제1부

신흥 기술안보의 복합지정학

제1장

동아태 사이버 안보 거버넌스: 국제협력과 지역규범의 모색

김상배(서울대학교)

이 장에서는 글로벌 차원에서 진행되는 국제규범 논의의 연속선상에서 동아태 지역의 고유한 특성을 반영한 사이버 안보 거버넌스 모델이 얼마나 가능한지를 검토했다. 특히 세 가지 요소, 즉 사이버 공격이 발생하는 사이버 공간의 기술 시스템적 특성, 사이버 공격에 임하는 국가 및 비국가 행위자의 복합 네트워크적 특성, 동아태 지역의 고유한 지정학적 특성 등을 복합적으로 반영한 거버넌스 모델이 필요함을 주장했다. 이러한 시각에서 볼 때 동아태 지역의 사이버 안보 거버넌스는 현재 적어도 세 층위에서 복합적으로 진행되고 있는 것으로 파악된다. 첫째, 동아태 지역의 지정학적 특성상 사이버 공격으로 인해 피해를 보는 당사국들이 나서서 사이버 공격의 원인제공자로 추정되는 국가들과 합의하려는 시도가 나타나고 있다. 둘째, 피해를 보는 국가들 간의 국제공조를 통해서 책임귀속(attribution)의 메커니즘을 가동시키거나 더 나아가 기존의 오프라인 동맹을 온라인 공간으로 확장하여 대응전선을 구축하려는 노력이 나타나고 있다. 셋째, 동아태 차원에서 지역협력의 제도와 규범을 만들자는 문제제기가 활발히 이루어지고 있다. 물론 이러한 다층적 협력 모델의 이면에 동아태 사이버 안보 거버넌스의 주도권을 장악하기 위한 경쟁 구도가 겹쳐지고 있음을 놓쳐서는 안 된다. 이는 미국이 주도하여 동북아(특히 일본)와 태평양을 엮으려는 '아태 모델'과 동남아가 앞장서며 동북아(특히 중국)를 포괄하는 '동아시아 모델'의 경합으로 나타나고 있다. '동북아'나 '동아시아' 또는 '아태'와 같은 통상적인 지역 개념이 아니라 '동아태'라는 용어를 사용한 이유가 바로 여기에 있다.

I. 머리말

최근 사이버 공격이 양적으로 점점 더 늘어나는 가운데 그 목적과 수법도 다양화되는 현상이 발생하고 있다. 사이버 안보는 단순한 해킹 공격의 문제를 넘어서 통상 마찰, 데이터 안보, 심리전 등과 같은 여타 세계정치의 쟁점들과 연계되고 있을 뿐만 아니라 미국과 중국, 그리고 유럽과 러시아 등이 벌이는 국가 간 갈등의 현안이 되었다. 이러한 과정에서 사이버 안보는 일국 차원의 대응을 넘어 주변 국가들과의 공조와 협력을 통해서 풀어나가야 할 문제인 동시에 지역 및 글로벌 차원의 규범 형성이 필요한 문제로 인식되고 있다. 그야말로 사이버 안보는 복합적인 양상을 보이는 21세기 세계정치의 대표적인 사례 중의 하나인 것이다. 이러한 인식을 바탕으로 이 장에서는 동아시아·태평양(이하 동아태) 지역에서 벌어지고 있는 사이버 안보 분야의 국제협력과 지역규범 모색의 현황과 과제를 살펴보고자 한다. 특히 글로벌 차

원에서 진행되는 국제규범 논의의 연속선상에서 동아태 지역의 고유한 특성을 반영한 사이버 안보 거버넌스 모델이 얼마나 가능한지를 검토하고자 한다.

사이버 공격에 대응하는 국제협력과 지역규범의 모색은 동아태 지역에서도 예전부터 있어왔다. 일국 차원의 노력만으로는 효과적으로 대응하기 어렵다는 인식을 바탕으로 피해 당사국들은 서로 협력해 왔다. 예를 들어, 미국이 주도하여 아태 지역에서 일본, 호주와 협력체계를 구축하고 한국과도 협의를 벌였다. 또한 사이버 갈등을 겪었던 공격 및 피해의 당사국들이 나서서 상호 합의를 통해서 문제를 풀려는 시도도 했다. 예를 들어, 2015년에 미국과 중국은 민간시설만큼은 서로 공격하지 않겠다는 합의를 이끌어내기도 했다. 더 나아가 동남아시아의 아세안(ASEAN) 회원국들이 중심이 되어 역내 국가들의 책임 있는 행동을 보장할 수 있는 국제규범의 필요성에 대해 선언하기도 했다. 전통안보 분야에서 지역규범 형성의 경험이 부재한 동아태 지역이지만 사이버 안보와 같은 신흥 분야를 중심으로 국제협력을 추구하여 지역규범 마련의 돌파구를 만들어보자는 문제제기였다.

