사이버 안보의 국제정치학: 기본개념의 탐구

2023

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 1호
발간일: 2023년 12월 27일

김상배 (서울대학교)

〈요 약〉

최근 들어 크고 작은 사이버 공격이 양적으로 꾸준히 늘어나고 있다. 더 중요하게는 그러한 사이버 공격의 대상과 주체 및 수법이 질적으로도 변화하고 있다. 이러한 과정에서 사이버 안보 이슈들은 여타 기술·산업과 사회·경제 및 정보·심리 이슈들과 복잡하게 연계되고 있다. 이른바 다양한 경제안보와 신흥안보의 위협으로 비화하는 일이 잦아지고 있다. 최근에는 물리적 전쟁의 발발과 만나면서 지정학적 임계점을 넘었다. 사이버 공격이 양적으로 증가하고 질적으로 다변화되는 만큼 이에 대응하는 국가적 차원의 정책과 전략도 더욱 체계적으로 추진될 필요성이 제기된다. 사이버 안보 분야의 기술역량과 인적자원을 확보하고 정보공유와 민관협력의 체계를 마련하려는 노력이 가속화되고 있다. 공공 및 군사 영역의 사이버 대응 전략은 점점 더 적극적이고 능동적인 방향으로 치달아 가면서 단순 방어 차원을 넘어서는 공세적 작전의 개념이 출현하고 있다. 사이버 공격의 복잡한 전개에 대응하기 위해 국가전략을 마련하고 추진체계를 정비하고 새로이 법·제도를 마련하는 노력도 펼쳐지고 있다. 아울러 일국적 차원의 대응을 넘어서 국제협력도 강조되고 있다.

이러한 현실의 변화에 직면하여 국제정치학계의 정책적·학술적 연구도 좀 더 체계적이고 심층적으로 추진될 필요성이 제기되고 있다. 사이버 안보는 이제 명실상부하게 국제정치학의 독자적인 일 분야로 자리를 잡았다. 사이버 안보 이슈가 국제정치의 다양한 이슈와 접맥되면서 사이버 안보의 국제정치학적 논제들을 탐구하는 개념적·실천적 연구가 필요하다. 이러한 문제의식을 바탕으로 이 글은 국제정치학의 시각에서 살펴보아야 할 사이버 안보 관련 12개의 논제를 다룬 단행본의 총론 격으로 집필되었다. 이 글은 사이버 안보의 국제정치학 분야를 형성하는 개론적 주제로서 세 그룹의 개념들이 선정된 배경과 취지 및 주요 내용을 설명하였다. 먼저, 사이버 공격과 방어의 구도에서 보는 사이버 범죄, 테러, 간첩, 전쟁, 그리고 이에 대응하는 전략 차원에서 거론되는 사이버 억지와 법·제도 및 거버넌스의 문제를 검토하였다. 아울러 사이버 안보의 경제, 정치, 사회 분야에서 제기되는 공급망 안보, 주권, 문화, 윤리의 개념도 검토하였다. 끝으로, 포괄적인 의미에서 본 사이버 안보의 국제정치 이슈로서 사이버 외교, 동맹, 국제규범, 평화의 개념을 살펴보았다.

Ⅰ. 머리말

최근 들어 크고 작은 사이버 공격이 양적으로 꾸준히 늘어나고 있을 뿐만 아니라, 더 중요하게는 그러한 사이버 공격의 대상과 주체 및 수법이 질적으로도 변화하고 있다. 초기의 사이버 공격이 해커집단이나 테러리스트들의 시스템 교란과 첨단 기술 및 기밀 데이터의 탈취 등을 노리고 감행되었다면, 점점 더 국가 행위자를 배후에 두고 활동하는 조직에 의한 다양한 형태의 교란 행위와 금전탈취 목적의 랜섬웨어 공격 및 암호화폐 해킹 등이 늘어나고 있다. 게다가 인공지능을 활용한 사이버 공격의 자동화 또는 자율화 경향이 급부상하는 것도 최근 두드러지게 나타나는 변화이다. 이러한 과정에서 사이버 안보 이슈들은 여타 기술·산업과 사회·경제 및 정보·심리 이슈들과 복잡하게 연계되면서, 이른바 다양한 경제안보와 신흥안보의 위협으로 비화하는 일이 잦아지고 있다. 2022년 초 우크라이나 전쟁의 발발은 사이버전이 물리적 전쟁과 만나면서 지정학적 창발(emergence)의 정점을 찍은 사례이다(김상배 편, 2017).

사이버 공격이 양적으로 증가하고 질적으로 다변화되는 만큼 이에 대응하는 국가적 차원의 정책과 전략도 더욱 체계적으로 추진될 필요성이 제기된다. 사이버 안보 분야의 기술역량과 인적자원을 확보하고 정보공유와 민관협력의 시스템을 마련하려는 노력이 가속화되고 있다. 공공 및 군사 영역의 사이버 대응 전략이 점점 더 적극적이고 능동적인 방향으로 치달아 가면서 단순 방어 차원을 넘어서는 공세적 작전의 개념이 출현하고 있다. 사이버 공격의 복잡한 전개에 대응하기 위해 국가전략을 마련하고 추진체계를 정비하고 새로이 법·제도를 마련하는 노력도 펼쳐지고 있다. 아울러 일국적 차원의 대응을 넘어서 국제협력도 강조되고 있다. 그런데 여기서 주목할 것은, 이러한 국제협력이 주로 진영 내 우방국들끼리의 동맹이나 연대의 형태를 띠고 있는데 비해, 글로벌 차원에서 모든 국가가 수용할 수 있는 보편적 국제규범의 마련은 지지부진하다는 사실이다.

이러한 현실의 변화에 직면하여 국제정치학계의 정책적·학술적 연구도 좀 더 체계적이고 심층적으로 추진될 필요성이 제기되고 있다. 사이버 안보는 이제 명실상부하게 국제정치학의 독자적인 일 분야로 자리를 잡았다. 사이버 안보 이슈가 국제정치의 다양한 이슈와 접맥되면서 사이버 안보의 국제정치학적 논제들을 탐구하는 개념적·실천적 연구가 필요하다. 특히 사이버 안보와 관련된 이슈들은 과거 전통안보를 이해하는 개념적 분석틀로는 제대로 파악되지 않는 새로운 안보 패러다임의 영역에서 발생하는 위협이다. 특히 최근 발생하는 사이버 공격은 일상적 차원에서 이루어지는 기술, 경제, 사회, 문화의 문제인 것 같지만, 어느 순간엔가 양질전화와 복잡한 이슈연계의 과정을 거쳐서 지정학적 논제로 창발하는 문제이다. 이러한 과정에서 사이버 안보는 좁은 의미의 사이버 안보를 넘어서 국제정치 전반의 이슈로 확장되고 있다(김상배 편, 2023).

이러한 문제의식을 바탕으로 이 책은 국제정치학의 시각에서 살펴보아야 할 사이버 안보 관련 12개의 논제를 검토하여 향후 연구와 교육에 활용하기 위해서 기획 및 집필되었다. 이 책의 총론 격인 이 글은 사이버 안보의 국제정치학 분야를 형성하는 개론적 주제로서 세 그룹의 개념들이 선정된 배경과 취지 및 주요 내용을 설명하였다. 먼저, 사이버 공격과 방어의 구도에서 보는 사이버 범죄, 테러, 간첩, 전쟁, 그리고 이에 대응하는 전략 차원에서 거론되는 사이버 억지와 법·제도 및 거버넌스의 문제를 검토하였다. 아울러 사이버 안보의 경제, 정치, 사회 분야에서 제기되는 공급망 안보, 주권, 문화, 윤리의 개념도 검토하였다. 끝으로, 포괄적인 의미에서 본 사이버 안보의 국제정치 이슈로서 사이버 외교, 동맹, 국제규범, 평화의 개념을 살펴보았다.

Ⅱ. 사이버 공격과 방어

1. 사이버 공격

최근 사이버 공격이 양적으로 늘어났을 뿐만 아니라 그 패턴이 다양화되면서 질적으로도 변화하고 있다. 초기의 사이버 공격은 국가 기간시설의 시스템을 교란할 목적으로 이루어졌다. 아울러 기업의 첨단기술과 공공기관이나 군의 기밀 데이터를 유출하기 위해서 행해졌다. 2015년 미국 연방인사관리처 해킹이나 2016년 미국 연방예금보험공사 해킹 등이 대표적 사례이다. 2007년 F-22와 F-35 스텔스 전투기에 대한 중국의 해킹, 2017년 F-15 전투기에 대한 북한의 해킹, 2018년 초음속 대함 미사일에 대한 중국의 해킹 등이 감행되어 관련 기밀 데이터의 절취가 발생했다. 최근 들어 사이버 공격은 경제적 이득을 위해 금전을 요구하는 사이버 범죄와 결합했는데, 금융기관에 대한 해킹뿐만 아니라 표적형 랜섬웨어 공격이나 암호화폐 해킹 등이 감행되고 있다. 한편, 허위조작정보의 유포를 통한 사이버 영향공작 또는 사이버 정보심리전의 수행도 최근 큰 논란거리가 된 사이버 공격의 양식이다.

사이버 공격은 고유한 특성을 갖는데, 무엇보다도 그 공격이 인터넷이라는 복합 네트워크를 배경으로 발생하는 안보위협 문제이다. 인터넷 자체가 '착취혈(exploit)', 즉 취약점을 안고 있어 그 틈새를 공략하는 '비대칭 공격'이 발생한다. 따라서 사이버 안보는 공격이 방어보다 유리한 게임이며, 피해 대상을 구분하기도 어렵고, 때에 따라서는 공격자에게도 피해가 전파될 가능성이 있다. 또한 사이버 공격에서는 과학기술 변수가 중요한 수단으로 활용된다. 컴퓨터 바이러스, 악성코드, 디도스 공격에서 좀비PC, 지능형지속공격(APT), 스턱스넷, 랜섬웨어 등이 이른바 '비인간(non-human) 행위자'로서 작동하며 사이버 공격의 핵심을 이룬다. 최근에는 인공지능을 기반으로 한 자동화 또는 자율화된 사이버 공격과 방어가 급부상하고 있다. 또한 생성형 AI를 대상으로 한 데이터 오염도 심각한 문제로 우려를 낳고 있다. 이러한 과정에서 사이버 안보 분야는 객관적으로 실재하는 위협만큼이나 주관적으로 위협을 구성하는 안보화(securitization)가 중요한 변수라는 점도 빼놓지 말아야 한다(김상배, 2018).

