출판용 최종제출본 | 2020-08-29

미중경쟁 시대 한국의 사이버 안보 전략:

중견국 외교론의 시각

김 상 배 | 서울대학교

<핵심논지>

1. 최근 첨단기술 분야에서 미중 간에 벌어지는 사이버 안보 갈등은 해킹 공격이나 시스템의 교란과 파괴, 금전탈취나 정보절취 등을 노리는 단순한 해킹의 문제를 넘어서, 기술-산업-통상-데이터-군사-외교-정치-법제도-국제규범 등에 걸친 미래 패권경쟁의 복합적인 쟁점으로 진화하고 있다.
2. 사이버 안보 분야에서 형성되는 세 차원의 구조, 즉 미중경쟁이 창출하는 지정학적 이해갈등의 권력구조, 서방 및 비서방 진영 또는 선진국 및 개도국 진영 간의 대립이 형성하는 제도적 구조, 글로벌 인터넷 거버넌스의 방식을 둘러싼 관념형성의 구조 등은 중견국 한국의 사이버 안보 전략에 영향을 미치는 주요 변수이다.
3. 한국은 사이버 안보 분야에서 전개되는 세계정치 구조변동에 대응하는 전략이 단순한 기술 선택의 문제나 해킹 공격에 대비하는 차원을 넘어서, 전통적인 동맹과 외교의 문제를 포함한, 좀 더 복잡한 지정학적 또는 외교전략적 선택을 강요할 가능성이 높은 문제라는 점을 인식하고 이에 대한 적절한 대응책을 마련해야 할 것이다.

<정책제언>

1. 무엇보다도 미중경쟁 시대의 사이버 안보전략이 지니는 의미가 단순히 기술과 공학 분야의 대응책이 아니라 중견국 외교전략의 성격을 띠고 있음을 인식해야 한다. 한국의 사이버 안보전략은 미국과 중국의 패권경쟁의 사이에서 생존과 번영을 모색하는 문제인 동시에, 이러한 과정에서 전통적인 한미동맹의 틀을 유지하면서도 새로이 한중협력을 확대해 나가야 할 미래전략 전반의 과제와 연결됨을 명심해야 할 것이다.
2. 좀 더 구체적으로 사이버 안보 분야에서 다층적으로 형성되는 '구조적 공백'의 틈새를 공략하는 '적극적 중개자'의 역할을 모색해야 할 뿐만 아니라, 이러한 중개의 역할을 완수하기 위해서 동지국가들을 규합함으로써 국제사회 전반의 지지를 이끌어 내며, 새롭게 형성되는 사이버 안보 분야 국제규범의 형성 활동에 참여하는 중견국 외교의 리더십을 발휘하기 위해서 노력해야 할 것이다.
3. 국내 사이버 안보전략의 추진체계 전반을 정비하는 노력과 함께 사이버 안보외교 분야의 추진체계도 정비하는 작업에 대한 고민이 필요하다. 정부 각 유관 실무부처 및 청와대 컨트롤타워를 포괄하는 사이버 안보 전략의 추진체계 정비 작업을 진행해야 하며, 이외에도 전문가들과의 협업 강화를 통해서 지식 집약적인 사이버 안보외교 분야의 수요에 부응하는 정책지식 네트워크의 구축도 필요하다.

Ⅰ. 머리말

최근 미중갈등의 불꽃이 어느 한 영역에만 국한되지 않고 미중관계 전반으로 번져가는 양상을 보이고 있다. 그야말로 미중경쟁은 미래권력을 놓고 벌이는 패권경쟁을 방불케 한다. 이러한 면모를 단적으로 보여주는 사례가 '선도부문'(leading sector)으로서 '4차 산업혁명' 부문에서 벌어지는 양국의 기술패권 경쟁이다. 역사적으로 해당 시기의 선도부문에서 벌어졌던 기술패권 경쟁의 향배는 패권국과 도전국의 승패를 가르고 국제질서의 구조를 변동시켰다. 오늘날 선도부문의 미중경쟁도 그러한 의미를 갖는다. 다만 이전의 경우와 다른 특징이 있다면, 지금의 경쟁은 사이버 공간을 매개로 한 네트워크 환경에서 진행되며, 이러한 과정에서 사이버 안보가 중요한 현안으로 불거졌다는 사실이다. 실제로 2010년대 초중반을 거치면서 사이버 안보는 명실상부한 국제정치학의 어젠다로 자리 잡았다(김상배. 2018a).

이제 사이버 안보는 시스템의 교란과 파괴, 금전탈취나 정보절취 등을 노리는 단순한 해킹의 문제를 넘어서 기술-산업-통상-데이터-군사-외교-정치-법제도-국제규범 등에 걸친 미래 패권경쟁의 복합적인 쟁점으로 진화하고 있다. 미시적 차원의 안전 문제일지라도 그 수량이 늘어나고, 여타 이슈들과 연계되면서, 거시적 차원의 지정학적 위기로 창발(創發)하는 '신흥안보'(emerging security) 현상의 전형적인 특징을 보이고 있다. 사이버 공격은 더 이상 해커들의 장난거리나 범죄집단의 사기행각, 또는 테러집단의 저항수단만은 아니다. 타국의 주요 기간시설에 대한 해킹의 이면에 국가 차원의 체계적 지원이 있음은 공공연한 비밀이 되었다. 국가안보를 이유로 사이버 안보에 위협이 되는 IT보안제품의 수출입 규제가 가해지며 데이터의 초국적 유통이 통제되기도 한다. 국제적으로도 사이버 안보는 동맹세력을 규합하는 명분이자 첨단 군비경쟁의 빌미가 된다.

사이버 안보 문제가 국가 간 갈등을 야기할 가능성이 커지면서, 전통 지정학의 시각을 원용하여 이 문제를 보려는 경향도 득세하고 있다. 그아말로 기술 문제가 '지정학적 리스크(geopolitical risk)'를 야기하는 변수가 되었다. 실제로 사이버 공격의 문제는 전쟁 수행이라는 군사전략 차원에서 고려되고, 이를 지원하는 물적·인적 자원의 확보가 중시된다. 자국의 주요 기반시설을 노린 사이버 공격에 대해서는 맞공격을 가해서라도 억지하겠다는 행보가 힘을 얻고 있다. 그럼에도 사이버 안보의 세계정치는 과거의 현실에서 잉태된 전통 지정학의 시각을 그대로 적용하여 이해하기에는 너무나도 복잡한 양상으로 진화해 가고 있다. 이러한 문제의식을 바탕으로 이 글은 전통 지정학의 경계를 넘어서는 다양한 변수들을 포괄적으로 고려하는 새로운 시각으로서 '복합지정학'(Complex Geopolitics)을 제안한다(김상배. 2018a).

복합지정학의 시각에서 본 미중 사이버 안보 갈등은 다양한 영역에 걸쳐서 진화하고 있다. 제일 눈에 띄는 것은 기술패권 경쟁이라는 명목으로 벌어지는 지정학적 경쟁이다. 이는 '화웨이 사태'와 같은 사이버 안보 논란뿐만 아니라 여타 민군겸용기술과 관련된 정치·군사안보 문제와 연계될 조짐을 보이고 있다. 이러한 갈등은 표면적으로는 미국의 기술경쟁력 하락에서 비롯된 양국 간 통상마찰 문제와 이에 수반된 보호주의적 법·제도의 마찰 문제로 나타나고 있다. 게다가 이렇게 복합적인 양상을 보이는 미중 사이버 갈등의 전면에서 첨단기술의 문제를 국가안보 문제로 '안보화(securitization)'하는 미중 두 나라의 안보담론 경쟁이 벌어지고 있다(Hansen and Nissenbaum, 2009). 이러한 안보담론 경쟁을 통해 미중 양국은 동맹국들을 결속하고 동지국가들과 연대하면서 자국에 유리한 사이버 공간의 국제규범을 마련하려는 경쟁을 벌이고 있다.

이렇듯 복합지정학적 지평을 펼쳐놓고 있는 미중경쟁에 한국은 어떻게 대응해야 할까? 최

근 어느 국내업체의 화웨이 장비 도입을 둘러싼 논란에서도 나타난 바와 같이, 미중 사이버 안보 갈등은 단순한 기술과 산업의 문제가 아니라 안보와 정치의 문제로 다가올 가능성이 있다. 자칫 미중 기술패권 경쟁이 그 사이에 낀 한국에 지정학적 위기를 야기하는 상황이 벌어질지도 모른다. 다시 말해, 미중 사이버 경쟁은 한국으로 하여금 단순한 기술 선택의 문제가 아니라, 전통적인 동맹과 외교의 문제를 포함한, 좀 더 복잡한 지정학적 선택을 강요할 가능성도 없지 않다. 복합지정학의 시각에서 미중 사이버 안보 경쟁에 대한 적절한 대응책을 마련하는 지혜가 절실하게 필요한 시점이다. 이 글은 한국에 닥친 전략적 선택의 문제를 중개외교, 연대외교, 규범외교 등으로 대변되는 중견국 외교론의 시각에서 검토하였다(김상배, 2016).

이 글은 크게 네 부분으로 구성되었다. 제2장은 미중 사이버 안보 경쟁의 복합지정학을 미중 사이버 갈등과 기술패권 경쟁, 데이터 레짐마찰, 국제규범 경쟁 등의 사례를 통해서 살펴보았다. 제3장은 중개외교의 시각에서 본 한국의 사이버 안보전략을 미중이 벌이는 기술과 제도 및 담론의 표준경쟁이라는 시각에서 살펴보았다. 제4장은 연대외교의 시각에서 본 한국의 사이버 안보전략을 미중이 벌이는 동맹과 연대의 네트워크 외교라는 맥락에서 살펴보았다. 제5장은 규범외교의 시각에서 보는 한국의 사이버 안보전략을 사이버 안보의 국제규범 형성과정에서 나타나는 중견국 규범외교 모델에 대한 논의에 비추어 살펴보았다. 끝으로, 맺음말에서는 이 글의 주장을 종합·요약하고 대외적으로 사이버 안보의 중견국 외교를 추진하기 위해서 필요한 국내 추진체계 정비의 과제를 짚어보았다.

Ⅱ. 미중 사이버 안보 경쟁의 복합지정학

1. 미중 사이버 안보 갈등의 진화

길게 보면 사이버 안보를 둘러싼 미중갈등의 역사는 20여 년 전으로 거슬러 올라간다. 1999년 5월 미군이 유고 주재 중국 대사관을 오폭하여 당시 중국 해커들이 미국 내 사이트에 대해 보복 해킹을 가한 사건이 발생하였다. 2001년 4월 중국 전투기가 미군 정찰기와 충돌 후 중국 하이난에 추락하는 사고가 발생하자 중국 해커들이 사이버 공격을 감행하기도 했다. 당시 언론에서 '미중 사이버 전쟁'이라는 말이 처음으로 사용되기도 했다. 2003년 중국산으로 추정되는 웰치아 바이러스가 미국 정부 전산망을 공격하여 비자 발급업무가 일시 중단되는 일이 발생하고, 같은 해 미국 내 군사연구소와 미 항공우주국, 세계은행 등을 해킹한 '타이탄 레인 공격'은 미중 사이버 공방의 본격적인 신호탄이 됐다. 2009년에는 구글, 아도비, 시스코 등 30여개 미 IT기업들에 대한 중국 해커들의 대대적인 공격이 있었는데, 이는 '오로라 공격'으로 알려져 있다. 2011년의 '쉐이디 랫(Shady RAT) 공격'은 미국의 정부, 국제기구, 기업, 연구소 등 72개 기관에 대한 중국의 해킹 공격이었다.

미국의 주요 기반시설에 대한 중국 해커들의 공격은 2010년대로 넘어오면서 오바마 행정부로 하여금 군사적 방안까지 포함한 맞대응 카드를 꺼내들게 했다. 이른바 '중국 해커 위협론'은 2010년대 초중반 미중관계를 달구었던 뜨거운 현안 중의 하나였다. 2013년 미국의 정보보안업체인 맨디언트의 보고서는, 1997년에 창설된 중국의 해커 부대인 61398부대가 미국의 기업과 공공기관을 해킹하여 지적재산을 탈취하고 있다고 폭로했으며, 이는 2014년 5월 미 법무부가 이들 61398부대의 장교 5인을 기소하는 조치로 이어졌다. 이때에 즈음하여 오바

마 행정부는 국가 기간시설에 대한 해킹을 국가안보 문제로 '안보화'(securitization)하고 때로는 미사일을 발사해서라도 대응하겠다는 '군사화'의 논리를 내세우며 사이버 안보를 국가 안보전략의 핵심 항목으로 격상시켰다. 급기야 사이버 안보 문제는 2013년 6월 미중 정상회담의 공식의제로 채택되는 상황에까지 이르렀다.

