오시라크 원자로를 폭격했지만, 21세기 미국과 이스라엘은 사이버 공격으로 이란 원심분리기 약 20%를 파괴할 수 있었다 (Nacht, Schuster, and Uribe 2019.: 33). 한편, 최근 북한은 핵·미사일 개발자금을 마련하기 위해 사이버 화폐를 갈취하거나 불법적으로 획득했다고 알려졌다. 물리적 위협을 제한하고자 경제 제재를 가하고 있지만 그러한 국제사회의 노력을 무력화할 수 있는 방안이 사이버 공간에서 강구되고 있다.

그동안 미국의 사이버 전략의 핵심은 억지(deterrence)였다. 전통적인 세력균형 아이디어를 바탕으로 상대의 공격을 사전에 차단하는 목표를 지향했다. 하지만 앞 절에서 설명한 바와 같이 공격자를 식별하기 어렵고 공격 역량과 수비 역량의 구분이 모호한 상황에서 사이버 안보 딜레마는 상수가 되버렸다. 사이버에서 수비에 치중할 경우 불리하다는 인식이 일반적이다. 그동안 사이버 억지를 지속적으로 추구했지만 트럼프 행정부는 본격적으로 '선제적 방어'(defend forward) 개념을 도입했다 (변진석 2022: 63-64). 적대세력의 공격을 선제적으로 차단하고 필요한 경우 군사력을 동원해 보복할 수 있다는 적극적 전략이었다. 군사·경제·사회 위협을 야기하는 사이버 공격에 적극적으로 대응해야 한다는 인식의 반영이었다. 테러와의 전쟁에서 전투원과 민간인 구분이 어려웠다면, 사이버전에서 적군 자체가 보이지 않기에 공격과 방어 전략의 경계가 모호해진 것이다.

이러한 사이버 안보전략의 변화는 강대국이 주도하는 「민주주의 대 권위주의」 구도를 배경으로 한다. 2010년대 들어서 중국의 공세적 외교를 둘러싼 미국과 주변국의 우려를 고조시키면서 새로운 냉전을 전망하는 목소리가 커져왔다. 대다수는 이러한 두 집단의 충돌이 인도태평양, 특히 대만과 남중국해에서 발발할 가능성이 높다고 예상한다. 하지만 민주주의와 권위주의 간 사이버 충돌은 이미 현실이다. 「The Dyadic Cyber Incident Dataset v2.0」에 따르면 2000년부터 2021년까지 양국 간 사이버 충돌은 총 425건이다 (Valeriano 2022). 정치체제를 민주주의, 혼합체제, 권위주의로 나눌 때,[1] 민주주의-민주주의 분쟁과 권위주의-권위주의 분쟁의 각각 29회(6.82%)와 25회(5.88%)에 불과한 반면, 민주주의-권위주의 분쟁과 민주주의-혼합체제 분쟁은 각각 222회(52.24%), 97회(22.82%)에 이른다([그림1] 참조).[2] 전체 사이버 분쟁 중 상이한 정치체제 간 발생한 비율이 79.06%(336건)에 이른다.

1) Polity V 데이터의 Polity2 변수를 활용하여 6점 이상일 경우 민주주의, -6점 이하일 경우 권위주의, 그 밖의 경우는 혼합체제로 측정한다.

2) 민주-민주(6.82%); 혼합-혼합(8.24%); 권위-권위(5.88%); 민주-혼합(22.82%); 민주-권위(52.24%); 혼합-권위(4.00%)



[그림1] 사이버 분쟁과 정치체제, 2000-2021
출처: 정성철 (2024: 357[그림 11.1])

