사이버 안보와 문화

2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 8호
발간일: 2023년 12월 28일

양종민 (정보통신정책연구원)

〈요 약〉

이 글은 사이버 공간의 안보를 문화의 렌즈를 통해 살펴본다. 문화와 안보라는 생경한 영역은 세가지의 모습으로 서로 연결, 결합, 추동되고 있는데, 기계적 연결, 사이버 안보의 전략문화, 사이버 공간의 인간중심 보안문화로 살펴볼 수 있다. 우선 비교적 최근에 나타나고 있는 문화와 안보의 기계적 연결은 중국의 한국 문화 콘텐츠에 대한 한한령과 미국과 중국 사이의 틱톡을 둘러싼 패권대결에서 나타났다. 그동안 연결되지 않았던 영역들이 서로 연결되면서 새로운 문제를 만들어낼 수 있다는 차원에서 문화와 안보의 기계적 연결을 단순히 우연적인 사건으로 생각할 수 없지만, 이를 사이버안보의 신흥안보적 창발로 생각하기에는 임계점을 통과하지 못했다는 한계를 지닌다. 두 번째의 연계는 사이버안보의 전략문화인데, 군사안보의 공간으로서 사이버 공간이 가지는 특질은 전략문화를 통한 사이버안보의 파악을 위해 중요하며, 전략문화는 국가의 사이버력에 대한 인식과 행위의 선호를 설명하는 데에 중요한 도구로 사용될 수 있다. 하지만 비과학적 방법론의 한계를 그대로 간직한다는 차원에서 전략문화는 사이버공간의 안보이슈를 만들어내는 독립변수이기보다 매개변수나 개입변수로서 다루어져야 한다. 마지막의 연결은 사이버안보로부터 만들어지는 인간중심 문화이다. 탑다운방식의 전통적보안관리와 달리 인간중심의 보안문화형성을 통한 대응은 인간의 행동을 관리하는 아래로부터의 관리체계를 말하며, 자율중심의 조직문화는 보안사고를 줄이면서도 유연하게 대처할 수 있게 하는데 도움을 줄 수 있다. 또한 인간을 중심으로 하는 가치를 국가 안보, 더 나아가 세계 질서의 중심에 놓게 되면, 안보의 궁극적인 수혜자로서 인간을 다루면서도 새로운 디지털 문명/문화를 만들어갈 가능성을 열어준다는 점에서 의미가 있다.

I. 서론

사이버 공간의 안보와 전략, 그리고 분쟁과 전쟁의 영역에서, 국제관계의 여러 행위자는 서로 다르게 행동한다. 즉, 사이버공간에서 다른 목적을 가지고 다른 방법을 통해 자신들이 가지는 사이버 능력을 행사한다(Valeriano 2018). 러시아가 2016년 미국 대통령 선거에 개입했던 것처럼 파괴적인 공격과 함께 여론을 조작하는 목적으로 영향력을 행사하려고 했다면, 미국은 이스라엘과 함께했던 이란의 핵 농축 시설에 대한 스턱스넷 웜 공격에서 살펴볼 수 있는 것처럼, 지휘통제 시스템 등의 작전 대상을 핀포인트 하는 것으로 특징지어 볼 수 있다. 더불어 중국은 클라우드 호퍼 작전에서도 살펴볼 수 있는 것처럼 네트워크의 원활한 작동을 방해하고 서구 선진국과 기술적 격차를 줄이기 위해 지적재산을 가장 활발하게 훔치려 한다. 이란은 상대방의 시스템의 정상 운영을 방해하기 위해 분산 서비스 거부 공격(DDoS Attack)을 가장 효과적인 방법으로 택하지만, 북한은 거의 모든 국가 운영전략의 효과적인 도구로서 사이버력을 사용하고 있으며, 최근에는 국정에서의 경제적 어려움을 타개하기 위해서 암호화폐를 탈취하는 데에 주력하고 있다(Valeriano 2018; Joyce 2018).

사이버 공간에서 국가들의 다른 전략적 행위를 일반화해서 이해할 수 있을까? 국가행위자가 모두 같은 기능을 가지고 합리적으로 계산해서 전략 행위에 대한 선호를 구성할 수 있다면, 같은 공간에서 비슷한 자극에 따라 나오는 대응의 양상은 비슷해야 할 것이다. 행위자의 안을 들여다보지 않고, 행위자가 가지고 있는 속성적 측면, 또는 사이버 공간이 가지는 모호성과 불확실성으로 국가의 사이버 공간에서의 여러 가지 다양한 전략적 행위를 이해하고 해석하기에는 여러 가지 다양한 동기, 즉 사이버 공간에서의 전략적 행위에 숨겨져 있는 그 무엇인가가 작동하고 있는 것으로 보인다. 다시 말해서, 사이버 공간에서 다양한 전략적 행동을 이해하기 위해서 행위자의 의사결정의 뒤에 있는 요소를 살펴보아야 할 필요가 있으며, 그것은 바로 합리적 행위자라는 블랙박스를 열어보아야 한다는 것을 뜻하기도 한다.

이러한 블랙박스의 안을 구성하는 문화라는 요소를 통해 전략적 행위의 근원을 이해하려는 시도가 진행되는 데에는 그동안에 분리된 영역에서 자리하고 있는 것으로 생각되던 문화와 안보라는 정치학적 요소들이 디지털 기술의 발전과 사이버 공간의 창발을 만나 다소 생경한 결합을 통해 이슈를 만드는 상황과 무관하지 않다. 이러한 소위 '문화와 안보의 연결'은 신흥안보의 시발점으로서 생각해 볼 수도 있지만, 연결만으로 신흥안보의 창발을 논하기에는 어려운 면이 존재한다. 각 국가는 역사적 경험에 기반해서 독특한 전략문화를 가지고 있으며, 전략문화를 통해 같은 문제를 다르게 인식하며 처리하는 방식을 이해할 수 있다는 일종의 대안적 설명을 위해 문화라는 요소를 이용했다. 전략이 만들어지는 과정에서, 그리고 그 안에서 무력의 정당한 사용에 관한 결정이 내려지는 상황에서 특정한 선택의 길이 생성된다는 것이다. 한편 문화라는 요소, 또는 변수는 사이버공간에서의 안보를 연구하는 데에 또 다른 단계에서도 발견된다. 국가적 차원의 사이버 보안문화의 정착이라든지, 민간 영역에서의 조직적인 차원에서의 인간중심 보안문화의 개선이라는 표현에서 살펴볼 수 있는 것처럼, 사이버 공간을 사용하는 개인적 차원에서의 "안전", "권리", "실천"의 모습을 만들어낼 수 있는 근원이자 맥락으로 문화라는 용어가 사용된다. 아무리 좋은 안보/보안정책이 마련되어 있다고 하더라도, 그것을 실제로 운용하는 것은 개인과 그 개인들이 속해 있는 조직이라 할 수 있고, 개인이나 조직이 가지고 있는 문화가 규범이나 정책과 서로 맞아떨어지지 않는다면 안전의 문제가 시작될 수 있는 근원으로 작동할 수 있다.

이 글은 비교적 새롭게 등장하고 있는 사이버안보 영역에 문화라는 렌즈를 넣어서 생각해 본

다면 어떠한 모습이 나타날지를 살펴보는 것을 목적으로 한다.[1] 따라서 본 연구의 연구 질문은 다음과 같다. 첫째, 안보와 문화의 만남은 어떠한 국제정치적 문제를 새롭게 야기하고 있는가? 둘째, 사이버 공간은 안보-문화의 넥서스로서 어떠한 모습을 가지는가? 사이버 공간과 물리적 공간의 연속성-단절성은 안보와 문화의 연결을 어떻게 뒤트는가? 셋째, 사이버 전략문화는 무엇을 의미하는가? 전략문화가 국가의 사이버안보 전략 선호에 어떠한 영향을 주는가? 넷째, 사이버 보안문화의 주체는 누구이며, 그 내용은 어떠한가?

이러한 질문에 답하기 위해서 이 연구는 다음과 같이 구성된다. 먼저 2장에서는 사이버 공간에서 문화와 안보의 만남 현상에 주목한다. 이러한 현상의 중심에는 4차 산업혁명으로 급격히 중요성이 더해지는 사이버 공간이 있고 신흥안보로서 창발의 단초를 제공하나, 미완성의 한계를 가진다. 3장에서는 본격적으로 사이버안보에 있어서 전략문화의 역할에 대해서 살펴본다. 전략문화는 사이버 공간에서 전략 선호에 영향을 주는 독립변수인 것처럼 작동하지만 실제로는 매개변수, 또는 개입변수로서 기능을 한다. 4장에서는 국가 또는 조직의 사이버안보/보안 정책의 결과로서 나타나는 문화를 살펴본다. 국가 또는 조직이 만들어내는 규범적, 실질적 목표에 어떻게 개인들이 따르게 할 수 있을지의 차원으로 문화가 사용되고 있으며, 그러기 위해서 목표나 정책에 어떠한 부분이 새롭게 작성되고 있는지를 종합적으로 검토한다. 5장에서는 글의 내용을 요약하고 함의를 제시하는 것으로 마무리한다.

II. 문화-안보/안보-문화

1. 문화와 안보의 얽힘

한 국가의 문화는 국가 구성원들에게 공유된 사고방식과 정체성의 중심을 구성하는 기능을 한다. 따라서 자국의 문화를 보호하면서 외국의 강력한 문화에 오염되는 것을 막으려는 시도는 늘 있었지만, 안보 영역과 문화 영역이 사이버공간을 중심으로 얽혀 나타나는 소위 문화-안보적/안보-문화적[2] 양상은 비교적 최근에 나타나고 있다. 한국과 중국사이에서 벌어지고 있는 한국 문화콘텐츠에 대한 한한령, 그리고 미국과 중국사이에서 숏폼 비디오 플랫폼인 틱톡을 둘러싸고 벌어진 갈등은 이러한 문화와 안보의 만남현상을 보여주는 예로서 생각해 볼 수 있다.

“협의로는 중국 내에서 한국에서 제작된 콘텐츠 또는 한국 연예인이 출연하는 광고 등의 송출을 금지하는 것에서부터 광의로는 한국 기업과 한국 브랜드 등 한국을 담고 있는 모든 요소와 TV광고까지 금지하는 대대적인 조치”(김휘정 2017, 1)를 의미하는 한한령(限韓令)은 2016년 한국 정부가 사드(THAAD, 고고도미사일방어체계) 배치를 공식화하자 중국정부의 국방, 외교적 문제를 넘어서서 문화영역에 대한 일종의 보복 조치로서 등장했다. 2000년대에 접어들어 한국 대중문화가 동아시아, 특히 중국 시장에서 인기를 얻으면서 한국정부는 한류 붐을 조성하기 위한

1) 문화와 안보 변수의 얽힘 현상을 이슈별로 다루는 연구가 속속 등장하고 있다. 각각의 연구는 국제정치학적, 문화정치학적 이론을 중심으로 현상을 분석한다. 이 글은 기존연구와 달리 문화와 안보의 변수가 사이버공간에서 얽히는 모습을 더욱 입체적으로 파악하고자 하는 목적을 가지므로 일종의 탐색적 연구라고 할 수 있다. 따라서 이 글에서는 이러한 문화와 안보의 여러 모습을 하나의 이론적 틀로 무리하게 엮어내는 시도를 하지 않는다.

2) 이렇게 문화와 안보가 기계적, 일시적으로 서로 얽혀 나타나는 현상을 한 단어, 또는 어구로 표현하는 방법은 현재 존재하지 않는다. 따라서 다소 의미의 왜곡이 있을 수 있지만, 문화-안보 또는 안보-문화를 병치함으로써 이러한 기계적인 연결을 표현하고자 한다.

산업정책적 지원을 시작했다(김규찬 2013, 277). 이러한 배경 아래에서 수출에 급물살을 타고 있던 한류 문화콘텐츠는 한한령으로 인해 중국으로 건너갈 수 있는 길이 대부분 막혀버렸다. 그동안 전통안보차원의 국제분쟁에 있어 중국은 여러 가지 형태로 경제보복을 했지만, 문화적인 차원으로까지 확장되지는 않았었다. 그러다 유독 사드 배치에 관해서는 한국문화의 중국 수입금지라는 보복을 선택한 것이다.