2017년 트럼프 행정부 출범 이후 미중 사이버 갈등은 좀 더 복합적인 양상으로 전개되었다. 예상과는 달리 미중 사이버 공방은 군사적 충돌로 비화되기보다는 오히려 산업과 통상 문제와 긴밀히 연계되는 양상을 보였다. 트럼프 행정부는 이른바 '중국산 IT보안제품 위협론'을 내세워 중국 기업들의 IT보안제품에 대한 규제를 강화했다. 특히 5G 이동통신 분야와 같은 4차 산업혁명 분야에서 기술경쟁력을 쌓고 있는 중국 기업들에 대한 미국의 견제가 가해졌다. 실제로 화웨이, ZTE, 차이나모바일, DJI, 하이크비전, 푸젠진화 등과 같은 중국 IT기업들이 미국 시장에 진출하는 과정에서 다양한 문제들이 빌미가 되어 발목이 잡혔다. 기술경쟁과 통상마찰의 외양을 한 이들 문제는 사이버 안보나 데이터 주권 등의 쟁점과 연계되면서 그 복잡성이 더해갔다. 국가안보의 함의가 큰 민군겸용기술(dual-use technology) 분야에서 벌어졌던, 과거 1990년대 미일 패권경쟁의 전례를 떠올리게 하는 양상이 벌어졌다(김상배. 2018b).

2. 화웨이 사태와 미중 기술패권 경쟁

미중 사이버 안보 갈등의 가장 핵심적인 쟁점은 중국의 통신장비 업체인 화웨이를 둘러싼 논란이었다. 그전에도 미국 정부와 화웨이의 갈등은 없지 않았지만, 그것이 미중 양국의 기술패권 경쟁이라는 맥락에서 이해될 정도로 격화되기 시작한 것은, 2018년 2월 CIA, FBI, NSA 등 미국 정보기관들이 화웨이 제품을 사용하지 말라는 경고를 내리면서 부터였다. 미국은 2018년 8월에는 <국방수권법>을 통과시키며 미 공공기관 등에서 중국산 네트워크 장비의 사용을 금지했다. 2018년 12월에는 화웨이 창업자의 큰 딸인 멍완저우 화웨이 최고재무책임자(CFO) 겸 부회장이 대이란 제재 위반 혐의로 체포되며 화웨이 장비 도입 문제를 둘러싼 미중 양국의 갈등은 클라이맥스에 다다랐다(김상배. 2019c).

이른바 '화웨이 사태'로 불리는, 이러한 사이버 안보 논란의 과정에서 5G 이동통신 기술 분야에서 선두를 달리는 화웨이의 네트워크 장비가 표적이 되었다. 화웨이 장비가 이른바 백도어를 통해서 미국의 국가안보에 크게 영향을 미칠 수 있는 정보를 유출시킬 가능성이 있기 때문에 미국의 정부기관뿐만 아니라 민간 기업들도 이를 도입하지 말아야 한다는 것이었다. 4차 산업혁명 시대의 초연결 사회에서 화웨이 장비의 위험성은 단순한 기술의 문제가 아니라 국가안보의 문제라는 것이 강조되었다. 이러한 과정에서 화웨이 백도어가 실재하는 안보위협이라는 주장과 이는 단지 미국이 '안보화'의 과정을 통해서 구성해 낸 위협일 뿐이라는 주장이 팽팽히 맞섰다.

미국 정부가 주장하듯이 중국산 네트워크 장비의 도입은 보안위협이 될 수 있다. 특히 중국 정부의 지원을 받아 성장한 화웨이의 행보나 투명성이 부족한 기업문화와 성격을 보면 이러한 주장은 '합리적 의심'으로 인정될 수 있다. 그렇지만 정작 미국 정부가 보안위협의 객관적 증거를 제시하고 있는 것도 아니어서 문제의 복잡성이 커졌다. 이러한 공세에 대해 화웨이도 자사의 제품이 보안위협이 아니라는 명백한 증거를 제시하고 있는 것도 아니다. 화웨이의 입장은 자사 장비의 보안문제가 발생한 적이 아직까지 없으며, 만약에 문제가 발생한다면 회사 문이라도 닫겠다는 식이었다. 마치 '블랙박스'를 가운데 두고 누구 말이 맞는지 믿어달라고 '말싸움'을 벌이는 모습이었다.

화웨이의 통신장비가 미국의 국가안보에 실제 위협인지에 대해서는 논란의 여지가 있을지 몰라도, 화웨이로 대변되는 중국 기업들의 기술추격이 5G시대 미국의 기술패권에 대한 위협임은 분명하다. 화웨이 제품은 가격경쟁력을 보유하고 있을 뿐만 아니라 기술력도 세계 최고의 수준을 자랑하며, 2018년 현재 화웨이의 글로벌 이동통신 장비 시장점유율은 28%로 세계 1위이다. 화웨이 사태의 이면에 중국의 '5G 기술굴기'에 대한 미국의 견제의식이 강하게 깔려 있음을 추측할 수 있게 하는 대목이다. 특히 미국의 불만은, 중국이 기술기밀을 훔치거나 기술이전을 강요하는 행태를 보이면서 성장했다는 데 있다. 미국 정부가 '중국제조 2025'와 같이 중국의 정부 주도 정책에 불만을 제기하는 것도 비슷한 맥락에서 이해할 수 있다.

화웨이 사태는 2019년 5월 14일 트럼프 대통령의 행정명령으로 새로운 국면에 접어들었다. 미국 당국은 국가안보를 위협한다는 이유로, 화웨이를 거래 제한 기업 리스트에 올렸고, 주요 민간 IT기업들에게 거래 중지를 요구했다. 트럼프 행정부는 화웨이와 거래하는 자국 기업의 피해를 최소화한다는 이유로 이러한 제재조치를 180일 간 유예했으나, 화웨이의 숨통을 죄기 위한 조치들은 여기서 그치지 않았다. 구글, MS, 인텔, 퀄컴, 브로드컴, 마이크론, ARM 등 주요 기업들은 화웨이와 제품 공급 계약을 중지하고 기술 계약을 해지하기도 했다.

3. 데이터 레짐마찰과 국제규범 경쟁

이상에서 살펴본 미중 사이버 갈등의 이면에는 데이터 레짐에 대한 이익갈등도 걸려 있다. 2013년 에드워드 스노든 사건 이후 개인정보보호와 데이터 안보는 미중 국가안보의 쟁점이 됐다. 미국의 다국적 기업에 의한 데이터 유출의 경계는 중국에서 <인터넷안전법>(또는 네트워크안전법)을 출현시켰다. 이 법에 의하면, 중국에서 수집된 개인정보를 다루는 외국 기업들은 반드시 중국 내에 데이터 서버를 두어야 하며, 사업상의 이유로 데이터를 해외로 옮기려면 중국 공안당국의 보안평가를 받아야 한다. 미국 기업들의 중국 내 서비스를 검열·통제하고, 개인정보가 담긴 데이터의 국외 이전을 데이터 주권이라는 명목으로 금지하려는 취지로 해석되었다. 이 법은 2018년 7월부터 본격 시행됐지만 외국 기업들이 반발해 법 시행이 2019년 초로 유예되기도 했다.

실제로 이 법에 의거해서 중국 정부는 구글을 비롯한 페이스북, 유튜브, 인스타그램, 와츠앱 등의 외국 기업들의 인터넷 서비스를 규제했다. 2017년 7월 31일 애플은 중국 앱스토어에서 인터넷 검열시스템을 우회하는 가상사설망(VPN) 관련 애플리케이션 60여 개를 삭제해야만 했다. 또한 아마존웹서비스(AWS)도 2017년 11월 중국사업부 자산을 매각했다. 2018년 초 마이크로소프트와 아마존은 자사 데이터를 각기 베이징과 닝샤의 데이터센터로 옮겼다. 또한 <인터넷안전법> 시행 직후 애플도 중국 내 사용자들의 개인정보와 관리권을 모두 중국 구이저우 지방정부에 넘겨야 했으며, 2018년 2월에는 제2데이터센터를 중국 네이멍 자치구에 건설할 계획을 발표했다.

이러한 중국의 행보가 인터넷을 대하는 미중 양국의 정책과 이념의 차이를 반영하는 것이었다면, 2014년부터 시작해서 2018년의 제5회에 이르기까지 중국이 저장성 우전에서 개최하고 있는 '세계인터넷대회'는 사이버 공간의 국제규범 형성에 대한 양국의 입장 차이를 보여주는 사례이다. 중국의 세계인터넷대회 개최는 글로벌 인터넷 거버넌스에 대한 미국의 주도권에 맞불을 놓으려는 의도를 담고 있다. 출범 당시부터 세계인터넷대회는 '사이버공간총회'로 대변되는 서방 진영의 행보에 대항하는 성격을 띠었다. 특히 2013년 스노든 사건 이후 중국은 글로벌 인터넷 거버넌스를 주도하는 미국을 견제하고, 중국이 주도하는 비(非)서방 국제진영을

결집하고자 했다. 미국이 주도하는 현행 체제 하에서는 중국의 사이버 주권이 제약될 수밖에 없다는 인식을 바탕으로 한 도전적 행보였다(김상배. 2018a).

이러한 태세의 이면에는 중국 국내체제의 성격뿐만 아니라 사이버 공간의 미래질서를 보는 중국의 구상이 담겨 있다. 이러한 구상은 서방 진영에 대항하여 사이버 공간의 독자적 관할을 모색하는 세계인터넷대회의 정치적 비전과도 통한다. 아마도 중국의 속내는 미국이 주도하는 체제에 단순히 편입하기보다는 중국이 중심이 되는 새로운 질서를 구축하는 데 있을 것이다. 사이버 공간의 미래질서를 구축하는 과정에서 '아메리칸 드림'을 대신하여 '중국몽(中國夢)'을 밑그림으로 삼고 싶을 것이다. 아마도 그 과정은 과거 화려했던 중국의 천하질서(天下秩序)를 디지털 시대로 옮겨와서 재현하려는 시도일 가능성이 크다.

요컨대, 사이버 안보 분야에서 복합적으로 벌어지는 미국과 중국이라는 두 강대국이 벌이는 경쟁은 단순히 두 나라의 관계에만 그치는 것이 아니라, 세계정치와 동아시아 정치의 구조 전반을 엿보게 하는 중요한 주제이다. 그도 그럴 것이 21세기 세계정치에서 자웅을 겨룰 강대국인 두 나라의 관계는 단순한 양자관계의 의미를 넘어서 한국을 포함한 세계 모든 나라에 영향을 미치는 세계정치 구조의 양대 축을 의미하기 때문이다. 이런 점에서 두 강대국의 경쟁이 야기하는 변화의 소용돌이로부터 한국도 자유로울 수는 없다. 특히 최근 양국 사이에서 중견국으로서 외교전략을 고민하고 한국의 입장에서 볼 때 사이버 안보의 문제는 전통안보의 문제에 못지않게 중요한 국가적 사안임이 분명하다.

Ⅲ. 미중경쟁 사이 한국의 중개외교?

이상에서 살펴본 사이버 안보의 미중경쟁은 기술경쟁의 문제일 뿐만 아니라 사이버 공간의 새로운 질서와 국내외 제도 및 규범 형성을 놓고 벌이는 담론과 법제도 경쟁의 문제라고 할 수 있다. 미중의 '사이버 전쟁'은 실제로 해킹 공격이 가해지고 이를 막기 위한 방책을 고안하는 차원을 넘어서는 좀 더 추상적인 경쟁의 양상으로 나타난다. 이 글은 이러한 사이버 경쟁을 3차원적인 표준경쟁, 즉 기술-제도-담론의 표준경쟁이라는 시각에서 이해한다. 최근 미국과 중국 사이에서 중견국으로서 외교전략을 고민하고 있는 한국의 입장에서 볼 때, 이러한 복합적인 양상으로 전개되고 있는 사이버 안보 분야 미중경쟁의 동향을 제대로 파악하는 것은 중요한 사안이 아닐 수 없다.

1. 미중 기술표준경쟁 사이에서

사이버 안보 분야에서 벌어지는 미국과 중국의 경쟁은 미국이 주도하고 있는 인터넷과 사이버 안보 분야의 기술패권에 대항하는 중국의 독자적인 표준전략에서 발견되는 기술표준경쟁으로서 이해할 수 있다. 사실 PC시대부터 정보통신산업 분야에서 미국의 IT기업들과 중국 정부(또는 중국 기업)와 벌인 기술표준에 대한 논란은 잘 알려져 있는 사실이다. 인터넷 시대의 사이버 안보 분야에서도 이러한 기술표준을 둘러싼 경쟁은 미국과 중국이 사이버 갈등을 치루는 수면 아래에서 치열하게 벌어지고 있다. 주로 미국의 IT기업들이 제공하는 컴퓨터 운영체계나 인터넷 시스템 장비에 대한 보안문제가 중국 정부의 큰 우려사항이었다.