이러한 사이버 분쟁은 한정된 국가 사이에서 발생하는 특징을 보인다. 앞선 언급한 총 425건의 사이버 분쟁은 31개국 사이에서만 일어났다.[3] 사이버 분쟁을 20회 이상 겪은 양자는 미국-중국(63회), 미국-러시아(47회), 한국-북한(38회), 미국-이란(30회), 우크라이나-러시아(30회), 이스라엘-이란(28회), 인도-파키스탄(24회), 미국-북한(20회)으로 제한된다. 인도태평양에서 갈등 중인 미국과 중국, 혹은 그 동맹과 우방들이 대다수 사이버 분쟁의 당사국인 셈이다. 따라서 사이버 안보를 증진하고 사이버 규범을 확립할 때 인도태평양의 안정적 질서을 수립하는 것이 가능할 수 있다. 반대로 사이버가 불안한 상황에서 인도태평양의 안정을 달성하는 것은 어려워질 수밖에 없다. 사이버 영역에서 미국은 중국, 러시아, 북한, 이란 등과 같은 물리적 공간의 주요 라이벌과 충돌을 이어가고 있다.

미국의 사이버 적대세력은 디지털 권위주의를 주도하며 미국의 사이버 전략에 영향을 주고 있다. 21세기 미국의 새로운 위협은 사이버 중심의 다영역망의 형태 속에서 전개되고 있다. 이러한 위협의 핵심 주체는 중국과 러시아를 중심으로 하는 권위주의 국가이다. 비록 미국이 사이버를 비롯한 주요 영역에서 앞선 기술을 보유했다 할지라도, 공격 우위라는 사이버의 특성과 개방적이고 투명한 민주주의 제도는 미국의 사이버 취약성을 부각시키고 있다. 이러한 비대칭적 위협에 대한 미국의 우려와 고민은 핵심 물자의 공급망을 재편할 뿐 아니라 인터넷망의 분리에 대한 논의를 촉발시켰다. 이는 20세기 중후반부터 급속히 진행된 세계화의 중단 혹은 재편을 의미하는 것으로 상호의존망의 약화를 가져올 것으로 예상된다. 세계가 더 이상 하나의 마을을 지향하

3) 참고로 Correlates of War 프로젝트의 Militarized Interstate Disputes 4.02 Dataset에 따르면 2000년부터 2014년까지 총 142개국이 무력분쟁을 경험하였다.

지 않은 채 일정한 거리두기에 나선 것이다.

2. 통합 억지와 디지털 생태계

2000년대부터 미국은 '다영역 억지'(cross-domain deterrence) 혹은 '통합억지'(integrated deterrence)의 틀 속에서 사이버 억지를 추구하였다. 바이든 행정부의 안보전략의 핵심 개념인 통합 억지는 세 가지 수준의 통합 - (1) 모든 영역(육·해·공·우주·사이버 등), (2) 모든 수단(군사·비군사), (3) 미국과 동맹, 파트너의 역량 - 을 지향한다 (설인효 2022: 279-285). 이는 국가안보를 위해 국방·경제·외교 등의 총체적 노력을 우방과 함께 기울이는 전략으로 확장된 안보개념을 바탕에 둔다. 안보를 "획득한 가치에 대한 위협의 부재"라고 정의했을 때 (Wolfers 1952: 485), 그 위협의 근원이 다양해진 것이다. 근대국가가 영토국가(territorial state)일 때는 군사적 위협과 정복이 핵심 위협이었다. 하지만 근대국가가 무역국가(trading state)로 전환된 이후 경제적 위협이 부상하였다. 무역과 투자로 상호의존망이 형성되었지만 비대칭 관계 속에서 제재와 반제재는 더욱 활성화되었다. 이러한 경제 갈등의 이면에는 기술혁신이 자리 잡고 있다. 세계 선도국이 결국 앞선 기술을 바탕으로 핵심 영역을 차지했기 때문이다.

한편, 바이든 행정부는 중국과의 경쟁 속에서 각 영역에서 (소)다자주의를 활용하여 사이버 협력을 강화한다. 그동안 아시아와 유럽의 양자·다자 군사동맹 뿐 아니라 오커스(미국-영국-호주)와 쿼드(미국-일본-호주-인도)를 (재)가동한 바 있다. 인도태평양프레임워크는 오바마 행정부가 추구한 환태평양경제협력기구(TPP)를 대체하는 미국 주도 경제망의 핵심으로 부상 중이다. 중국을 배제한 반도체 공급망 건설을 위해 미국은 한국·대만·일본·네덜란드 등과 긴밀한 협력을 시작하여 일정한 성과를 내고 있다. 기존 파이브아이즈를 강화할 뿐 아니라 한국, 일본, 독일 등을 포함한 확대된 정보동맹에 대한 논의도 지속적으로 진행되고 있다. 최근 수 년 동안 돈독해진 한미일 삼각협력은 다영역 협력을 기반으로 자유주의 네트워크의 중심으로 기능하리라 기대를 받는다. 이러한 미국이 주도하고 참여하는 (소)다자협력에서 사이버와 인터넷, 핵심기술과 공급망은 핵심 의제로 협력의 핵심으로 기능한다.