중국이 한국의 안보 이슈에 대해 문화 산업적으로 대응하게 된 데에는 몇 가지로 분석해볼 수 있다. 우선 경제적인 측면에서 문화산업이 가지는 통상분쟁의 비민감성의 차원이다. '한류'와 관련된 문화콘텐츠 분야는 국제무역에서 예외 조항에 해당하기 때문에 자유로운 무역을 막는다고 해도 무역분쟁으로 비화할 가능성이 작다(정덕현 2017). 또한 문화 분야는 경제적인 보복을 한다고 하더라도 중국에 대한 재보복의 가능성이 적은 분야이다. 즉 긴밀하게 연결된 산업 분야에 대한 보복은 다시 중국의 산업발전에 악영향을 미칠 수 있기 때문에 이러한 가능성이 작은 문화분야를 선택했을 수도 있다(김수한, 유다형 2017). 마지막으로 기존에 진행되던 중국의 문화정책의 연장선에서 한류의 성공에 대한 대응, 즉 사드는 중국의 자국 문화산업 보호 발전을 위한 과정에서 단지 물꼬를 튼 하나의 역할에 불과한 것이며, 문화안보적인 차원에서 중국의 움직임을 살펴보아야 한다는 주장도 있다 (류설리 2017; 안창현 2018). 어떠한 이유이건 간에, 중국의 '한한령'을 중심으로 안보영역과 문화영역이 연결하는 모습을 보인다는 것에는 이견이 없다.

한류에 대한 한한령을 둘러싼 문제를 안보분야와 문화분야의 본격적인 연계로서 생각하기에는 다소 무리한 해석이 필요해 보이나, 미국과 중국 사이에 틱톡을 둘러싸고 벌어진 공방은 새로운 기술혁신으로 인한 신흥 패권경쟁의 양상, 인터넷과 네트워크의 공간에서 벌어지는 안보화의 모습이 더욱 생생하게 그려진다. 15초에서 최대 60초의 짧은 동영상을 공유하는 앱인 틱톡은 중국을 기반으로 하는 스타트업인 바이트댄스가 개발하였는데, 바이트댄스는 이용자가 립싱크 영상을 찍어 공유하는 플랫폼이었던 '뮤지컬리(Musical.ly)' 앱을 벤치마킹하여 2016년 9월 더우인 앱을 출시하며 중국과 태국에서 1억명의 이용자를 모았다. 바이트댄스는 1년만에 더우인의 글로벌 버전인 틱톡을 출시하고 같은해 11월 뮤지컬리를 인수하는 데에 성공하면서 글로벌 시장에서 급속도로 인기를 얻었다(장재웅 2020). 2023년 틱톡은 미국 내 월 활성이용자수가 1억 5000만명에 달하며, 이는 트럼프의 틱톡에 대한 행정명령이 떨어진 2020년의 1억명에서 50퍼센트가 증가한 것이다(김희원 2023).

2020년에 트럼프 대통령은 바이트댄스의 틱톡 사용자들의 개인정보, 네트워크 정보가 축적되어 중국으로 흘러들어가 미국의 국가안보를 해칠 위협을 가할 수 있다며 틱톡의 미국 내 자산을 매각할 것을 요구하는 행정명령에 서명했다(김민혁 2020). 이에 중국 상무부는 12년동안 개정되지 않았던 「수출 금지·제한 기술목록」을 조정하여 핵심 기술을 해외 이전하게 될 때 중국정부의 승인을 받도록 하였으며, 바이트댄스는 이에 따라 매각을 처리할 것이라고 공식적으로 성명을 발표했다(박민숙, 김영선 2020). 미중간의 줄다리기 속에서 틱톡은 갈피를 잡을 수 없었다. 2021년 바이든 대통령은 미국 법원에 의해 가처분 신청이 받아들여진 틱톡 매각 문제를 해결하기 위해 기존의 행정명령을 철회하고 대신에 적대적인 활동으로부터 미국인의 민감한 데이터를 보호하기 위한 새로운 행정명령에 서명했다. 미국정부와 의회는 지속적으로 바이트댄스가 틱톡 이용자 정보를 중국 정부에 제공할 수 있다는 우려를 제기하고 있으며 결국 2023년에 바이든 대통령은 연방정부 공무원이 정부기관의 기기에서 틱톡을 사용하는 것을 금지하는 법안에 서명하면서 직접적인 틱톡 제재에 나선 상황이다(추동훈 2023).

2. 연결의 장소로서 사이버 공간

안보와 무관해 보이는 문화영역의 서비스나 상품에 대해 몇몇 국가들이 안보적인 차원으로 대응하게 된 배경에는 사이버공간, 그리고 그 안을 구성하는 4차산업혁명의 기술혁신이라는 변수가 작동하고 있다. 우선 한류의 시작과 함께했던 표층적 의미에는 한국의 대중문화와 연예인들에 빠져 있는 중국 젊은이들의 유행을 경계하고자 하는 일종의 한국에 대한 적의와 문화침투의 차원으로 한국 문화상품을 인식하는 경향이 있었지만(이지한 2018, 359), 한국이 바라보고 있었던 한류의 중심에는 한류문화산업의 세계시장의 진출이 가져오는 경제적 이익에 관한 관심과 함께, 한류 문화콘텐츠가 생산, 전파되는 과정에서 디지털 기술과 인터넷 공간이 일정한 역할을 하고 있었다는 특징을 생각해 볼 수 있을 것이다. 한류 문화콘텐츠가 만들어지는 데에 필수적인 디지털 기술은 한국이 보유한 지식역량을 바탕으로 하며 문화의 산업화를 위한 핵심이 된다. 이러한 일련의 문화기술은 좁게 보아서 문화상품의 생산, 유통, 소비에 활용되거나 관련되는 서비스에 사용되는 기술로 볼 수 있지만, 문화콘텐츠가 담고 있는 문화유산, 생활의 양상 등으로 범위를 넓힌다면 정보통신을 포함하는 기술뿐만 아니라 인문사회에서의 지식을 융합하여 만들어지는 인간의 문화 활동을 통해 삶의 질을 다루는 복합적인 총합으로 볼 수 있다(우운택 2020, 11). 더불어 한류의 중국시장에서의 성공에는 인터넷상에서 동아시아 신세대들을 중심으로 활발히 이루어지는 디지털 문화콘텐츠의 교류, 그리고 이를 매개로 한 지식의 공개와 공유의 관념이 존재한다. 김상배(2007)에 의하면, 한류는 동아시아 지역의 젊은이들에게 일정한 정도로 네트워킹의 요소를 제공하고 있다. 1990년대 이후에 동아시아 젊은 층에서 소비되는 대중문화는 자국문화와 서구문화가 복합된 형태였는데, 각 지역의 근대화 과정에서 서로 얽히면서 한류의 대중문화가 수용될 수 있었으며, 경제적으로 먼저 성공한 한국을 동경하고 그리는 일종의 준거집단으로 삼고자 하는 막연한 유대감이 형성될 수 있었다. 그래서 한류 문화콘텐츠의 중국시장에서의 성공을 인터넷 공간을 중심으로 형성되는 동아시아 문화 네트워크의 차원으로 생각해 볼 수 있는 것이다.

한류가 중국시장에서 성공을 거두던 상황에서 한한령이라는 장벽으로 인해 어려움을 겪고 있는 이유를 산업적 차원, 경제적 차원으로만 생각할 수 없는 지점이 있다. 바로 중국이 “문화안보”의 개념을 확립하고 지속적으로 강화하고 있었기 때문이다. 중국의 문화안보는 서구문화의 침투와 확장이 중국민족문화의 생존과 발전에 심각한 위협으로 인식되는 상황에서 수립되었다. 사회주의 시장경제 체제에서 경제적으로 급성장을 이룩하면서 중국 대중들에게 서구 대중문화가 급격히 확산되었는데, 이 중 한국 한류 문화콘텐츠는 형식적으로는 서구의 대중문화를 수용하면서도, 내용적으로는 익숙한 동아시아적 정서를 성공적으로 조합하고 있었기 때문에, 중국의 당시 상황에서 서구문화의 세찬 물결에 적응할 수 있었던 계기로 사용되었다. 결국 한국 대중문화는 서구문화의 직접 침투를 막는 1차적 장벽이었던 동시에 자국 문화산업을 발전시킬 수 있는 마중물의 역할을 하게 되었던 것이다. 항한류의 역풍에서도 한국 문화콘텐츠들은 인터넷 스트리밍, OTT 서비스를 통해서 중국으로 확산될 수 있었는데, 중국은 이러한 흐름에 문화안보를 위한 규제를 늘려 자국의 문화산업의 성장을 위해 자체생산능력을 늘리고자 하였다. 인터넷은 한류의 확산통로가 되었던 동시에, 상품의 진입을 막고 그 안의 내용, 노하우를 흡수하여 역흐름을 만들기 위한 필터의 역할을 하고 있다(이지한 2018).

한편, 틱톡사례에서 보이는 문화와 안보의 연결은 이전의 사드-한한령으로 이어지는 한중간의 문화안보사례보다는 더욱 복잡하고 긴밀한 모습을 살펴볼 수 있다. 겉보기에는 틱톡이라는 일개의 문화콘텐츠 플랫폼이 안보와 무관해 보일 수도 있다. 하지만 미국의 틱톡견제는 단순 중국의

앱에 대한 제제 이상을 의미한다. 데이터와 개인정보가 가지는 민감성이 극대화되는 4차 산업혁명의 기술혁신으로 인해 스몰 데이터 환경에서 야기되는 전통안보적 차원의 문제가 아니라 빅데이터 환경에서 발생하는 신흥안보적 차원의 문제가 나타날 수 있다. 데이터 한 조각은 국가안보나 군사안보와 무관할 수 있지만, 양이 늘어나고 여러 가지의 이슈가 복잡하게 연계되다 보면 그동안에는 예측할 수 없었던 새로운 형태의 국가안보적 의미를 가지는 중요성이 창발할 수 있다(김상배 2021a, 38). 그렇기 때문에 플랫폼을 통과하는 수많은 데이터들은 4차 산업혁명시대에 국가의 주요한 권력 요소이자 안보적 함의를 가지게 된다. 문화 플랫폼일지라도 특정 국가가 이를 장악한다면 플랫폼을 스쳐가는, 그리고 플랫폼이 저장하고 처리하는 수 많은 데이터들에 접근하여 사용할 수 있는 능력을 지닐 수 있게 되는 것이다.

3. 기계적 연결과 신흥안보

앞에서 살펴본 문화와 안보 이슈의 얽힘 현상은 그동안에는 관심을 두지 못했던 서로 떨어져 존재하던 분야들이 만나 새로운 형태의 국제정치학적 이슈를 만들어내는 모습으로 생각해 볼 수 있다. 하지만 이러한 만남만으로 완벽하게 비전통적 안보, 또는 신흥안보의 개념으로 인식하고 살펴보기에는 어려운 점들이 존재한다. 단순한 연결의 상황은 신흥안보의 창발에 필요한 이슈 연계의 모습으로 살펴볼 수는 있지만, 임계점을 넘어 새로운 안보 이슈로까지 만들어내는 모습까지는 도달하지 못했기 때문이다.

신흥안보 이슈들은 일상생활의 미시적 차원에서 발생하는 일종의 '안전'의 문제들이 특정한 계기를 만나서 거시적 '안보'의 문제로 증폭되는 특징을 지닌다(김상배 2016, 77). 한 분야에서 나타나는 전통안보 이슈와 달리 다양한 행위자가 관여하고 여러 가지 이슈들이 연계하면서 작은 위험이 다른 분야의 큰 위협으로 확산, 파급되기 때문에 원인과 과정, 그리고 효과를 예측하는 것이 쉽지 않다. 더욱 문제는 신흥안보의 이슈는 제대로 대처하지 않으면 극단적 사건의 형태로 발현될 가능성이 높을 뿐만 아니라 맥락에 따라 다르게 나타날 가능성이 높아서 보편적인 해법을 마련하기도 어렵다. 다시 말해서 신흥안보가 가지는 특성을 고려했을 때, 초기의 위험이 임계점에 도달하기 전에 연계의 고리를 끊지 않으면 거시적 차원의 안보문제로 전환될 가능성이 크다. 위험은 양적으로 커질 수 있으며, 이슈 연계를 통해 질적으로 변환될 수도 있다. 또한 위험이 커지면서 다른 이슈와 연계가 동시에 나타날 수 있다. 이렇게 신흥안보 이슈는 불확실한 단계에서부터 출발해서 동태적인 과정을 통해서 안보문제로 전환되는 메커니즘을 지닌다(윤정현 2019, 24).