사이버 공격에 관여하는 공격의 주체도 점점 더 다양화될 뿐만 아니라 복잡해지고 있다. 특히 사이버 안보 분야는 국가 행위자 이외에도 비국가(non-state) 행위자들의 위협이 문제시되는데, 초기에는 해커들의 장난거리로 시작했지만 테러리스트들의 저항과 비대칭 공격의 수단이고 기술과 데이터 탈취를 위한 사이버 간첩 행위와 연계되면서 꾸준히 진화해 왔다. 최근에는 다양한 범죄 수법과 연결되면서 이른바 '사이버 범죄-테러-간첩 행위의 복합 넥서스'를 거론하게 되는 상황이 나타나고 있다. 이러한 경향은 최근 국가 배후 사이버 공격의 증가와 연계되면서 정책결정자들의 대응을 촉발했는데, 이는 실제 물리적 전쟁과 연계된 사이버전이 발생하는 정도에까지는 이르지 않더라도 국가적 차원에서는 결코 좌시할 수 없는 위협이 제기되는 상황이라고 할 수 있다. 그야말로 미시적 차원의 사이버 공격이 거시적 차원의 지정학적 위협으로 창발하는 상황이라고 할 수 있다.

제2장은 오늘날 안보 문제가 연계성과 융합성, 전일성을 특성으로 한다는 인식을 바탕으로 논의를 시작한다. 서로 다른 차원에서 존재했던 다양한 문제와 이슈들이 서로 얽히고, 관계 맺고, 하나로 어우러지면서 해당 문제나 이슈의 질적인 변화가 일어나게 된다는 것이다. 사이버 안보의 문제는 이와 같은 안보의 초연결성과 영역의 붕괴, 전일적 혼재성이 나타나는 신흥안보의 대표적

인 사례이다. 사이버 공간에서 나타나는 범죄와 테러, 간첩 행위는 서로 혼재되어 있으며 긴밀하게 연계되어 있다. 이러한 신흥안보의 대표적인 속성을 지닌 사이버 안보 문제는 궁극적으로 지정학적 문턱을 넘어서 전통안보의 문제와 만나기도 한다. 사이버 범죄-테러-간첩 행위와 같은 미시적 또는 중층적 문제들이 점점 더 중요한 거시적 국가안보의 어젠다가 되는 것이다.

이러한 문제의식을 바탕으로 제2장은 전쟁 이전 단계에서 나타나는 사이버 공간에서의 다양한 범죄, 테러, 간첩 행위에 대한 기본개념을 탐색하였다. 제2장에서는 우크라이나 전쟁과 같은 본격적인 전쟁(a full-scale war) 이전 단계에서 벌어지는 다양한 사이버 공격과 침해 행위의 기본개념을 탐색하고 국가안보 및 국제안보의 함의를 도출하고자 하였다. 이와 같은 공격과 침해 행위는 사이버 범죄, 사이버 테러, 사이버 간첩 행위의 형태로 나타난다. 제2장에서 제시하는 다양한 사이버 공격과 침해 행위에 대한 기본개념의 구분과 이해는, 여전히 만족스럽지는 않지만 애매모호하게 뒤섞여 있어 규정하기 어려운 여러 가지 양태의 사이버 공격을 이해하고 규정하는 데 있어 분석틀을 제공한다. 그리고 이를 통해 어떤 사이버 안보의 이슈들을 국가안보 및 국제안보의 의제로 다루어야 할지에 대한 잣대를 마련할 수 있을 것이다.

2. 사이버 전쟁

최근 국가 행위자들이 사이버 공격의 전면으로 나서고 있다. 사이버 공격의 배후에서 해커그룹이나 댓글부대 등을 이용하는 차원을 넘어서 사이버 공격의 주체로 나서고 있는 것이다. 사이버 공격에 드리운 국가의 그림자는 러시아가 감행했던 수 차례의 사이버 공격에서 나타난 바 있다. 2007년 에스토니아에 대한 공격, 2008년 조지아에 대한 공격, 2014년 우크라이나에 대한 공격 등이 그 사례이다. 2010년 이란의 핵 시설에 대한 미국의 스턱스넷 공격과 2012년 미국과 사우디 및 카타르에 대한 이란의 사이버 공격도 국가 행위자가 나선 사례이다. 2010년대 미국과 중국의 사이버 공방도 미중 글로벌 패권경쟁의 일환으로 진행된 국가간 게임으로 이해해야 한다. 특히 2021년 전반기는 미국과 러시아, 그리고 중국 간의 사이버 갈등으로 유난히 떠들썩했던 시기였다. 미 바이든 대통령이 자국에 대해서 행해지는 사이버 공격이 실제 전쟁을 초래할 수도 있다고 경고하기까지 했다.

2022년 2월의 우크라이나 전쟁은 물리적 전쟁의 개시를 전후하여 사이버전이 어떻게 활용되는지를 여실히 보여주었다, 개전 직전 러시아는 우크라이나의 기간시설에 대해서 여러 차례에 걸쳐서 디도스 공격을 가했다. 그러나 러시아의 과거 사이버 공격이 우크라이나에 끼친 영향에 비해서 2022년의 공격은 큰 피해를 초래하지는 않은 것으로 알려져 있다. 그 이유에 대해서는 여러 해석이 가능하겠지만 미국과 유럽 국가들의 사이버전 지원이 큰 역할을 했다. 특히 미국의 민간 빅테크들의 역할이 컸는데, 마이크로소프트나 스페이스X 등과 같은 기업이 큰 역할을 했다. 게다가 사이버 방어 역량이 부족한 우크라이나에 대한 국제사회의 지원도 큰 몫을 담당했다. 우크라이나 정부의 호소로 이른바 '사이버 부대(IT Army)'가 소집되기도 하고, 어나니머스와 같은 핵티비스트 그룹도 참전했다. 러시아의 가짜뉴스를 차단하는 서방 플랫폼 기업들의 활약도 커서 러시아가 원조로 알려진 사이버 정보심리전 또는 인지전 분야에서 오히려 우크라이나가 선전하는 양상이 나타나기도 했다.

미래전에서 사이버전의 수행이 지니는 효용과 가치는 갈수록 더 커질 것이다. 미래전에서 사이버 공간을 장악하는 역량은 육·해·공·우주 공간의 지배를 보장하고 전쟁의 승패를 좌우할 수 있는 핵심 전력으로서의 의미를 갖는다. 사이버전은 '독립적 작전'이 아니라 육·해·공·우주 공간에서 벌어지는, 기존의 전쟁과 연계된 다영역 작전(Multi-Domain Operation)의 한 축을 담당하게

되었다. 이러한 과정에서 사이버 전력은 다영역 작전의 모든 임무를 아울러서 널리 확장될 것으로 전망된다. 최근 사이버전이 여타 군사작전과 복합되면서 '사이버전 복합 넥서스'의 부상이 거론되는데, 사이버-재래전, 사이버-핵전, 사이버-전자전, 사이버-우주전, 사이버-인지전, 사이버-AI전 등의 개념이 출현하였다. 사이버전의 수행은 미래전 환경에서 일국의 국방 전력의 수준을 보여주는 핵심 지표 중의 하나가 되었다.

제3장은 사이버전이 물리적 전쟁의 일부라는 시각에서 사이버전에 대한 개념적 논의를 펼쳤다. 사이버전은 사이버 첩보, 사이버 방해, 사이버 성능저하 등의 작전유형별로 이해되어야 한다. 사이버 공격수단은 웹사이트 변조, 디도스 공격, 침범, 침투 등으로 구분된다. 사이버전이 계속 진화하는 만큼, 사이버전에 대한 기술적 이해를 넘어서 사이버전의 발전 방향을 가늠할 기준을 마련하기 위해서는 사이버전을 둘러싼 쟁점들을 파악하는 것이 중요하다. 우선 전술적인 차원에서 사이버전이 재래식 군사력에 부수적인 작전인지, 아니면 독립적 작전인지를 구분하는 것이 쟁점이다. 좀 더 포괄적인 차원에서 사이버전이 승리나 강압에 결정적인 변수인지도 중요한 쟁점이다. 궁극적으로 사이버전이 국제 권력정치의 변화와 관련하여 약자에게 유리한 무기인지, 아니면 강자에게 유리한 무기인지도 사이버전의 이해를 중요한 쟁점이다.

제3장은 우크라이나 사이버전과 그 이전의 사례들의 비교를 통해서 사이버전의 쟁점과 관련하여 획기적인 변화가 출현했다고 볼 수는 없다고 주장한다. 여태까지 사이버전은 재래식 공격과 연계되기보다는 사회적 혼란을 초래하는 저강도 공세의 수단으로 주로 활용되고 있다는 것이다. 더구나 사이버전은 결정적인 승리와 강압을 달성하는 수단으로서 효과를 분명히 보여주지 못했다는 것이다. 또한 약자의 무기라는 이미지와 다르게 역설적으로 약소국에 대한 강대국의 강압에 주로 활용되고 있다는 것이 제3장의 인식이다. 그럼에도 우크라이나 전쟁에서 드러난 사이버전의 양상은 향후 좀 더 위력적인 사이버전의 도래를 예고하기도 했다. 이에 향후 미중경쟁의 전개 및 인공지능의 기술적 발전을 바탕으로 사이버전이 미래전에서 더욱 중심적인 위치를 차지할 가능성을 엿보게 한다는 것이다.