그럼에도 학계의 연구 현황을 돌아보면 동아태 지역의 사이버 안보 거버넌스 문제를 국제정치학의 시각에서 체계적으로 다룬 연구는 매우 드물다.[1] 특히 이론적 시각에서 동아태 지역의 고유한 특성에 맞는 사이버 안보 거버넌스 양식을 고민하려는 시도는 거의 없었다고 해도 과언이 아니다. 기존의 국제법과 전쟁법의 논리를 사이버 안보 분야에 적용하려는 유럽 지역의 시도는 상대적으로 활발했지만, 유럽의 경험에서 도출된 프레임을 동아태 지역의 현실에 그대로 적용할 수는

1 구체적으로 동아태 지역의 사이버 안보 거버넌스를 다룬 연구로는 Thomas(2009), Lee and Kim(2013), Burton(2013), Noor(2015), Access Partnership(2017) 등이 있다.

없을 것이다. 이러한 시각에서 볼 때 동아태 사이버 안보 거버넌스의 연구는 사이버 공간의 기술적·사회적 속성뿐만 아니라 동아태 지역의 지정학적 특성 등을 복합적으로 고려한 모델을 탐구해야 한다는 숙제를 안고 있다. 이러한 문제의식을 가지고 사이버 위협에 대응하는 동아태 국가들의 국제협력과 지역규범의 모색에 대한 경험적·이론적 논의를 펼쳐보고자 한다.

아직 구체적으로 진행된 연구는 많지 않지만, 국제정치이론의 시각에서 동아태 사이버 안보 거버넌스 모델에 대한 이론적 논의를 펼칠 여지는 없지 않다. 특히 최근 지정학적 시각의 부활을 부추기는 현실의 변화로 미루어볼 때, 현실주의 국제정치이론의 시각에서 사이버 안보의 문제를 전통안보의 연속선상에서 이해하고 국가 행위자 간의 합의와 동맹이라는 시각을 원용하는 분석과 해법을 도모할 수 있을 것이다. 자유주의 국제정치이론의 시각에서 볼 때도 동아태 지역에서 전통 국제법이나 국제레짐의 논의를 원용하여 국가 및 비국가 행위자들이 만들어가는 제도 수립의 가능성을 논의해봄직하다. 구성주의 국제정치이론의 관점도 동아태 지역의 독특한 현실을 배경으로 지역규범과 정체성을 구축하려는 시도에 기여하는 바가 클 것이다. 그럼에도 이러한 국제정치이론의 논의들은 아직까지 사이버 공간과 동아태 지역의 속성을 복합적으로 고려한 이론적 분석틀을 제공하는 데까지는 나아가지 못하고 있다.

이 장에서는 신흥안보로서의 사이버 안보의 특성과 이에 적합한 거버넌스 모델을 가늠하는 이론적 논의를 원용했다. 사이버 공간의 복잡계 환경을 배경으로 발생하는 사이버 공격에는 다양한 비국가 행위자들이 가담하지만 그 배후에 국가 행위자가 중요한 역할을 담당하고 있다. 동아태 사이버 안보 거버넌스를 연구할 때는 사이버 공격의 특

성과 아울러 이러한 게임이 발생하는 지정학적 공간으로서 동아태 지역의 특성을 간과해서는 안 된다. 이러한 맥락에서 이 장에서는 세 가지 요소, 즉 사이버 공격이 발생하는 사이버 공간의 기술 시스템적 특성, 사이버 공격에 임하는 국가 및 비국가 행위자의 복합 네트워크적 특성, 동아태 지역의 고유한 지정학적 특성 등을 복합적으로 반영한 거버넌스 모델이 필요함을 주장했다. 결국 동아태 사이버 안보 거버넌스는 전통안보와 같은 (고전)지정학적 관리 메커니즘의 단일한 도입만으로는 충족될 수 없으며, (고전)지정학 이외에도 비지정학과 비판지정학 및 탈지정학의 시각을 도입한 복합지정학(complex geopolitics)의 시각을 원용하여 모색되어야 한다(김상배 2018, 제2장).

이러한 복합지정학의 시각에서 볼 때, 동아태 지역의 사이버 안보 거버넌스는 현재 적어도 세 층위에서 복합적으로 진행되고 있는 것으로 파악된다. 첫째, 동아태 지역의 지정학적 특성상 사이버 공격으로 인해 피해를 보는 당사국들이 나서서 사이버 공격의 원인제공자로 추정되는 국가들과 합의하려는 시도가 나타나고 있다. 둘째, 피해를 보는 국가들 간의 국제공조를 통해서 책임귀속(attribution)의 메커니즘을 가동시키거나 더 나아가 기존의 오프라인 동맹을 온라인 공간으로 확장하여 대응전선을 구축하려는 노력이 나타나고 있다. 셋째, 동아태 차원에서 지역협력의 제도와 규범을 만들자는 문제제기가 활발히 이루어지고 있다. 물론 이러한 다층적 협력 모델의 이면에 동아태 사이버 안보 거버넌스의 주도권을 장악하기 위한 경쟁 구도가 겹쳐지고 있음을 놓쳐서는 안 된다. 이는 미국이 주도하여 동북아(특히 일본)와 태평양을 엮으려는 '아태 모델'과 동남아가 앞장서며 동북아(특히 중국)를 포괄하는 '동아시아 모델'의 경합으로 나타나고 있다. 이 장에서 '동북아'나 '동아시아' 또는 '아태'와 같은 통상적인 지역 개념이 아니라 '동아태'라는 용어를 사용한 이유가 바로 여기에 있다.