신흥안보의 이슈가 창발하기 위해서 일종의 임계점을 넘어야 한다. 양적증가가 질적인 변화를 야기하는 양질전화의 임계점, 이슈들간의 질적 연계성이 높아지다가 전체 이슈구조의 변동이 발생하는 이슈연계의 임계점, 마지막으로 신흥안보의 이슈가 전통안보 이슈와 연계되어 국가 사이 분쟁의 대상이 되는 지정학적 임계점이다. 이러한 임계점은 창발 초기부터 순차적으로 나타나는 것이 아니라, 서로 중첩되어 벌어질 수도 있으며, 때에 따라서는 동시에 발생하기도 한다(김상배 2016, 83-85). 문화영역에서 나타날 수 있는 신흥안보의 창발을 가상적으로 예를 들어 본다면, 인터넷 공간에서 나타나는 개개인의 특수한 문화적 정체성의 충돌 양상이 문화 플랫폼을 통해 조금씩 발현되다 전혀 무관한 사건을 계기로 해킹, 테러와 연계되고 상대국가에 심각한 안보적 위협으로 나타나 국가 행위자가 개입하는 근거가 발생하고 문제의 해결을 위한 국제협력의 메커니즘이 가동되는 것을 생각해 볼 수 있다.

하지만, 단순한 이슈의 연결을 임계점 통과로 볼 수는 없다. 중국의 '문화안보' 개념은 신흥안

보적 차원에서의 문화와 국가안보 이슈의 적극적 융합으로 해석하기 어렵기 때문이다. 중국이 외국문화의 무분별한 유입을 막고자 하는 배경에는 통제에서 벗어난 대중에 대한 두려움과 함께하는 문화안보의 개념이 자리하고 있다. 2004년부터 중국은 국가안보전략을 확정하면서 문화를 정치, 경제, 정보와 함께 국가의 주요한 안보의 대상이자 목표로서 다루고 있다(안창현 2018, 124). 여기에서의 문화안보 개념은 중국의 문화정체성을 유지, 발전시키고, 서구의 세련된 대중문화콘텐츠의 문화적, 경제적 공격으로부터 중국 문화의 오염을 막으면서 자국의 문화산업을 발전시키려는 의도를 담고 있다. 즉, 타국의 문화를 공격하고 있다기보다는 자국의 사회통제관리의 차원으로 이용하고 있다. 한한령을 둘러싼 이슈가 중국 대중에게서 볼 수 있는 한국문화에 대한 불만으로부터 시작해서 갑자기 사드를 둘러싼 양국간의 군사안보적 문제로 확장되었다면 어느 정도 신흥안보의 임계점을 적용해 볼 수 있겠지만 실제로는 그렇게 진행되지 않았다. 더불어 한한령으로 인해 공식적으로 한국 문화가 수입되는 길이 막힌 상황에서 중국 대중은 불법적이고 우회 경로를 통해서 그대로 한국 대중문화콘텐츠를 즐기고 있었다는 점을 고려했을 때 문화적 이슈가 안보적 이슈로 연계되는 임계점을 통과했다고 살펴보기에는 어려운 면이 있다.

결과적으로 신흥안보의 개념을 통해 문화-안보의 연결 현상을 파악한다면 기존과는 다른 방식의 접근이 필요하다. 각각의 다른 특징을 가지고 있는 이슈들의 위험양상은 전통적 안보 문제들과 달리 초기에서부터 살펴보기 어려우며 맥락에 따라서도 다르게 발현된다. 그러나 이 장에서 다루는 문화와 안보의 기계적 연결 현상은 신흥안보의 모습으로 살펴보기에 무리가 있다. 물론 틱톡사례는 빅 데이터 환경에서의 신흥안보적인 문제로 창발할 가능성이 충분히 있지만, 현재의 중국과 미국의 대응은 국제정치적 차원에서의 기술패권 주도 다툼에 머물러 있으므로 여전히 전통안보적 차원에서 새로운 이슈에 대한 대응으로도 설명할 수 있다. 다시 말해서 21세기의 복합적인 안보환경과 신흥안보의 개념으로만 설명할 수 있는 정도까지 완벽히 무르익지 못했다는 모습을 가진다는 것이다. 특히 한한령과 관련한 안보 쟁점은 서로의 연계 현상이 임계점을 넘어서 새로운 안보 문제로 발화했다기보다 일종의 우연적인 연결, 또는 기존 안보 쟁점의 연장선상에서 촉매재의 역할 그 이상, 이하도 아닌 것으로 파악할 수 있을 것이다.

III. 사이버 전략문화

1. 전략문화

안보연구에서 전략문화를 국가의 행위를 설명하기 위한 주요한 원인으로 도입하려는 시도는 미국과 소련 사이에서 나타나는 미러이미징(mirror imaging), 즉 특정한 갈등 상황에서 비슷한 크기의 기술 수준, 국가권력을 가지는 행위자는 비슷하게 반응할 것이다라는 국가의 합리성을 기반으로 안보전략을 설명하는 현실주의이론의 문제를 풀어내기 위해, 국가행위자들이 가지는 전략적 사고의 차이를 이해하고 설명할 필요성에서 출발했다. 이 접근법의 선구자인 잭 스나이더는 소련의 핵전략이 미국과 다르게 나타나는 이유는 국가 안보전략을 수립하는 그룹의 구성원들이 지시라든지 모방을 통해서 서로 습득하고 공유하는 사상, 제한적으로 나타나는 정서적인 반응, 인지적으로 가이드된 습관적 행동의 패턴의 총합으로 나타나는 특수한 전략문화를 가지고 있기 때문이라고 설명한다(Snyder 1977, 8). 그는 국가안보 전략에 관한 이슈를 처리하고 실제 정책의 결정에 영향을 주게 되는 일종의 인식적인 렌즈로서 생각의 틀을 형성하고, 전략적 문제가

공식화되는 방식에 영향을 미치는 태도와 신념의 실체로서 전략문화를 들고 이를 전략선호와 안보정책의 설정에 대한 설명변수로서 사용한다(Snyder 1977, 9).

1980년대 초부터 등장했다고 할 수 있는 전략문화연구의 1세대는 스나이더의 문화변수를 엄격한 학문적인 개념으로 만들었다. 콜린 그레이는 특정한 국가가 가지는 역사적인 경험이 바로 전략문화로 결집된다고 보고, 안보전략을 설명하는 데에 전략문화는 주요한 전략적 국가의 신념으로 이어지는 힘에 대한 사고와 행동의 양식으로 파악한다. 이와 달리 데이비드 존스는 전략문화가 형성되는 데 중요한 요소를 거시적 환경, 사회적, 미시적 수준[3]으로 나누어 생각한다. 이렇게 1세대의 전략문화연구는 문화 개념을 구체화하고 안보연구에서 문화개념을 포함한 방법론적인 원리를 확립하기 위해서 노력하고 있으나, 전략문화의 정의에 광범위한 문화적 사회적 변수를 포함하고 있어서 하나를 설명하기 위해 모든 것을 드는 엄밀성과 일관성의 차원에서 문제가 있는 것으로 비판받는다(Johnston 1995a, 36-37).

1980년대 중후반에 시작된 전략문화연구의 2세대는 지도자들이 공공연하게 언급하는 것으로 나타나는 전략행동의 표면적인 동기와 해당하는 행위자가 뿌리 깊게 가지고 있는 실제적인 동기 사이의 차이를 고려하면서 실제 전략적 운영과 선언적인 전략 사이에 나타나는 불일치를 다룬다. 여기에서 전략문화는 국가의 선언적인 전략을 지탱하면서 안보전략결정을 하는 엘리트들의 그람시안적 헤게모니를 형성하는 데에 사용되지만, 실제 작전에서 사용되는 전략은 단순하게 이들 의사결정권자의 구체적인 관심사를 반영한다고 주장된다. 국가행위자의 공식 안보전략, 선언적으로 나타나는 전략은 운영전략에서의 국가 행동이 문화적으로 얼마나 수용가능한지에 대한 정당성을 형성하는, 그리고 잠재적인 정치적 도전자들의 대안적인 행동전략의 정당성을 줄이고, 이들을 오도하기 위한 노력의 하나로 해당 국가의 특수한 전략문화에서 유래한다고 보는 것이다(Klein 1988, 136; Stuart 1982). 그러나 2세대의 연구에서 사용되는 전략문화는 엘리트들의 의사결정에 영향을 미치지 못하거나, 문화적 제약을 비교적 쉽게 극복할 수 있다고 보고 있어서, 전략문화를 도구적인 수단으로만 다루고 있다는 비판을 받는다(Johnston 1995a, 39-41).

1990년대에 등장한 3세대는 2세대와 달리 전략문화가 국가의 전략적행위에 영향을 미친다는 주장을 다시 한번 확인하면서 전략문화의 과학적 방법론을 구축하고자 한다. 이들은 특정한 정책결정에 영향을 미치는 구체적인 요소를 추적하는데, 독립변수로서 전략문화는 매우 긴 시간의 범위를 가진 역사적 요인에서 나타나는 것이 아니라 최근의 경험과 실제 사례에서 만들어지는 것으로 보고, 국가의 전략적 행위에 대한 구체적인 전략의 선택으로 종속변수의 범위를 한정했다. 이안 존스턴은 전략문화에서 비전략적 문화변수를 구분해야 한다고 주장하면서, 전략문화를 "국제관계에서 군사력의 역할과 효과에 대한 개념을 형성하고, 전략선호가 독특하게 현실적이면서도 효과적으로 보이게 하는 사실성의 아우라와 같은 개념으로 포장함으로써 비교적 오래 지속되는 전략선호를 특정하게 확립하는 역할을 하는 일종의 상징이나 기호 시스템[4]"으로 정의한다(Johnston 1995a, 46).

전략문화연구의 4세대는 구성주의이론에 근거해서 전략문화를 "특수하게 확립된 사고의 방식으로 사회화된 엘리트들의 신념, 태도, 행동양식의 집합"으로 보는 스나이더의 정의로 돌아가는 모습을 보인다(Lantis 2002, 104). 그러면서 이들은 한 국가의 전략문화가 정적으로 확고하게 자리하는 것이 아니며, 전략문화 안에는 여러 하위문화가 존재할 수 있고, 이러한 하위문화 사이

3) 거시적인 환경 수준으로서 지정학적 위치와 역사, 사회적 수준으로 사회의 특정한 구조, 그리고 미시적 수준으로 군사조직의 현재 상태와 민군관계의 흐름으로 요약할 수 있다.

4) 상징 시스템은 1. 인간의 세계에서 전쟁의 역할, 2. 적과 위협의 성격, 3. 무력사용의 효과로 이루어지는 전략환경의 질서성에 대한 기본 가정과 함께, 이렇게 구성된 위협환경에 대응하기 위해서 어떠한 전략적인 선택이 가장 효율적일 수 있는지에 대한 보다 실질적인 선호의 레벨에 대한 가정들로 구성되어 있다(Johnston 1995a, 47).

에서 나타나는 담론적 경쟁이 한 국가에서 선택할 수 있는 여러 가지의 전략적 옵션을 만들어낼 수 있다고 주장한다(Howlett and Glenn 2005). 한 국가 안에서 여러 가지로 존재할 수 있는 서로 다른 하위문화는 국가의 전략문화에 영향을 미치며, 조직 간 또는 조직 안에서의 담론의 형성과 경쟁을 이해하게 될 때, 결과적으로 국가의 전략문화가 어떻게 변화하는지, 그대로 기존의 전략문화를 고수하게 되는지를 살펴볼 수 있다는 것이다(Bloomfield 2012; Liebel 2016).

이러한 이론적 발전에도 불구하고, 여전히 정확하게 어떠한 것을 연구해야 하는지에 대한 신뢰할만한 방법론을 정립하지 못하고 있다(Horton-Eddison 2018). 특히 어떠한 것이 전략문화를 구성하는지에 대한 문제에 대해서 지리적인 요소, 기후나 천연자원의 존재 여부와 같은 국가의 물질적인 요소나 정치체제의 특성과 같이 보다 거시적인 요인들에 의한 생각의 틀의 구성을 바라보고 있는 연구가 있는가하면, 정책결정그룹이 역사적으로 공유하는 사회적 문화적인 신념체계로 살펴보고 있는 연구도 존재한다. 다시 말해서 거시적인 요인들은 전략문화의 형성에 영향을 미치는 간접적인 배경요인으로서, 공유된 신념체계는 실제 특정한 전략문화를 구성하는 데 있어서 중요한 요인으로 생각하고 있다고 볼 수 있다(황일도 2013). 이러한 것들을 하나하나 적절하게 배치하지 않고 모두 문화를 형성하는 요소로 그대로 생각한다면 한 나라가 고유하게 가지는 물리적 요소와 역사적 경험을 토대로 형성하는 전략문화적 가치를 도출하고 이것이 특정 국가의 안보전략을 형성하는데 있어서 중요한 역할을 하는 일종의 결정주의적 오류를 범하거나, 문화를 변화하는 맥락으로 생각한다면 행위가 문화를 형성하고, 다시 문화가 행위자의 행위를 구성한다고 보게 됨으로써, 국가안보전략적 행위를 설명하는 데에 있어서 어떠한 해석도 참이 되는 동어반복의 오류를 범할 가능성이 높다고 할 수 있다.