3. 사이버 억지

최근 국내외에서는 양적·질적으로 진화하는 사이버 위협에 적극적으로 대응하는 다양한 방안들이 모색되고 있다. 그중의 하나가 핵전략 분야에서 유래하는 억지(deterrence)의 개념을 사이버 안보 분야에 적용하려는 시도이다. 특히 최근 사이버 억지에 대한 논의는 전통적인 '보복(punishment)에 의한 억지' 개념에서 시작한다. 그런데 사이버 안보 분야의 성격상 이러한 전통 억지 개념에 기반을 둔 주장은 결연한 의지를 표명하는 의미는 있겠지만, 실제로 그 효과를 거둘 수 있느냐에 대해서는 의문이 제기된다. 오히려 최근 학계의 연구 경향은 사이버 억지의 '적용무용론'으로 기울어 왔다. 이러한 과정에서 '거부(denial)에 의한 억지' 개념이 주목받기도 했다. 특히 사이버 공간의 고유한 특성을 바탕으로 하는 디지털 인프라 및 역량의 비대칭성, 책임귀속(attribution)의 복잡성, 공격 주체와 보복 대상의 다양성 등의 문제로 인해서, 공격자에 비용을 부과하는 것이 복잡할 뿐만 아니라 공격 자체를 원천적으로 거부하는 것이 제약되기 때문에, 전통억지 모델을 사이버 분야에 적용하기 힘들다는 것이었다.

그러나 사이버 억지론은 기존의 '적용-무용의 이분법' 구도에서 벗어날 필요가 있다. 사이버 안보 분야에 억지 개념의 적용이 어려운 것은 맞지만, 그렇다고 사이버 억지 전략 자체가 무용한 것은 아니다. 오히려 필요한 것은 여러 유형의 사이버 억지 전략이 작동하는 방식과 조건 및 효과를 구체적으로 탐구하는 작업이다. 이러한 이분법적 발상이 지배했던 것은, 적의 공격을 원천

봉쇄해야 한다는 '절대적 억지'에 대한 미국 정책서클의 고전지정학적 강박감이 작용했기 때문일 수도 있다. 그러나 핵 공격과는 달리 사이버 공격의 경우에는 그것이 일정한 수위 이하에서 지속적으로 감행되는 것으로 전제하고, 그 공격의 빈도와 정도를 어떻게 제한하느냐를 고민하는 '상대적 억지'의 개념으로 다루어야 한다. 특히 억지 개념을 사이버 분야에 적용하는 것이 가능한지를 묻는 '단순계적 발상'을 넘어서, 사이버 공간의 특성을 고려한 유연하고도 통합적인 '복잡계적 시각'의 도입이 필요하다(김상배, 2023a).

이러한 문제의식을 바탕으로 제4장은 사이버 억지 전략을 수립하는 데 필요한 개념적 논의를 검토하였다. 사이버 공간은 이미 공격과 방어가 이루어지는 전장 공간이지만 사이버 억지를 위한 이론적 논의는 크게 발전하지 못했다는 것이 제4장의 인식이다. 핵억지를 중심으로 발전한 물리적 전장에서의 억지 개념을 그대로 적용가능한 것인지, 사이버 공간만의 특수한 개념이 필요할 것인지에 대한 논쟁 수준을 넘어서 사이버 위협을 억지하기 위한 요건과 고려 사항을 구체화할 필요가 있다는 것이다. 이를 위해 제4장은 사이버 공간의 전략적 특성, 공격과 방어의 수행 방식, 사이버 억지의 개념과 발전 과정, 사이버 억지의 대상, 내용, 방법 등에 대한 국내외의 다양한 논의를 검토하였다. 이를 위해서 제4장이 제시하는 두 가지 관점은 '사이버 영역에서의 억지(in Cyber)'와 '사이버 영역을 통한 억지(through Cyber)'이다. 이를 바탕으로 제4장은 누구로부터, 무엇을, 어떻게 억지할 것인가의 세 가지 질문을 제시한다.

첫째, 누구를 억지할 것인가에 대한 질문이다. 사이버 위협은 목적과 주체에 따라 구분할 수 있는데, 이는 위협 주체의 '귀속성'을 밝힐 수 있는지, 얼마나 신속하게 특정할 수 있는지의 질문으로 이어진다. 둘째, 무슨 행동을 억지할 것인가의 질문은 레드라인과 대응 행동을 포함하는 억지 메시지로서 답할 수 있다고 한다. 상대에 대해 믿을만한 시그널링을 보내기 위해서는 대응 행동의 '비례성'에 대한 검토를 요구한다. 셋째, 어떻게 억지할 것인가의 질문이다. 억지를 위한 다양한 개념과 방법들이 제시되었지만, 사이버 공격의 전·중·후의 시간적 구분에 따라서 거부(resistance)-응징(retribution)-복원(resilience)으로 억지 방법을 개념화할 수 있다. 그리고 억지를 위한 모든 방법과 수단은 '효과성'을 담보할 수 있어야 한다. 아울러 제4장은 사이버 억지를 위한 정책제언으로, 사이버 억지를 위한 실질적인 능력 구비, 국가 차원의 대응 전략 수립, 국내 및 국제사회의 사이버 안보 거버넌스의 정립을 제시하였다.

4. 사이버 법제도

사이버 안보 위협이 거세어지는 것만큼, 전략적 차원의 대응 이외에도, 이에 대응하는 다양한 노력이 한창 진행되고 있다. 사이버 안보 위협에 대응하여 각국은 기술적으로 방어역량을 강화하는 것 외에도 공세적 방어의 전략을 제시하고 각종 정책과 법·제도를 정비하거나 국제협력을 강화하는 등의 대책 마련에 힘쓰고 있다. 그야말로 사이버 안보는 단순히 사이버 보안 전문가들의 기술개발 문제를 넘어서 다양한 분야를 아울러 종합적인 대응책을 마련해야 하는 미래 국가전략의 문제가 되었다. 특히 사이버 안보 위협에 대한 대응 거버넌스의 제도화를 위한 노력에 각국의 정책적 관심이 집중되고 있다. 이러한 과정에서 유의할 점은 이러한 제도화의 노력 이면에 아직 수면 아래에서 창발하고 있는 미래의 안보위협을 주관적으로 구성하는 안보화(securitization)의 메커니즘이 강하게 작동한다는 사실이다. 눈에 보이는 대상을 상대로 법제도와 거버넌스의 방책을 모색하던 전통안보의 경우와는 달리, 눈에 보이지 않는 대상을 대하는 새로운 대응 방식이 사이버 안보 분야에 필요한 이유이다.

실제로 날로 교묘해지고 있는 사이버 공격을 막아내는 데 있어 전통안보의 대응 방식은 역부

족이다. 사이버 안보의 특성상 기술적으로 철벽 방어를 구축하려는 단순 발상은 해법이 될 수 없다. 오히려 사전 예방과 사후 복원까지도 고려하는 복합적인 방식이 필요하다. 정책내용 면에서 기술, 국방, 법제도, 국제협력에 이르기까지 다양한 노력이 필요하며, 추진 주체 면에서도 어느 한 기관이 전담하는 모델보다는 해당 주체들이 역할과 책임을 다하는 가운데 그 상위에 총괄·조정역을 설계하는 중층모델이 필요하다. 물론 국가마다 차이는 있을 수밖에 없을 것이다. 정치와 사회와 문화의 차이가 있기 때문이고, 여타 정책이나 제도와의 관계 또는 역사적 경로의존성의 제약을 받기 때문이다. 더 중요하게는 국가마다 사이버 위협의 기원과 성격, 그리고 각국이 처한 국제적 위상 등이 다르기 때문에, 각기 상이한 해법을 모색하는 것은 당연하다. 그럼에도 지난 10여 년 동안 세계 각국이 사이버 위협에 대처하기 위해서 모색해 온 해법들은 전통안보의 경우와는 달리 좀 더 새롭고 복합적인 내용과 형식을 보여주고 있다(김상배 편, 2019b).

사이버 안보의 법제도와 거버넌스에 대한 논의를 펼치고 있는, 제5장은 시장을 통한 사이버 위험분배의 실패가 정부에 의한 시장개입을 요구하고 있다는 인식에서 출발한다. 민주주의와 시장경제 체제하에서 국가의 시장개입은 특별한 경우에 한해서, 법적 근거에 기초하여 이루어지고 있다. 국가의 개입이 시장의 자율성을 저해하여 비효율과 비용을 양산할 수 있기 때문이다. 국가는 시장에 개입하여 사이버 위험이 이슈연계와 양질전화를 거치면서 안보화되어 거시적 차원에서 사이버 안보의 문제로 확산되는 경로를 차단하기 위한 거버넌스 구조를 정립하고자 한다. 이러한 경우 국가는 위협(threat)과 취약성(vulnerability) 및 결과발생(consequence)을 감소시키거나 제거하기 위한 법제도와 거버넌스를 선택하여 사이버 안보 문제가 안보화되는 과정의 연결고리를 차단 또는 저지하고자 한다는 것이다.

제5장은 미국의 사례를 통해서 이러한 법제도와 거버넌스의 수립 과정을 살펴보았다. 2000년대 미국 정부, 특히 부시 행정부는 사이버 문제를 국가안보 이슈의 하나로 인식하지 못하고 사이버 보안의 기반을 마련하는 정도에만 중점을 두었다. 오바마 행정부 초기에도 사이버 위험에 대한 대응에 있어 국가 중심보다는 시장의 자율에 맡기고자 하였다. 그렇지만 소니 해킹 사건을 계기로 사이버 위험이 미국 내에서 현실화되면서 좀 더 적극적으로 개입하는 쪽으로 정책 방향이 선회했다. 트럼프 행정부는 이미 안보화 과정을 넘어선 사이버 문제에 대해 사이버 위협의 적극적인 감경, 공급망 재편을 통한 취약성의 극복, 회복력의 효율성과 탄력성 확보 등을 위해 적극적으로 국가가 개입하여 위험을 관리하는 방향으로 법제도와 거버넌스의 체계를 정비하였다. 바이든 행정부는 사이버 위험의 안보화를 차단 또는 감경시키기 위하여 사이버 위협을 감경시키고 취약성을 감소시키며 결과 발생의 방지, 즉 회복력 강화를 위한 법제도와 거버넌스의 정비와 개선을 지속하고 있다.