한국은 사이버 안보 분야에서 경합하는 미국과 중국의 상이한 기술표준 사이에서 기회와 도전에 동시에 맞닥뜨릴 가능성이 있다. 사실 사이버 안보 분야의 중개 이슈는 미국과 중국

사이에서 기술표준을 선택하는 문제와 관련된다. 한국은 미국의 지배표준과 호환성을 유지해야 하는지, 아니면 지배표준의 문턱을 넘어서 중국이 구축하려는 대안표준의 진영으로 이동해야 하는지가 관건일 수밖에 없다. 중국이 사이버 안보 분야에서 기술표준의 공세를 벌일 경우 마이크로소프트의 운영체계와 인터넷 익스플로러, 시스코의 네트워크 장비 등과 같은 미국의 기술표준에 크게 의존하고 있는 한국은 어떠한 결정을 내려야 할까? 실제로 이와 유사한 사태가 2014년 초 중국의 통신업체인 화웨이로부터 한국의 정보통신기업인 LG 유플러스가 네트워크 장비를 도입하려 했을 때 미국이 나서서 만류했을 때 나타난 바 있다.

사실 화웨이는 미중 사이버 안보 갈등에서 미묘한 위치에 놓여 있다. 화웨이는 스마트폰뿐만 아니라 안테나와 무선 송수신기기 등 통신장비를 생산하는데, 중국 정부가 이를 이용해 미국에서 첩보활동을 한다는 논란이 2012년부터 일었다. 당시 미국 하원 정보위원회가 중국의 스파이 활동에 화웨이가 협조한다는 의혹을 제기한 뒤 미국 행정부에 화웨이 통신장비 구매금지를 요구했다. 미 CIA 전직 국장이 하원에 출석해 “화웨이가 세계 각국에서 구축한 통신시스템 비밀 정보를 중국 당국과 공유해왔다”고 증언한 후, 미국뿐만 아니라 유럽과 캐나다에서도 화웨이 통신장비 규제론이 제기된 바 있었다. 100여 개국에 통신장비를 수출하는 화웨이는 스웨덴 에릭슨과 함께 세계 최대 통신장비 공급업체로 꼽힌다(김상배. 2019c).

한국에게 이러한 종류의 선택이 부과된다는 것은 쉽지 않은 일인데, 외교적 문제와 관련되는 경우 더욱 그러하다. 예를 들어, 사이버 안보 분야에서 한국은 한미동맹을 고수할 것이냐 아니면 한중협력을 강화할 것이냐의 선택에 놓일 수도 있다. 참으로 이러한 선택은 한편으로는 새로운 관계를 수립하고 다른 한편으로는 기존의 관계를 끊는 ‘맺고 끊기’ 또는 비대칭적 관계조율의 과정을 의미한다. 이러한 관계의 연결과 단절의 과정은 중개외교의 핵심인데, 간혹 중개의 과정은 네트워크의 구조를 바꾸고 완전히 새로운 네트워크 환경을 만들어 네트워크 게임의 의제 자체를 바꾸기도 한다. 그러나 이렇게 한국이 미국과 중국 사이에서 비대칭적 관계조율을 추구하는 중개외교를 모색함에 있어서 두 나라를 허브로 하는 강대국 간의 망제정치에서 호환성을 잃지 말아야 함을 명심해야 할 것이다.

그렇다면 미중 간의 사이버 안보 관련 논란에서 한국이 할 만한 일이 얼마나 있느냐가 관건이다. 예를 들어 소니 영화사에 대한 북한의 사이버 공격 이후 미국이 북한의 소행임을 입증하는 과정에서 한국이 정보를 제공했던 사례를 들 수 있다. 그러나 한국이 긴히 필요한 것은 첨단 사이버 공격 및 방어 기술이지만, 이와 관련된 한미협력은 원활치 못하다. 게다가 군사적 용도를 전제로 한 사이버 기술을 미국으로부터 도입하는 것에 대해서 중국이 반길 리 만무하다. CERT 차원의 한중 협력은 잘 진행되고 있는 것으로 알려져 있다. 그런데 한국이 정작 필요로 하는 것은 북한의 사이버 공격과 관련된 경유지 정보인데, 이 부분에서는 한국과 중국 두 나라 간의 협력이 쉽지 않다. 게다가 최근 미국은 한국이 중국과 너무 가까워질까 봐 우려하고 있다.

2. 미중 제도표준경쟁 사이에서

사이버 안보 분야에서 벌어지는 미국과 중국의 표준경쟁은 사이버 안보와 관련된 인터넷 정책과 제도를 놓고 벌어지는 제도표준경쟁의 양상으로 나타나고 있다. 기술표준 분야의 도전에서는 중국이 미국 IT기업들의 벽을 쉽게 넘을 수 없었던 반면, 제도표준의 분야에서는 나름대로 효과적으로 미국의 공세를 견제하고 있다. 중국 시장에 진출하려는 기업은 누구라도 중국 정부의 규제지침을 따라야만 중국 시장에 진출할 수 있기 때문이다. 게다가 중국의 인구와

시장 규모의 힘은 일차적으로는 무역장벽으로 작동할 수 있으며 장기적으로는 독자표준을 추구할 배후지가 된다. 중국이 아직까지는 역부족이었지만 지속적으로 독자적인 기술표준을 모색하는 것은 바로 이러한 맥락에서 보아야 한다.

미중 사이에서 사이버 안보 문제가 한국의 중개외교에 부과하는 기회와 도전은 양국의 인터넷 관련 정책과 규제제도, 즉 인터넷 거버넌스 상의 차이에서도 발견된다. 미국 내에서 IT 기업들이 상대적으로 정부의 간섭을 받지 않고 사실상 표준을 장악하기 위한 경쟁을 벌인다면, 중국에서는 아무리 잘나가는 기업이라도 정부가 정하는 법률상 표준을 따르지 않을 수 없는 상황이다. 이는 사이버 안보 분야에서 양국이 국내정책과 제도모델을 모색하는 과정의 차이와도 연결된다. 이러한 와중에 한국은 어느 쪽의 손을 들어 주어야 할 것인가? 미국이 주창하는 민간 주도의 이해당사자주의 모델인가, 아니면 중국이 고수하려고 하는 국가 주도의 인터넷 통제 모델인가? 만약에 사이버 안보 분야에서 워싱턴 컨센서스나 베이징 컨센서스와 같은 정치경제 모델을 설정할 수 있다면, 그 사이에서 중견국으로서 한국이 추구할 사이버 안보 분야의 새로운 모델을 제시하는 것이 가능할까?

인터넷 거버넌스 모델을 세움에 있어서 한국의 선택은 미국이 추구하는 민간 주도 모델과 중국이 지지하는 국가 개입 모델을 복합하는 방향으로 갈 수밖에 없다. 그렇다면 한국은 일견 호환되지 않는 양국의 인터넷 거버넌스 모델 사이에서 중개의 역할을 할 가능성이 있는가? 이 대목에서 중개자로서 중견국의 역할은, 완전히 새로운 모델을 창출하는 것보다는, 기존 모델들을 결합하고 복합하는 전략과 친화성에 있다는 사실에 주목할 필요가 있다. 이 글은, 이를 실질적으로 새로운 콘텐츠를 생산하는 모델과 대비되는 의미에서, '메타모델'이라고 부르고자 한다. 중개자로서 중견국은, 비록 완전히 새로운 것을 발명할 수는 없더라도, 이미 존재하는 것들을 창의적으로 엮는 '메타능력'을 발휘할 수 있다. 중개자의 역할이 매력적이냐 아니냐의 문제는 그 나라가 채택한 전략의 콘텐츠 문제가 아니라, 기존의 다양한 콘텐츠들을 어떻게 통합하고 엮어서 주변 국가들이 무난하게 수용하게 만들 수 있느냐에 달려 있다.

이른바 '서울 컨센서스'로 대변되는 한국의 정치경제 모델은 이와 관련된 좋은 사례를 제공한다(손열 편, 2007). 정치경제 분야에서 이른바 '한국모델'은 개도국들의 관심사뿐만 아니라 선진국들의 관심사를 모두 품으면서 결합한다는 의미에서 성공적인 '메타모델'의 사례이다. 실제로 한국모델은 최근 '베이징 컨센서스'로 개념화되는, 경제성장을 추구하는 권위주의 모델에서 시작했지만, 괄목할만한 경제발전을 달성한 이후에는 정치적 민주주의의 목표도 달성하는, 이른바 '워싱턴 컨센서스'로 이르는 동태적인 모델이다. 이러한 맥락에서 보면, 사이버 안보에서도 이른바 서울 컨센서스의 모델을 개발하여 대외적으로 알리는 방안은 미국과 중국을 동시에 만족시키고, 더 나아가 선진국과 개도국 진영을 모두 끌어안는 그럴듯한 시나리오가 될 수 있다. 그러나 최근 한국의 상황을 돌아보면, 민간부문이 주도하는 인터넷 경제의 번영을 달성하였음에도 불구하고, 아직도 사이버 공간의 시민사회의 활동에 대해서 국가가 개입하는 나라로 간주되는 현실은 이러한 시나리오의 실효성을 떨어뜨리는 큰 한계로 작용한다.

3. 미중 담론표준경쟁 사이에서

사이버 안보 분야의 미중 표준경쟁은 사이버 위협의 원인이 무엇이고 사이버 안보의 대상과 주체가 무엇인지에 대한 담론을 둘러싸고 벌어지는 표준경쟁이다. 현재 미국과 중국 간에 벌어지는 사이버 안보와 관련된 논점의 차이는 문제 자체를 보는 시각의 차이에서 비롯된다. 미국의 사이버 안보담론은 미국 내뿐만 아니라 글로벌 차원의 물리적 네트워크 인프라의 안정

성을 확보하는 데 주 관심을 두는데, 그 이면에는 인터넷 자유와 프라이버시의 보호에 대한 관심이 있다. 이에 비해 중국은 반(反)패권주의적이고 민족주의적인 국가주권의 안보담론을 펼치고 있는데, 사이버 공간을 국가 차원의 정보인프라 위에 구축된 공간으로 간주하고 그 안에서 이루어지는 활동은 국가주권의 관할권 하에 있는 것으로 인식하고 있다.

사이버 안보 분야 한국의 중개외교는 글로벌 인터넷 거버넌스와 관련하여 발견되는 두 가지 상이한 입장 사이에서 기회와 도전을 동시에 맞고 있다. 최근 한국은 글로벌 인터넷 거버넌스의 미래를 그리는 두 가지 상이한 비전 사이에서 자국의 위치를 잡는 데 큰 어려움을 겪고 있다. 이러한 상황을 이해하고 타개하는 데 있어 한국의 공식적인 입장은 유엔, ITU, OECD, ICANN 등이 주도하는 글로벌 인터넷 거버넌스에 대해 개방적이고 유연한 자세를 취하여 모두 참여하고 모두 지지하는 '망라(網羅)형 모델'로 알려져 있다. 이러한 입장은 현재 경합하고 있는 두 가지 비전을 복합하는 전략으로 이해될 수 있다. 그러나 이렇게 모든 것을 망라하는 스타일의 혼합전략은 일종의 딜레마 상황에 처했을 때 한국의 구조적 위치잡기에 큰 도움을 주지 못한다.

이러한 연속선상에서 볼 때, 서방과 비서방 진영, 좀 더 구체적으로는 미국과 중국 사이에서 어느 쪽을 선택해야 할까? 한국의 전략적 선택으로 먼저 생각해 볼 수 있는 것은 미국식 민간 주도 모델을 지지하고 커뮤니티와 전문 활동가를 활성화하는 것이다. 그런데 영미권의 사회문화에 기반을 둔 미국식 인터넷 거버넌스 모델을 다른 사회문화권에 속하는 한국에서 구현하기란 쉽지 않다. 오랫동안 정부가 주도하는 정책 모델에 익숙한 한국에서는 민간 중심의 의사결정권을 강조하는 다중이해당사자주의 모델이 정착하기도 쉽지 않다. 다중이해당사자주의 담론과 이를 추진하는 사회경제세력 사이의 괴리 문제도 간단치 않다. 글로벌 스탠더드로서 미국 모델에 마음은 가지만, 한국의 현실에서는 실제로 몸이 따라가지 못하는 상황이 발생하곤 한다.

그렇다면 생각해 볼 수 있는 한국의 대안적 선택은 국가 모델 또는 국가간다자주의 모델의 지지이다. 지난 산업화와 정보화의 역사를 되돌아보면, 한국은 정부 중심의 프레임 짜기에 익숙한 것이 사실이다. 이러한 역사에서 한국에서는 이른바 이해당사자들이 이미 '존재'해 있었다기보다는 정부에 의해서 위로부터 그 이해관계가 '구성'되고 '동원'된 측면이 없지 않다. 인터넷 거버넌스나 사이버 안보 분야의 국제적 해법을 모색함에 있어서도 정부가 나서서 한미 또는 한중의 정부간 협의를 활용하려는 경향이 강하다. 그러나 한국이 이러한 접근을 지속할 경우 국제적으로는 국가중심 접근의 경향을 추수할 가능성이 크다, 그러나 인터넷 거버넌스와 사이버 안보 분야에서 '국가간다자주의'의 표방은 '안보 변수'를 근간으로 하는 한미관계를 불편하게 만들 가능성이 있다. 이러한 선택은 중국식 글로벌 인터넷 거버넌스 모델의 지지, 유엔과 같은 전통 국제기구 중심 사이버 외교 추진, 사이버 공간에서 국가주권의 역할 강조 등을 의미할 것이기 때문이다.