전략문화를 통해 국가의 안보적 행위를 설명하기 위한 시도는 포괄적으로 보면, 상대방의 군사정책을 분석하고 예측하는 과정에서 자국이 가지는 일정한 생각의 틀, 사고방식에 끼워맞추어 해석하는 문제를 어느 정도 보완할 수 있다는 장점과 함께, 일국의 일반적인 군사정책을 만들어가는 과정에서 자국이 가지고 있었던 전체적인 문화적 배경과의 관계를 살펴볼 수 있다는 의미를 생각해 볼 수 있다. 한 국가의 안보전략에 기반한 행위는 그 국가를 구성하는 문화를 벗어나기 어려운 면이 있다. 물론 특정한 행동이 문화를 벗어나 일탈적인 모습을 보일 수도 있지만, 그러한 일탈적인 안보 행동조차도 문화가 어떻게 만들어져 있는가에 따라서 설명해 볼 수 있다. 특정한 안보전략적인 문제를 다루는 데에 어떠한 행위자라도 문제와 관련하고 있는 주변배경과 함께 자신이 할 수 있는 안보전략적 행위에 대한 여러 가지 선택지, 과거의 사례에서의 교훈, 그리고 각 선택지가 가지고 올 수 있는 비용과 편익을 생각하지 않을 수 없다. 이러한 계산에 있어 과거의 경험이나 역사에게서 오는 일정한 생각의 틀, 문화와 완전히 단절될 수 없으므로, 전략문화가 국가의 안보전략적 행위에 가지는 역할을 무시할 수는 없다.

2. 사이버안보와 전략문화

전략문화가 하위문화 사이에서 담론적 경쟁을 통해 만들어진다는 점(Howlett and Glenn 2005)을 생각해 본다면, 전략문화가 안보전략적인 이익을 달성하는 데에 정당성을 만들어 행위에 도움을 줄 수도 있지만, 반대로 안보전략적 행위를 일관적으로 하지 못하게 만들 수도 있다. 세대의 변화에 따라서, 기술의 발전에 따라서, 때로는 그동안 경험하지 못했던 안보전략적 이슈가 등장함에 따라 특정한 하위문화, 기존의 전략문화와 부합하지 않는 문화가 나타나 합리적이라고 간주하던 특정 전략의 선택을 쉽게 하지 못하게 할 수도 있다. 더불어 이러한 변화무쌍한 전략문화의 성격은 타국의 전략문화를 제대로 파악하지 못하게 하여 안보전략적인 문제에 제대로

대응하게 하지 못할 수도 있다. 전략문화는 국가의 안보전략을 수립하고 이에 따라서 행동하는 데에 기초가 되기 때문에, 이슈의 안보화과정에서부터 작동하며 사회에서 납득할 수 있는 방식으로 움직인다. 안정된 사회가 지속되면서 역사는 축적되는 과정에서 전략문화도 국가의 안보전략적 경험을 반영하게 된다. 따라서 사이버 공간에서의 안보와 같이 새로운 이슈가 등장하고, 기존 공간에서의 일반적인 안보행위와 관련한 요소와 다른 외부적인 요소가 등장한다고 해서 일정 기간을 통해 만들어진 전략문화가 급격하게 변화할 것으로 생각할 수는 없다. 다만, 사이버공간의 안보전략적 구성요소를 전통적차원의 안보와 얼마나 연결지어 생각해 볼 수 있는가의 여부는 각 국가행위자마다 다르게 개념화할 수 있으며, 연속성의 정도에 따라서 기존의 전략문화를 얼마나 적용할 수 있는가의 차원도 달라지게 될 것이다.

여기에서 사이버공간이 가지는 물리적 공간과의 안보전략적인 연속성과 단절성이 전략문화와 사이버안보를 생각하는 데에 중요하게 작동한다는 점을 생각해 볼 수 있다. 과연 물리적 공간에서 국가행위자의 안보전략 수립과 안보전략적 행위에 대한 선호를 그 국가의 전략문화를 통해서 설명하려는 시도를 사이버공간에도 그대로 국가 행위자의 행동 설명에 적용할 수 있을까? 각 국가가 사이버공간을 국가안보의 공간으로 어떻게 인식하느냐의 정도의 차원에 달려 있지만, 사이버공간이 물리적 공간과 완전히 단절된 것도, 완전히 연결된 것도 아닌 모호한 상태로 존재한다는 점을 생각해 보았을 때, 국가행위자의 사이버공간에서의 안보전략적 위협인식과 그러한 위협인식에 따르는 대응의 선택에 있어 안보전략문화의 구성은 어느정도 영향을 주고 있다고 할 수 있다. 그렇다면 질문은 다시 안보와 전략문화의 관계로 돌아간다. 사이버공간에서의 국가의 행위에 영향을 미치는 요인으로 해당 국가가 가지는 전략문화를 어디에 위치시켜야 할 것인가? 앞에서부터 언급했듯, 전략문화는 논리적으로 다소 일관적이지 못하고, 여전히 모호하게 정의되고 있지만, 사이버공간의 안보를 구성하는 국가행위자의 프레임워크와 행위의 선호를 설명하는 데에 맥락을 제공하는 도구로 사용할 수 있다.

사이버공간에서의 국가의 안보전략적 행위와 선호를 설명하는 전략문화를 구성하는 요소로는 여러 가지를 들 수 있겠지만, 크게 나누어보아 국가의 속성적 요인, 해당국가가 가지는 정치군사적 요인, 사회문화적 요인과 함께 전 세계를 아우르는 규범적 요인의 네 가지로 나누어 볼 수 있다. 이러한 요인들 모두, 또는 몇가지 중요한 요인의 선택, 때로는 필요한 요인들의 연결을 통해 사이버공간에 대한 전략문화가 다양하게 구성된다.

우선, 국가의 지정학적 요인, 자원과 기술의 발전, 세대변화의 양상과 같은 속성적 요인들은 국가의 전략적 사고와 행위를 형성하는 핵심적인 요인이자 전략문화를 이루는 중요한 원천이다. 그러나 사이버공간에까지 물리적 공간의 지정학적 요인을 적용하는 것은 무리가 있을 수 있다. 그럼에도 살펴보아야 하는 이유는 전략문화의 틀 자체가 어떻게 형성되어 있는가를 살펴보기 위해서 해당 국가가 가지는 안보전략적 상황인식에서 지정학적 위치가 중요하게 작동하는 요소이기 때문이다. 또한, 국가행위자의 전략적 선택지를 구성하는 사이버력에 대한 인식의 정도와 함께, 전략문화가 주로 형성되는 시기에 대한 분석의 시간적 범위의 설정도 필요하다. 이 중에 중요하게 생각해야 할 것은 사이버력을 만들어내는 기술의 발전 양상과 사회에서 사이버공간에서의 국가 행위를 가능하게 하는 기술을 받아들이는 정도라고 할 수 있으며, 시간범위의 설정에 있어서도 각 하위문화의 경쟁의 양상이 다르게 나타나고 사이버공간의 특수성이 나타날 수 있는 부분이기 때문에 관심있게 지켜보아야 한다.

두 번째는 역사적 경험, 국가의 국민성, 레짐이나 군사조직으로 나타나는 정치군사적인 요인이다. 국가의 안정적인 체제가 형성되어 있지 않은 상황에서는 전략문화에 기인하는 사이버 공간에서의 국가의 정체성 자체가 흔들릴 가능성이 있다. 국가가 경험하는 독특한 역사적 경험은 국가

를 구성하는 국민들의 성격, 생각의 틀 등을 구성하는 데에 중요한 역할을 한다. 국민성이나 정체성은 같은 안보전략적 이슈에 대해서 국가들이 다르게 받아들이게 하는 요인으로 작동한다. 같은 정보라도 어떻게 처리하느냐에 따라서 합리적, 이성적으로 받아들일 수도 있고, 실제로는 그렇지 않더라도 합리적, 이성적으로 포장되어서 생각될 수도 있다. 또한 한 국가가 가지는 군사조직적 차원도 중요하다. 하나의 위계적인 사회에서 만들어지는 문화와 여러 경쟁하는 하위문화에서 나타나는 전략문화는 다르게 나타날 수밖에 없기 때문이다. 특히 사이버공간과 관련해서, 안보군사부문을 군사조직이 전적으로 담당하고 있는가, 아니면 민-군의 유기적인 연결을 통해 대응하려 하는가의 차이는 국가행위자의 사이버공간에서의 안보전략 선호에 크게 영향을 준다고 할 수 있다.

세 번째는 신화나 상징물, 군사전략적 고전으로 볼 수 있는 사회문화적 요인이다. 신화나 상징물은 문화의 구성에 있어 중요하며, 특정 행위자의 정체성이 구성되고, 때에 따라서는 변화하게 하는 요소로 작용할 수 있다. 특히 신화는 근본이 되는 신념의 실체로서, 정치적인 가치를 가지는 이념을 극적으로 표현한다. 물론 정치적 신화는 진실일 수도 거짓일 수도 있지만, 그것의 논리를 따지기보다, 문화를 구성하는 일종의 믿음이나 신념으로 보아야 한다. 또한 전략문화연구에서 군사전략적 고전은 주된 소재가 된다. 예를 들어 중국의 전략문화로서 손자병법이나, 근대유럽 전략문화의 근원으로 펠로폰네소스 전쟁사나 전쟁론을 살펴본다든지, 북한의 전략문화를 살펴보기 위해서 김일성의 주체사상을 파헤치는 것이다. 그러나 사이버공간의 전략문화에까지 이러한 고전들이 얼마나 영향을 주는지에 대해서는 재고의 가치가 있다.

마지막으로 사이버 공간을 규율하는 초국가적인 규범도 전략문화의 근원으로 생각해 볼 수 있다. 초국가적 규범은 군사혁신의 목적과 가능성을 규정하고, 특정한 무력 사용과 관련한 지침을 제공할 수 있다(Terriff 2002). 초국가적 규범은 정치적 동원을 통해서 대상이 되는 행위자로 하여금 새로운 규범을 수용하도록 압력을 가하거나, 사회적 학습을 통해서 자발적으로 수용하도록 함으로써 전략문화로 나타날 수 있다. 시간의 흐름에 따라서 규범의 이식과정은 점진적인 수용의 모습으로 나타나게 되고 초국가적 규범과 국가가 고유하게 가지는 규범이 문화적으로 결합한다. 이러한 맥락에서 현재 사이버공간을 둘러싸고 벌어지고 있는 각 국가의 질서 확립을 위한 경쟁의 모습은 전략문화 구성의 차원에서도 중요하게 작동한다. 질서가 어떠한 방향으로 만들어지느냐에 따라서 사이버공간에서의 국가의 행위에 대한 정당성을 구성할 수 있게 되고, 사이버력을 늘리기 위한 각 국가 행위의 틀도 마련되기 때문이다.

이렇게 살펴볼 수 있는 전략문화를 기반으로 국가의 사이버공간에서의 안보전략 행위, 그리고 선호를 살펴볼 수 있는 대상은 크게 보아 선언적 전략, 사이버공간의 안보관련 기술발전, 그리고 국가 조직구조로 나눌 수 있다. 우선 선언적 전략은 국가 지도자나 안보전략 전문가의 공식적, 비공식적 발언이나 정부의 공식적 문건에서 찾아볼 수 있는데, 전략문화의 2세대 연구자들이 지적하고 있는 것처럼 선언적 전략과 실제로 운영되는 전략에는 차이가 있을 수 있다. 그러나 운영전략이 선언적 전략과 크게 다르지 않게 작동한다면, 그만큼 전략문화가 더 크게 작용한다는 강력한 근거가 될 수 있다. 선언적 전략안에서 전략문화에 영향을 받는 부분은 국가에서의 힘의 역할에 대한 인식, 적과 사이버 위협에 대한 본질 인식으로 생각해 볼 수 있다. 두 번째로는 기술이다. 사이버공간에서의 안보전략적 이슈에 대응하기 위해서 국가가 공격적, 또는 방어적 행위를 하는 데에 필요한 기술을 어떻게 발전시키고 있는가를 본다. 만일, 국가가 사이버공간에서의 안보전략적 행위를 하기 위해서 사이버력을 행사할 수 있는 기술을 새롭게, 또는 기존에 존재하는 기술을 사용한다면, 이러한 기술이 사용되는 방식은 해당하는 국가의 전략문화에서 만들어지는 선호에 따를 수 있다. 기술의 선호는 기술로서 만들어지는 사이버력을 사용하는 효과성에 대

한 인식으로 나타난다. 마지막으로 조직구조를 살펴봄으로써 국가의 사이버안보를 파악할 수 있다. 사이버안보를 국가의 어떠한 조직에서 주로 관장하고 있는지를 살펴보는 것은 그 안에 국가가 어떠한 의도를 가지고 사이버력을 행사하려고 하는지, 여러 가지 선택지 중에 어떠한 선호에서 우선순위를 설정하고 있는지를 확인할 수 있다. 전략문화를 각 국가 조직들이 가지고 있는 하위문화의 경쟁으로 생각해볼 수 있다면, 정보부문, 외교부문, 국방부문이 사이버공간의 안보를 위해서 얼마나 조직적으로 결합해 있는지를 살펴봄으로써 전략문화가 국가의 특정 안보적 행위를 끌어내는 연결고리를 살펴볼 수 있게 될 것이다. 이는 사이버력을 행사하는 데 있어서 법적 체계가 어떻게 되어 있는지, 민간 행위자들을 국가의 안보를 위해서 어떻게 참여시킬 수 있는지에 대한 방법들로 찾아볼 수 있다.