미국의 사례에서 나타난 바와 같이, 사이버 문제의 안보화에 대응하는 법제도와 거버넌스 체계의 모색 과정을 참고하여, 한국의 실정에 맞는 법제도와 거버넌스를 구축할 필요가 있다. 국가가 시장에 개입하여 위협과 취약성을 제거하고 회복력을 강화하여 사이버 공간의 안전성을 확보하는 것은 관련된 비용의 증대를 초래한다는 사실을 명심할 필요가 있다. 따라서 한국의 실정에 적합한 사이버 안보 법제도와 거버넌스의 구축과 운영을 위해서는 비용과 안보라는 두 가지 가치의 사이에서 최적의 균형점을 찾아야 한다. 결국 국가는 위험의 제거 또는 감소에 필요한 비용과 사이버 보안 강화로 증대되는 사회적 복리를 비교하여 가장 효율적인 법제도와 거버넌스의 체계를 선택할 수밖에 없다.

Ⅲ. 사이버 안보와 경제사회

1. 사이버 안보와 경제

사이버 안보 이슈가 확장되는 과정에서 여타 다양한 이슈들과 연계되고 있는데, 그중에서도 특히 '경제' 이슈와의 연계가 최근의 논란거리가 되었다. 사이버 안보가 경제와 만나는 대표적인 이슈는 경제안보 중에서도 공급망 안보이다. 2020년대 들어서 SW개발업체, 제조업체, IT서비스 관리업체 등의 ICT 공급망을 대상으로 한 사이버 공격이 증가했다. 이는 (기술)제품 생산과 서비스를 위한 기간망뿐만 아니라 데이터가 이동하는 정보통신 기간망에 대한 사이버 위협도 포함한다. 이러한 사이버 공격은 대부분 공급업체 코드에 집중되었는데, 최근에 발생한 공급망 공격의 66%가 '코드 공격'이다. 그 대표적인 사례로는 2020년 12월 미국 최대 보안 솔루션 업체인 솔라윈즈에 대한 러시아의 해킹, 2021년 4월 방위산업 관련 SW 보안 솔루션 업체인 펄스시큐어의 VPN 취약점에 대한 중국의 악성코드 공격, 그해 7월 시스템 제어 소프트웨어 업체 카세야에 대한 러시아의 랜섬웨어 공격 등이 있다. 또한 2021년 5월 미국 동부의 연료를 공급하는 콜로니얼 파이프라인사에 대한 랜섬웨어 공격과 그해 6월의 JBS 육류가공회사에 대한 랜섬웨어 공격도 크게 화제가 되었다(김상배, 2022).

경제 이슈와 연계된 사이버 안보 문제는 2010년대 후반 중국의 기술추격에 대한 미국의 수출입 통제의 행보와 만났다. 미국은 중국산 제품에 숨겨진 백도어를 통해서 국가안보가 달린 데이터가 유출된다고 '안보화'(securitization)했다. 5G 차세대 이동통신 장비를 수출하는 화웨이에 대한 수출입 규제가 대표적 사례였다. 비슷한 맥락에서 글로벌 민간 드론 시장을 석권하고 있는 중국업체인 DJI의 드론도 '잠재적 위협'이라고 규제를 받았다. 중국업체인 하이크비전과 다후아 등이 생산하는 CCTV도 규제 대상이 되었는데, 이는 중국 내 소수민족 감시에 사용된다는 의심을 샀다. 이와 유사한 정치적 이유로 안면인식AI를 생산하는 중국 기업인 센스타임, 메그비, 이투 등도 규제를 받았다. 한편, 중국 스타트업인 바이트 댄스의 짧은 동영상 서비스인 틱톡도 규제 대상에 올랐으며, 중국의 지배적 SNS인 위챗도 제재의 대상으로 거론되기도 했다. 이밖에도 중국 기업인 ZPMC가 제공하는 대형 항만 크레인도 데이터 안보를 해치는 우려의 대상으로 지적되었으며, 최근에는 중국산 전기차도 이러한 데이터 안보 관련 제재 리스트에 이름을 올렸다.

제6장은 하드웨어, 소프트웨어, 데이터 분야에서 발생한 사이버 안보와 경제안보의 넥서스를 분석하였다. 하드웨어와 관련한 사이버 안보 문제가 크게 제기된 것은 2018년경 중국 기업인 화웨이의 5G 인프라를 둘러싸고 벌어진 논란이었다. 그 이후 미국의 주요 대응은 수출통제 정책들을 통해 이루어졌는데, 이들 정책은 미국의 경제적 이익 도모, 기술적 우위 고수, 사이버 안보 강화, 그리고 국가안보 확보라는 경제와 안보를 강하게 연계시키는 인식에 기반을 두고 있었다. 소프트웨어 관련해서는, 대내적으로 '제로 트러스트' 개념에 기반을 두고 '소프트웨어 자재명세서(SBOM)' 등을 제시하는 행보를 보였다.

하드웨어 및 소프트웨어와 관련된 정책들이 위협 요소들을 공급망에서 배제하기 위해서 도입되었다면, 데이터 안보의 이슈는 데이터의 자유로운 국경 간 이동을 지향했으며, 이와 관련된 경제와 안보의 연계 전략도 이에 맞추어 조정되었다. 무역 협정들은 데이터의 자유로운 이동을 위해 경제와 안보 연계의 가시성을 낮추었으며, 유사한 맥락에서 미국과 유럽연합(EU) 간의 '세이프 하버'나 '프라이버시 실드'도 운용되었다. 이와는 대조적으로 〈해외 데이터 이용 합법화 법률〉, 즉 이른바 〈클라우드법(Cloud Act)〉은 공공질서나 국가안보와의 연계를 통해, 데이터의 자유로운 이동을 촉진하는 미국의 정책을 지원하는 법으로 출현하였다. 유럽연합이나 세계 다른 나라들도 유사한 제도를 준비해 나가고 있는데, 앞으로 이러한 경제와 안보의 연계는 다양한 양상

을 띨 것으로 전망된다.

2. 사이버 안보와 주권

사이버 안보의 이슈연계 과정은 다양한 국가 간 갈등을 야기하고 있는데, 그중에서도 국제정치학의 관심을 끄는 것은 사이버 주권의 개념에 대한 논의이다. 이는 초국적 데이터 유통에 대응하는 과정에서 제기되었으며, 각국은 상이한 국가주권의 관념을 상정하고 있다. 예를 들어, 미국은 자본의 시각에서 국경을 넘나드는 데이터의 자유로운 흐름을 강조하며 이를 통제하는 국가주권의 고수가 사실상 무용하다는 입장을 취한다. 이 분야를 주도하고 있는 미국 빅테크 플랫폼 기업들의 이익을 옹호하기 위해서 규제를 최소화하고 이에 맞는 글로벌 질서를 만들고 싶은 강대국으로서 미국의 의도가 숨어 있다. 이에 비해 중국을 비롯한 러시아나 개도국들은 초국적 데이터 유통을 규제하는 것은, 국가 본연의 주권적 권리에 속한다는 시각에서 문제에 접근한다. 데이터의 자유로운 유통보다는 오히려 빅데이터 역량을 장악하고 있는 선진국 기업들의 침투로부터 자국의 사이버 주권이 잠식될지도 모른다는 점을 우려하는 것이다.

이러한 맥락에서 볼 때, 사이버 안보 분야에서 드러나는 중국의 관심은 미국 기업들의 사이버 패권으로부터 자국의 독자적인 사이버 공간을 지켜내고 자국의 시장과 표준을 수호하는 데 있다. 이러한 연장선에서 중국형 사이버 안보화의 특징이, 하드웨어 인프라의 사이버 안보를 강조한 미국의 경우와는 달리, 소프트웨어와 정보 콘텐츠 및 데이터에 대한 주권적 통제를 확보하는 데 있다는 것을 이해하는 것이 중요하다. 이러한 중국의 인식은 중국 시장에 진출하여 사업을 하는 미국 빅테크들에 대한 규제정책에 반영되었다. 표면적으로는 인터넷상의 유해한 정보에 대한 검열 필요성을 내세웠지만, 대내적으로는 중국 정부에 정치적으로 반대하는 콘텐츠를 걸러내고, 대외적으로는 핵심 정보와 데이터가 국외로 유출되는 것을 막으려는 주권적 통제의 의도가 깔려 있었다. 이러한 사이버 주권 논쟁은 미국과 중국이 벌이는 디지털 패권경쟁을 추동하는 요인이기도 하다.

제7장은 디지털 시대 규범과 거버넌스의 핵심 논제인 사이버 공간의 주권 논쟁을 살펴보고, 주권 개념과 연계된 오랜 정치적 논쟁들이 어떻게 사이버 안보와 연계되어 나타나는지를 분석하였다. 특히 제7장은 사이버 공간의 안보화 관점에서 유럽연합(EU)과 중국의 주권 개념을 비교분석하는 작업을 벌였다. 디지털 시대를 맞아 영토경계가 불분명한 사이버 공간의 부상과 함께 주권 개념 논쟁이 새롭게 점화되었고, 최근 사이버 주권 논쟁은 강대국 경쟁의 부활, 자유주의 국제질서의 쇠락, 권위주의 국가의 부상이라는 국제질서 변화와 밀접히 연계되어 나타나고 있다. 사이버 주권은 사이버 공간을 둘러싼 담론경쟁, 규범경쟁, 거버넌스 경쟁의 핵심 주제이다. 전통적 주권 개념의 사이버 공간에 대한 적용과 이를 둘러싼 중국과 서구의 논쟁은 글로벌 인터넷 거버넌스와 사이버 안보 협력을 위한 보편 원칙과 규범 창출 및 이행에 대한 제약요인이 될 수 있다. 중국은 '중국 특색의 인터넷 관리 방안'을 주장하고, 반패권과 반강권, 내정불간섭의 관점에서 사이버 주권을 강조하고 있으며, 사이버 주권 원칙에 따라 사이버 공간에 대한 국제 규칙을 제정하는 것을 주요한 원칙으로 내세우고 있다.