이 장은 크게 세 부분으로 구성되었다. 2절에서는 기술 시스템을 배경으로 하여 발생하는 신흥안보로서 사이버 안보 거버넌스 모델에 대한 논의를 바탕으로 복합 네트워크로서 사이버 공간의 사회적 특성과 동아태 지역의 지정학적 현실을 감안한 다층적 분석틀을 모색하기 위한 이론적 논의를 진행했다. 3절에서는 사이버 안보 위협에 대응하려는 글로벌 차원의 국제규범의 모색 현황을 국가 간 프레임, 정부 간 프레임, 글로벌 거버넌스 프레임의 세 가지 차원에서 살펴보고 이러한 국제규범의 프레임들을 동아태 지역의 사이버 안보 거버넌스에 적용하려는 논의의 기초로 삼았다. 4절에서는 최근 동아태 지역에서 모색되고 있는 사이버 안보 거버넌스의 양상을 당사국 간 양자합의, 국제공조와 동맹 구축, 지역협력체와 다자규범의 모색이라는 세 가지 층위에서 살펴보았다. 끝으로 맺음말에서는 이 장에서의 주장을 종합·요약하고 동아태 지역에서 사이버 안보 거버넌스를 모색하려는 시도가 안고 있는 향후 과제를 지적했다.

II. 사이버 안보 거버넌스의 분석틀

사이버 안보는 '신흥안보(新興安保, emerging security)'의 대표적 사례이다. 이 장에서 원용하는 신흥안보라는 말은 단순히 '새로운 안보'라는 의미만은 아니다. '신흥'은 복잡계 이론에서 흔히 창발(創發)로 부르는 'emergence'의 번역어이다. 신흥안보는 미시적 차원에서는 단순히 소규모 단위의 안전(安全, safety)의 문제였는데, 거시적 차원으로 가면서 좀 더 대규모 단위의 안보(安保, security) 문제로 창발하

는 현상을 의미한다. 복잡계 이론의 논의를 원용하면, 신흥안보로서 사이버 안보의 위험은 양질전화(量質轉化)–이슈 연계–지정학적 연계로 형성되는 세 단계의 '임계점(critical point)'을 넘어서 창발한다(페르 박 2012; 김상배 2018, 제1장). 신흥안보 거버넌스 연구의 관점에서 볼 때, 이러한 사이버 안보의 속성에 적합한 거버넌스 양식을 개발하는 것이 관건이다. 이와 관련하여 이 절에서는 세 단계의 임계점에서 발생하는 특성에 대응하여 사이버 안보 거버넌스의 분석틀을 제시하고자 한다.

1. 기술 시스템과 거버넌스

이러한 분석틀의 마련을 위해서 먼저 주목할 것은 기술 시스템으로서 사이버 안보의 특성과 그에 적합한 거버넌스 구조의 유형에 대한 이론적 논의이다(Kitschelt 1991; Yoon 2015; 김상배 2016). 사이버 안보와 같은 기술 시스템, 좀 더 포괄적으로 말하면 컴퓨터 네트워크를 매개로 발생하는 신흥안보 위험은 '시스템의 결합도'가 높아서 갑작스레 시스템 전체로 번져서 돌발할 가능성이 많은 위험이다. 따라서 어느 한 부문에서 발생한 문제가 인접한 다른 부문으로 급속히 전화되는 것을 방지하기 위해 집중 거버넌스 구조를 도입하는 것이 효과적이다. 일차적으로 사이버 공격의 피해가 발생한 국가 차원에서 신속한 재난 복구가 우선적 대책으로 도입되는 것은 바로 이러한 이유 때문이다(김상배 2016, 89-93).

한편 사이버 공격의 배경이 되는 사이버 공간의 기술 시스템은 '상호작용의 복잡도'가 높아서 위험의 파급 범위가 무한하기 때문에 사이버 공격으로 인해서 발생할 피해를 일찌감치 감지하는 것이 어렵고 발생한 재난에 대해서 그 파급 결과를 예측하는 것이 쉽지 않다. 이러한 특징으로 인해서 사이버 공격으로 인한 피해를 인지하고 복구하는 작업을 할 때 일국 차원의 노력에는 한계가 있을 수밖에 없기 때문에 주변 국가들과의 양자간, 그리고 가능한 경우 다자간 국제협력을 펼치는 것이 보완책이다. 이러한 점에서 사이버 안보와 같은 유형의 신흥안보 위험에 대응하는 거버넌스 모델로는 영토의 경계를 넘어서 이루어지는 '정부 간 협력 모델'이 일차적으로 유용하다(김상배 2016, 89-93).