3. 사이버 전략문화의 한계

전략문화를 통해 사이버공간의 안보를 이해하기 위한 시도는 그동안 현실주의적 이론에 입각한 접근방법과 다른 모습을 가진다. 다시 말해서 국제정치학에서 안보연구는 실증적, 과학적인 접근방식을 취하고 있는 반면에, 전략문화 연구는 선험적인 접근방식을 따른다. 현실주의의 미러이미징이 가지는 문제를 극복하기 위한 전략문화연구의 시도는 장점이자 단점으로 나타난다. 전통적 안보연구는 사회과학적 연구방법론적인 차원에서 독립변수와 종속변수를 설정하고 이러한 변수들 사이의 인과관계를 규명하려는 소위 “과학적” 연구이기 때문에, 반증과 반론의 가능성을 항상 가지고 있다. 그러나 대부분의 전략문화연구는 과학적 연구의 변수 사이의 관계를 규명하려고 하기보다는, 역사적인 고증을 통해 나타나는 각 국가의 독특한 안보전략의 속성을 맥락화해서 분석하고 있으며, 이러한 연구방법론에는 과학적 반증 가능성이 없이 대안적인 설명이 되기 전까지는 보편적인 명제로서만 이해될 수밖에 없다. 따라서 검증하기가 어렵다는 문제를 가진다. 전략문화연구는 각 국가의 전략문화를 통시적인 하나의 개념으로 정의하기 위해서 고전이나 이념에서 찾아볼 수 있는 일종의 역사적 경험을 과잉일반화하려는 경향을 보인다. 예를 들어 중국의 전략문화를 유교적인 차원에서부터, 또는 손자병법에서부터 근원을 찾으려고 시도하는 한편, 일본을 사무라이 무사도에 입각한 전략문화로 과도하게 일반화해버리는 문제가 있을 수 있다. 더욱이 한 국가 내에서도 실제로는 여러 가지의 다른 전략문화로 구성될 수 있으므로 서로 상충하지만 비교하기 어려운 상대성의 문제를 피할 수 없다.

두 번째로 전략문화연구는 문화결정론의 한계를 가진다. 전통안보연구에서 국가의 전략적 선택은 여러 가능한 대안을 설정하고, 각 선택을 했을 때 나타날 수 있는 비용과 효과를 고려해서 이루어지는 행위자의 합리성을 가정하고 이루어진다. 그러나 전략문화연구에서는 전적으로 해당 국가의 과거 역사나 사회문화에 의해서 영향을 받기 때문에, 국가 안보전략적 행위에 대한 결정은 행위자의 의지나 합리적인 계산과 관계없이 문화적인 속성에 의해서 예정되어 있다. 마치 전략문화가 행위를 결정하는 것처럼 설명하게 된다는 것이다. 하지만, 전략문화가 행위를 추동하는 중요한 인과적인 요인으로 설명할 수는 있을지라도 다른 요인들을 통제한 상태에서 문화의 유무를 확인할 수 없으므로 전략문화를 독립변수로 설정하기는 어렵다(Gray 1999, 142). 따라서 중심 패러다임이 가지는 특징을 파악하고 특정 행위자가 가지는 물리적 요인들과 사이버공간에서 나타나는 안보전략적 이슈를 어떠한 방향으로 이끌 수 있는 요인으로, 다시 말해서 인과관계를 설정할 수 있는 독립변수로 보기보다 독립변수의 인과성에 영향을 줄 수 있는 매개변수나 개입변수로 생각해야 할 것이다.[5)]

마지막으로 전략문화연구에서 국가는 역사적이고 특수한 행위자로서 단일하지도 않고 합리적

이지도 않은 행위자이다. 보편적인 이론, 법칙을 찾기 어렵다는 것이다. 합리적인 행위자라면 과거의 역사적 경험과 무관하게 국가이익을 추구하기 때문에 동일한 상황에서 같은 안보전략적 선택을 할 것으로 예상할 수 있으나, 전략문화연구에서의 국가는 같은 속성을 가진 단일한 행위자가 아니며 서로 다른 전략문화를 가지고 있으므로 동일한 여건과 상황이라고 하더라도 다른 선택을 한다. 따라서 전략문화연구를 통해 국가의 사이버 안보전략적 선택에 대한 풍부한 설명은 될 수 있을지라도, 예측의 차원에서는 한계를 지닌다.

이와 같은 사이버 전략문화연구의 한계로 인해, 전략문화를 통해 사이버공간에서 국가행위자의 안보전략적 행위를 설명하는 데에 주의해야 할 점이 몇 가지 있다. 우선 전략문화가 만들어지고 특징으로 굳어지는데 중요한 시기를 조심스럽게 설정할 필요가 있다. 역사적으로 연구의 대상 시기가 어떻게 설정되는가에 따라 같은 국가행위자라도 다른 전략문화가 나타날 수 있기 때문이다. 예를 들어 중국의 경우, 역사 전체를 놓고 보면 유교사상에 입각한 소위 전쟁혐오의 전쟁관이 보편적인 것으로 나타날 수 있지만(박창희 2015), 공산혁명 이후로 시기를 한정하면 현실주의적 전략문화로 급격히 전환되는 것으로 파악될 수도 있다(박창희 2013b). 사이버 안보에 관해 이러한 문제는 더욱 복잡해지는데, 전략문화는 전통과 오래된 철학의 기반 아래에서 만들어지는 것이 보통이지만 고정되어 존재하지 않는다. 최근의 경험을 통해 사람들은 전략문화를 간주관적으로 규정하며, 이렇게 만들어진 전략문화는 다시 사람들의 생각을 특정한 방향으로 이끌게 된다. 더군다나 일국의 전략문화가 하위문화의 경쟁으로 나타나는 상황이라면 새로운 공간에서 나타나는 전통안보와는 다른 이슈와 연관한 전략문화는 기존 전략문화연구에서의 시간설정과는 다르게 되어야 할 것이다. 사이버안보와 관련해서 도메인에서 행동이 만들어내는 인과적 함수로서 전략문화를 검토하고, 전략문화가 다시 같은 도메인에서의 행동을 유발한다고 주장한다면 일종의 순환론적인 함정에 빠질 수 있다.

두 번째로, 전략문화의 분석수준에 따라 결과는 다르게 나타날 수 있다. 일반적으로 정치 사상적 수준에 초점을 맞추게 될 때 대부분의 국가는 전쟁을 혐오하는 문화를 가지지만, 군사 전략적 수준에 초점을 맞추면, 국가는 정치적 목적을 달성하기 위해서 군사력을 적극적으로 사용하는 모습을 보여주기도 한다(박창희 2013a). 중국의 경우, 전략문화를 정치 사상적 수준으로 분석하면 중국은 전쟁을 혐오하는 '공자-맹자' 패러다임을 가지게 되지만(Fairbank 1974), 군사 전략적 수준으로 무경칠서를 분석하면 중국도 서구와 별반 다르지 않은 전쟁 추구의 패러다임을 가지고 있는 것으로 나타난다(Johnston 1995b). 따라서, 전략문화의 연구에서 어떠한 분석수준을 설정하는 것이 해당하는 안보전략적 이슈를 설명하는 데에 더욱 설명력을 가질 수 있게 되는가의 선택이 중요하며, 역사적인 전략문화의 연속성을 이해하는 가운데에서도 새로운 환경의 도래에 따르는 전략문화의 변화 가능성도 항상 염두에 두어야 한다.

IV. 사이버 보안 문화[6)]

1. 사이버공간과 전통적보안관리

5) 물론 매개변수와 개입변수로 설정하게 될 때, 과연 독립변수는 어떻게 설정해야 할 것인가의 문제를 풀어내기 쉽지 않다는 한계를 가진다.

6) 앞의 장과 달리, 여기에서 보안이라는 단어를 사용하고 있지만, 이는 영어의 'security'를 다양한 주체, 공간, 주제에 적용하면서 나오는 차이에 불과하다.

사이버공격이 지능화, 고도화되면서 우리는 매일 새로운 사이버 보안 위협에 직면하고 있다. OpenAI가 2022년 말에 출시한 ChatGPT는 자연어 처리 기반 대화형 인공지능 서비스로서 대중의 관심을 세계적으로 얻었다. 하지만 ChatGPT가 사이버 범죄에 이용될 수 있다는 주장이 제기되었다. 자연어의 학습 과정에서 개인정보나 조직에 민감한 데이터가 유출될 수 있다는 것이다. 또한 인공지능을 이용해서 기업이나 국가조직의 네트워크 취약점을 식별하고, 실제로 데이터를 탈취하거나 랜섬웨어 공격에 필요한 악성코드를 제작하거나(최은희 2022), 다크웹 플랫폼을 새롭게 만들 수 있는 코드를 생성할 수 있었다(Check Point Research 2023). 최근에는 암호화폐 거래나 스마트 계약을 대상으로 하는 위협도 늘어나고 있다. 북한은 해커조직 '라자루스'를 필두로 스피어피싱이나 소프트웨어 취약점을 공격하는 등의 다양한 형태의 사이버공격을 이어가고 있는데, 최근에는 디파이 시장에서 블록체인 비디오 게임 '엑시 인피니티'와 블록체인 기술 기업 하모니의 '호라이즌 브리지'를 해킹하고 불법으로 확보한 자금을 이전하고 세탁하여 사용하고 있는 것으로 드러났다(U.S. Department of the Treasury 2023, 24). 한국은 초고속 인터넷 인프라가 잘 발달되어 있어서 공격의 경유지를 넘어 표적이 되는 사이버 위협이 지속적으로 증가하고 있다. 2023년 만 하더라도 중국 해커조직인 '샤오치잉(Xiaoqiying)'이 보안이 취약한 한국 학술연구기관 11곳을 공격하여 웹페이지의 화면을 변조하거나 데이터를 유출하여 개인정보가 공개되기도 했다(오현주 2023). 2023년 1월에는 LG유플러스가 사이버 공격을 당해 고객 29만여 명의 개인정보가 유출되었다. 조사 점검단에 따르면 네트워크 침입 차단 보안 시스템 부족, 보안 정책 미비, 정보보호책임자 등 보안관련 인력 부족 등 보안을 위한 대비태세가 총체적으로 부실했던 점이 원인으로 지적되었다(이혜선 2023).

기술적으로 취약성이 있는 시스템을 사용함으로써 사고가 발생하기보다 사람의 실수 또는 관리소홀로 인한 경우가 많아지고 있다. 조직의 전현직 직원, 협력업체 직원 등 내부 인프라 시스템에 접근 권한이 있는 내부인에 의해서 사회공학적 취약점을 통해 발생했다. 보안사고는 피해규모가 크다는 문제 뿐만 아니라 사고에 대한 대응이 늦어지면 질수록 피해가 기하급수적으로 증가한다는 특징을 가지고 있는데, 이렇게 내부 직원의 실수와 관리 소홀로 인한 사고는 피해 사실을 인지하는 데에 외부 공격으로 인한 보안사고에 비해 대응에 많은 시간이 걸릴 수밖에 없다. 왜냐하면 내부 직원에 의해서 인지하지 못한 채로 노출된 취약성은 사전에 예측하기도, 공격에 대비하기도 까다롭기 때문이다. 이는 단순하게 우리가 비밀번호에 대해서 어떻게 생각하고 있는지를 예로 들 수 있다. 인터넷 시대에 비밀번호는 정보보호를 위해서 필수적이다. 어떠한 사이트, 어떠한 시스템을 이용하든지 간에 매번 비밀번호를 설정해야 한다는 것은 번거로운 일이고, 여러 가지의 계정을 사용함에 따라 더욱 복잡해지는 비밀번호를 모두 기억하는 것은 귀찮을 수밖에 없다. 따라서 모든 계정의 비밀번호를 동일하게 설정하거나, 다르게 설정하더라도 아이디와 비밀번호를 암기하지 않고 수첩이나 지갑에 수기로 기재하거나 문서로 저장하고 사용한다(한국인터넷진흥원 2020, 45). 개인에 대한 사이버공격이 기업 및 사회조직에 대한 해킹 공격으로 이어질 수 있는 부분이 바로 여기에 존재하는 것이다.