이에 비해 유럽연합(EU)은 중국과 러시아가 사이버 주권이라는 표어 아래 정보흐름의 대내외적 통제와 체제 유지라는 외교 어젠다를 추구해 왔다고 비판한다. 유럽연합(EU)은 권위주의 국가들의 주권 논의와 실질적으로 다른 사이버 주권 개념을 설정하고 데이터 주권과 기술주권 등을 포괄하는 넓은 관점에서 사이버 주권을 강조하였다. 유럽의 사이버 주권 개념은 중국 및 러시아의 주권 개념과도 다르지만, 미국의 입장과도 대비된다. 특히 유럽연합(EU)은 자유로운 데이

터의 초국적 유통으로 인해 침해될 수 있는 개인권리의 보호라는 관점에서 접근한다. 유럽연합이 원용하는 주권의 개념은 비즈니스의 이익을 반영한 국가주권의 무용론이나 전통적인 국가주권의 복원론 차원을 넘어서는 좀 더 복합적인 맥락에서 보는, 일종의 시민주권론이라고 할 수 있다. 유럽이 제시하는 사이버 주권 개념은 근대 국가주권 개념을 넘어서려는 시도라는 관점에서도 해석된다.

3. 사이버 안보와 문화

사이버 안보는 경제와 산업, 무역 등의 이슈를 넘어서 좀 더 포괄적인 의미에서 본 문화 이슈와도 관련된다. 전통적으로 안보와 문화는 사회과학뿐만 아니라 국제정치학의 오랜 논제인데, 사이버 공간을 배경으로 해서도 안보 변수와 문화 변수는 독립변수와 종속변수로서의 위치를 바꾸어 가면서 서로 영향을 미치는 양상을 드러내고 있다. 안보와 문화, 두 변수 간의 관계를 대략 '도구론'과 '인과론' 및 '구성론'의 구도에서 놓고 보면, 다음과 같은 사이버 안보와 문화에 대한 논제를 제기해 볼 수 있을 것이다.

도구론의 구도에서 볼 때, 문화 변수는 사이버 안보의 목적을 달성하기 위해서 동원되는 수단이자 대상이다. 최근 쟁점이 된 것은, 사이버 안보의 시각에서 본 문화안보, 특히 디지털 문화콘텐츠의 안보 문제이다. 다시 말해, K-콘텐츠가 생산 및 유통되는 문화공간으로서 사이버 공간에 대한 사이버 공격과 이러한 과정에서 문화콘텐츠의 사이버 안보를 수호하는 문제이다. 최근 가짜뉴스나 딥페이크 등이 사이버 영향공작의 주요한 수단으로 활용되고 있다. 디지털 게임, 소셜 미디어, 기타 디지털 콘텐츠 등과 관련된 정보와 데이터가 사이버 공격의 대상이 된다. 최근 미국이 문제를 제기한 틱톡과 같은 동영상 서비스의 사례도 들 수 있는데, 이는 사이버 '안보화'의 변수가 문화콘텐츠의 영역에 작동하는 사례이다.

인과론의 구도에서 볼 때, 문화 변수가 안보 분야에 미치는 영향을 탐구하는 것도 중요한 논제이다. 각국의 '전략문화(strategic culture)' 또는 '안보문화(security culture)'가 각국의 안보전략에 미치는 영향에 대한 연구는 국제정치 안보연구의 하위 분야로서 오랫동안 명맥을 이어왔다. 이러한 맥락에서 보면 미국과 중국의 각기 다른 전략문화는 양국의 사이버 안보에 대한 인식과 전략에 영향을 미치는 중요한 변수이다. 사실 최근 전개되는 사이버 공격의 양상이나 사이버 안보와 관련된 법제도의 형성 및 집행 과정 등은 미국과 중국의 고유한 전략문화의 영향을 받는 것으로 평가된다. 이러한 시각에서 보면 각국의 '전략 사이버 문화(strategic cyber culture)'라는 개념적 범주를 설정할 수도 있을 것이다.

구성론의 구도에서 볼 때, 문화와 안보는 정체성과 규범 및 가치를 구성하는 변수들이다. 이러한 연장선에서 사이버 안보 확보를 위한 정체성과 규범 및 가치 차원에서 본 문화 형성에 대한 논제를 설정해 볼 수 있다. 다시 말해, '사이버 안보 문화'라는 개념을 전제로 하고 '정체성 안보'를 확보하는 차원에서 '건전한' 사이버 안보 환경 조성을 위한 사이버 정책을 상정할 수 있다. 실제로 이러한 문제의식을 바탕으로 건전한 디지털 게임 문화 또는 SNS 문화 조성 등을 위한 정책적 노력이 진행되고 있다. 사실 이러한 '전략 사이버 문화'는 일종의 국제정치 문화권력으로 작동하는 면모도 없지 않다. 더 나아가 미래 사이버 문명의 도래라는 거시적 시각에서 보는 사이버 안보 문화의 창출에 대한 고민도 학계가 안고 있는 숙제이다.

이러한 논의와 유사한 맥락에서 제8장은 사이버 공간의 문화와 안보가 기계적 연결, 사이버 안보의 전략문화, 사이버 공간의 인간중심 보안문화라는 세 가지 차원에서 서로 연결, 결합, 추동되고 있다고 주장한다. 우선 비교적 최근에 나타나고 있는 문화와 안보의 기계적 연결은 중국

의 한국 문화콘텐츠에 대한 한한령(限韓令)이나 미국과 중국 사이의 틱톡을 둘러싼 데이터 안보 논란에서 나타났다. 그동안 연결되지 않았던 영역들이 서로 연결되면서 새로운 문제를 만들어 낼 수 있다는 차원에서 문화와 안보의 기계적 연결을 단순히 우연한 사건으로만 생각할 수는 없다. 그러나 이를 사이버 안보의 신흥안보적 창발로 생각하기에는 아직까지는 지정학적 임계점을 넘지 못했다는 한계를 지닌다.

두 번째의 연계는 사이버 안보의 전략문화와 관련해서 제기된다. 사이버 공간은 군사안보의 공간이라는 성격도 가지는데, 이러한 특징은 전략문화의 렌즈를 통해서 사이버 안보의 문제를 파악하는 데 있어서 중요한 함의를 던진다. 이러한 점에서 어느 나라의 전략문화는 그 국가의 사이버 국력에 대한 인식과 행위의 선호를 설명하는 데에 중요한 도구로 사용될 수 있다. 그러나 전략문화 변수는 사이버 공간의 안보 이슈를 만들어 내는 독립변수이기보다 매개변수나 개입변수로서 다루어져야 한다.

마지막의 연결은 사이버 안보로부터 만들어지는 인간중심 문화이다. 위로부터 방식의 전통적 보안관리와 달리 인간중심의 보안문화 형성을 통한 대응은 인간의 행동을 관리하는 아래로부터의 관리체계를 의미한다. 제8장의 설명에 따르면, 이러한 자율중심의 조직문화는 사이버 보안사고를 줄이면서도 유연하게 대처하는 방안을 마련하는 데 도움을 줄 수 있다는 것이다. 또한 인간을 중심으로 하는 가치를 국가안보, 더 나아가 세계질서의 중심에 놓게 되면, 안보의 궁극적인 수혜자로서 인간을 다루면서도 새로운 디지털 문명/문화를 만들어 갈 가능성을 열어준다는 점에서 의미가 있다고 주장한다.

4. 사이버 안보와 윤리

사이버 공간이 우리 삶의 필수적인 공간으로 자리 잡아 가고 있는 상황에서 인간과 사회, 국가가 지켜야 할 사이버 공간의 윤리를 마련할 필요성도 제기되고 있다. 그 일환으로 사이버 ㅇ나보 분야에서도 도덕적인 윤리규범을 마련할 필요성이 거론된다. 아무리 사이버 공격을 하더라도 마땅히 지켜야 할 윤리가 있다는 인식은 향후 무분별한 디지털 기술의 개발과 적용에서 발생할 문제점들을 성찰하는 플랫폼의 역할을 할 것이다. 사이버 안보 윤리의 마련은 사이버 공간의 악의적 활용에 의한 인간과 사회, 국가의 기본가치에 대한 침해, 그 기본가치 중에서도 각 주체의 존재론적 가치(ontological value)에 대한 침해를 방지하는 문제와 관련된다. 예를 들어 사이버 공간의 안보를 지키겠다는 논리를 내세워 수행되는 사이버 감시나 통제로 인해서 인간과 사회, 국가가 지켜야 할 기본적인 존엄이나 인권, 자유, 평등, 정의 등의 가치에 대한 침해를 용인하지 않는 문제이다. 이는 궁극적으로 사이버 활동을 통한 인류의 보편가치 구현이라는 세계시민주의적 문제의식과 통한다.

사이버 안보를 지키려는 활동의 과도화로 인해서 사이버 안보 윤리가 침해당할 우려에 대해서는 여러 가지 사안들이 거론된다. 예를 들어, 소셜 미디어 오용이나 가짜뉴스와 인종차별 정보 확산 및 데이터 침해 행위, 온라인상으로 벌어지는 인권유린과 아동 대상 성 학대와 착취, 세계보건기구(WHO)를 비롯한 병원 및 제약 연구소를 대상으로 한 사이버 공격, 디지털 기술 발전이 야기하는 환경과 생태계 파괴, 인공지능을 활용한 사이버 사찰이나 사이버 무기 기술의 과도한 개발 등이 그 사례들이다. 이러한 사이버 윤리 문제 중에서도 사이버 안보를 지키려는 행위와 프라이버시 보호 간의 균형을 유지하는 것이 큰 논란거리이다. 특히 국가 차원에서 수행되는 사이버 활동의 자의성이나 불투명성, 사이버 감시기술의 확대 등이 개인의 프라이버시 및 권리를 침해할지도 모른다는 우려가 제기된다. 이는 민주주의 가치의 침해 문제와도 연결되는데, 정당한

목적과 적법한 수단으로만 사이버 안보 활동을 수행할 것이며, 이러한 과정에서 불가피하게 발생하는 국민 기본권 제한은 최소화해야 한다는 것이다.