결국 한국의 전략적 선택은 미국식과 중국식 논의에 동시에 참여하는 복합외교 전략 또는 좀 더 적극적으로 말해 중개외교 전략일 수밖에 없다. 현재 한국은 사이버 안보와 관련된 중개외교에서 글로벌 거버넌스 모델과 국제기구를 모두 모색하는 개방적이고 유연한 접근(open and flexible approach)을 취하고 있다. 이는 사이버 안보의 미중경쟁과 세계정치 과정에서 위치잡기를 하기 위한 기본적인 전제이다. 그러나 한발 더 나아가 현재 한국의 사이버 안보 외교전략에서 필요한 것은 이 분야에서 경합을 벌이고 있는 양국의 관계를 조율하는 중개외교의 발상이다. 이를 실현하기 위해서 한국은 진화하는 사이버 안보 분야의 구조적 조건 하에서 다층적으로 형성되는 비대칭적인 관계를 조율하는 외교적 능력을 발휘해야 한다. 이를 통해서

한국은 단순한 연결자가 아니라 상이한 행위자들 간의 관계에 상호작동성과 호환성을 제공하는 적극적 중개자로서 행동할 수 있을 것이다.

Ⅲ. 미중경쟁 사이 한국의 연대외교?

1. 미국의 사이버 동맹외교와 그 균열

2018년 초부터 미국은 오프라인 첩보동맹을 맺고 있는 영국, 캐나다, 호주, 뉴질랜드 등, 이른바 '파이브 아이즈'(Five Eyes) 국가들에 화웨이 통신장비를 도입하지 말라고 요청했다. 이에 따라 영국 정부는 2018년 초 중국산 통신장비의 보안취약성 문제를 제기하였으며, 캐나다의 경우도 2018년 초 의회가 나서서 캐나다 업체들이 화웨이와 교류하는 것을 자제하도록 요청했으며, 캐나다 정부도 사이버 보안에 필요한 조치를 약속하였다. 호주는 미국에 대해 화웨이에 대한 행동을 촉구했다고 알려질 정도로 적극적인 입장을 취했는데, 2018년에는 5G 장비입찰에 화웨이 도입을 반대했을 뿐만 아니라 남태평양 국가들이 장거리 해저 케이블망 부설 사업의 계약자로 화웨이를 선택하지 말라고 압력을 행사했다. 이밖에 독일과 프랑스도 미국의 화웨이 견제 전선에 동참하였다(김대호, 2018).

2018년 들어 트럼프 행정부는 동맹국들에 대한 화웨이 제재의 요구를 강화하였다. 영국은 대형 통신업체인 BT그룹이 화웨이와 ZTE 제품을 5G 사업에서 배제하려는 움직임을 보였다. 캐나다는 중국과의 무역마찰을 무릅쓰고 미국의 요청에 따라 화웨이의 부회장인 멍완저우를 체포했다. 호주와 뉴질랜드는 5G 이동통신 사업에 중국 업체가 참가하지 못하도록 하는 방침을 내렸다. 여기에 일본까지 가세해서, 정부 차원의 통신장비 입찰에서 중국 화웨이와 ZTE를 배제하기로 결정했으며, 일본의 3대 이동통신사도 기지국 등의 통신설비에서 화웨이와 ZTE 제품을 배제하기로 했다(고성혁, 2018). 이러한 행보를 보고 기존의 '파이브 아이즈'에 일본, 독일, 프랑스 등 3개국이 합류한 '파이브 아이즈+3'의 출현이 거론되기도 했다.

그런데 2019년 2월말을 넘어서면서 미국의 압박에 동참했던 영국과 뉴질랜드 등 '파이브 아이즈' 국가들이 '사이버 동맹전선'에서 이탈하는 조짐을 보였다. 영국 국가사이버보안센터(NCSC)는 화웨이 장비의 위험을 관리할 수 있어 그 사용을 전면 금지할 필요는 없다는 잠정 결론을 내렸다. 미국의 요청에 따라 화웨이를 배제했던 뉴질랜드도 저신다 아던 총리가 직접 나서 화웨이를 완전히 배제하지 않았다는 점을 분명히 했다. 이밖에도 독일 역시 특정 업체를 직접 배제하는 것은 법적으로 가능하지 않다는 점을 밝혔고, 프랑스도 특정 기업에 대한 보이콧은 하지 않겠다는 입장을 내놨으며, 이탈리아도 화웨이를 5G 네트워크 구축 사업에서 배제하지 않겠다는 보도를 부인했다. 또한 일찍이 화웨이 장비의 배제 입장을 내놓았던 일본 역시 그러한 제한은 정부기관과 공공부문 조달에만 해당되며, 5G 네트워크 구축에는 포함되지 않는다고 한발 빼기도 했다.

이들 국가들이 입장을 변화한 이유는, 화웨이를 배제한 채 자체 기술로 5G 네트워크를 구축하는 것이 현실적으로 어려운 상황이 작용한 때문으로 해석되었다. 만약에 이들 국가들이 화웨이 장비를 도입하지 않는다면 5G 출범이 2년가량 지체되는 차질을 빚을 것이라는 전망도 나왔다. 역설적으로 미국이 제기한 '미국 우선주의'의 영향을 받아 이들 국가들이 자국 우선주의로 돌아섰다는 분석이다. 여기에 더해서 2019년 초 파리평화회담과 뮌헨안보회의 등을 거치면서 미국이 이들 동맹국들을 무리하게 밀어붙인 것도 반발을 초래했다. 2019년 2월 마이크

폼페이오 미 국무부 장관은 “만약 어떤 나라가 화웨이 장비를 채택하고 중대한 정보를 넣는다면 우리는 그들과 정보를 공유할 수 없다. 우리는 그들과 함께 일할 수 없을 것”이라고 경고했다. 또한 리처드 그리넬 독일 주재 미국대사도 올라프 숄츠 독일 재무장관에게 “독일이 5G 네트워크를 구축하면서 화웨이 또는 다른 중국 기업의 설비를 사용할 경우 미국의 정보를 얻지 못할 것”이라는 서한을 보냈다(*Economist,* Mar 21, 2019).

화웨이의 5G 장비 도입을 금지하는 ‘사이버 동맹전선’이 흔들리면서 트럼프 행정부는 몇 가지 추가조치를 취했다. 표면적으로는 초강경 자세를 다소 완화하는 제스처를 보였는데, 2019년 2월 21일 트럼프 대통령은 자신의 트위터에 “미국이 가능한 한 빨리 5G, 심지어 6G 기술을 원한다”며 “미국 기업들이 노력하지 않으면 뒤처질 수밖에” 없으니, “더 선진화된 기술을 막기보다는 경쟁을 통해 미국이 승리하길 바란다”고 적었다(조슬기나. 2019). 이는 트럼프 대통령이 화웨이에 대한 입장을 바꿀 조짐으로 해석되기도 했으나, 2019년 5월에 이르러서는 오히려 더 강경한 대응전략을 채택하는 양면전술을 드러냈다. 게다가 화웨이 제재의 ‘사이버 동맹전선’이 흔들리는 조짐을 보이자, 트럼프 대통령은 화웨이 통신장비의 국내 도입 금지뿐만 아니라 5G 네트워크 구축에 필요한 핵심 부품을 제공해온 미 기업들의 화웨이에 대한 수출을 금지하는 행정명령을 내리기에까지 이르렀다.

사이버 안보를 내세운 미국의 동맹결속 전략은 미국의 인도·태평양 전략에서도 나타났다. 2019년 4월에는 미국을 위협하는 북한과 중국의 사이버 공격에 대응하기 위한 국제협력체 신설을 골자로 하는 ‘인도·태평양 국가 사이버 리그(CLIPS)’ 법안이 상원에서 발의됐다. 이 법안에 따르면, 클립스(CLIPS)에는 인도·태평양 지역의 미국 동맹국과 파트너 국가들이 참여한다. 한편 미 국방부는 2019년 6월 1일 공개한 ‘인도·태평양 전략보고서’에서 중국의 일대일로(一帶一路) 전략에 맞서 인도·태평양 전략을 강화하였으며, 화웨이 사태를 ‘하이브리드 전쟁’의 개념을 빌어 이해하는 모습을 보였다. 하이브리드 전쟁은 핵무기를 사용하기 힘든 상황에서 재래전뿐만 아니라 정치, 경제 등 비군사적 요소와 사이버전, 심리전 등을 포함하여 전방위로 전개하는 새로운 개념의 전쟁을 의미한다(김상배. 2019c).

한국의 입장에서 볼 때 관건은, 이렇게 미국이 주도하는 아태지역 동맹체제의 구축과정에 한미동맹이라는 양자 협력 차원을 넘어서 얼마나 더 적극적으로 참여할 것이냐의 문제일 것이다. 다시 말해, 최근 한중 경제협력의 진전과 북한과 대치하고 있는 특수한 상황을 고려할 때, 만약에 미국이 사이버 안보 분야에서 한미관계와 아태 지역동맹을 유럽의 수준으로 강화하려고 할 경우, 한국은 어떠한 선택을 할 것인가가 쟁점이 될 가능성이 있다. 다시 말해, 유럽에서 나토가 상정하는 적 개념이 주 위협으로서 러시아의 사이버 공격을 상정하고 있다면, 아태지역에 미국 주도의 사이버 동맹이 상정하는 적 개념은 무엇이며, 그리고 이러한 대결구도에서 한국이 취할 수 있는 입장은 무엇인지에 대한 고민이 필요할 것이다.

2. 화웨이의 항변과 중국의 일대일로 행보

화웨이 사태가 불거지기 전부터 ‘파이브 아이즈’로 대변되는 미국의 우방국들은 화웨이 통신장비를 사용하고 있다. 영국은 2005년 유럽에서 처음으로 화웨이 통신장비를 도입했으며, 현재 영국의 양대 통신사인 BT그룹과 보다폰은 화웨이 장비를 사용한다. 영국이외에도 캐나다, 호주, 뉴질랜드 등도 화웨이 장비를 사용한다. 이들 국가들이 화웨이 장비를 도입한 이유는 경쟁사 대비 저렴한 가격과 앞선 기술력 때문이다. 런정페이 화웨이 창업자 겸 회장은 2019년 1월 CCTV와의 인터뷰에서 “5G와 마이크로파 통신 장비를 동시에 가장 잘 만드는 회

사는 세계에서 화웨이가 유일합니다. 기술은 경쟁입니다. 다른 국가들이 화웨이 제품을 사지 않고 배길 수 있을까요?"라고 말한 바 있다(『인민망 한국어판』, 2019년 1월 28일).

이러한 상황에서 화웨이는 "사이버 보안 강화를 위해 최선을 다하고 있으며, 보안과 관련해 의혹을 제기 받은 사안은 단 한 번도 없다"는 입장을 취했다. 또한 화웨이는 "현재 전 세계 주요 이동통신사, 포춘(Fortune) 500대 기업, 170여 개 이상 국가의 소비자들이 화웨이의 제품과 솔루션을 사용하고 있다. 화웨이는 '글로벌 가치사슬' 전반에 걸쳐 전 세계 기업들의 신뢰를 얻은 파트너로 자리매김한지 오래"라며 자신감을 보였다. 아울러 화웨이는 "전 세계 선도적인 글로벌 ICT 솔루션 제공업체로서 비즈니스를 운영하는 해당 지역의 관련 법과 규정을 준수"하고 있으며, "미국뿐만 아니라 유엔과 유럽연합을 비롯한 국제사회에서 공포된 수출 규제 조치를 따르는 데 최선을 다하고 있다"는 입장을 보였다(원병철, 2018).

미국이 우방국들을 동원하여 화웨이 제품을 도입하지 말라는 압력을 목소리를 높여가는 와중에, 화웨이는 보안 강화를 위한 20억 달러 투자 계획을 발표했고, 보안을 최우선 강령으로 내세우겠다며 맞대응하기도 했다. 이와 더불어 화웨이는 자사가 스페인의 정보보안 평가기관인 E&E(Epoche and Espri)에서 'CC(Common Criteria)인증'을 받는다는 사실을 강조하는 등 자사 통신장비가 보안에 문제가 없다는 점을 적극적으로 소명하고 있다. E&E는 통신 장비 설계·개발을 포함해 실제 고객사에 납품되는 최종 장비에 이르기까지 모든 범위에 대해 보안 평가를 수행하는데, 그 중 대표적인 것이 CC인증이다. CC인증은 IT 장비의 보안을 검증하고 인증을 발급하는 과정을 말한다(김상배. 2019c).