이러한 이론적 예측에 따르면, 각국의 기반 인프라에 대해 돌발적으로 감행되는 사이버 공격에 대응하고 그 피해를 복구하는 거버넌스는 일차적으로 일국 차원에서 정부뿐만 아니라 다양한 민간 행위자들까지도 나서서 모색해야 한다. 기본적으로 기반 인프라의 설치와 관리가 일국 단위로 이루어지고 있는 현실은 네트워크 시스템의 다운과 같은 돌발적 위험에 대한 대응의 주체로 각국 정부를 상정하지 않을 수 없는 상황을 창출한다. 실제로 각국 정부 차원에서 사이버 위협에 대응하여 사전예방과 사후복원까지 고려하는 기술역량의 강화뿐만 아니라 공세적 방어의 군사전략을 제시하고 추진체계와 법제도를 정비하는 등의 종합적인 대책 마련에 힘쓰고 있다.

그런데 신흥안보로서 사이버 안보가 지니는 상호작용의 복잡성은 일국 차원을 넘어서는 거버넌스의 도입도 동시에 요구한다. 국가안보론의 시각에서 거론되는 사이버 안보의 위험은 그 숫자가 양적으로 증가하여 질적 변화가 나타나는 이른바 양질전화의 임계점을 넘을 때 발생한다. 평소에는 개별 단위 차원의 안전이 문제시될 정도의 미미한 사건들이지만, 그 발생 숫자가 늘어나서 갑작스럽게 양질전화의 임계점을 넘게 되면 국가와 사회의 안보를 위협하는 심각한 문제가 된다. 이러한 와중에 미시적 안전과 거시적 안보를 구분하던 종전의 경계가 무너지고

사소한 일상생활 속의 안전 문제라도 거시적 안보의 관점에서 다루고 대비해야 하는 일이 된다(김상배 2016, 83).

실제로 사이버 안보 분야를 보면 사이버 공격의 건수는 매년 가파르게 증가하고 있다. 특히 사이버 공격은 국가 기간시설의 교란에서부터 금전 취득을 위한 해킹, 개인·기업 정보의 탈취, 심리적 선동과 교란 등에 이르기까지 그 목적이 다변화되고 있다. 봇넷(botnet) 공격, 악성코드 침투, 랜섬웨어(Ransomware) 유포, 인공지능 활용 등 공격 수법도 다양화되고 있다. 무엇보다도 최근에 나타나고 있는 제일 큰 변화는 이러한 사이버 공격이 일견 비국가 행위자인 해커 집단의 소행으로 보이지만 그 이면에 러시아, 중국, 이란, 북한 등과 같은 국가 행위자의 그림자가 점점 더 짙게 드리워져 있다는 사실이다. 그야말로 사이버 공격은 국가 및 비국가 행위자가 복합적으로 관여하는 게임이 되었다고 할 수 있다.

이러한 주체와 행위 면에서 본 복잡성의 증대는 일국 차원의 노력만으로는 사이버 공격을 미리 탐지하거나 근원지를 추적하여 책임소재를 밝히는 일을 어렵게 하고 있다. 대부분의 사이버 공격이 여러 나라의 국경을 넘나드는 초국적인 형태로 발생하기 때문에 자국에 피해를 입힌 사이버 공격의 근원지를 추적하여 알아내더라도 그 구체적인 증거를 찾아내기 위해서는 사이버 공격의 근원지 또는 경유지가 된 나라(들)과의 기술공조와 위협 정보의 공유가 불가피하게 필요하다. 사이버 안보 분야에서 일국 차원을 넘어서는 국제공조와 지역협력의 필요성이 강조되는 이유는 바로 이 때문이다.

2. 소셜 네트워크와 거버넌스

사이버 안보 거버넌스의 분석틀을 마련하기 위해서는 이상에서 살펴

본 기술 시스템 변수의 특성에 대한 논의와 더불어 사이버 공간의 사회적 속성을 이해해야 한다. 이는 사이버 안보의 게임과 이에 참여하는 행위자들의 복합성에 대한 논의와 밀접히 관련된다(김상배 2018, 제3장). 기본적으로 사이버 공격은 체계적으로 조직되지 않은 비국가 행위자들이 수행하는 네트워크 게임이다. 게다가 비국가 행위자들의 스펙트럼은 매우 넓다. 일반 사용자가 공격자가 될 수 있고 악의적인 공격의 대상이 되기도 하며 디도스(DDoS) 공격에 이용되는 것처럼 자신도 알지 못하는 사이에 봇넷에 동원되는 소스가 되기도 한다. 앞서 언급한 바와 같이 최근에는 이러한 비국가 행위자들의 이면에 국가 행위자들이 알게 모르게 관여하는 경우가 늘어나고 있는데, 국가 고용 해커나 해커 부대원, 루머-댓글 유포부대도 사이버 공격에 점점 더 적극적으로 가담하고 있다. 그런데 이들 해커 집단의 활동은 아무리 국가 지원 해커라고 하더라도 국가에 의해 완벽히 통제되지 않는다는 특징을 지닌다.