그러나 이러한 윤리적 규범에 대한 논의는 항시 '진영적 가치'에 대한 논란으로 기울 우려가 있다. 최근 미국과 중국이 벌이는 패권경쟁의 맥락에서 제기되는 사이버 윤리의 문제가 대표적인 사례인데, 안면인식AI나 CCTV 등을 정치적으로 사용하는 중국 정부와 이러한 기술을 제공하는 중국 기업들에 대한 미국의 제재가 논란이 되고 있다. 이러한 강대국들의 '진영적 가치'의 갈등에서 중견국으로서 한국이 추구할 윤리규범과 기본가치에 대한 고민이 깊어 가고 있다. 디지털 강국의 양적 성과를 넘어서, 그리고 개도국으로서의 국제적 위상을 넘어서 중견국 한국은 사이버 안보 윤리에 대한 고민을 어떻게 펼칠 것인가? 기술적 효율성의 문제를 넘어서 개인과 사회와 국가 차원에서 한국이 국제사회를 향해서 내세우려는 윤리와 가치의 내용은 무엇인가? 강대국의 경우와 대비하여 미래지향적 시각에서 한국이 추구할 고유한 사이버 윤리가 무엇인지에 대한 진지한 논의가 필요하다.

이러한 맥락에서 제9장은 사이버 안보 윤리에 대한 고민을 펼쳐나갈 기준점에 대한 윤리학적 논의를 제시하였다. 인터넷의 등장과 사이버 공간의 확장은 사회의 발전과 인류의 진보를 그리는 낙관적 기대를 일부 실현하는 한편 사이버 위협에 대한 노출을 증가시키는 결과도 낳았다. 사이버 안보 문제가 국가안보의 이슈가 되는 경향은 보편적으로 발견되며, 그 결과 정부가 사이버 위협에 대응하기 위해 취하는 조치는 국민의 프라이버시를 침해하거나 민주주의 가치를 훼손할 소지가 있어 논란을 일으킨다. 사이버 안보, 프라이버시, 민주주의 등은 모두 인간의 좋은 삶을 뒷받침하는 가치로서 이들이 충돌할 때 간단히 어느 하나를 선택하기는 어렵다. 즉, 다양한 가치를 평가하고 그 우열을 판단할 수 있도록 하는 윤리학이 사이버 안보에 적용될 필요가 있다. 제9장은 주요한 윤리적 관점인 덕 윤리, 의무론, 결과론을 사이버 안보에 적용할 것을 제안한다. 특히 국가의 행복과 이를 구성하는 국가 구성원 개개인의 행복이라는 양자 관계를 고려해야 한다는 것이다. 사이버 안보, 프라이버시, 민주주의 등의 가치가 국가와 개인의 관계 속에서 충돌하는 경우, 지나치지도 모자라지도 않는 중용을 파악하고 실천하는 것이 중요한 과제라고 주장한다.

Ⅳ. 사이버 안보와 국제정치

1. 사이버 안보와 외교

사이버 안보와 외교에 대한 논의는 최근 관심을 끌고 있는 과학기술외교의 맥락에서 이해할 필요가 있다. 최근 과학기술외교는 과학기술 전담 부처가 담당하는 대외협력 정도로 생각하던 수준을 넘어서 국가적 차원에서 수행되는 외교안보 전략 일반의 맥락으로 그 외연을 확장하고 있다. 과학기술외교의 외연은 넓어졌지만, 그 내포는 오히려 조밀해져서 '국가간 갈등 조정'이라는 구체적 미션을 수행하는 차원에서 과학기술외교가 고민되고 있다. 이렇게 기존의 과학기술외교를 새롭게 업그레이드해서 추진할 필요성은 최근 지정학 환경의 출현으로 인해서 제기되었다. 다시 말해, 기술과 외교의 관계를 '안보의 프레임'으로 보는 경향이 부상한 것이다. 게다가 기술과 관련된 객관적 안보위협만 논하는 것이 아니라 안보위협이 주관적으로 구성하는 안보화의 메커니즘이 작동하고 있다. 이러한 맥락에서 기술 변수가 경제와 산업의 경계를 넘어서. 안보와 외교의

문제로서 자리매김하고 있으며, 이러한 과정에서 기술안보는 '지정학적 임계점'을 넘어서 위기를 야기하는 '기술지정학(Tech-geopolitics)'의 논제가 되었다.

오늘날 과학기술외교는 반도체, 5G, 인공지능, 그린테크 등과 같은 좁은 의미의 과학기술 분야를 넘어서 디지털 산업과 플랫폼 경제, 공공외교 분야 등으로 확대되면서 다양한 이슈들과 연계되고 있다. 특히 앞서 언급한 사이버와 경제의 이슈연계라는 관점에서 볼 때, 첨단기술 제품과 핵심광물의 공급망 안보 확보를 위한 외교적 노력이 최근 국제정치의 관건이다. 이른바 디지털 플랫폼 경쟁 시대의 데이터 유통규범을 마련하려는 외교적 과정에서 데이터 주권, 데이터 국지화, 데이터 안보가 쟁점으로 거론된다. 최근에는 소셜 미디어를 기반으로 하는 가짜뉴스, 허위조작정보 등의 유포에 대한 국제적 공조도 외교의 아이템이 되었는데, 앞서 언급한 사이버 영향공작 또는 사이버 정보심리전/인지전에 대한 대응이 디지털 외교 또는 사이버 외교의 주요 이슈가 된 것이다. 이는 기존의 디지털 외교가 주로 '소프트 파워(soft power)'의 증진을 위한 공공외교에 중점을 두던 것에서 비해, 최근에는 이른바 '사프 파워(sharp power)'의 국제정치가 새로운 공공외교의 쟁점으로 부각된 것을 의미한다.

지정학적 임계점을 넘어서 전통적인 외교안보 이슈와 연계된 사이버 안보 분야의 외교는 양자-소다자-다자 차원에서 진행된다. 양자 차원에서 진행된 사이버 안보 외교로는 미국과 중국, 그리고 미국과 러시아가 정상회담에서 다룬 사이버 안보 관련 갈등의 조정에 주목할 필요가 있다. 최근 한미 정상회담을 통해서 이룬 사이버 안보 동맹의 성과도 양자외교의 산물이다. 한미일 안보협력체나 오커스(미국, 영국, 호주), 쿼드(미국, 일본, 호주, 인도), 파이브아이브(미국, 영국, 캐나다, 호주, 뉴질랜드) 등의 소다자 프레임워크에서도 사이버 안보 외교가 진행되고 있다. G7 플러스, 나토, 유럽연합(EU) 등과 같은 다자외교의 장에서도 사이버 안보 문제가 논의된다. 이밖에 선진국들의 정부간협의체도 가동 중인데, '사이버 안보 분야의 랜섬웨어 대응 이니셔티브(Counter Ransomware Initiative, CRI)나 인공지능 분야의 GPAI와 REAIM 등을 주목해야 한다. 한국과 같은 중견국에 사이버 안보 분야의 동지국가(同志國家, like-minded countries) 연대 외교의 추진은 매우 중요하며, 동아시아 역내 협의체(예를 들어, ARF)와 지역 간 협력체(예를 들어 한-나토 사이버 협력, 한-OSCE 사이버 협력)에서 벌이는 사이버 규범외교도 매우 중요한 사이버 안보 외교의 아이템이다(김상배. 2019).

제10장은 사이버 안보 분야에서 벌어지는 외교의 의미와 그 배경이 되는 사이버 공간이 외교의 영역으로 편입되는 상황을 잘 소개하고 있다. 초국가적 공공재의 성격을 갖는 사이버 공간은 현대 국가의 통신, 행정, 교육, 금융, 외교, 군사 활동이 수행되는, 외부의 공격으로부터 국가가 반드시 지켜내야 하는 주권 수호의 공간이기도 하다. 사이버 공간은 첨단 신기술과 결합되면서 더욱 고도화되고 있고 군의 지휘통제 체제는 사이버 공간을 통해 연결되고 있기 때문에 사이버 공간은 지속적으로 안보화되고 있다는 것이다. 그런데 사이버 공간에서 발생하는 수많은 문제는 일개 국가가 홀로 해결할 수 없으므로 국가는 외교활동을 통해 다양한 위협으로부터 사이버 공간을 안전하게 보호하고 개방된 사이버 공간을 자유롭게 사용하기 위한 국제협력을 추구하고 있다. 각국은 자국과 타국의 디지털 역량과 회복력을 강화하기 위한 국제협력을 도모하기 위해 양자외교와 소자다외교, 다자외교를 펼침과 동시에 주로 적성국 간 공격 혹은 초국가 사이버 범죄에 대응하는 전략토론과 군사훈련 등 동맹 및 우호국과 진영외교를 추구하고 있다.

2. 사이버 안보와 동맹

사이버 안보 외교 중에서도 최근에 힘을 받고 있는 것은 동맹외교의 행보이다. 특히 화웨이

사태를 계기로 사이버 동맹이 이슈가 되었다. 미국의 화웨이 제재에 파이브아이즈 국가가 동조하고 일본, 독일, 프랑스도 가담하면서 '파이브 아이즈+3'이라는 말이 나오기도 했다. 좀 더 넓은 맥락에서 사이버 동맹의 전개는 미국의 인도·태평양 전략과 중국의 '일대일로' 이니셔티브의 경합이라는 구도에서 보아야 한다. 이러한 구도는 2020년 트럼프 행정부 당시 미국의 '클린 네트워크'와 중국의 '글로벌 데이터 안보 이니셔티브'가 갈등하는 양상으로 비화되기도 했다. 이러한 사이버 동맹외교의 양상은 바이든 행정부에서도 지속되었다. 파이브아이즈 이외에도 쿼드나 오커스 등 소다자 협의체에서 동맹에 준하는 협력이 거론되고 있다. 이러한 사이버 동맹의 과정에서 주목할 것은 사이버 안보 또는 디지털 기술과 관련된 가치와 규범이 강조되는데, '민주주의정상회의'의 연장선에서 보는 '인터넷 미래의 선언'이 대표적인 사례이다.