또한 화웨이는 사이버 보안의 국제표준에 부합하는 조치를 위하는 일환으로, 2019년 3월 5일 벨기에 브뤼셀에 사이버안보연구소를 개설했다. 화웨이가 다른 곳이 아닌 유럽연합 본부가 있는 브뤼셀에 관련 연구소를 연 것은 자사 통신장비가 중국 정부에 기밀을 빼돌리는 스파이 행위에 이용될 수 있다는 미국의 주장에 적극적으로 대응하기 위한 조치로 풀이된다. 화웨이는 유럽연합의 정책 담당자들을 상대로 미국이 제기하는 보안논란을 불식시키는 데 초점을 맞춰 왔다. 화웨이는 이미 2018년 11월 독일 본에 브뤼셀과 비슷한 연구소를 개설했으며, 영국 정부가 구성한 화웨이 사이버보안평가센터(HCSEC·Huawei Cyber Security Evaluation Centre)를 지원하기도 했다.

화웨이는 미국에 국방수권법에 대해서도 적극적으로 문제제기했다. 화웨이는 2019년 3월 4일 자사 제품 사용을 금지한 미국 정부에 소송을 제기할 예정이라고 밝혔다. 소송 내용은 2018년 미국 연방정부가 '심각한 안보 위협'을 이유로 자사제품 사용을 금지한 방침이 부당하다는 것이다. 미 국방수권법 제889조는 미국 정부가 화웨이, ZTE 등 중국 통신장비 업체들의 기술을 이용하거나, 이들 기업의 기술을 이용하는 다른 사업체와 거래하는 것을 금지하는 규정을 담고 있다. 화웨이는 이 법안이 헌법 위반이라고 주장할 것이며, 재판 없이 개인이나 단체를 처벌하는 법안을 의회가 통과시켜서는 안 된다는 주장을 펼친다는 것이다.

미국의 화웨이 견제에도 불구하고 중국 정부는 일대일로 추진 차원에서 해외 통신 인프라 확충을 가속화하고 있다. 2018년 4월 시진핑 중국 국가주석은 일대일로 건설을 계기로 관련 국가들, 특히 개도국에 인터넷 기반시설을 건설하고 디지털 경제와 사이버 보안 등 다방면에서 협력을 강화하여 '21세기 디지털 실크로드'를 건설해야 한다고 강조한 바 있다. 이러한 맥락에서 보면 동남아 국가들이 화웨이를 선호하는 조치를 취한 최근의 행보를 이해할 수 있다. 태국은 2019년 2월 8일 5G 실증 테스트를 시작하면서 화웨이의 참여를 허용했으며, 말레이시아, 싱가포르, 인도 등도 화웨이 장비로 5G 테스트를 진행할 계획을 밝혔다.

이밖에도 화웨이와 중국 정부는 서방국가들에 대한 우호적 공세도 진행했다. 2018년 2월

초 테레사 메이 영국 총리는 쑨 야팡 화웨이 회장과 면담을 가졌고, 3월 화웨이는 영국에 향후 5년간 30억 유로(42억 달러)를 투자하겠다고 선언했다. 화웨이는 2019년 2월 캐나다에서 연구개발 투자를 확대하고 일부 지적재산권을 넘기겠다고 밝히는 등 주요국들을 설득하기 위한 여론전에도 나섰다. 2019년 3월 25일에는 시진핑 주석이 이탈리아와 일대일로 양해각서를 체결했다. 한편, 유럽연합의 집행기관인 EC는 화웨이가 사이버 보안을 위협한다는 미국의 주장이 근거가 없다고 발표했다. 특히 EC는 이러한 발표를 시진핑 주석이 파리에서 에마뉘엘 마크롱 프랑스 대통령, 앙겔라 메르켈 독일 총리, 장 클로드 융커 EU 집행위원장과 회동하는 행사에 맞춰서 진행했다.

이러한 행보에 힘입은 덕분인지 유럽의 이동통신사들은 여전히 화웨이 장비를 선택하는 추세이다. 화웨이는 2019년 6월말 기준으로 전 세계에서 50건의 5G 장비 공급 계약을 맺은 것으로 알려졌다. 이 가운데 28건은 유럽에서 맺은 계약으로 전체 56%에 달한다. 같은 기간 화웨이의 경쟁사인 노키아와 에릭슨은 각각 43건, 22건의 계약을 맺었다. 화웨이의 중국 경쟁자인 ZTE는 25건의 계약을 체결했다. 화웨이는 2018년 최대 시장인 유럽·중동·아프리카에서 모두 2,045억 위안(약 34조 9347억 원)의 매출을 올렸으며 이는 전체 매출 가운데 28.4%를 차지하는 금액이다. 해당 금액은 미국과 아시아·태평양(중국 제외) 시장의 매출을 모두 합한 것보다 많다(『미주 한국일보』, 2019년 7월 22일).

3. 동아태 사이버 안보 연대외교

중견국 연대외교는 주로 글로벌 거버넌스의 장이나 국제규범의 형성과정에서 나타나는데, 사이버 안보 분야의 국제규범 형성과정에서도 마찬가지이다. 예를 들어 강대국들의 입장이 대립하는 경우, 그 사이에서 외로이 입장을 설정하려하기보다는 비슷한 처지에 있는 국가들과 공동보조를 맞추는 것이 좀 더 유용할 수가 있다. 이러한 연대외교의 노력은 사이버 안보분야에서 서로 상이한 해법을 가진 강대국들 사이에서 발생할 수도 있는 중개자로서의 딜레마를 완화시키는 데도 도움이 될 것이다. 사실 미국과 중국 사이에서 복합적으로 얽혀 있는 사이버 안보 분야의 이익구조 하에서 한국이 혼자 나서서 효과적인 결과를 얻어내기는 쉽지 않기 때문이다. 이러한 상황에서 한국이 처한 특수한 상황의 보편적 의미를 잘 설파하여 생각을 공유하고 행동을 같이할 수 있는 동지국가들을 모으는 것은 유용한 대안일 수 있다.

이러한 맥락에서 최근 동아태 지역 국가들 간의 역내협력의 모색에 주목할 필요가 있다(김상배, 2019a). 이러한 노력은 사이버 안보 문제를 다루는 새로운 제도적 틀을 고안하는 것일 수도 있겠지만, 아세안, ARF, APEC 등과 같은 기존의 제도적 틀 안에서 사이버 안보 문제를 다루는 구체적인 협력방안을 모색하는 것일 수도 있다. 이러한 정부간 협력과 제도화의 시도는 구성주의 시각에서 보는 역내 구성원들의 지역안보 정체성 및 규범형성에 대한 논의로 연결된다. 이러한 정체성과 규범에 대한 논의는 유럽 지역에서 진행되는 논의와는 구별되는 동아태 지역의 지정학적 특성을 고려하는 것이어야 한다(Burton, 2013).

이와 관련하여 최근 아세안 국가들이 제기하고 있는 사이버 안보 협력과 규범에 대한 논의에 주목할 필요가 있다. 예를 들어, 2018년 4월 27일 싱가포르에서 열린 제32차 아세안 정상회담에서 사이버 위협의 긴박성에 공감하여 역내 국가들의 복원역량 및 협력방안 강화가 논의됐을 뿐만 아니라, 책임 있는 국가행동을 보장하기 위한 국제규범의 필요성이 거론됐다. 2018년 10월에는 아세안 10개국이 모두 합류하여 동남아시아 역내 테러에 대응하는 정보공유 네트워크인 '아워 아이즈(Our Eyes)'를 결성하기도 했다. 아워 아이즈는 파이브 아이즈를 벤치

마킹한 것으로 2018년 1월 인도네시아에 의해 제안되어, 1차로 아세안 6개국이 발족한 이래, 동년 10월에 이르러 10개국이 모두 참여하게 된 것이다. 아워 아이즈는 지역평화 및 대테러 협조 강화, 공해 안전 및 사이버 안보를 위해 협력하는 것으로 목표로 내걸었다.

아세안이 한 목소리를 모아 사이버 안보 규범의 필요성을 강조하는 데 비해, 동북아 3국인 한중일의 사이버 안보 분야 협력은 지지부진하지만 협의의 틀은 계속 유지해 오고 있다. 사실 역사적으로 볼 때 동북아에서 한중일 3국은 IT장관회의를 통해 협력해온 경험이 있다. 한중일 IT장관회의는 2002년에 모로코에서 제1차 회의가 개최된 이후 2003년에 제주에서 제2차 회의와 2004년에 일본 삿포로에서 제3차 회의가 개최되었고, 2006년 3월에 중국 샤먼에서 제4차 회의가 개최된 바 있었다(Thomas, 2009). 그러던 것이 2000년대 후반 3국간 IT협력이 다소 소강상태를 거치고 나서 최근 사이버 위협에 대한 공동대응의 차원에서 협력에 대한 논의가 다시 피어나고 있다. 2014년 10월 베이징에서 사이버 안보 분야의 3국 간 첫 고위급 회의로서 제1차 한중일 사이버정책협의회가 열린 이후 2015년 10월 제2차(서울), 2017년 2월 제3차(일본)가 열려 각국별 사이버 정책 및 제도, 사이버 공간에 적용 가능한 국제규범, 지역적·국제적 사이버 협력, 3국 간 향후 협력이 가능한 분야 등에 대한 논의를 펼쳤다.

아울러 아태지역 국가들이 역내 안정을 추구하기 위해 1994년 출범시킨 다자간 정치·안보 협의체인 ARF(ASEAN Regional Forum) 차원에서 진행되는 사이버 협력에도 주목할 필요가 있다. 역내 안정을 위해 1994년 출범한 다자간 정치·안보 협의체인 ARF에는 아세안 10개국, 아세안 대화상대국 10개국, 기타 아시아 지역 국가 7개국이 회원국으로 가입했으며 2000년대 중반 이후 중국의 적극적 참여와 2010년 미국의 참여로 영향력이 확대되고 있다. 2007년에는 한국의 주최로 ARF 사이버 테러 세미나를 서울에서 개최하였으며, 2012년 제19차 프놈펜 회의에서는 중국의 주도 하에 사이버 위협에 공동 대처하기 위한 합동전략의 개발 협력에 합의했다. 2013년 7월 브루나이에서 열린 제20회 ARF에서는 대테러 작전과 초국가 범죄와 관련해 사이버 안보 이슈가 핵심 의제로 논의되었다. 2015년 8월 ARF 외교장관회담에서는 회원국 간 신뢰구축을 통해 분쟁을 방지하고, 상호 이해를 제고하기 위해 사이버 안보 작업계획을 채택했다. 2018년 8월 싱가포르에서 개최된 제25차 ARF 외교장관회담에서도 역내의 사이버 안보 문제가 심도 있게 다루어졌다.

그럼에도 향후 동아태 지역에서 의미 있는 사이버 안보 국제규범을 도출하기 위해서는 ARF와 아세안 정상회담의 사례처럼 선언적 차원에서 협력과 규범을 논하는 수준을 넘어서야 한다. 유엔 GGE 활동이 성과를 내기만을 바라보고 있을 수도 없다. 동아태 지역에서는 유럽과 같은 형태의 협력과 규범의 틀을 그대로 적용할 수 없음도 알아야 한다. 우선 유사한 생각을 가진 국가들의 정부가 나서서 원칙과 관행을 개발하고 역내 국가들이 준수할 규범을 만드는 것이 중요하다. 민간 부문이나 시민사회가 나서 규범 개발을 주도할 수도 있을 것이다. 유럽 지역보다도 지정학적 영향이 큰 동아태 지역에서는 사이버 안보 거버넌스의 모색에 더 많은 시간이 걸릴 가능성이 없지 않다.

동아태 지역 거버넌스를 주도하려는 한국의 구상을 보여준 사례로는 박근혜 정부의 '동북아 평화협력 구상'(이하 동평구)이 있었다. 동평구는 동북아 지역의 공동 위협요인이 되는 원자력 안전, 에너지 안보, 기후변화와 환경, 재난관리, 사이버 공간, 마약 및 보건 분야에서의 협력 사업을 지속적으로 진전시켜 참여국가들 간에 공감대가 형성되면 점진적으로 정치군사적 갈등이 주류를 이루는 전통안보 의제로 논의를 확대시켜 나간다는 것이었다. 이는 문재인 정부의 '동북아 평화협력 플랫폼' 구상으로 이어져 온다. 동북아 평화협력 플랫폼은 문재인 정부 100대 국정과제인 '동북아플러스 책임공동체 형성'의 세부 실천과제 중 하나로서, 테러, 전염

병, 자연재난, 사이버 범죄 등과 같은 초국가적 위협에 효율적으로 대응하기 위한 협력의 모색을 명시하고 있다

사실 사이버 안보 분야의 연대외교를 추진함에 있어서 연대 파트너를 선정하는 것만큼이나 중요한 것은 적절한 연대외교의 이슈를 개발하고 상호 연계하는 문제이다. 사이버 안보의 중견국 연대외교를 추진함에 있어 일차적으로는 글로벌 인터넷 거버넌스의 다양한 이슈들이 이슈연계의 후보가 될 수 있을 것이다. 더 나아가 인터넷 거버넌스의 경계를 넘어서 연대외교의 효과성을 증진시키기 위해서 여타 경제와 안보 이슈들을 사이버 안보의 이슈들과 연계하는 방안도 실현 가능성이 높은 선택지이다. 예를 들어, 공적개발원조(ODA)는 사이버 안보 분야의 중견국 외교와 연계시켜서 의미 있는 효과를 볼 수 있는 분야로 거론되고 있다. 또한 원자력 안전, 환경안보, 보건안보 등과 같은 여타 신흥안보 분야의 이슈들도 중견국 외교의 차원에서 사이버 안보와 결합될 수 있는 아이템들이다.