이러한 사정을 고려해서 보면, 비국가 행위자들이 나서는 사이버 공격에 대한 규제의 주체로 피해 당사국들의 정부를 설정하고 풀어가려는 '정부 간 협력모델'에만 의존하는 것은 적절한 방법이 아니다. 사이버 안보 게임의 특성상 관련 행위자들이 내면적으로 수용하는 원칙과 국제적으로 통용되는 규범 마련의 필요성이 논의되는 것은 바로 이러한 맥락이다. 사이버 안보 분야에서 이러한 원칙과 규범의 광범위한 채택은 사회 및 경제 발전을 촉진하고 국제적 안정성을 확보하며 각국이 추구하는 정책을 조율하는 기반을 조성함으로써 안전한 사이버 환경을 창출하는 데 기여할 것으로 기대되고 있다. 게다가 이러한 원칙과 규범은 구성원의 관계를 조율하는 제도화의 의미를 넘어서 세계정치의 이면에 흐르는 도덕성과 당위성을 담아내는 플랫폼이 된다. 오늘날 세계정치에

서 이러한 종류의 원칙과 규범은 핵확산이나 인권 등과 같은 분야에서 채택된 바 있다.

그런데 여기서 유의해야 할 점은 전통안보 분야와는 달리 사이버 안보는 한 가지 종류의 규범만으로 포괄되지 않는 이슈의 복잡성을 특징으로 한다는 사실이다. 사실 최근 사이버 안보의 이슈는 매우 다양한 세계정치의 이슈들과 연계되고 있다. 예를 들어, 최근 사이버 공격이 원자력 시설을 포함한 주요 국가시설을 겨냥함으로써 민감한 국가안보의 사안으로 비화되는 경우가 많아졌다. 또한 대부분의 사이버 공격이 경제적 가치가 높은 산업기밀과 지적재산과 연관된 부문을 겨냥함으로써 국가적 차원의 경제안보 문제로 인식되고 있다. 최근 미국과 중국, 그리고 러시아 등은 사이버 안보의 문제를 야기할 가능성이 있는 IT제품의 수출입을 규제하기도 하고 이 분야에서 활동하는 다국적 기업들의 데이터 비즈니스를 통상 마찰 문제를 넘어서는 데이터 안보의 관점에서 바라보기 시작했다. 해킹 문제가 정보전 또는 심리전의 관점에서 이해되기 시작한 것도 이미 오래되었다.

이렇게 복잡하게 이슈가 연계되고 있는 사이버 안보 분야의 규범 문제를 전통안보를 다루는 것과 같은 국가 간 프레임에서만 바라보는 것은 바람직하지 않다. 다양한 비국가 행위자들이 전면에 나서고 있는 사이버 안보의 게임에서 문제의 책임을 국가 단위로 귀속시키는 기존의 단순한 발상은 한계를 안고 있다. 사이버 안보의 탈영토성과 이에 관여하는 행위자들의 다양성을 고려한 새로운 규범을 모색하는 복합적인 접근이 필요하다. 실제로 사이버 안보 분야의 국제규범 모색은 매우 다양한 양상으로 나타나고 있다. 다음 절에서 살펴볼 테지만, 나토(NAT0) 차원의 탈린매뉴얼(Tallinn Manual) 시도나 유엔 정부전문가그룹(Group of Governmental Experts, GGE)의 활동 이외에도 사이버공간

총회(Conference on Cyberspace), 유럽사이버범죄협약(European Convention on Cybercrime, COC), 상하이협력기구(Shanghai Cooperation Organization, SCO), 국제인터넷주소관리기구(Internet Corporation for Assigned Names and Numbers, ICANN), 국제전기통신연합(International Telecommunication Union, ITU), 인터넷거버넌스포럼(Internet Governance Forum, IGF), 아세안지역안보포럼(ARF) 등과 같은 프레임이 모색되고 있다. 이러한 복잡성에 주목하여 일부 국제정치학자들은 이 분야에서 나타나는 규범 모색의 양상을 '레짐 복합체(regime complex)'의 부상으로 보기도 한다(Choucri et al. 2014; Nye 2014).

3. 동아태 지역구조와 거버넌스

양질전화나 이슈 연계의 임계점을 넘어서 창발하는 사이버 안보 이슈가 전통안보 분야의 지정학적 이슈와 연계되는 경우에 이는 명실상부한 국가안보의 문제가 된다. 최근에 사이버 공격이 해당 지역의 지정학적 이슈와 연계되는 사례가 부쩍 많이 발생하고 있는데, 2007년 에스토니아, 2008년 조지아, 2014년 우크라이나 등에 대한 러시아의 사이버 공격을 가장 대표적인 사례로 들 수 있다. 최근에는 각국이 사이버 공간을 이른바 '제5의 전장'으로 인식하면서 사이버 안보의 지정학적 연계 가능성이 더욱 커지고 있다. 게다가 사이버 안보는 재래식 전쟁뿐만 아니라 핵안보 문제와 연계되기도 한다. 최근에는 4차 산업혁명의 진전과 더불어 인공지능(AI), 로봇, 드론, 우주무기 등과 연계될 가능성도 커졌다. 이렇게 지정학적 논제로 연계되는 사이버 공격에 대응하기 위해서 세계 주요국들은 사이버 부대나 사이버 사령부를 신설하거나 확대 및 격상하는 조치를 취하고 있다.