최근 바이든 행정부의 사이버 국가전략은 디지털 생태계 건설에 초점을 맞추고 있다. 방어할 수 있고 회복력 있는 디지털 생태계를 동맹과 우방과 더불어 건설한다는 '사이버안보 국가전략'(미국 백악관)이 발표된 이후 '미국 국제 사이버공간·디지털 정책 전략'(US International Cyberspace & Digital Policy Strategy)이 공개되었다. 트럼프 행정부의 사이버 국가전략과 마찬가지로 사이버 위협의 증가를 언급하면서 동맹·우방·민간·기업과의 협력, 사이버 규범과 국제법의 중요성을 강조한다. 다만 사이버 억지에서 디지털 생태계로 초점을 옮기고 있다. 2018년 사이버 국가전략에서 24회 등장한 용어 억지(deter 혹은 deterrence)는 2023년 사이버안보 국가전략에서 자취를 감추었다. 그 대신 디지털 생태계라는 용어가 새로이 등장하였다 ([표2] 참조). 2022년 조셉 나이는 사이버 아나키의 종식을 위한 디지털 규범의 창출을 강조한 바 있다 (Nye 2022). 이에 대한 바이든 행정부의 호응이 바로 디지털 생태계 전략으로 볼 수 있다.

	2018년 사이버 국가전략 (National Cyber Strategy)	2023년 사이버안보 국가전략 (National Cybersecurity Strategy)
위협 (threat)	37	57
권위주의 (authoritarian or authoritarianism)	3	3
규범 (norm or normative)	6	10
규칙 (rule)	0	9
법 (law)	21	30
동맹 (allies, allied, or alliances)	10	28
우방 (partner[s])	35	70
억지 (deter or deterrence)	24	0
생태계 (ecosystem)	3	44
디지털 생태계 (digital ecosystem)	0	39

[표2] 2018년과 2023년 사이버 국가전략의 핵심어 사용
(단위: 회)

디지털 생태계의 구체적 모습은 무엇일까? 미국 국제개발처(USAID)에 따르면 디지털 생태계는 세 기둥 - (1) 디지털 인프라와 수용, (2) 디지털 사회·권위·거버넌스, (3) 디지털 경제 - 으로 구성되면서 네 가지 주제 - (1) 포용(inclusion), (2) 사이버안보, (3) 신흥 기술, (4) 지정학 위상(positioning) - 를 포괄한다 (USAID 2022). 달리 말하면, 안보와 번영을 추구하는 정치·사회·경제 생태계라고 이해할 수 있다. 현재 미국과 중국 사이에서 벌어지는 다영역 경쟁 뿐 아니라 개인·집단·국가 간 불평등과 이들 간 협력의 문제도 디지털 생태계의 주요 이슈로 다룰 수 있다. 이러한 점에서 디지털 생태계는 다양한 이해당사자가 정치·군사·경제·사회·문화 전반에 걸친 영향을 사이버에서 주고받는 현실을 충실히 반영한 개념으로 이해할 수 있다.