Ⅳ. 미중경쟁 사이 한국의 규범외교?

1. 사이버 안보 규범경쟁 사이에서

최근 사이버 안보의 국제규범에 대한 논의는 크게 세 가지 차원에서 진행되었다. 첫째, 글로벌 인터넷 거버넌스의 차원에서 진행되는 사이버 안보 관련 국제규범에 대한 논의이다. 초창기부터 인터넷을 관리해온 미국 캘리포니아 소재 민간기관인 ICANN과 이에 대비되며 관할권을 넓혀 가고 있는 ITU와 WSIS(World Summit on the Information Society), 그리고 그 후속 포맷으로 진행되고 있는 IGF(Internet Governance Forum) 사이에서 경합구도가 형성되고 있다. 둘째, 전통적인 국제법(특히 전쟁법)과 국제기구의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격에 대응하려는 시도이다. 기존 국제법의 틀을 원용하는 사례로서 나토의 탈린 매뉴얼과 유엔 GGE를 중심으로 한 국제법 적용의 검토작업이 여기에 해당된다(Schmitt, 2012). 끝으로, 사이버 안보의 국제규범을 마련하기 위해서 서방 선진국들이 원용하는 일종의 클럽 모델이다. 2011년에 시작된 사이버공간총회가 대표적인 사례이며, 2001년 조인된, 유럽 사이버범죄협약(일명 부다페스트 협약)이나 상하이협력기구(SCO)와 같은 지역협력기구 등에서 다루어지는 사이버 안보 국제규범에 대한 논의이다.

이렇게 세 가지 층위에서 복합적으로 전개되고 있는 사이버 안보의 제도화 과정에 크게 두 진영의 관념과 이익이 대립하고 있다. 우선 ICANN 모델이 추구하는 다중이해당사자주의(multistakeholderism)와 유엔이나 ITU같은 전통 국제기구를 원용한 국가간다자주의(multilateralism)로 대별되는 두 가지 관념이 각을 세우고 있다. 이러한 관념의 대립 이면에는 미국과 유럽 국가들이 주도하는 서방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 비서방 진영을 다른 한편으로 하는 두 진영이 대립하는 지정학적 구도가 겹쳐진다. 넓은 의미의 글로벌 인터넷 거버넌스에서도 이러한 입장 차이가 드러난다. 서방 진영은 사이버 공간에서 표현의 자유, 개방, 신뢰 등의 기본 원칙을 존중하면서 개인, 업계, 시민사회 및 정부기관 등과 같은 다양한 이해당사자들의 의견이 수렴되는 방향으로 글로벌 질서를 모색해야 한다고 주장한다. 이에 대해 러시아와 중국으로 대변되는 비서방 진영은 사이버 공간은 국가주권의 공간이며 필요시 정보통제도 가능한 공간이므로 기존의 인터넷 거버넌스를 주도해 온 서방 진영의 주장처럼 민간 중심의 다중이해당사자주의에 의해서 사이버 공간을 관리할 수는 없다고

주장한다. 요컨대, 현재 사이버 안보(넓게는 인터넷 거버넌스)의 국제규범 형성과정은 두 개의 네트워크가 다층적으로 경쟁하는 양상을 보이고 있다(김상배, 2018a).

이러한 복합적인 국제규범 모색의 과정에서 각국은 자국에게 유리한 국제규범을 실현하기 위한 '프레임 경쟁'을 벌이고 있다(Gitlin, 1980; 레이코프, 2007). 이 글에서 파악한 사이버 안보 분야 프레임 경쟁의 양상은 앞서 언급한 세 가지 층위 또는 프레임 내에서 벌어지는 규범경쟁인 동시에, 더 중요하게는 세 가지 층위를 가로질러서 나타나는 '프레임 간 규범경쟁'의 모습이다. 이러한 프레임 경쟁의 기저에는 미국과 유럽 국가들이 주도하는 서방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 비서방 진영을 다른 한편으로 하는 두 진영 간의 지정학적 대립구도가 겹쳐진다. 서방 진영이 글로벌 거버넌스의 프레임을 앞세우고 정부간 프레임으로 지원하면서 자신들에게 유리한 국제규범의 도출을 위한 노력을 펼친다면, 이에 대항하는 러시아나 중국 등 비서방 진영의 프레임은 국가간 프레임을 고수하는 모양새를 나타내고 있다. 서방 진영이 정부간 프레임과 글로벌 거버넌스 프레임을 결합한 복합 아키텍처의 국제규범을 모색한다면, 비서방 진영의 시도는 근대 국제질서의 아키텍처를 기반으로 하는 국가간 프레임에 입각해 있다.

이러한 프레임 경쟁의 가장 밑바닥에는 글로벌 질서의 미래상과 관련하여 서방 진영과 비서방 진영이 지닌 근본적으로 상이한 관념이 자리잡고 있음에도 주목해야 한다. 서방 진영은 사이버 공간에서 표현의 자유, 개방, 신뢰 등의 기본 원칙을 존중하면서 개인, 업계, 시민사회 및 정부기관 등과 같은 다양한 이해당사자들의 의견이 수렴되는 방향으로 글로벌 질서를 모색해야 한다고 주장한다. 이에 대해 러시아와 중국으로 대변되는 비서방 진영은 사이버 공간은 국가주권의 공간이며 필요시 정보통제도 가능한 공간이라는 주장하며 이에 동조하는 국가들의 국제연대담론을 내세우고 있다. 다시 말해, 전자의 입장이 민간 영역의 인터넷 전문가들이나 민간 행위자들이 전면에 나서야 한다는 이른바 다중이해당사자주의의 관념으로 요약될 수 있다면, 후자는 인터넷 분야에서도 국가 행위자들이 나서 합의의 틀을 만들어야 한다는 국가간 프레임의 외연확대 담론으로 요약해 볼 수 있다(김상배, 2018a).

이러한 국제규범 형성의 구도에서 한국은 어떤 입장을 취해야 할까? 한국은 중견국 외교의 시각에서 강대국들이 주도하는 국제규범 형성에 단순히 참여하는 전략의 차원을 넘어서 사이버 안보 분야의 특성에 부합하는 규범을 제시하는 적극성을 보일 필요가 있다. 사실 역사적으로 국제규범을 설계하는 외교는 강대국의 몫이었다. 그러나 중견국도 강대국이 만든 세계질서의 규범적 타당성에 문제를 제기하고 좀 더 보편적인 규범의 필요성을 강조하는 이른바 규범외교를 모색할 수 있을 것이다. 특히 규범외교의 전략은 기성 세계질서의 운영방식에 대한 보완적 비전을 제시함으로써 강대국 위주의 논리에 대한 어느 정도의 반론을 제기하는 효과가 있다. 여기서 강대국들이 주도하고 있는 사이버 안보 국제규범의 정당성을 문제시하는 중견국 규범외교의 설 자리가 생긴다. 군사적 능력이나 경제적 자원이 부족한 중견국에게 있어, 권력지향적 외교와 대비되는 의미에서 보는, 규범지향적인 외교는 효과적인 방책이 될 수 있다. 보편적 규범에 친화적인 외교는 글로벌 청중에게 매력적으로 비칠 뿐만 아니라, 중견국이 추구할 규범외교의 매우 중요한 내용이 될 수 있다는 것이다.

2. 중견국의 사이버 안보 규범외교

그렇다면 구체적으로 사이버 안보의 국제규범 형성 과정에서 중견국이 담당할 역할이 무엇인가? 전통안보 분야의 국제규범 형성이 그러했듯이, 사이버 안보의 국제규범도 강대국들이

주도하여 만들 것인가? 아니면 강대국이 아닌 나라들, 특히 중견국도 자신들의 구상을 제시하고 이해관계를 반영하는 역할을 담당할 수 있을까? 중견국 규범외교는 얼마만큼 가능하며 그 내용과 범위는 어디까지인가? 개별 국가의 이익을 반영하는 차원을 넘어서 중견국이 보편적 규범을 주도할 가능성은 얼마나 있을까? 그리고 중견국 한국은 사이버 안보 분야에서 어떠한 규범외교를 추진해야 할 것인가? 강대국들이 서로 상이한 사이버 공간의 안보담론을 내세우며 경쟁을 벌이는 와중에 한국이 제시하는 대안은 무엇인가? 중견국으로서 한국이 새로운 안보담론을 생성할 여지는 있을까?

중견국도 세계질서 전체를 설계할 수는 없더라도 주어진 분야의 하위 설계자 정도의 역할은 할 수 있다. 예를 들어, 강대국이 만든 세계질서의 규범적 타당성에 문제를 제기하고 좀 더 보편적인 규범의 필요성을 강조하는 규범외교의 모색이 가능할 것이다. 이러한 과정에서 강대국 중심의 제로섬 게임 담론의 구조적 공백을 공략하는 중개외교와 이러한 행보에 힘을 싣기 위한 연대외교의 전략이 복합적으로 동원될 수 있다. 상대적으로 군사력이나 경제력에서 약세인 중견국의 입장에서 볼 때 이러한 규범외교의 추구는 일정한 효과를 얻을 수 있는 것이 사실이다. 특히 규범외교의 전략은 기성 세계질서의 운영방식에 대한 보완적 비전을 제시함으로써 강대국 위주의 논리에 대한 어느 정도의 반론을 제기하는 효과가 있다.

이러한 문제의식을 바탕으로 김상배(2019b)는 최근 사이버 안보 분야에서 활발한 활동으로 주목받고 있는, 에스토니아, 네덜란드, 핀란드, '스위스'[1] 등의 네 가지 사례를 비교분석하였다. 이들 국가는 사이버 안보의 국제규범과 관련하여 유사한 입장을 갖고 있는 동지국가들이라고 할 수 있다.[2] 그럼에도 자세히 살펴보면 이들 네 가지 사례는 서로 대비되는 중견국 규범외교의 경로를 추구하는 특성을 보여준다. 각 사례는 사이버 안보의 규범외교를 국가동맹, 정부간레짐, 지역협력체, 평화윤리 등으로 각기 다르게 초점을 두어 접근하는데, 일견 상호 경쟁하는 양상을 보이고 있다. 또한 이들 네 가지 사례는 각기 현실주의, 자유주의, 구성주의(공동체주의), 범세계주의 등으로 대변되는 국제정치이론의 시각에서 본 국제규범에 대한 논의의 스펙트럼 전반을 보여주는 사례들이기도 하다.

이러한 비교분석의 이론틀에 비추어 본 네 가지 사례는 사이버 안보 분야에서 나름의 경로를 따라서 모색되고 있는 중견국 규범외교의 각기 다른 모델을 대표한다. 이러한 차이는 이들 사례가 처해 있는 구조적 상황과 이에 대응하는 행위자의 성격, 그리고 구체적으로 추진되는 전략의 과정에서 나타난다. 김상배(2019b)는 각 모델이 설정한 기본 프레임과 전략적 지향이라는 두 가지 잣대에 의거하여, 네 가지 유형의 프로세스를 개념화하였다. 이렇게 볼 때, 사이버 안보의 중견국 규범외교는 에스토니아가 주도하는 '탈린 프로세스', 네덜란드가 주도하는 '헤이그 프로세스', 핀란드가 주도하는 '헬싱키 프로세스', 스위스의 중립국 이미지를 빌어서 마이크로소프트가 제안한 '제네바 프로세스' 등의 네 가지 모델로 요약된다. 이들 프로세스는 아직 어느 것도 '표준'으로 정착되지 못하고 상호 경쟁하고 있으며, 강대국들이 벌이는 규범경쟁의 틈바구니에서 중견국 외교의 독자적 공간을 확보하기 위한 노력을 벌이고 있다(<그림-1>

1) 이 글에서 다룬 '스위스'의 사례는, 스위스라는 국가가 일국 차원에서 추구하는 사이버 안보전략의 사례라기보다는, 중립국으로서 스위스의 적십자정신을 상징으로 내걸고 최근 진행되고 있는 중견국들과 민간 기업들의 행보를 염두에 두고 선정하였다.

2) 흥미롭게도 이들 네 가지 사례는 유엔 정부전문가그룹(Group of Governmental Experts, GGE)의 제5차 회의과정(2016-17)에서 논란이 되었던 '적절한 성의'(Due Diligence, DD)의 원칙을 옹호한 6개국 중에서 유럽의 4개국이다. '적절한 성의'(DD)의 원칙은 사이버 공격의 경유지가 된 제3국의 책임이 국제법으로 성립되는지 아니면 비구속적(non-binding) 규범인지에 대한 것으로, 강대국들의 견해와는 달리, 6개 중견국은 DD의 국제법적 지위를 주장했다. 6개국 중 나머지 두 나라는 한국과 일본이다; 이에 대한 자세한 내용은 김상배(2018a), p.335를 참조하라.