사이버 안보 이슈는 양질전화와 이슈 연계의 사다리를 타고서 순차적으로 창발하여 지정학적 임계점에 도달할 수 있지만, 원래부터 지정학적 갈등 관계였던 국가들 간에는 이러한 창발의 메커니즘이 다소 급진적 경로를 타고 발현될 가능성이 크다(김상배 2016, 84). 따라서 동아태 사이버 안보 거버넌스를 제대로 이해하기 위해서는 지정학적 임계점에 해당하는 이 지역의 특성을 살펴보는 것이 중요하다. 사실 동아태 지역, 그중에서도 동북아 지역에서는 전통적인 지정학적 위협과 갈등이 두드러진다(김상배·신범식 편 2017). 남북한의 정치군사적 대결, 중국과 대만의 양안 갈등, 중일과 러일의 해양도서 분쟁, 한일의 독도영유권 문제, 남중국해 문제 등과 같은 지정학적 갈등이 발생하고 있어서 지역 차원의 협력이 난항을 겪고 있다. 그야말로 역내 국가들의 고질적인 불신과 갈등이 산재해 있는 것이다. 이러한 상황에서 신흥안보로서 사이버 안보 분야의 위험 발생은 다른 지역에 비해 이 지역에서 더 쉽게 지정학적 임계점을 넘을 가능성이 있다.

이러한 맥락에서 동아태 지역의 지정학적 특성이 다른 지역, 특히 유럽 지역의 지정학적 특성과 어떻게 다르며 그 차이가 사이버 안보의 영역에서 어떻게 발현되는지, 그리하여 동아태 지역의 지정학적 특성과 사이버 안보 거버넌스 모델이 어떻게 결합되어야 하는지를 검토하는 문제는 중요할 수밖에 없다. 여타 지역과 달리 동아태의 지정학적 특성이 사이버 안보의 창발에 영향을 미침으로써 이에 대응하는 국제협력이나 지역규범의 방향과 내용도 규정할 것이기 때문이다. 이렇게 보면 동아태 지역에서는 유럽 지역에서 모색되는 것과는 다른 양식의 거버넌스 모델이 도입될 가능성과 필요성이 있다. 특히 유럽과는 달리 동아태에는 전통안보 규범 형성의 경험이 부재하다는 점도 큰 변수가 될 것이다. 역으로 사이버 안보 분야에서 잉태된 혁신적 국제규범의 구상을 매개로

해서 동아태 지역 전반에 도입할 지역규범 형성의 물꼬를 틀 가능성도 없지 않다.

요컨대 사이버 안보의 기술적 속성이 유일한 인과적 변수로 이 분야 거버넌스의 내용을 결정하는 것은 아니겠지만 이론적으로 도출한 적합한 거버넌스 양식의 도입이 일차적으로 이 분야의 위험에 효과적으로 대응하는 해법을 제공할 가능성이 크다. 그러나 실제로 사이버 공격이 야기하는 위험에 효과적으로 대처하기 위해서는 기술 시스템의 속성 이외에도 사이버 공간의 사회적 속성이나 해당 지역의 지정학적 특성을 동시에 고려해야 한다. 이러한 복합적인 고려를 통해서 동아태 지역에서 사이버 안보 이슈가 전통안보의 지정학적 임계점을 넘어서 갈등으로 치달을 수 있는 가능성을 미리 탐지하고 이에 대응하는 전략을 적절히 모색할 수 있을 것이다. 궁극적으로 사이버 안보의 성격과 거버넌스 모델, 해당 지역의 지정학적 특성 간의 관계를 복합적으로 고려한 모델을 마련할 필요가 있다.

III. 사이버 안보 국제규범 모색의 현황

사이버 안보의 국제협력 및 규범의 틀을 동아태 지역에 적용하려는 구체적인 논의는 아직 본격적으로 시작되지 않고 있다. 글로벌 차원의 현황을 보아도 사이버 공격이 양적·질적으로 빠르게 진화하는 데 비해 국제규범의 형성은 매우 더디게 진행되고 있는 것이 사실이다. 현재 유엔 GGE 활동이나 탈린매뉴얼 등과 같이 기존의 국제법과 전쟁법을 적용하려는 시도에서부터 사이버공간총회, 유럽사이버범죄협약, 상하이협력기구 등과 같은 정부간협의체 또는 지역협력기구 등에 이

르기까지 다양한 프레임의 국제규범들이 경합하고 있는 것이 현실이다(김상배 2018, 제9장). 이러한 국제규범의 형성 과정에서 동원되는 프레임은 대략 '국가 간(inter-national)', '정부 간(inter-governmental)', '글로벌 거버넌스(global governance)'의 세 가지 차원에서 이해할 수 있다.