그렇다면 미국이 추진하는 디지털 생태계의 주요 동반자는 누구인가? 다양한 민간과 기업과 더불어 민주국가와 사이버 연대를 확장하려는 노력이 진행 중이다. 특히 사이버 역량을 갖춘 민주국가는 미국이 추진하는 사이버 동맹의 핵심 구성원이다. 현재 사이버 역량을 갖춘 국가 간 협력은 양자·소다자·다자 형태로 급속히 강화되고 있다. 미국이 주도하는 국제 협력체에서 사이버, 인터넷, 기술혁신은 핵심 이슈이다. 유럽연합의 경우도 디지털 파트너십을 2022년부터 일본, 한국, 싱가포르, 캐나다 등과 체결하면서 사이버 협력의 외연을 확장하고 있다. 이러한 사이버 협력의 특징은 이념과 역량이 상대적으로 유사한 국가 사이에서 발생한다는 점이다. 아래 [표3]

는 사이버 역량 상위20개국을 정리한 것이다. 미국을 포함하여 총 17개국은 나토의 사이버방위센터(CCDCOE)에 참여하고 있다. 2007년 러시아의 에스토니아 사이버 공격 이후 출범한 사이버방위센터는 세계 최대 규모의 사이버방위훈련 등을 실시하는 안보협력체로 대한민국도 2022년 정회원으로 가입하였다. 미국이 주도하는 소다자협력체인 쿼드, 오커스, 한미일 협력국은 모두 사이버 강국이다.

과거 군사협력은 역량의 비대칭성에도 불구하고 발생했다면, 현재 사이버 협력은 역량의 대칭성을 전제로 일어난다. 안보-자율성 교환모델은 지리적 요충지를 차지하는 약소국이 군사와 경제 역량을 보유한 강대국과 동맹을 형성하는 사례를 설명하였다. 주권국가의 자율성을 일부 양보하면서 비강대국은 자국의 안보를 위해 강대국의 도움을 받을 수 있었다 (Morrow 1991). 하지만 비대칭적 안보협력은 사이버 공간에서 드물게 발생한다. 그 대신 선진국 간 역량결집의 형태로 국제 연대가 빈번하게 이루어지고 있다 (정성철 2024: 366-367). 최근 사이버 역량을 갖추지 못한 국가는 다양한 형태로 부상하는 (소)다자협력에서 일정 부분 배제되고 있다. 에너지 전환과 반도체 생산과 관련되어 주목받고 있는 광물 생산지인 일부 국가만이 선진국의 주목을 받고 있는 상황이다.

		나토 사이버방위 센터(CCDCOE)	EU 디지털 파트너십	쿼드	오커스	한미일
1	미국	○		○	○	○
2	중국					
3	러시아					
4	영국	○			○	
5	호주	○		○	○	
6	네덜란드	○				
7	베트남					
8	한국	○	○			○
9	프랑스	○				
10	이란					
11	독일	○				
12	우크라이나	○				
13	캐나다	○	○			
14	북한					
15	스페인	○				
16	일본	○	○	○		○
17	싱가포르		○			
18	뉴질랜드					
19	이스라엘					
20	스웨덴	○				
21	사우디아라비아					
22	스위스	○				
23	터키	○				
24	이집트					
25	에스토니아	○				
26	인도			○		
27	이탈리아	○				
28	말레이시아					
29	리투아니아	○				
30	브라질					
	합	17	3	4	3	3

[표3] 사이버 역량 상위 20개국

출처: Voo, Hemani, and Cassidy (2022)

현재 미국과 중국이 주도하는 「민주주의 대 권위주의」 구도는 유사국가가 국가군을 이루면서 발생하고 있다. 미국이 주도하는 자유주의 연대망은 유사한 이념 뿐 아니라 뛰어난 역량을 갖춘 국가들 사이에서 다각도로 강화된다는 특징을 보인다. 흔히 미국의 대중국 압박정책을 인도태평

양전략으로 치환하고 있지만, 이러한 인도태평양전략이 미국과 아시아 국가 간 연대에 제한되지 않는 이유는 사이버를 중심으로 펼쳐지는 다영역 연계 때문이다. 가상공간을 통해 물리적 공간에서 심대한 피해를 입힐 수 있고, 주요 국가의 국부가 사이버를 통한 경제활동에 뿌리를 두고 있으며, 세계인의 개인정보와 주요 핵심기술이 가상공간에 저장되는 상황에서 미중 경쟁에 전세계 국가 및 비국가 행위자가 휘말릴 수밖에 없는 상황이다.