4차 산업혁명 시대에 정보통신 기술이 발전하고 사회적, 경제적 의존도가 높아지면서 사이버 보안 문제가 커졌고, 각 사회경제적 조직은 편리한 기술을 넓게 사용하기에 앞서서 기술이 야기할 수 있는 보안에 대한 중요성을 인식하고 그 관리대책을 수립하고 있다. 보안정책을 통한 안전관리는 조직의 정보와 정보처리과정을 보호하기 위한 예방 장치이므로 일관성 있는 관리기준, 절차 등을 수립하고 조직원으로 하여금 준수하도록 하여야 한다. 이러한 보안관리정책은 현재 조직이 사용하고 있는 상대적인 보안의 수준을 측정하고, 조직이 보유하고 처리하는 정보를 보호하는 데 관련되는 필수적 법적 요구사항을 따르는 것으로 정보보안의 안전성을 담보하기 위한 기

술적, 관리적, 물리적 차원의 보호대책으로 이루어져 있다. 정보에 대한 위협은 여러 가지의 형태로 나타날 수 있지만 일반적으로 위협으로부터 무엇을 안전하게 만들어야 하는지에 대해 넓은 보안관리의 목표로서 기밀성, 무결성, 가용성의 3요소(CIA triad; Confidentiality, Integrity, and Availability)로 인식되어 있다(Samonas 2014).

이러한 전통적보안관리의 방법은 기술적, 통제적, 정책적 체계로서 위로부터 내려오는 하방방식의 체계이다. 문제는 아무리 촘촘한 관리체계를 만들고 이를 엄격하게 적용한다고 해도 개개인이 따르지 않는다면 어딘가에는 취약점이 생긴다는 것이다. 다시 말해서 인간이 자발적으로 따를 수 있는 보안문화를 정립하지 않고 통제만을 요구하는 것은 한계가 있다. 우선 전통적인 보안관리방식은 사이버 보안 위협과 사고가 발생할 때 이에 대한 사후적 대응의 차원으로 더욱 강력한 통제 관리체계를 조직에 요구한다. 그러나 인간은 정보보안을 위해 설정된 여러 가지의 귀찮은 단계를 거치면서까지 생산적인 일을 하기보다는 어떻게든지 더욱 일을 쉽게 하도록 우회 경로를 찾게 된다. 악의적인 이유를 가지고 보안정책을 우회하기 위해서 고의로 승인되지 않은 프로그램을 사용하는 것이 아니다. 오히려 자신의 업무 성과를 높이고 업무를 더 쉽게 처리하기 위해서 우회의 방법을 이용한다. 또한 사이버 위협이 될 수 있는 방식과 요소들이 다양화되면서 조직 전체를 통제할 가능성이 떨어지고 있으나, 대응은 더욱 구체적인 보안대책의 마련이고 정책으로 대표되는 일종의 통제를 강조한다. 제로 트러스트 등의 정보보안 대책은 기본적으로 의심을 기반으로 예상되는 위험을 사전부터 통제하고자 하는 성향을 지니고 있으며, 잠재적인 위험요소를 통제하기 위해 일반의 자연스러운 행위를 매끄럽지 못하게 만든다. 대책은 언제나 마련되지만 대다수는 보안정책을 따라야 하는 것으로 생각하기보다 귀찮다는 인식을 가진다는 것이다. 사이버 공간에서 나타날 수 있는 소수의 악의적인 행동을 기반으로 하고, 대책은 정부를 중심으로 관료주의적으로 시행되기 때문에 관리 및 준수에 대한 모니터링에 들어가는 비용이 많이 들어서 더욱 커지고 있는 디지털경제의 혁신성, 유연성을 저해하게 된다는 문제점을 가진다(김정덕 2022).

2. 인간중심의 보안문화 형성

앞에서 살펴볼 수 있듯이 사이버공간의 정보보안을 위해서 조직보다는 결국 사람의 자발적인 움직임이 필요하다는 것을 알 수 있었다. 전통적보안관리 체계와 달리 인간이 중심이 되는 보안전략은 엄격한 정책의 하달과 준수로 안전을 만들어내는 것이 아니라 보안 문화를 형성함으로써 인간의 행동을 적절하게 움직이게 할 수 있다는 것을 인식하는 데에서 출발한다. 조직이론, 산업보안 전문가들은 특정 조직이 가지고 있는 보안에 대한 인식 수준과 조직원들이 따르는 실제 행동에 따라서 문화가 형성될 수 있으며, 문화에 대한 이해와 진단을 바탕으로 조직이 처한 보안환경과 잠재적인 위협상황에 적절하게 조직원의 일상을 관리할 수 있는 보안정책을 수립해야 한다고 지적한다(Van Niekerk and Solms 2010).

사이버공간에서의 정보안전에 대한 위협에 대처하기 위해서 이에 맞는 보안문화를 형성시킬 수 있어야 한다는 명제는 바로 인간이 중심에 있는 보안개념으로 연결된다. 인간중심보안 전략은 잠재적인 위험을 미리부터 통제하고자 하는 불가능한 목표를 세우지 않는다. 반대로 회복탄력성을 기반으로 가시화된 위험을 받아들이고 인간의 인식과 이해를 통해 행동을 교정하는데에 중심목표가 있다. 이는 위험에 집중한 대응이기 때문에 선의를 가지는 대다수의 일반에게 영향을 끼치지 않으며, 오히려 보안관리가 일에 있어서 귀찮은 단계를 더하기보다는 필요한 단계를 거치는 것이라는 인식을 심어줄 수 있다. 모범사례를 기반으로 하고 있어서 정보안전이라는 목표를 지속적이고 효과적으로 달성하는 데에 도움을 줄 수 있다. 개개인이 받아들일 수 있는 문화를 형성

하는 과정에서 신념, 행위, 생각의 틀이 작동하기 때문에 조직원들의 행동을 위에서부터 관리해야 하는 비용이 들지 않으며 사이버공간과 디지털경제의 혁신성과 유연성을 적극적으로 이용할 수 있다는 장점이 있다(김정덕 2022).

문화는 인간의 행동에 영향을 주는데, 특히 불확실한 상황에서 특정하게 생각, 행동하게 하는 틀을 제시할 수 있고 사회조직, 국가에서 형성되는 문화는 일반적으로 한순간에 주어지는 것이 아니라 개개인의 상호작용과 역사적 경험에 따라서 만들어지기 때문에 시간에 따라서 변화하는 역동성을 가진다. 공동체의 문화는 구성원들이 공유하는 가치판단의 틀로서 행동에 영향을 주는 핵심가치가 되며, 환경의 특성과 개인의 행동 사이의 관계를 설정하고 때로는 조정할 수 있기 때문에 행동을 결정하는 데에 중요한 역할을 한다(Chang and Lin 2007). 그러나 문화를 특징짓는 것은 쉽지 않은 일이다. 공동체의 문화는 복합적이고 포괄적이며 애매한 요인들로 이루어져 있고, 그 성격상 구성원들이 당연하게 여기는 가치에 근거하기 때문에 도전받지 않고서는 자각되기 어려우며 객관적으로 평가하기는 더더욱 어렵다(Cameron and Freeman 1991, 25).

경영조직학에서는 조직의 문화를 진단하고 분석하기 위해서 경쟁가치모형 (Competing Value Model)을 제시하였다. 일반적인 조직문화유형을 신축성/역동성과 안정성/통제, 내부지향성과 외부지향성을 기반으로 네 가지 유형, 다시 말해서 관계지향문화, 혁신지향문화, 위계지향문화, 시장지향문화로 구분한다. 각각의 조직문화는 조직원의 목표와 행동에 영향을 미치므로 특성에 맞는 문화를 형성하고 개개인의 행동에 영향을 주기 위한 노력을 하는 것이 필요하다(Cameron and Quinn 2011, 38-51). 이를 정보보안과 관련해서 적용해 본다면 조직에서의 보안통제의 정도(자율/통제)와 보안전략이 가지고 있는 주요한 초점(내부적/외부적)으로 설정하고 보안문화를 네가지 유형으로 구분할 수 있을 것이다. 우선 자율을 중심으로 하는 보안행위와 내부적 가치를 중시하는 신뢰 중심의 보안문화는 조직원에게 인간 관계를 기반으로 공동체에 대한 몰입을 높이고, 느슨한 통제와 외부적 가치를 중시하는 자율 중심의 보안문화는 역동적, 진취적이기 때문에 개인은 위험을 감수하려는 성향을 보이며, 유연성과 혁신과 같은 디지털 경제에서의 효율성을 높이고 회복탄력성을 갖춘 체계의 구축을 강조한다. 위로부터의 강력한 통제와 내부적 가치를 중시하는 프로세스 중심의 보안문화는 결과 중심적이기 때문에 업적이나 목표의 달성을 중점적으로 고려하며, 표준화된 보안절차를 강조해서 안정적이고 가시적인 보안활동을 중시한다. 마지막으로 강력한 통제를 기반으로 하는 보안행위와 외부위협에 대한 대응으로서 주어진 보안정책을 중시하는 준수 중심의 보안문화는 조직원의 행동을 통제적으로 구조화하여 이에 맞는 행동을 요구하기 때문에 법규 준거성, 반복 가능성, 정책의 문서화를 통한 외부감사나 대응활동을 강조한다(김정덕 2022). 각 조직마다 현재의 상태를 파악하기 위해서 이러한 요인들을 면밀하게 분석할 수 있고, 그래야 인간중심의 보안문화를 형성하기 위한 조직적인 움직임을 만들어내어 이에 맞는 보안관리체계를 적용할 수 있다. 좋은 전략과 계획도 구성원들의 문화와 연계되지 않으면 실효성을 거두기 어렵기 때문이다.

조직의 보안문화를 진단하고 그에 맞는 정보보안정책을 마련하는 것에 앞서, 보안문화 변화를 만들어내기 위한 목표도 설정할 필요가 있다. 인간중심의 보안관점에서 중요한 조직의 가치는 구성원간의 신뢰라 할 수 있다. 신뢰가 높은 조직은 위험도가 높은 상황에서도 오히려 낮은 사고발생률과 사고 이후 회복이 빠른 점에 착안한 '고 신뢰조직(high-reliability organization)'의 개념을 보안영역에 적용해서 보안사고에 대한 대응 능력을 높이고 인간중심의 보안문화를 구축하기 위한 방안을 생각해 볼 수 있다(Hayden 2016, 203). 헤이든의 보안 FORCE 행위 모델에 따르면 인간중심의 신뢰도가 높은 보안정책을 구축하기 위해서 다섯가지의 가치(FORCE; Failure, Operation, Resilience, Complexity, Expertise)가 반영된 행위를 수행함으로써 보안문

화를 형성, 변화시킬 수 있다.

첫 번째는 실패이다. 실패는 인간이 만들어내는 고도화되고 복잡한 기술 혁신에도 불구하고 모든 실패, 또는 실수로 이루어지는 사고를 완벽하게 통제할 수는 없다는 전제에서 출발한다. 그렇다면 실패를 통해 무엇을 어떻게 교훈으로 삼을 수 있는지, 현재의 정보보안을 위한 조치에서 부족한 점은 무엇인지, 앞으로의 예상치 못한 사고에 대해서 어떻게 유연하게 대처할 수 있을 것인지에 대한 준비가 필요하다. 실패를 받아들이지 못하는 문화보다는 실패를 두려워하지 않고 적극적으로 받아들임으로써 시나리오를 개발하고 문제와 취약점을 미리 적극적으로 탐지할 수 있는 행동을 장려하며 이전에 발생했던 사고를 분석하여 다시 발생하지 않도록 하는 체계를 구축하는 것을 중요하게 생각한다(Hayden 2016, 210).

두 번째는 운영이다. 보안 사고에 대한 매뉴얼은 어떠한 조직이든 가지고 있지만, 실제로 일어나는 상황과 매뉴얼에서 예측하는 것은 다를 수 밖에 없다. 그렇다면 매뉴얼에 따라서 사전에 예측된 상황대로 보안업무를 따르는 소극적인 운영을 하기 보다 한 단계 더 나아간 적극적인 모니터링을 해서 보안위협과 사고의 위험을 빠르게 탐지해 낼 수 있다. 이를 위해서는 현재의 상황을 투명하게 평가하고 공동체 전체가 받아들일 수 있도록 결과를 공유하는 것이 필요하다(Hayden 2016, 210).