1. '국가 간 프레임'의 시각

국가 간 프레임의 가장 대표적인 사례는 유엔 GGE에서 이루어지는 사이버 안보 국제규범에 대한 논의이다. 유엔 GGE는 그동안 2004년, 2009년, 2012년, 2014년, 2016년 등 다섯 차례에 걸쳐서 구성되었다. 2016~2017년에 진행된 제5차 GGE 회의에 이르면서 국내적, 지역·국제적 차원의 신뢰구축조치 이행방안 제시, 역량 강화를 위한 협력적 조치의 개발, 기존에 GGE에서 권고된 자발적 규범·규칙·원칙의 구체적 적용 방법에 대한 권고 등에 있어 나름대로 진전을 이루었다(Noor 2015, 157). 그런데 유엔 GGE 차원의 국제규범 논의를 동아태로 끌어오기에는 그 활동 자체가 난항을 겪고 있다는 점이 한계로 작용한다.

유엔 GGE 중에서도 2013년 6월의 제3차 GGE에서 합의하여 도출한 최종 권고안이 의미를 갖는다. 이 회의에서 전체 참여국들은 사이버 공간에도 유엔헌장과 같은 기존의 국제법이 적용될 수 있다는 점에 합의하고 이러한 규범을 어떻게 적용할 수 있는지에 대해서 지속적으로 연구하기로 했다. 그 이전부터 기존의 국제법이 사이버 공간에 적용되는지의 여부에 대한 서방과 비서방 진영 간의 논란이 있었지만 제3차 GGE에 이르러 양 진영 모두가 조금씩 양보하는 모양새를 취하게 되었다. 궁극적으로 최종 보고서에 기존의 국제법이 사이버 공간에도 적용된다고 기술함으로써 이전의 논란거리들이 일단은 해소되었다.

이후 제4·5차 유엔 GGE에서는 사이버 공간의 특별한 성격을 고려할 때 어떤 국제법을 적용해야 할 것인가의 문제가 쟁점이었다. 특히 제5차 회의까지 진행되는 동안 GGE의 주요 임무는 사이버 공간에 적용되는 국제법을 새로 제정하는 문제가 아니라 기존의 국제법을 사이버 공간의 이슈에 적용하면 무엇이 문제될 것인지를 검토하는 데 한정되어 있었다. 그러나 유엔 GGE 활동은 2017년 6월 제5차 회의에서의 합의 도출에 실패했는데, 이는 기존의 국제법을 사이버 공간에 적용하는 문제와 관련된 핵심의제에서 서방 진영과 비서방 진영 간의 이견이 표출되었기 때문이었다. 현재 양 진영은 2019년부터 제6차 GGE를 재개한다는 정도의 내용만 합의한 상태이다.

국제법, 특히 전쟁법을 적용하는 나토 차원의 시도인 탈린매뉴얼도 국가 간 프레임으로 사이버 안보의 국제규범을 마련하려는 대표적인 시도이다. 탈린매뉴얼은 2013년 3월에 나토 합동사이버방위센터(Cooperative Cyber Defence Centre of Excellence, CCDCOE)의 총괄하에 20여 명의 국제법 전문가들이 2009년부터 3년 동안 공동연구를 거쳐 발표한 총 95개 항의 사이버전(cyber warfare) 지침서이다. 탈린매뉴얼의 골자는 사이버 공간에서도 전통적인 교전수칙이 적용될 수 있으며, 사이버 공격으로 인해 인명 피해가 발생할 경우에 해당 국가나 그룹에 대한 군사적 보복이 가능하고, 더 나아가 사이버 공격의 배후지를 제공한 국가나 그룹에 대해서도 국제법과 전쟁법을 적용하여 책임을 묻겠다는 것이다(Schmitt 2012).

이러한 탈린매뉴얼을 동아태 지역에 적용하려는 시도의 전망은 그리 밝지만은 않다. 탈린매뉴얼은 주로 나토 중심으로 진행되어 러시

아, 중국 등이 참여하지 않은 포맷이며 이러한 탈린매뉴얼과 같은 시도가 앞으로 동아태 지역에서 얼마나 넓은 공감대를 확보할지 알 수 없기 때문이다. 그러나 탈린매뉴얼과 관련하여 한 가지 유념해야 할 점은 "현재 여타 포괄적인 사이버 안보 규범의 형성 노력이 부재한 상태에서 탈린매뉴얼은 사이버 공간의 교전과 관련된 일정 정도의 준거점으로 활용될 가능성이 크다."는 사실이다(Noor 2015, 156).

한편 탈린매뉴얼로 대변되는 국제법 적용의 프레임은 최근 들어 진전을 보이고 있는데, 2017년 2월에는 그 두 번째 버전인 탈린매뉴얼 2.0이 발표되었다. '사이버전에 적용 가능한 국제법'을 논한 탈린매뉴얼 1.0과 달리 탈린매뉴얼 2.0은 '사이버 작전(cyber operation)에 적용 가능한 국제법'을 논했다. 탈린매뉴얼 2.0은 전쟁 수준에는 미치지 않지만 사회적으로 큰 충격을 주는 공격 행위에 대한 법 적용을 어떻게 하느냐의 문제를 다루고 있다(Schmitt ed. 2017).