Ⅳ. 한미 사이버 협력: 지정학 동맹에서 포괄적 동맹으로

한미동맹 70주년을 맞이한 정상회담에서 양국 정상은 2023년 4월 26일 글로벌 포괄적 전략동맹의 구축을 재천명하였다. 한국 대통령실과 미국 백악관은 “한미 정상 공동성명” 이외 “워싱턴 선언”, “차세대 핵심신흥기술 대화 공동성명”, “전략적 사이버안보 협력 프레임워크”, “한국전 명예훈장 수여자의 신원확인에 관한 공동성명”을 발표하였다. 정상회담 브리핑에서 국가안보실은 양국의 가치동맹 주춧돌 위에 다섯 기둥 - 안보동맹, 경제동맹, 기술동맹, 문화동맹, 정보동맹 - 이 자리 잡았다고 발표하였다. 이 다섯 기둥은 한반도에 국한되지 않고 인도태평양 전역에 걸친 긴밀한 협력을 상징한다.

이처럼 한미동맹 70주년을 기념하면서 양국은 한미 동맹을 “인도태평양 지역의 평화와 번영의 핵심축”으로 규정하였다. 북대서양조약기구, G7, 민주주의 정상회의, 오커스에 대한 언급과 더불어 양국은 러시아의 우크라이나 침략을 규탄하며 북한문제 해결에 대한 의지를 밝힘과 동시에 인도태평양 전역에서의 협력 확대를 천명했다. 대만해협의 평화와 안정을 강조하고 일방적 현상변경에 대한 강력한 반대를 표명한 양국은 중국과 러시아의 위협, 즉 권위주의 부상에 대한 우려와 경계를 공유하고 있다. 미국은 아시아태평양에서 인도태평양으로 초점을 옮긴 후 본격적인 인도태평양 전략을 수립하여 실행에 옮기고 있다. 작년 말 인도태평양 전략을 발표한 한국 역시 미국이 주도하는 국제질서 수호에 적극 동참한 것이다.

한미 글로벌·포괄적 동맹과 한미일 삼각협력의 핵심에 사이버 협력이 존재한다. 한미 양국은 정상회담문과 사이버안보협력 프레임워크에서 북한문제를 포함한 안보문제에서 사이버의 중요성에 인식을 함께 했다. 지난 한미일 캠프데이비드 정상회의 이후 삼국은 지난 11월 삼국 간 고위급 사이버 협의체 신설 계획을 발표하였다 (곽민서 2023). 이는 한국, 미국, 일본 모두 동아시아와 인도태평양의 안정에 있어서 사이버 공격을 억지하고 사이버 범죄를 예방해야 할 필요성에 합의하고 있음을 보여준다. 현재 주목받는 이슈는 북한의 사이버 범죄를 통한 자금 확보이다. 북한 비핵화를 위한 노력의 일환으로 대북제재를 지속하지만, 북한의 사이버 활동으로 물리적 공간의 제재가 무력화된다는 우려가 커진 것이다. 사이버 협력 없이 더 이상 공동 안보의 달성이 어려운 것이 현실이다.

향후 한미 동맹은 양국 간 사이버 협력의 토대 위에 성장할 것이다. 민주주의의 권위주위 위협론 기저에는 ‘민주주의 후퇴’(democratic backsliding)라는 전세계적 현상이 존재한다. 2000년대부터 유럽과 남미, 아시아 전역에 걸쳐 다수 민주국가들은 포퓰리즘과 선거부정, 코로나19와 국가주의를 경험하면서 권위주의화를 경험했다 ([그림3] 참조). 이는 중국과 러시아의 부상, 특히 이들 국가들의 디지털 기술을 활용한 국내통제와 해외개입을 우려하는 목소리와 맞물려 ‘민주주의 수호’의 필요성을 부각시키고 있다 (Ikenberry 2020). 한국과 미국이 자유와 인권에 대한 가치 존중을 함께 강조할수록 양국이 수행하는 사이버 협력의 무게는 커질 수밖에 없다. 사

이버 규칙기반질서가 부재한 상황에서 민주주의의 온전한 지속은 불가능한 시대를 살아가고 있기 때문이다.