세 번째는 회복탄력성이다. 어떻게 조직이 보안사고에 대응하느냐의 문제는 보안시스템이 실패하는가 또는 언제 실패하는가의 문제만큼이나 중요하다. 사고는 피할 수 없지만 사고에 의해서 대응되는 시스템이 마비되는 경우는 막을 수 있다. 회복탄력성은 사고에 대한 예방보다는 실제로 사고가 발생했을 때에 빠르게 탐지하고 이를 복구해내는 능력을 제고하는 것을 의미한다. 정보보안에 대한 교육이나 모범사례를 공유하는 것이 회복탄력성을 만들어내기 위한 방법으로 사용될 수 있다(Hayden 2016, 210-211).

네 번째는 복잡성이다. 실제로 나타나는 보안위협은 단순하지 않다. 복잡한 환경과 위협은 이에 대응하기 위한 효과적인 의사결정을 내리는 데에 어려움을 겪게 하는 데, 대부분 문제는 복잡한 문제에 단순화된 모델을 적용하고 있기 때문이다. 지나친 일반화는 대응할 수 없는 사각지대를 만들어 잘못된 해결책을 결정하거나, 부분적으로만 해결하려는 우를 범하게 할 가능성이 있다. 따라서 복잡성에서 파생되는 보안의 가치는 보안사고 이면에 존재하는 잠재적이고 복합적인 원인을 파악하고 이에 대응하는 관리 조직적 측면 모두를 복합적으로 다룰 수 있어야 한다(Hayden 2016, 211).

마지막으로 전문성이다. 보안 전문가와 네트워크를 형성해야 한다. 정보 보안에 대한 전문지식을 항상 위계를 가진 사람이 가질 수 있는 것은 아니며, 이는 인간중심 보안문화의 민주성을 위해서도 바람직하지 않다. 오히려 경직된 명령 체계와 계층적 권력 구조는 위기의 상황에서 효과적인 운영을 방해할 수 있다. 조직 내에서 의사결정 권한을 분산하여 효율성과 영향력을 극대화하고, 새로운 위협에 대응하는 데에 가장 적합하게 대응하고 조치를 취할 수 있도록 신뢰와 협력을 기반으로 유연한 배치가 필요하다(Hayden 2016, 211).

3. 미래 디지털/사이버 문명을 향한 인간 중심의 가치

앞 절의 인간중심 문화 논의에서 국가 차원의 안전/보안/안보, 그리고 사회조직을 넘어 국가 차원의 문화는 빠져 있다. 국가는 인간중심의 안보문화와 관련해서 아무런 관련도 없다는 의미는 아니다. 각 국가는 '건전한' 사이버 문화를 정착하는 데에 필요한 가치를 들고 사이버안보와 관련해 세계적으로 자신이 지향하는 질서를 정착시키고자 한다. 이 절에서는 이러한 국가들의 논의가

어떻게 진행되고 있는가를 살펴보고, 인간중심의 사이버안보 질서와 연관 지어 생각해 보고자 한다.

문화를 창출한다는 말은 작은 공동체에서 가능한 일일지도 모르지만, 국가적 차원에서는 쉽지 않으며, 가능하다고 할지라도 자국이 발전시킨 문화를 국가를 넘어 전체 사이버 공간을 아우르는 문화로까지 발전시킨다는 것은 그 말의 어색함 만큼 어렵다. 그래서 각 국가는 사이버 공간의 이상적인 방향을 상정하는 데에 머무르고 있다. 이는 사이버 공간의 특성, 즉 물리적 공간과 완벽히 단절된 공간도 아니고, 물리적 공간과 완벽히 연결된 지정학적 공간도 아닌 복합적인 성격을 지닌다는 점과 함께, 각자 정보에 대해서 가지는 관념의 상이성 때문에 나타나는 현상이기도 하다. 각 국가는 사이버 공간을 인식하고 사용하는 데에, 전통적인 차원의 지정학적 공간으로 인식하는 것에서부터, 사이버 공간으로서 새롭게 나타나는 특성을 최대한 이용할 수 있는 방향으로 인식하는 데에까지 다양한 수준의 모습을 가진다.

따라서 사이버 공간에 대한 대부분의 국제적 논의는 사이버안보와 관련한 국제질서를 어떻게 마련할 수 있을 것인가의 문제에 치중해 있다. 문화와 관련해서 사이버 공간의 질서는 크게 미국과 유럽으로 대표되는 서구의 버전과 중국으로 대표되는 버전으로 나누어 볼 수 있다. 세계사이버공간총회는 주로 사이버 테러나 공격을 받아 피해를 받을만한 인프라를 가진 국가들이 참여해서 안보 의제를 논의하기 위해서 2011년부터 정기적으로 모인다. 참여국은 사이버안보, 안전, 자유와 프라이버시와 함께 사이버안보에 대한 인식과 문화의 의제를 포괄적으로 다룬다. 세계사이버공간총회는 참여국들의 구체적인 이익이 걸려 있는 안보의 문제를 가지고 실효성 있는 방안을 도출하고자 하고 있지만(김상배 2013, 90), 2020년 미국의 클린 네트워크 구상으로 시작된 동맹 네트워크를 구성하는 가치와, 유럽이 상정하는 네트워크를 위한 가치가 달라지면서 서방 안에서도 사이버 공간, 특히 인터넷의 미래가 분할될 가능성을 보이고 있다. 미국의 경우 국가안보와 범죄예방 등의 건전한 사이버 환경 구축을 위한 노력에 초점을 맞추고 있는 반면에, 유럽의 경우 개인의 프라이버시와 개인정보 보호를 강조하는 방향으로 가치를 맞추고 있다(김상배 2021b, 70).

중국은 디지털 권위주의 모델에서의 통제의 가치, 사이버 주권을 강조한다. 자국 영토 내 인터넷을 통제하는 이러한 주권의 원칙은 정보의 중립성, 자유로운 정보의 흐름을 강조하는 사이버 공간에서의 정보의 기본 원리와 상충하지만, 중국은 각 국가가 독립적으로 사이버 공간을 규제하고, 인터넷 정책을 가지면서 권리와 문화를 구축하는 방향을 상정한다. 이 안에서 사이버 안보문화는 정보환경과 시민의 행동을 통제하는 정부의 권한을 강화하는 방향으로, 그리고 시민들에 대한 검열을 선제적으로 실시할 가능성을 위한 밑그림이다. 중국 네티즌들의 자기검열, 사회적 신용 시스템에 의한 감독, 상호감시의 문화는 정부에 대한 대항 담론이 형성되는 데에 사전 차단의 효과를 가지며, 권위주의적 정권이 표방하는 가치와 규범을 강화하는 방향으로 이어질 수 있다. 중국의 디지털 실크로드 이니셔티브는 이러한 모델을 개발도상국에 전파해 확장되고 있다는 점에서 우려를 낳고 있다.

문화와 관련해서, 각 국가의 사이버 질서는 어떠한 가치를 그 중심에 두고 있는가의 차원으로 생각해 볼 수 있다. 그렇지만 여기에서도 빠져 있는 것이 있다. 바로 '인간'이라는 것이다. 국가의 사이버 공간 질서는 국가행위자 중심의 인식을 기반으로 한다. 국가를 기반으로 사이버안보를 인식하게 되면, 민주주의가 아닌 전체주의나 비자유주의적 레짐과도 맥을 같이 하게 되고, 많은 정부는 사이버안보의 긴급성 차원에서 검열, 감시, 사이버 스파이, 가짜뉴스, 표현의 자유에 대한 제한, 데이터에 대한 접근과 통제 등과 같은 문제에 적극적으로 움직이는 정당성을 만들어내기 위해 가치를 든다.

그러나 사실, 사이버안보와 사이버 질서의 수혜자는 국가가 아니라 인간이 되어야 한다. 사이버안보의 인간중심 가치를 생각해 본다면, 국제질서는 개인에게 이익이 되어야 하며, 주권국가는 이러한 자격의 대리자로 개념 지어 볼 수 있을 것이다. 국가에 사이버안보를 관할하는 독점적 권리를 준다면, 공공의 영역과 민간의 영역이 분리되어 공공영역에만 통제되지 않은 규율 권력을 주게 됨으로써 실제로 사이버 공간을 구성하고 사용하는 일반 대중, 즉 개인과 분리되는 문제를 가져올 수 있다. 즉, 사이버안보를 지정학적, 전통안보적 차원과 연관해서 보면서 인간중심의 가치는 그 중요성의 차원에서 뒤로 밀려나 규율을 받아야 하는 상황으로, 논의의 차원에서도 중심에서 벗어나 부차적인 것으로 다루어질 가능성이 있다는 문제를 가진다는 것이다.

한국정부는 2023년 9월에 디지털 공동번영사회를 위한 디지털 권리장전을 발표했다. 디지털 권리장전은 디지털 시대에 맞는 국가적 차원의 기준과 원칙과 함께 글로벌 디지털 질서 규범의 기본방향을 담은 것으로서 인간의 보편적 권리로 보장할 수 있는 디지털 규범의 형성에 앞장서겠다는 의지를 보여주고 있다(박수형 2023). 한국은 새로운 디지털/사이버 공간에서의 문화를 기반으로 새로운 문명을 준비하는 과정에서 국가가 어떠한 역할을 할 수 있을지의 고민을 기반으로 권리장전을 선언하게 되었다고 평가해 볼 수 있다. 물론 선언으로 실제적인 결과를 만들어 낼 수 있을지의 여부, 다시 말해서 앞으로 국제 사회에서 인간 중심의 디지털 문화 형성과 안보적 차원에서 이해당사자들의 관리체계를 효과적으로 만들 수 있을지의 넘어야 할 산이 있다. 그러나 사이버 공간의 안보/보안의 문제는 수혜자로서 인간을 중심으로 하는 논의를 거쳐 새로운 디지털 문명/문화의 창발, 실질적으로는 안보를 넘어 사이버 평화로까지 나아갈 수도 있는 실마리를 제공할 수 있다는 점에서 의미가 있다.

단순히 인간이 중심이 되는 사이버 공간에서의 가치와 행동 원칙을 명시하고, 선언하는 것만으로 현재 벌어지는 사이버 공간에서의 패권 경쟁의 양상, 경쟁 우위의 상황이 바로 바뀌지는 않을 것으로 보인다. 그만큼 국가 또는 진영 사이의 경쟁이 복잡하고 치열하게 벌어지고 있기 때문이다. 하지만 인간 중심의 사이버안보를 만들기 위한 조그마한 움직임은 이해당사자들이 모두 참여하고, 자신들의 이익 이상의 관점에서 각자의 가치들이 인간을 향해 갈 수 있도록 정당화하는 데에 첫걸음이 될 수는 있을 것이다. 또한 점점 압축되어가고 복잡해지는 사이버 공간에서 인간의 권리가 보호되는 공통의 환경을 어떻게 만들어낼 수 있는지에 대한 집단적인 관심을 이끌어내는 데에 도움이 될 수 있을 것이다. 경쟁에서도 모두가 잊지 않아야 할 것은 중심에 인간이 있어야 한다는 것, 그리고 그 안에 더욱 중요한 것은 합의된 질서와 디지털 공간에서 창발할 수 있는 문명을 만드는 차원에서 문화가 조성되어야 한다는 것이다.

V. 결론

이 글은 새롭게 나타나는 사이버 공간의 안보를 문화의 렌즈를 통해 살펴보았고, 세 가지의 양상을 발견할 수 있었다. 우선 서로 간에 연결될 것 같지 않아 보이던 두 영역이 기계적으로나마 만나 국제정치학적 문제를 만들어내는 모습은 비교적 최근에 나타나고 있으며, 한국의 사드 배치를 계기로 시작된 한류 문화콘텐츠에 대한 중국의 수입금지조치, 그리고 미국과 중국 사이의 틱톡을 둘러싼 공방의 모습에서 살펴볼 수 있다. 안보의 문제가 전통 군사적 차원에서만 벌어지는 것이 아니라, 여러 가지 다른 영역에서부터 촉발될 수 있다는 차원에서 이러한 예들을 단순히 우연적으로 발생한 사건으로만 생각할 수는 없다. 특히 문화는 다른 분야에 비해 비교적 안

보화되기 쉽고, 패권을 두고 다툼이 심해지는 상황에서 언제 어디에서 급작스레 나타날 수 있다는 가능성을 배제하기 쉽지 않다. 하지만 이 글이 강조한 것은 이러한 기계적 연결을 바로 사이버안보의 신흥안보적 차원으로 확장해서 생각할 수는 없다는 것이었다. 신흥안보의 이슈가 창발하기 위해서는 일종의 임계점을 지나야 하는데, 서로 다른 영역의 이슈가 연계되었다는 사실 만으로 임계점을 통과했다고 보기는 어렵기 때문이다.