참조).

<그림-1> 중견국 규범외교의 네 가지 모델

	탈린 프로세스 (현실주의 국가동맹 모델)	헤이그 프로세스 (자유주의 정부간레짐 모델)	헬싱키 프로세스 (구성주의 지역협력체 모델)	제네바 프로세스 (범세계주의 평화윤리 모델)
구조적 상황	-러시아 vs. 나토	-서방 vs. 비서방	-유럽 vs. 러시아	-국가 vs. 민간
	-약소국, ICT강국	-상업국가	-탈핀란드화 정체성	-초국가적 네트워크
프레임 짜기	-현실주의 발상 -국가 안보관 -사이버전 대응의 군사 프레임	-자유주의 발상 -이해당사자 안전관 -사이버 안보협력의 외교 프레임	-구성주의 발상 -범유럽 포괄안보관 -사이버 위협대응의 실무협력 프레임	-범세계주의 발상 -세계사회 안보관 -민간인 보호의 평화윤리 프레임
맺고 끊기	-러시아 방어 위한 나토가입 -나토 가입의 노력 -사이버 안보의 동맹허브	-친서방 확대를 통한 대(對) 비서방 -서방진영내 차별화 -다자포럼외교의 중개허브	-러시아와의 갈등을 피하는 비(非)나토 유럽화 전략 -디지털 탈핀란드화 중립허브	-군사-민간의 분리 접근 -초국적 민간협력 -기술 적십자형 평화허브
내편 모으기	-나토CCDCOE -싸이콘(CyCon) -반(反) 러시아 동맹의 결속	-사이버공간총회 -자유온라인연합 -서방 선진국 진영의 연대	-나토, EU 등과 사이버 모의훈련 -유럽하이브리드위협 대응센터	-사이버안보기술협약 -다보스포럼 GCCS -파리 콜
표준 세우기	-탈린매뉴얼1.0 -사이버 정전론 -사이버 교전수칙	-탈린매뉴얼2.0 -이해당사국 포럼 -정부간 다자레짐	-범유럽 차원의 지역안보협력기구 -디지털 시대 CSCE	-디지털 제네바협정 -디지털 적십자모델 -초국가적 윤리규범

출처: 김상배(2019b), p.78

이러한 네 가지 모델이 한국이 모색할, 이른바 '서울 프로세스'에 주는 실천론적 함의도 크다. 어느 나라 못지않게 복잡한 구조적 상황에 놓인 한국이 추구할 사이버 안보 규범외교의 방향과 내용은 무엇일까? 미·중·일·러 사이에서, 그리고 서방 및 비서방 진영 사이에서 한국이 내세울 프레임의 구도는 무엇이며, 이를 풀어갈 전략적 지향성의 내용은 어떻게 채워야 할까? 탈린 프로세스와 같은 동맹의존 모델인가, 헤이그 프로세스와 같은 정부간레짐 모델인가, 헬싱키 프로세스 같은 지역협력체 모델인가, 아니면 제네바 프로세스와 같은 평화윤리 모델인가? 이 글의 주장은 이들 모델 중에 서울 프로세스가 벤치마킹할 어느 하나의 모델이 있다기보다는, 한국이 처한 구조적 상황을 고려하여 이들 네 가지 모델이 담고 있는 유용한 요소들을 선별적으로 추출해야 한다는 것이다. 결국 서울 프로세스가 지향하는 사이버 안보의 국제규범은 기존 모델을 복합적으로 엮어내는 '메타규범 모델'의 고안에서 찾아져야 할 것이다.

3. 사이버 안보의 '서울 프로세스' 모색

이상의 네 가지 사례에 비해 한국이 이상의 국가들과는 상이한 구조적 상황에 처해 있음을 명심해야 한다. 이들 국가에 비해서 한국의 사이버 안보 중견국 규범외교가 헤쳐 나가야 할 구조적 딜레마의 상황은 좀 더 복잡하다. 우선, 동북아 지역 차원에서 보면 한국은 패권경쟁을 벌이는 미국과 중국 사이에 놓여 있다. 이러한 미중경쟁은 최근 사이버 안보 분야에서도 치열하게 벌어지고 있다. 동아태 지역 차원에서 벌어지는 지역규범 모색에 있어서도 한국은 한미관계에 기반을 둔 미국 주도 아태동맹 정체성과 한중일과 아세안 지역협력을 기반으로 하

는 동아시아 정체성 사이에서 껴 있는 양상이다. 또한 글로벌 차원에서도 한국은 서방 진영과 비서방 진영 사이에서 또는 선진국 진영과 개도국 진영 사이에 껴 있는 중견국의 신세이다.

이렇게 복합적으로 펼쳐지는 구조적 딜레마에 직면하여 한국은 한미동맹이냐 한중협력이냐, 아태 국가냐 동아시아 국가냐, 선진국 편이냐 개도국 편이냐 등의 선택을 요구받고 있다. 게다가 한국은 'ICT강국'으로서 역량은 있으면서도 사이버 공격에 대한 대비 정도는 상대적으로 낮은 나라이면서, 외부로부터의 사이버 위협은 상존하지만 법제도는 제대로 정비하지 못하는 이중의 패러독스를 안고 있다. 이러한 상황에서 한국이 추구할 사이버 안보 중견국 외교의 방향은 어디인가? 좀 더 구체적으로 서울 프로세스에 담길 내용은 무엇인가? 그리고 이상에서 살펴본 네 가지 프로세스가 주는 함의와 이를 실제로 한국의 사례에 적용할 경우 발생할 문제점은 무엇일까? 사실 이러한 문제제기는 지난 5-6년 동안 한국이 추구해온 사이버 안보 전략의 고민과정에서 나타났으며, 앞으로의 전략 모색과정에서도 제기될 문제이기도 하다(김상배, 2019b).

첫째, 에스토니아가 추진한 탈린 프로세스의 현실주의 처방이 한국에 주는 함의는, 북한(또는 중국)의 사이버 위협이 엄존하는 상황에서 강대국 정치군사 동맹규범에 의지하는 모델이 가장 쉬운 처방임을 보여줬다는 데 있다. 이는 한미동맹의 강화나 미국이 주도하는 아태동맹, 한미일 협력, 또는 파이브 아이즈(Five Eyes) 네트워크 등에 적극적으로 편입하는 모델이다. 한국에 나토 CCDCOE와 같은 성격의 '아태 CCDCOE'를 설립하는 방안도 고려될 수 있다. 사실 한국이 외부로부터 당한 사이버 피해나 ICT강국으로서의 역량을 고려하면 충분히 추구해 봄직한 대안이며, 실제로 박근혜 정부 초반에 제기된 전략안이기도 하다. 그러나 이 모델은 한중관계의 특수성 때문에 현실적 대안이 되기는 쉽지 않다. 냉전 이후 러시아 변수가 에스토니아에 주는 의미와 최근 중국 변수가 한국에 주는 의미는 큰 차이가 있을 수밖에 없다. 사드(THAAD)의 한반도 배치 사태에서 경험한 바와 같이, 경제 분야에서 한중협력이 긴밀하게 진행되고 있는 상황에서 대미 편중의 노선은 한국에 예기치 않은 피해를 초래할 가능성이 있다. 이와 더불어 이 모델이 갖는 한계는 복합적인 네트워크 환경에서 사이버 정전론의 국제법적 적용과 같은 전통적인 발상이 얼마나 실효성이 있겠느냐는 의구심에서도 발견된다.

둘째, 네덜란드가 추진한 헤이그 프로세스의 자유주의 처방이 한국에 주는 함의는, ICT 강국이자 서방 국가들과 활발한 온라인·오프라인 교역을 벌이고 있는 한국이 사이버 공간을 안전한 환경으로 만들기 위해 친서방 외교를 펼치는 데 참고가 되는 모델이라는 데 있다. 실제로 한국은 2013년 제3차 사이버공간총회를 개최한 바 있으며, OECD차원에서도 다양한 사이버 안보 분야의 협력을 주도한 바 있기 때문에, 이 모델의 적극적 채택을 통해서 동지국가들의 내편 모으기를 모색하고 선진국들의 자유주의적 규범을 확산하는 계기를 마련하는 효과가 있을 것이다. 그러나 외부로부터의 사이버 위협이 엄연히 존재하는 상황에서 한국에게는 사이버 공간에서의 안전한 환경의 조성을 단순히 경제적 관심을 우선시하는 민간 주도 질서구축의 문제로만 볼 수 없는 속사정이 있다. 실제로 한국의 인터넷 및 사이버 안보 정책은 국가가 주도적인 역할을 담당했던 역사적 유산이 있어서 사이버 공간에서의 다중이해당사자들의 무제한적인 자유를 옹호하기에는 어려운 상황이 존재한다. 게다가 서방 진영이 표방하는 다중이해당사자주의 모델을 그대로 수용하기에는 국내적으로 한국의 민간 기업이나 시민사회의 역량이 얼마나 성숙했는가의 문제도 존재한다. 다중이해당사자주의가 한국과 같은 나라에는 이데올로기일 수도 있다는 비판이 나오는 것은 바로 이러한 이유 때문이다.

셋째, 핀란드가 추진한 헬싱키 프로세스의 구성주의 처방이 한국에 주는 함의는, 동아시아 차원에서 벌어지는 사이버 안보 다자협의체에 적극 참여하는 문제와 관련된다. 현재 동아태

지역에는 APEC이나 아세안 등과 같은 지역협력체의 형식을 빌려 사이버 안보 논의가 지속되고 있다. 한국도 아세안지역안보포럼(ARF)에 참여하고 서울안보대화(SDD)도 주최하고 있다. 이러한 활동을 발전시켜 유럽연합과 나토처럼 동아시아 포괄안보를 해치는 사이버 위협에 대응하는 사이버 모의훈련을 수행하거나, CSCE와 같은 지역안보협력체를 사이버 안보 분야에서도 추진하든지, '동아시아하이브리드위협대응센터'를 설치하는 방안을 생각해 볼 수 있다. 그러나 현재 지지부진한 한중일 협력이나 논의만 무성한 아세안 협력이 드러내는 한계로 인해서 동아시아 지역협력이 한국에게 주는 의미는, 신뢰구축과 역량강화를 위한 사이버 외교를 실시하는 것을 넘어서는 실질적 매력은 그리 크지 않다. 게다가 자칫 동아시아 지역협력의 강조가 미국으로 대변되는 태평양 세력과 거리를 두고 중국으로 대변되는 동아시아로의 선회로 비칠 가능성도 없지 않다. 한중일과 아세안 지역협력을 기반으로 하는 동아시아 정체성의 구축에 주력하기보다는, 한미관계에 기반을 둔 미국 주도 아태동맹 정체성을 개방적으로 포용하는 외교적 발상을 병행하는 것이 사이버 안보 분야에서도 필요하다.

끝으로, 제네바 프로세스의 범세계주의 처방이 한국에 주는 함의는, 강대국들이 추구하는 힘의 논리에 기반을 둔 사이버 공간의 군사화 담론에 문제를 제기하고 중견국의 보편적 윤리 규범으로서 '탈(脫)군사화 담론'을 제시할 필요가 있다는 데서 발견된다. 중견국으로서 한국은 전통적인 제로섬 게임에 기반을 둔 국가안보의 전통적 발상을 넘어서 '탈(脫)국가 평화 발상'의 담론을 제기해볼 필요가 있다. 이는 사이버 윤리 분야에서 새로운 담론을 개발하여 힘의 논리에 기반을 둔 강대국들의 안보담론을 제어하는 의미를 가질 뿐만 아니라 최근 중견국 한국이 추구하는 '신뢰외교'나 '어진(仁)외교'의 취지와도 맥이 통한다. 그런데 이러한 모델의 채택은 정부 차원의 노력만으로는 안 되고 국내외 시민사회의 참여를 바탕으로 해야만 한다. 그러나 한국 시민사회의 현실을 고려할 때 이 모델의 추진은 다소 추상적 시도로 그칠 가능성이 크다. 게다가 글로벌 차원에서 보아도, 현재 국제정치의 프레임워크 안에서 제네바 프로세스의 시도는 공공 영역의 지원 없이는 민간 영역의 공허한 문제제기가 될 가능성이 없지 않다. 특히 정부의 포괄적 지원이나 세계공동체로의 외연 확대 없이는 제네바 프로세스의 시도가 당위론적 문제제기로 끝날 지도 모른다.