한미 사이버 협력은 군사 동맹에서 포괄적 동맹을 대표한다. 양극체제가 부상하는 상황에서 한국전쟁은 한국과 미국이 비대칭 군사동맹을 맺도록 이끌었다. 냉전이 종식된 이후에도 북한의 핵개발은 한미 양국이 군사동맹을 유지하며 안보 협력을 유지하는 공동위협으로 작동하였다. 더불어 한국의 민주주의와 경제성장은 '민주주의 대 권위주의' 구도 속에서 한미 양국이 역량과 이념을 바탕으로 포괄적 동맹을 키워나가는 원천이 되고 있다. 지정학을 기초로 한 군사동맹을 유지하는 단계에서 벗어나 군사·경제·기술·사회 전반에 걸쳐 공동안보를 추구하는 수준으로 거듭나고 있다. 양국의 지도부와 시민사회 모두 한미 동맹을 지정학을 넘어선 복합(지정학과 비지정학) 동맹이라는 인식을 바탕으로 협력의 수준과 범위를 확장시키는 작업이 한층 필요한 시점이다.

Benin	Ethiopia	Mali	Serbia
Bolivia	Fiji	Montenegro	Tanzania
Brazil	Georgia	Myanmar	Thailand
Burkina Faso	Guatemala	Nicaragua	Tunisia
Comoros	Hungary	Nigeria	Turkey
El Salvador	India	Philippines	United States
Egypt	Madagascar	Poland	

[그림3] 2005년 이후 민주주의 후퇴국
출처: Carothers and Press (2022: 5[Figure 1]

Ⅴ. 나가는 글

글로벌 팬데믹 이후 국제적 거리두기는 본격화되었다. 바이든 행정부는 중국 때리기 혹은 미중 디커플링이 아니라 민주주의와 권위주의 세력 간 거리두기를 주도하고 있다. 모든 영역에서

양분된 세계를 추구하지 않기에 신냉전을 추구한다고 평가할 수 없으나, 선진 산업과 첨단 기술에서 중국과 러시아를 배제하는 전략은 미국의 관여정책이 종말을 고했음을 보여준다. 이렇듯 권위주의와의 거리두기는 양극화로 몸살을 앓고 있는 미국 사회 전체가 합의할 수 있는 전략의 하나로 당분간 지속되리라 예상된다. 분명 이슬람과 이주자, 자유주의 국제질서와 유럽-인태의 연계에 대한 민주당과 공화당의 입장차는 존재하지만, 권위주의 세력으로부터 안전하고 회복력있는 미국을 건설해야 한다는 공동의 목표 의식은 분명하다.

이러한 차원에서 미국이 향후 사이버 봉쇄를 주도할 가능성이 있다. 지리적 이점과 수비 우위가 부재한 사이버에서 미국이 권위주의 세력에 대한 봉쇄를 택할 유인은 한층 커졌다. 과거 인터넷이 정보 투입과 공유의 주요 통로로 작동하리라는 믿음 속에서 장밋빛 미래를 예견했다면, 이제 우리 경제와 사회를 보호해야 한다는 위기 의식이 민주국가 사이에서 널리 존재한다. 한국 역시 이러한 사이버 취약성을 최소화할 수 있는 인프라와 정치·경제·사회를 구축하기 위해 민간 및 동맹과 더불어 디지털 생태계 구축에 적극적으로 나설 때이다. 사이버 아나키에서 우리의 일상과 안전은 위협받을 수밖에 없기 때문이다.

<참고문헌>

강영두. 2018. “美, 北사이버공격 첫 제재…소니픽처스 해킹 등 北해커 기소,” 『연합뉴스』(9월 7일). https://www.yna.co.kr/view/AKR20180906184451071?input=1195m (검색일: 2024/5/10).

곽민서. 2023. “한미일 고위급 사이버 협의체 신설...북 사이버활동 차단,”『연합뉴스』(11월 6일). yna.co.kr/view/AKR20231106061900001 (검색일: 2024/7/12).