두 번째로 이 글이 살펴본 문화와 안보의 연계는 국가의 사이버 안보전략적 행위를 전략문화를 통해서 설명하고자 하는 움직임이었다. 안보연구에서 국가의 행위를 설명하기 위해 전략문화를 주요한 원인으로 두려는 시도는 국가행위자가 합리적으로 동일한 성격을 가진다라는 국제정치학의 현실주의적 방법론을 벗어나고자 하는 차원에서 시작되었다. 군사안보의 공간으로서 사이버 공간이 가지는 물리적 공간과의 연속성과 단절성은 전략문화와 사이버안보를 생각하는 데에 중요하게 작동하며, 전략문화 자체가 논리적으로 일관적이지 않고 모호하게 정의되고 있을지라도 사이버안보를 구성하는 국가의 사이버력에 대한 인식과 행위의 선호를 설명하는 데에 중요한 도구로 사용될 수 있다. 그러나 전략문화연구가 가지는 비과학적 방법론의 한계를 그대로 이어받고 있다는 점에서 문제가 있으며, 사이버공간에서 나타나는 안보 이슈를 전적으로 결정하는 독립변수로 전략문화를 보기보다 독립변수의 인과적 영향력에 영향을 주는 맥락에서 작동하는 매개변수나 개입변수로서 전략문화를 다루어야 할 것이라는 점을 밝혔다.

세 번째, 이 글은 안보와 문화의 순서를 바꾸어 사이버안보로부터 만들어지는 문화의 양상을 살펴보았다. 다양한 사이버공격이 지속적으로 증가하면서 시스템의 취약성을 줄이고자 하는 기술적, 정책적 대응은 더욱 늘어나고 있지만, 그럼에도 인간의 실수 또는 관리소홀로 인한 사고로 인해 보다 넓은 차원의 대응을 필요로 하게 되었다. 하방방식의 전통적보안관리와 달리 인간중심의 보안문화형성을 통한 대응은 문화에 대한 이해와 적절한 진단을 통해 환경과 상황에 적절히 인간의 행동을 관리할 수 있는 아래로부터의 관리체계를 말한다. 통제보다 자율중심의 조직문화는 보안사고를 줄이고, 유연하게 대처하는 데 필요한 밑거름이 된다. 인간을 중심으로 하는 가치를 국가적 차원, 세계적 차원의 안보로 상정하게 되면, 인간이 궁극적인 안보의 수혜자가 되면서, 새로운 디지털 문명/문화를 만들어갈 가능성을 열어준다는 점에서 의미가 있다.

마지막으로 이 글의 연구 설계와 관련해서, 본 연구가 가지는 한계점과 향후 연구 방향성에 대해서 짧게나마 언급하고자 한다. 이 글은 문화와 안보라는 거대한 개념을 사이버 공간에서 어떻게 연결 지어볼 수 있을지에 대한 고민에서부터 시작되었다. 이러한 연결은 일종의 탐색적 목적으로 연역적으로 상정되었고, 현실에서 일어나는 사례들을 통해 뒷받침하고자 하였다. 따라서 어떠한 통합적인 분석 틀을 제시하는 데에까지는 미치지 못하고, 새로운 사례들과 그것을 설명할 수 있는 인과적 메커니즘을 향후 연구를 위해 제시하는 데에 그쳤다. 이 연구를 바탕으로 향후 연구에서는 과학적 연구방법론을 통해 사례들이 가지는 의미와 그것을 설명하는 관계의 분석적 검증이 이어져야 할 것이다.

〈참고문헌〉

김수한, 유다형, 2017 “사드 배치에 따른 한중 갈등 현황 및 전망,”『IN China Brief』Vo. 336, 인천발전연구원.

김휘정, 2017, “중국의 한한령(限韓令)과 문화콘텐츠산업의 과제,” 『이슈와 논점』제1264호, 국회입법조사처.

김규찬, 2017, “한국 문화콘텐츠산업 진흥정책의 내용과 성과,” 『언론정보연구』제50권 제1호, 서울대학교 언론정보연구소. pp. 276-309.

김민혁, 2020, ““90일내 틱톡 팔아라” 트럼프, 행정명령 서명,” 서울경제, 8월 15일. https://www.sedaily.com/NewsView/1Z6L83Z84V

김상배, 2007, “한류의 매력과 동아시아 문화네트워크,”『세계정치 7』제28집 1호, 봄·여름, pp. 193-233.

김상배, 2013, “사이버 공간의 글로벌 지식질서: 네트워크 이론으로 보는 구조와 동학의 이해,” 『국가전략』제19권 3호, pp. 75-109.

김상배, 2016, “신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해,” 『한국정치학회보』제50집 1호, 봄, pp. 75-104.

김상배, 2021a, “디지털 안보의 세계정치: 이론적 분석틀의 모색,” 김상배 엮음,『디지털 안보의 세계정치: 미중 패권경쟁 사이의 한국』, 파주: 한울아카데미. pp. 19-55.

김상배, 2021b, “디지털 플랫폼 경쟁의 국제정치경제: 미중 기술패권 경쟁의 진화,” 『국제·지역연구』30권 1호, 봄. pp. 41-76.

김정덕, 2022, “보안도 결국은 사람의 문제, 전략 앞서 문화부터 바꿔라,”『DBR』4월호. https://dbr.donga.com/article/view/1206/article_no/10429/ac/magazine

류설리, 2017, “한한령의 도전과 ‘포스트 한류’의 응전,”『한류스토리』, 4월호, 한국문화산업교류재단. pp. 12-16.

박민숙, 김영선, 2020, “중국「수출 금지·제한 기술목록」조정의 주요 내용 및 시사점,”『KIEP 세계경제 포커스』, 10월 20일 Vol. 3 No. 33. 세종: 대외경제정책연구원.

박수형, 2023, ““디지털 새 질서 주도”...정부, 디지털 권리장전 내놨다,”『ZDNET Korea』, 9월 25일. https://zdnet.co.kr/view/?no=20230925141057

박창희, 2013a, “제10장 전략문화,”『군사전략론: 국가대전략과 작전술의 원천』. 서울: 플래닛미디어. pp. 375-437.

박창희, 2013b, “중국의 공산혁명과 전략문화: ‘유교적 전략문화’에서 ‘현실주의적 전략문화’로의 이행,”『신아세아』2권 1호. pp. 95-123.

박창희, 2015, “중국의 유교적 전략문화: 공자-맹사 사상을 중심으로,”『민족연구』63호. pp. 36-57.

안창현, 2018, “한한령의 현상과 본질, 그리고 우리의 대안 모색,”『글로벌문화콘텐츠』제33호, pp. 113-131.

오현주, 2023, “中해커 ‘샤오치잉’ 국내 서버 5곳 추가 공격... 인터넷 진흥원 “해킹 경로 확인중”,”『뉴스 1』, 2월 15일. https://www.news1.kr/articles/4954257

우운택, 2020, “문화기술, 신한류의 날개,”『한류NOW』9+10월호 vol. 38, pp. 9-17.

윤정현, 2019, “신흥안보 거버넌스: 이론적 고찰과 대안적 분석틀의 모색,”『국가안보와 전략』제19권 3호, 가을, pp. 1-46.

이지한, 2018, “한류를 바라보는 두 개의 시선 - 한국의 문화산업과 중국의 문화안보,”『中國學』 제65호. pp. 357-378.
이혜선, 2023, “LG유플러스 개인정보 유출, 시스템 부재서 비롯,”『B!z watch』, 4월 27일. http://news.bizwatch.co.kr/article/mobile/2023/04/27/0041
장재웅, 2020, “틱톡의 인기와 ‘숏폼’ 콘텐츠의 미래,”『DBR』, 12월 Issue 2, https://dbr.donga.com/article/view/1202/article_no/9864
추동훈, 2023, “틱톡發 미중 무역 전쟁 2라운드... 전면 금지해야 vs. 경제효과 더 크다,”『매경LUXMEN』2월, 제149호. https://m.mk.co.kr/luxmen/view.php?sc=42600117&year=2023&no=124284
최은희, 2022, “해외 사이버 보안 연구원 “챗GPT, 보안 결함 이용해 코드 작성”,”『CWN』, 12월 8일. https://www.cwn.kr/news/articleView.html?idxno=13896
한국인터넷진흥원, 2020, “계정관리 보안 실태 설문조사 결과,”『2020년 3분기 사이버 위협 동향 보고서』, 나주: 한국인터넷진흥원. pp. 38-45.
황일도, 2013, “전략문화 이론의 소개와 북한에 대한 적용: 최근 상황과 관련한 시사점,”『JPI 정책포럼』2013-06/07/08. pp. 41-53.

Buchanan, Ben, 2017, The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. London: Hurst & Company.
Cameron, Kim S. and Sarah J. Freeman, 1991, “Cultural Congruence, Strength, and Type: Relationships to Effectiveness,” Reserarch in Organizational Change and Development Vol. 5, pp. 23-58.
Cameron, Kim S. and Robert E. Quinn, 2011, Diagnosing and Changing Organizational Culture (the third edition), San Francisco, CA: Jossry-Bass.
Chang, Shuchih Ernest and Chin-Shien Lin, 2007, “Exploring organization culture for information security management,” Industrial Management & Data Systems Vol. 107, No. 3, pp. 438-458.
Chech Point Research, 2023, “OPWNAI: Cybercriminals Starting to Use ChatGPT,” Research Blog, January 6th. https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/
Egoloff, Florian J., 2020, “Public attribution of cyber intrusions,” Journal of Cybersecurity 6 (1). pp. 1-12.
Geer, Daniel et al., 2003, Cyberinsecurity: the Cost of Monopoly - how the dominance of Microsoft’s Products poses a risk to security, September 27. http://cryptome.org/cyberinsecurity.htm.
Gray, Colin S., 1999, Modern Strategy, Oxford: Oxford University Press.
Hayden, Lance, 2016, People-centric Security: Transforming Your Enterprise Security Culture, New York and Chicago: McGraw Hill Education.
Howlett, Darryl and John Glenn, 2005, “Epilogue: Nordic Strategic Culture,” Cooperation and Conflict: Journal of the Nordic International Studies Association, 40(1). pp. 121-140.

Johnston, Alastair I., 1995a, “Thinking about Strategic Culture,” International Security, 19 (4). pp. 32-64.

Johnston, Alastair I., 1995b, Cultural Realism: Strategic Culture and Grand Strategy in Chinese History. Princeton: Princeton University Press.

Joyce, Rob, 2018, “NSA Talks: Cybersecurity,” Keynote Speech in DEFCON Conference, August 9-12, Las Vegas. https://www.youtube.com/watch?v=gmgV4r25XxA

Klein, Bradley S., 1988, “Hegemony and Strategic Culture: American Power Projection and Alliance Defence Politics,” Review of International Studies, 14 (2). pp. 133-148.

Lantis, Jeffrey S., 2002, “Strategic Culture and National Security Policy,” International Studies Review, 4 (3). pp. 87-113.

Libel, Tamir, 2016, “Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel’s changing national security policy,” Defence Studies, 16 (2). pp. 137-156.

Libicki, Martin C., 2007, Conquest in Cyberspace: National Security and Information Warfare. New York, NY: Cambridge University Press.

Lieberthal, Kenneth and Peter W. Singer, 2012, Cybersecurity and U.S. - China Relations, Washington, D.C.: Brookings Institution.

Nye, Joseph S., 2010, Cyber Power, Cambridge, MA.: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University.

Valeriano, Brandon, Benjamin Jensen and Ryan C. Maness, 2018, Cyber Strategy: The Evolving Character of Power and Coercion, Oxford: Oxford University Press.

Rid, Thomas, 2013, Cyber War Will Not Take Place, New York, NY: Oxford University Press.

Samonas, Spyridon, 2014, “The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security,” Journal of Information Systems Security 10(3), pp. 21-45.

Slayton, Rebecca, 2017, “What is the Cyber Offence-Defense Balance? Conceptions, Causes, and Assessment,” International Security 41 (3), pp. 72-109.

Snyder, Jack L., 1977, The Soviet Strategic Culture: Implications for Limited Nuclear Operations, Santa Monica, CA: the RAND Corporation.

Stuart, Reginald C., 1982, War and American Thought: From the Revolution to the Monroe Doctrine, Kent, OH: Kent State University Press.

Terriff, Terry, 2002, “U.S. Ideas and Military Change in NATO, 1989-1994,” in Theo Farrell and Terry Terriff eds. The Sources of Military Change, Boulder, CO: Lynne Rienner Publishers, Inc. pp. 91-116.

U.S. Department of the Treasury, 2023, Illicit Finance Risk Assessment of Decentralized Finance, Washington, D.C.: Department of the Treasury.

Van Niekerk, J. F. and R. Von Solms, 2010, “Information Security Culture: A

Management Perspective," Computers & Security 29, pp. 476-486.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.