이상의 내용을 종합해서 볼 때, 한국이 추구할 중견국 규범외교의 모델로서 '서울 프로세스'는, 이상의 네 가지 모델 중에서 어느 하나를 선택하기보다는, 각 모델이 지니고 있는 유용한 요소들을 추출하여 복합적으로 구성한 모델일 가능성이 크다. 예를 들어, 서울 프로세스 발상은 현실주의, 자유주의, 구성주의, 범세계주의 중에서 어느 하나에만 근거할 수는 없다. 맺고 끊기를 추구하는 관계조율의 전략도 동맹허브, 중개허브, 중립허브, 평화허브 등을 포괄하는 복합 기능허브이어야 한다. 내편 모으기의 메커니즘도 동맹국가, 선진국정부, 동아시아 이웃국가, 글로벌 시민사회 등을 모두 대상으로 진행되어야 할 것이다. 결국 서울 프로세스 모델은 동맹규범 모델이며 협력레짐 모델이고 지역협력 모델이며 초국적 윤리담론 모델을 모두 포괄하는 '메타규범 모델'이어야 할 것이다(김상배, 2019b).

그러나 이러한 '메타규범 모델'에 대한 논의는 한국이 추구할 전략의 방향성을 제시하는 데는 유용하지만, 그 내용적 요소들을 충분히 제시하지 못하는 한계를 안고 있다. 이 지점에서 이 글에서 수행한 사이버 안보 분야 중견국 규범외교 연구의 향후 과제가 제기된다. 다시 말해, 이 글에서 서울 프로세스가 지향할 모델로서 제시한 '메타규범 모델'의 형성 조건과 내용 및 구체적인 정책방안에 대한 좀 더 구체적인 연구가 필요하다. 사실 실천적 정책을 수립하는 관점에서 볼 때 '메타 모델'이라는 개념적 범주의 설정은 다소 막연하게 들릴 수도 있다. 구체적으로 발생하는 구조적 상황에 맞추어 그 대응 모델의 내용을 채우고 실제로 실천하는

데 원용할 수 있는 정책방안에 대한 논의를 도출할 수 있어야 할 것이다. 한국 모델이 '서울 프로세스'가 되기 위해서는 '형식'뿐만 아니라 '내용'을 제시하는 노력이 수반되어야 한다.

Ⅵ. 맺음말

한국은 최근 진행되고 있는 사이버 안보 관련 국제규범의 논의과정에 거의 모두 참여하고 있지만, 그 참여의 양상은 다소 파편적이고 분산적인 모습을 보이고 있다. 단순참여의 차원을 넘어서 한국의 이익을 반영하고 중견국으로서 역할을 발휘하는 참여외교가 되기 위해서는 적어도 복합지정학의 시각에서 다음과 같은 세 가지 구조 하에서 위치를 설정하는 전략을 구사해야 한다. 첫째, 미국과 중국의 경쟁이 형성하는, 또는 주변4망(網)이 만들어내는 고전지정학적 권력구조이다. 둘째, 서방 진영과 비서방 진영의 경쟁 사이, 또는 선진국과 개도국 사이에서 형성되는 비지정학적 제도의 구조이다. 끝으로, 다중이해당사자주의와 국가간다자주의의 관념이 경합하는 가운데 형성되는 글로벌 인터넷 거버넌스의 구조이다. 이러한 사이버 안보 분야의 구조적 조건을 파악하고 이를 활용하는 전략의 프레임을 짜고 그 안에서 상황파악과 위치설정을 하는 것은 한국이 중견국 외교를 성공적으로 추진하는 데 있어 필수적인 사안이 아닐 수 없다.

복합지정학의 시각에서 사이버 안보 외교의 필요성을 제기하는 일은 다음의 세 가지 차원에서 근거를 댈 수 있다. 첫째, 북한의 사이버 도발에 대한 국제사회에의 호소와 도움을 요청하는 차원에서 사이버 안보외교는 필요하다. 아직 국제규범이 마련되지 않은 상태에서 주변국가들을 활용하여 간접적으로 견제하거나 기술이 아닌 외교로 문제를 풀어나가는 양자 및 다자 협력의 필요성이 발생한다. 둘째, 미국과 중국의 21세기 패권경쟁의 사이에 놓인 한국의 생존과 번영을 모색하는 차원에서도 사이버 안보외교가 필요하다. 전통적인 한미동맹의 틀을 유지하면서도 한중협력을 확대해 나가야 할 과제가 사이버 안보 분야에서도 제기된다. 끝으로, 새롭게 형성되는 국제규범 형성과정에 참여하는 외교를 추구하는 차원에서 사이버 안보외교가 필요하다. 특히 한국은 신흥 분야 국제규범의 형성 활동에 참여하여 중견국으로서 외교적 리더십을 발휘할 과제를 안고 있다.

이를 위해서 이 글은 중견국 외교의 이론적 자원들을 적용하여 한국이 추구해야 할 사이버 안보 분야 외교전략의 방향을 세 가지 차원에서 제안한다. 우선 필요한 것은 사이버 안보 분야에서 경쟁하는 행위자들의 관계를 조율하는 중개외교이다. 특히 이 분야의 구조적 공백을 찾아내고 공략함으로써 새로운 관계구도를 창출하는 '맺고 끊기'의 외교적 발상이 필요하다. 둘째, 복합적으로 얽혀 있는 구조 하에서 어느 중견국이라도 혼자 나서서 효과적인 결과를 얻어내기는 쉽지 않다. 이러한 점에서 중견국 외교에서 가장 중요한 것은 생각을 공유하고 행동을 같이하는 동지국가들을 가능한 한 많이 모으는 연대외교이다. 끝으로, 중견국 외교가 염두에 두어야 할 또 하나의 과제는 중견국으로서 나름대로의 세계질서를 구상하는 설계외교를 추구해야 한다는 점이다. 특히 강대국들이 만들어 놓은 질서를 보완하는 차원에서 규범적 가치와 정당성을 추구하는 규범외교를 생각해 볼 수 있다.

부연컨대, 한국은 진화하는 사이버 안보 분야의 구조적 조건 하에서 다층적으로 형성되는 비대칭적인 관계를 조율하는 외교적 능력을 갖추어야 한다. 한국은 단순한 연결자가 아니라 상이한 행위자들 간의 관계에 상호작동성과 호환성을 제공하는 적극적 중개자로서 행동할 수 있다. 이러한 중개의 역할을 완수하기 위해서는 생각을 같이 하는 동지국가들을 규합하는 것

은 필수적이며 널리 글로벌 차원에서도 지지자들을 끌어 모을 수 있어야 할 것이다. 가장 추상적인 차원에서도 중견국으로서 한국은 전체 시스템의 설계자는 아니더라도 강대국이 운영하는 시스템의 프로그램을 보완하는 하위 설계자의 역할을 담당할 수 있을 것이다. 사이버 안보 분야는 이러한 중견국 외교의 복합적 역량을 가늠하는 실험대라고 할 수 있다.

최근 사이버 안보 분야에서는, 기존 국제정치의 규칙 하에서 자국의 이익을 추구하는 단순 경쟁이 아니라, 게임의 규칙 자체를 자신들에게 유리하게 설정하려는 복합경쟁이 벌어지고 있다. 이 글에서 다룬 중견국 규범외교는 이러한 복합경쟁으로서 규범경쟁 또는 프레임 경쟁이 진행되고 있음을 보여주는 사례이다. 중견국의 입장에서 이러한 규범경쟁에서 뒤지지 않고 적응하기 위해서는, 전통적인 국민국가나 동맹의 프레임에만 갇혀 있어서는 안 되며, 좀 더 복합적인 프레임에서 규범형성의 양상을 이해하고 대응하려는 노력이 필요하다. 아울러 새로운 프레임을 수용하기 위한 인식론적 발상 전환도 병행되어야 할 것이다. 이러한 맥락에서 볼 때, 이 글에서 살펴본 네 가지 모델은 한국이 이러한 복합적인 프레임을 개발하는 데 큰 시사점을 주는 사례가 아닐 수 없다.

중견국의 사이버 안보외교를 효과적으로 수행하기 위해서는, 국내 사이버 안보의 추진체계 전반의 정비 문제와는 별도로 또는 병행하여, 외교 분야 별도로 추진체계를 정비하는 작업에 대한 고민이 필요하다. 주변4망과의 사이버 협력방안이나 사이버 안보 각 분야별 국제규범의 논의동향에 대한 분석, 그리고 사이버 외교업무 영역의 재정의 작업을 바탕으로, 외교 전담부처의 조직을 재정비하고 더 나아가 정부 각 유관 실무부처 및 청와대 컨트롤타워를 포괄하는 추진체계의 정비 작업을 진행할 필요가 있다. 이외에도 전문가들과의 협업 강화를 통해서 지식 집약적인 사이버 안보외교 분야의 수요에 부응하는 정책지식 네트워크의 구축도 필요하다. 더 나아가 사이버 안보 이슈가 매우 복잡하게 상호 연관되어 있고 국가안보적 함의가 점점 더 커지고 있는 만큼 이러한 상황을 반영하는 국가모델 전반의 혁신에 대한 고민이 병행되어야 함은 물론이다.

이러한 정비작업을 제대로 추진하기 위해서는 사이버 안보 분야에서 외교적 접근이 필요한 고유 영역을 확인 또는 발굴하는 것이 우선되어야 하며, 이를 바탕으로 외교업무를 대내외적으로 새롭게 재정의할 필요가 있다. 사이버 공간을 둘러싼 세계정치 현상의 중요성이 커지면서 기존에는 해당 실무부처의 국제협력 부서와 민간 행위자들을 중심으로 진행되었던 사이버 안보의 외교업무에 외교 전담부처가 개입해야 하는 일이 늘어나고 있다. 사이버 안보 분야 국제협력의 경우, 표면적으로는 기술문제로 보일지라도 외교 전담부처의 식견과 경험을 요구하는 문제들이 많다. 따라서 유관 실무부처의 전문적인 국제협력 업무와 중복되지 않으면서도 외교 전담부처의 참여가 필요한 부분을 확인하고, 사이버 안보 관련 외교업무를 재정의하며, 이러한 작업을 바탕으로 관련 정부 부처들 간의 업무조정과 공조를 진행할 필요가 있다.

<참고문헌>

강하연. 2013. “ICT교역의 글로벌 거버넌스.” 서울대학교 국제문제연구소 편. 『커뮤니케이션 세계정치』 기획특집 <세계정치> 33(2). 사회평론, pp.73-109.

고성혁. 2018. “美 중국 화웨이 제품 퇴출은 안보전쟁.” 『미래한국』, 12월 26일.

김대호. 2018. “‘중국 화웨이는 위험한 기업’ 교류·협력 중단 전세계 확산… 미국+ 캐나다, 호주, 영국 등 ‘화웨이 주의보’.” 『글로벌이코노믹』, 3월 23일.

김상배. 2016. “제3세대 중견국 외교론의 모색: 네트워크 이론의 시각.” 손열·김상배·이승주 편. 『한국의 중견국 외교』, 명인문화사, pp.29-63.
김상배. 2018a. 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 한울.
김상배. 2018b. “트럼프 행정부의 사이버 안보 전략: 국가지원 해킹에 대한 복합지정학적 대응.” 『국제·지역연구』 27(4), pp.1-35.
김상배. 2019a. “동아태 사이버 안보 거버넌스: 국제협력과 지역규범의 모색.” 김상배·신범식 편. 『동북아 신흥안보 거버넌스: 복합지정학의 시각』 사회평론, pp.24-61.
김상배. 2019b. “사이버 안보와 중견국 규범외교: 네 가지 모델의 국제정치학적 성찰.” 『국제정치논총』, 59(2), pp.51-90.
김상배. 2019c. “화웨이 사태와 미중 기술패권 경쟁: 선도부문과 사이버 안보의 복합지정학.” 『국제·지역연구』 28(3), pp.125-156.
레이코프, 조지. 2007. 『프레임 전쟁: 보수에 맞서는 진보의 성공전략』, 창비.
『미주 한국일보』. 2019년 7월 22일. “화웨이, 미국 압박에도 5G 시장 석권.”
손열. 편. 2007. 『매력으로 엮는 동아시아: 지역성의 창조와 서울 컨센서스』 지식마당.
원병철, 2018. “세계 최초 5G 상용화와 화웨이 장비 보안성 논란.” 『보안뉴스』, 7월 26일.
『인민망 한국어판』. 2019년 1월 28일. “런정페이 화웨이 회장, 中 CCTV 인터뷰 동영상 전격 공개!”
조슬기나. 2019. “[주말에 읽는 글로벌 뉴스] 화웨이 사태.” 『아시아경제』, 2월 23일.

Burton, Joe. 2013. “Small States and Cyber Security: The Case of New Zealand,” *Political Science.* 65(2), 216-238
Economist. Mar 21, 2019. “Are Security Concerns over Huawei a Boon for its European Rivals?”
Gitlin, Todd. 1980. *The Whole World Is Watching: Mass Media in the Making and Unmaking of the New Left.* Berkeley: University of California Press.
Hansen, Lene and Helen Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly,* 53(4), pp.1155-1175.
Schmitt, Michael N. 2012. “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.” *Harvard International Law Journal.* 54, pp.13-37.
Thomas, Nicholas. 2009. “Cyber Security in East Asia: Governing Anarchy.” *Asian Security,* 5(1), pp.3-23.