사이버 동맹 이슈는 한미동맹의 맥락에서도 큰 쟁점이 되었다. 2023년 4월 열린 한미 정상회담의 큰 성과 중의 하나로 양국의 동맹을 사이버 공간에까지 확장하기로 한 선언을 들 수 있다. '전략적 사이버 안보 협력 프레임워크'라는 별도의 문서를 채택해 협력의 범위·원칙·체계 등의 내용도 구체화했다. 사이버 공간의 한미동맹이 어디까지 가야 하고 어떤 내용을 채울지, 그리고 이러한 양국동맹을 어느 나라로 확장시켜 나갈지는 앞으로 풀어가야 할 숙제이다. 특히 한미 정상회담 이후 미국 주도의 정보동맹인 파이브아이즈 수준의 협력을 목표로 하고, 영국, 일본, 캐나다 등과도 협력해 동맹을 확대하겠다는 구상이 제기되었다. 이러한 연장선에서 한국은 이러한 사이버 동맹의 프레임워크를 한미일 안보협력체뿐만 아니라 유럽 국가들, 특히 영국이나 네덜란드 등의 유럽 국가로 확대하고 있다.

제11장은 이러한 사이버 안보 분야의 복합동맹 양상을 다루었다. 오늘날 복합위기를 맞은 국제정치에서 대다수 동맹은 다영역에 걸친 공동 위협을 바탕으로 각국의 자원과 특성을 반영하여 다영역에 걸친 협력을 강화·확장하고 있다. 이러한 복합동맹에서 사이버 공간은 독립적 공간이면서 모든 물리적 공간을 연계하는 장이다. 최근 양자·다자 협력체에서 사이버 협력이 주요 의제로 부상하면서 복합동맹의 일부로 사이버 동맹에 대한 관심이 커졌다.

사이버 동맹은 일반 동맹과 마찬가지로 대외적 기능과 대내적 기능을 수행한다. 대외적 위협에 공동으로 대응하여 사이버 억지와 방어를 꾀한다. 나토 사이버방위센터(CCDCOE)의 확장, 한미 간 '전략적 사이버 안보 협력 프레임워크'의 체결이 최근 사례이다. 대내적으로 사이버 동맹은 표준을 공유하며 규범을 생성하고자 한다. 미국-유럽 무역기술위원회의 창설과 유럽연합이 동아시아 국가들과 맺은 디지털 파트너십에서 이러한 활동을 확인할 수 있다.

사이버 동맹은 사이버 역량을 갖춘 국가 간의 대칭적 의존관계라는 특징을 보인다. 비록 조약의무가 없더라도 사이버를 포함한 다영역에 걸친 상호 민감성과 취약성은 사이버 동맹의 지속과 강화를 낳을 전망이다. 향후 미국, 중국, 유럽이 주도하는 사이버 영역에서 '민주주의 대 권위주의' 대립이 심화할 가능성이 높지만, 강대국 정치뿐만 아니라 빅테크 기업의 영향 속에서 사이버 동맹 네트워크의 미래는 펼쳐질 것이다. 한국은 국제질서의 공동 건축자로 사이버 동맹을 활용하는 복합적 전략을 구비하고 이를 실행에 옮겨야 할 것이다.

3. 사이버 안보와 규범

국제정치의 사실상(de facto) 협력을 구성하는 사이버 동맹의 행보 이외에도 법률상(de jure) 차원에서 국제규범 형성에 참여하는 사이버 규범외교 활동에도 주목해야 한다. 최근 가장 주목을 받은 것은 유엔 정부자문가그룹(GGE)에서 진행된 사이버 안보 국제규범에 대한 논의였다. 그러나 유엔 GGE의 제5차 보고서 채택의 실패 이후 총회 결의에 따라 5년(2021-25) 회기의 신규

개방형워킹그룹(OEWG)이 출범했다. 그러나 전통 국제기구로서 유엔이라는 '국가간(inter-national)' 프레임을 빌어서 사이버 안보라는 신흥안보 이슈에 대한 규범형성의 논의를 진행하려는 시도에 대한 회의감도 만만치 않다는 점을 명심할 필요가 있다. 이밖에도 사이버 거버넌스 또는 좀 더 넓은 의미의 인터넷 거버넌스 분야에서는 국가 행위자 이외에도 민간 기업, 학계 전문가, 시민사회 활동가 등과 같은 다양한 비국가 행위자들이 참여하여 구성하는 '글로벌 거버넌스(global governance)' 프레임도 원용된다. 이러한 비국가 프레임에서 최근 빅테크 기업들의 역할이 커지고 있는 현상에 주목할 필요가 있다(김상배 편, 2019a).

사이버 안보 국제규범이 형성되는 다층적 구도를 가로질러서 미국과 유럽연합의 서방 진영을 한 축으로 하고, 중국과 러시아 및 개도국 등으로 구성되는 비서방 진영을 다른 한 축으로 하는 국가 진영간의 이해관계 대립이 전개되고 있다. 이러한 대립 구도의 이면에는 서방 진영의 이른바 '다중이해당사자주의(multistakeholderism)'와 비서방 진영의 정부 간 다자주의(multilateralism)라는 관념의 차이가 자리 잡고 있다. 이러한 다층적 대립의 구도는 유엔과 같은 전통 국제기구의 장뿐만 아니라 정부간 협의체나 여타 글로벌 거버넌스의 장에서 여러 가지 쟁점을 놓고 확장 및 심화되어 가고 있다. 이러한 과정에서 기존 국제법의 적용(주권 적용), 구속력 있는 규범의 필요성(비구속적 규범 제안 및 이행), 신뢰구축조치의 개발 및 이행, 역량 강화의 활동, 정례협의체 설치 등과 같은 주요 쟁점별로 진영 간의 근본적 시각 차이가 노정되고 있음을 놓치지 말아야 한다.

제12장은 이러한 사이버 안보 국제규범의 형성을 위한 노력의 전개 과정에서 제기된 쟁점과 이러한 규범 형성의 노력이 지닌 한계를 분석하였다. 특히 제12장은 지난 20여 년 동안 사이버 공간을 규율할 수 있는 규범 정립에 대한 논의가 지속되어 왔음에도, 사이버 공간을 악용한 공격은 지속되고 있으며 이에 대한 책임 부과는 전무하다고 비판한다. 2022년 발발한 러시아의 우크라이나에 대한 사이버 공격은 피해국인 우크라이나에 심각한 피해를 초래했음에도, 국제사회가 이에 대해 책임을 부과할 수 있는 국제규범은 아직 정립되지 않고 있다는 것을 사례로 들고 있다.

국제사회는 나토의 CCDCOE를 중심으로 강제성을 갖는 국제법 제정을 위한 노력을 진행했고, 동시에 비구속적·자발적 규범 정립을 위한 논의를 다자적 국제기구 차원과 지역기구 차원에서 진행했다. 또한 자발적 규범 정립 노력은 다양한 형태의 소다자 회의체와 양자 협력에서 다루어지기도 했다. 규범 형성을 위한 노력의 주체적 측면에서 보면, 이러한 플랫폼에서 국가 중심의 규범 형성에 대한 논의와 동시에 민간 기업이나 시민사회가 주도한 이니셔티브도 별개로 진행되었다. 이러한 가운데 국제사회는 국가가 주도한 사이버 공격 행위를 어떻게 규제 및 저지할 것인지에 대한 국제규범을 자국에 유리한 방향으로 정립하고자 치열히 경쟁해 왔으며, 그동안 미국과 영국으로 대표되는 서방 진영과 중국과 러시아로 대표되는 비서방 진영은 사이버 공간을 규율하는 규범 및 원칙 설립에 큰 이견을 보여 왔다.

이러한 규범 형성 논의들은 주로 국제법 및 주권 개념의 적용가능성, 비구속적 규범의 제안 및 이행 등을 다루었다. 특이한 사항은 해당 주제들이 논의되는 플랫폼과 관계없이 진영간 의견이 명확히 갈리고 있어, 합의점을 얻기 어려운 상황이라는 점이다. 이러한 문제의식을 바탕으로 제12장은 규범의 개념과 정의에 대해 살펴보고, 사이버 공간에 적용가능한 규범 정립 노력을 강제성의 측면, 규범 형성 주체의 측면에서 살펴보았다. 그리고 이들 논의가 주목하는 대주제별 진영간 입장과 논리도 살펴보았다. 앞으로 전개될 사이버 안보 국제규범 형성 논의의 방향을 전망함으로써, 해당 논의에서 한국의 역할과 시사점을 찾고자 했다.

4. 사이버 안보와 평화

사이버 안보 관련 개념에 대한 연구와 짝을 맞추는 차원에서 사이버 평화의 개념에 대한 탐구도 필요하다. 단순히 '전쟁 없는 평온한 상태'라는 전통적 시각으로만 평화를 이해해서는 오늘날 복잡다단한 맥락에서 제기되는 사이버 공간의 평화라는 문제가 제기하는 난제를 제대로 풀기 어렵다. 전쟁에까지 이르지 않더라도 우리 삶의 평화를 해치는 요인들은 너무나도 많아져서, '평온한 상태'를 준거로 평화를 추구하려는 소극적 차원의 노력만으로 평화를 달성하는 것은 요원한 이상이 될 가능성이 있다. 또한 안보위협에 대처하고 평화를 모색하는 방식도, 거시적 차원에서 발생하는 폭력적 분쟁에 대한 국가적 개입 이외에도, 미시적 차원의 갈등 해소와 신뢰 구축을 위한 다양한 행위자들의 활동도 포괄해야 한다. 그야말로 안보 분야 못지않게 평화 분야에서도 시대적 환경의 변화에 걸맞은 새로운 평화론과 대응전략에 대한 논의가 필요하다(김상배, 2023b).