권용립. 2010.『미국 외교의 역사』서울: 삼인.

김소정. 2023. “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점,” 국가안보전략연구원 이슈브리프 제423.

박현. 2012. “미-이란 해커전쟁...파네타 ‘사이버 진주만 공격 위험’,”『한겨레』(10월 14일). https://www.hani.co.kr/arti/international/america/555741.html (검색일: 2023/12/1)

변진석. 2022. “미국 사이버 안보전략의 등장과 발전,”『평화연구』30.1: 41-76.

설인효. 2022. “바이든 행정부의 안보·국방전략과 한국의 대응방향,”『전략연구』29.2: 257-296..

오일석·조은정. 2022. “미국 사이버전략의 평가와 전망,” INSS 전략보고 No. 175.

정성철. 2024. “사이버 안보와 동맹,” 김상배 편『사이버 안보의 국제정치학: 기본 개념의 탐구』서울: 사회평론.

팀 마샬. 2016. “제 2장: 미국: 지리적 축복과 전략적 영토 구입으로 세계최강국이 되다,” 김미선 역,『지리의 힘: 지리는 어떻게 개인의 운명을, 세계사를, 세계 경제를 좌우하는가』서울: 사이.

하채림.2020. “이란, 美에 '사이버 보복' 시작?…연방기관 웹 해킹돼,”『연합뉴스』1월 5일.https://www.yna.co.kr/view/AKR20200105046000009?input=1195m (검색일: 2024/5/10).

Carothers, Thomas and Benjamin Press. 2022. "Understanding and Responding to Global Democratic Backsliding," Working Paper, Carnegie Endowment for International Peace (October 20).

Craig, Anthony Craig and Brandon Valeriano. 2018. “Realism and Cyber Conflict: Securiy in the Digital Age,” E-International Relations (February 3). https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ (검색일: 2024/5/18).

Ikenberry, G. John. 2020. A World Safe for Democracy: Liberal Internationalism and the Crises of Global Order. New Haven: Yale University Press.

Kaginele, Pranav. 2024. “The Stopping Power of Water: An Outdated Concept?” E-International Relations (March 7). https://www.e-ir.info/2024/03/07/the-stopping-power-of-water-an-outdated-concept/ (검색일: 2024/7/12).

Mearsheiemr, John J. 2018. The Great Delusion: Liberal Dreams and International Realities. New Haven: Yale University Press.

Mearsheimer, John J. and Stephen M. Walt. 2016. “The Case for Offshore Balancing: A Superior US Grand Strategy,” Foreign Affairs 95.4: 70-83.

Morrow, James D. 1991. "Alliances and Asymmetry: An Alternative to the Capability Aggregation Model of Alliances," American Journal of Political Science 35.4 (1991): 904-933.

Nacht, Michael, Patricia Schuster, and Eva C. Uribe. 2019. “Cross-Domain Deterrence in American Foreign Policy,” In Cross-Domain Deterrence: Strategy in an Era of Complexity, edited by Jon R. Lindsay and Erik Gartzke. New York: Oxford University Press.

Nye, Joseph S. 2022. “The End of Cyber-Anarchy?: How to Build a New Digital Order,” Foreign Affairs 101.1: 32-43.

USAID(United States Agency for International Development). 2022. "Digital Ecosystem Framework," August 24. https://www.usaid.gov/digital-development/digital-ecosystem-framework (검색일: 2024/5/16).

Valeriano, Brandon. 2022 "Dyadic Cyber Incident Dataset v 2.0", https://doi.org/10.7910/DVN/CQOMYV, Harvard Dataverse. https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi%3A10.7910%2FDVN%2FCQOMYV&version=DRAFT

Voo, Julia, Irfan Hemani, and Daniel Cassidy. 2022. “National Cyber Power Index 2022,” Harvard Belfer Center, September.

Walt, Stephen M. Walt. 2018. The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of US Primacy. New York: Farrar, Straus and Giroux.

Wolfers, Arnold. 1952. "'National Security' as an Ambiguous Symbol," Political Science Quarterly 67.4: 481-502.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.