사이버 안보의 국제정치학적 주제 중에서 '사이버 평화'는 충분히 연구되지 않은 가장 대표적인 주제 중의 하나이다. 사이버 평화는 기존 평화연구에서 상정하는 거시적 차원의 '폭력의 부재'로만 이해할 수 없는 논제이다. 전쟁이 없어 평온해 보이는 상태이지만, 악성코드가 창궐하여 삶이 어지러운 상황을 '평화'라고 부를 수는 없기 때문이다. 거시적 차원에서 평화를 보는 기존의 시각만으로는 안보위협이 미시적 차원에서 발생해서 거시적 차원으로 창발하는 사이버 안보 분야의 평화 문제를 제대로 파악하기 어렵다. 전통 평화론의 시각에서 보면 사이버 평화는 평화를 거론 정도에 미치지 못하는, 그냥 '수면 아래의 현상'일 뿐이다. 그러나 신흥안보의 시대에는, 겉으로는 평온해 보이는 상태일지라도 그 이면에서는 계속 갈등을 생성하는 동태적 과정을 적극적으로 파악하는 평화연구가 필요하다.

제13장이 강조하듯이, 오늘날 사이버 공간은 기술과 사회의 발전을 주도하는 공간이 되고 있으며 끊임없이 확장되고 있다. 또한 사용자 간 그리고 물리적 공간과 사이버 공간 간 연결성이 강화되면서 사이버 공간의 양적 확장과 질적 변환도 가속화되는 중이다. 이처럼 진화하는 사이버 공간의 변화는 인류의 번영을 위해 현실 공간만큼이나 안정과 평화가 필요함을 시사하고 있다. 그러나 사이버 안보 이슈를 향한 관심과 대응 노력에 비해, 보다 궁극적 목표라 할 수 있는 사이버 공간의 안정성, 나아가 사이버 평화에 대한 심도 있는 논의는 거의 부재한 상황이다. '안전하고 평화적인 사이버 공간'이 갖는 포괄적 의미도 한정하기 어려워지고 있다. 특히 증대되고 있는 신흥안보 이슈의 부상은 사이버 공간의 평화 개념을 어디까지 확장할 것인가에 지대한 영향을 미치는 주요 변수로 자리 잡고 있다. 그중에서도 가상과 현실이 융합하고 이슈 간 경계를 허물어 버리는 사이버 공간의 진화는 사이버 안보뿐만 아니라 사이버 평화의 개념에 대해서도 새롭게 접근해야 할 필요성을 제기한다. 특히 사이버 공간이 갖는 동태적 확장성과 초월적 특징이라는 물리적 세계와의 차별성을 면밀히 고려하여 검토한 연구들은 부족한 실정이다.

이와 같은 문제의식에 착안하여, 제13장은 사이버 평화가 의미하는 개념을 좀 더 심층적으로 살펴보았다. 첫째, 논의에 앞서 사이버 공간이 구성되는 원리에서 사이버 평화를 실현하기 위한 주요 조건에 이르기까지를 탐색하고, 기존의 평화 개념을 사이버 공간에 그대로 대입하는 작업이 한계를 갖는 이유를 짚어 보았다. 둘째, 사이버 공간이라는 새로운 영역에서 국가뿐만 아니라 다양한 행위자들을 상정해야 하는 이유와 동태적 관점에서 '과정으로서의 평화'를 지향해야 하는 당위성을 제시하였다. 셋째, 우리는 왜 사이버 평화를 실현하려 하는가에 대한 궁극적 질문과 함께, 평화 자체가 가져다주는 안정감의 의미를 넘어 그것이 내재하는 근원적 가치들이 있음을 주장하였다. 대표적으로 지속가능한 사이버 평화의 프로세스를 안정적으로 확보하는 가운데 사이버

공간의 '자유'를 기대할 수 있음을 중요한 사례로 설명하였다. 사이버 안보가 안보의 영역에서 자리 잡는 데까지 일정 시간이 필요했던 만큼, 사이버 평화도 개념의 정교화를 거쳐 사이버 공간 질서의 유의미한 메커니즘으로 확립되기 위해서는 더 많은 실현 가치의 사례들이 뒷받침되어야 할 것이다.

Ⅴ. 맺음말

정보세계정치학의 어젠다 중에서 사이버 안보는 제일 먼저 국제정치학의 하위분야를 형성한 주제이다(김상배·민병원 편, 2018). 최근 세상의 변화는 사이버 안보의 문제가 기술·공학 분야 전문가들의 경계를 넘어서 좀 더 넓은 의미의 사회과학적 탐구의 대상이 되어야 함을 보여준다. 특히 사이버 안보를 둘러싸고 벌어지는 각국의 경쟁과 갈등은 이 문제가 이미 국제정치학의 영역으로 진입했음을 보여준다. 정보화시대의 초창기부터 전쟁과 안보 및 국제질서 등과 같은 국제정치학 논제가 없었던 것은 아니지만, 2000년대 말까지만 해도 사이버 안보 연구는 국제정치학의 본격적인 어젠다로 자리 잡지는 못했다. 그러던 중 2010년대에 닥쳐온 두 차례의 큰 계기를 만나면서 사이버 안보의 국제정치학이 제 얼굴을 드러냈다.

사이버 안보를 국제정치학의 시각에서 보아야 한다는 국내외 학계의 문제의식을 불러일으킨 계기는 2013년에 발생한 일련의 사건들을 통해서 마련되었다. 이들 사건은 이른바 '사이버 안보의 전회(轉回, turn)'라고 부를 정도의 파장을 낳았다(김상배, 2018). 특히 이 무렵부터 사이버 안보 문제를 군사전략의 시각에서 보기 시작했으며, 주요 국제협력의 대상으로 거론하기 시작했다. 2013년 특별히 세간의 이목을 끌었던 사건들로는, 3.20 사이버 공격. 탈린매뉴얼의 발표. 맨디언트 보고서 발간, 에드워드 스노든의 폭로, 미중 정상회담에서 사이버 안보 어젠다의 채택, 유엔 정부전문가그룹(GGE) 제3차 회의 최종 권고안 합의 도출, 서울 사이버스페이스총회 개최 등을 들 수 있다. 하나하나가 모두 국제정치학의 연구 주제로 손색이 없는 사건들이었다.

국제정치학계의 주위를 환기시킨 또 다른 계기는, 2018-19년에 정점에 달했던 이른바 '화웨이 사태'였다. 이는 복잡다단해지는 미중경쟁의 단면을 극명하게 보여준 사례였다. 일련의 과정에서 미국 정부는 화웨이의 5G 이동통신 장비 문제를 산업의 문제가 아닌 안보의 관점에서 봐야 한다고 강조했다. 화웨이 제품에 심어진 백도어를 통해서 미국의 국가안보를 해칠 정보와 데이터가 빠져나간다는 것이었다. 이러한 인식은 중국에 대한 미국의 수출입 규제와 이에 수반된 미중 양국 간의 공급망 마찰로 나타났으며, 이례적으로 우방국들을 동원해서라도 화웨이 제품의 확산을 견제하려는 미국의 '세(勢) 싸움' 작전으로 발전했다. 이러한 미국의 압력은 동맹국인 한국에도 가해지면서 단순한 기술·산업 문제가 아닌 외교안보 문제로 각인되기에 이르렀다. 이후 학계의 관심은 '제2의 화웨이 사태'가 발생하면 어떻게 할 것이냐의 문제를 천착하고 있다.

2020년대에 접어든 사이버 안보 이슈는 국제정치학의 전통적인 주제들과 만나면서 자기 증식을 거듭해 가고 있다. 특히 미중 기술패권 경쟁의 가속화와 우크라이나 전쟁의 발발이라는 변수가 '사이버 안보의 지정학' 현상을 증폭시키고 있다. 미중 간에 공급망 안보 교란, 사이버 동맹과 외교, 규범형성과 가치경쟁 등의 문제가 우여곡절을 겪으면서 난항을 거듭하고 있다. 우크라이나 전쟁의 발발은 사이버전과 물리적 전쟁의 연계뿐만 아니라 사이버 안보 분야에서의 공세적 방어, 사이버-핵 넥서스, 사이버 억지와 평화 등의 문제를 수면 위로 떠올렸다. 이 모두 향후 국제정치학적 연구가 다루어야 할 중요한 주제들임은 물론이다. 이러한 과정에서 정책연구나 사

례연구의 시각 이외에도 이론과 역사 및 사상의 시각에서 착안된 진지한 연구가 진행되어야 할 것이다.

〈참고문헌〉

김상배. 2018.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』. 한울.
김상배. 2019. “사이버 안보와 중견국 규범외교: 네 가지 모델의 국제정치학적 성찰.” 『국제정치논총』, 59(2), pp.51-90.
김상배. 2022.『미중 디지털 패권경쟁: 기술-안보-권력의 복합지정학』. 한울.
김상배. 2023a. “사이버 억지의 새로운 개념화: ‘한미 사이버 안보 동맹론’의 성찰적 맥락에서.” 『국제정치논총』, 63(2), pp.51-88.
김상배. 2023b. “신흥평화의 개념적 탐색: ‘창발(emergence)’의 시각에서 본 평화연구의 새로운 지평.”『한국정치학회보』, 57(1), pp.225-248.
김상배. 편, 2017.『사이버 안보의 국가전략: 국제정치학의 시각』. 사회평론.
김상배. 편. 2019a.『사이버 안보의 국가전략 2.0: 국제규범의 형성과 국제관계의 동학』. 사회평론.
김상배. 편. 2019b.『사이버 안보의 국가전략 3.0: 16개국의 전략형성과 추진체계 비교』. 사회평론.
김상배. 편. 2023.『신흥기술과 사이버 안보의 국가전략: 국제정치학적 어젠다의 발굴』. 사회평론.
김상배·민병원 편. 2018.『사이버 안보의 국제정치학적 지평: 전략과 외교 및 규범』. 사회평론.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.