2. '정부 간 프레임'의 시각

정부 간 프레임의 형태를 띠는 사이버공간총회는 사이버 공격의 피해를 보는 직접적인 이해당사국의 정부 대표들이 나서서 사이버 공간이라는 포괄적 의제를 명시적으로 내건 본격적인 논의의 장이다. 유엔 GGE의 활동이 '국가 간'의 틀을 빌어서 '안보' 문제에 주안점을 둔 것과 달리 사이버공간총회는 각국 정부가 주도했지만 다양한 민간 행위자들도 참여했고 안보 이외의 다양한 의제를 포괄적으로 논의하는 장으로 출발했다. 따라서 사이버공간총회는 정치외교적 합의 도출을 목표로 할 뿐만 아니라 사이버 공간에서의 인권, 경제사회적 이익 등을 포함한 다양한 의제의 균형적 논의를 지향했다. 2011년에 런던에서

제1차 회의를 개최한 이후 2012년(제2차 부다페스트), 2013년(제3차 서울), 2015년(제4차 헤이그)에 이어 2017년 제5차 회의를 뉴델리에서 개최했다. 그동안 참여자들이 늘어나고 논의도 활발하게 이루어졌지만, 사이버공간총회는 기본적으로 서방의 틀로 이해되어 비서방 진영은 미온적 반응을 보였다(배영자 2017, 105-106).

이렇게 서방 선진국들이 중심이 되어 사이버 공간의 범죄나 위협에 공동으로 대처하려는 시도의 역사는 좀 더 길다. 초창기 사이버 범죄에 대응해서 각국 정부들이 나서서 상호 간의 법제도를 조율하는 정부 간 네트워크를 구성한 초기 사례로는 미국과 유럽평의회(Council of Europe)의 주도로 2001년에 조인된 유럽사이버범죄협약, 즉 일명 부다페스트협약이 있다. 부다페스트협약은 사이버 범죄와 관련된 종합적인 내용을 포괄하고 법적으로 구속력을 갖는 최초의 국제협약으로, 범죄행위 규정, 절차법, 국제협력 등에 대한 내용을 담고 있다. 그러나 부다페스트협약은 가입 조건이 상대적으로 까다로운데다 서방 중심의 규범 설정이라는 비판을 받고 있어서 아직까지 보편적인 국제규범의 역할을 하지 못하고 있다. 한국도 기존의 국내 법제와의 충돌 문제 때문에 아직 가입하지 못하고 있는 상황이다.

이러한 서방 진영의 행보에 대항하여 중국과 러시아는 상하이협력기구와 같은 지역협력체의 틀을 활용하여 사이버 안보의 국제규범을 논의해왔다. 사이버 안보의 국제규범 과정에서 상하이협력기구에 주목하는 이유는 미국과 유럽 국가들의 입장에 반론을 제기하는 러시아나 중국 등의 프레임을 대변하기 때문이다. 실제로 2011년 9월에는 러시아, 중국, 타지키스탄, 우즈베키스탄 4개국의 유엔 대표들이 유럽 사이버범죄협약에 반대하면서 제66차 유엔 총회에서 '국제정보보안 행동규약(International Code of Conduct for Information Security)' 초

안을 제출했다. 이후 2015년 1월에는 카자흐스탄과 키르기스스탄이 추가로 참여해 6개국이 합의한 '국제정보보안행동규약' 개정안을 제69차 유엔 총회에 제출했다. 6개국의 대표들은 이 개정안을 통해 기존의 국제법을 직접적으로 적용하기보다는 새로운 국제법을 채택하는 것을 염두에 두고 있으며 사이버 공간에서도 국가의 주권적 통제가 필요하다는 주장을 펼쳤다.

이러한 국가 주권의 옹호 주장은 중국이 주도하여 2014년부터 중국 우전에서 개최하고 있는 세계인터넷대회(世界互联网大会, World Internet Conference)에서도 나타났다. 중국의 세계인터넷대회 개최는 사이버공간총회로 대변되는 서방 진영의 행보에 대항하는 성격을 지니고 있다. 특히 2013년의 에드워드 스노든(Edward Snowden) 사건 이후에 중국은 글로벌 인터넷 거버넌스를 주도하는 미국을 견제하면서 중국이 중심이 되는 사이버 진영의 건설을 목표로 국제협력을 강화하고 있다. 서방 진영이 주도하고 있는 현행 체제하에서는 중국이 독자적인 국제규범을 제시하는 데 한계가 있다는 판단을 바탕으로 한 행보였다. 개별 국가의 정치·사회의 다양성이 인정되고 국가 주권이 보장되는 사이버 환경을 구축해야 한다는 것이 주된 논리였다. 2018년 11월까지 총 5회 개최된 세계인터넷대회는 규모와 행사 면에서 확대되고 있으며 사이버 안보, 공유경제, 인터넷플러스, 사물인터넷(IoT), 가상현실, 빅데이터, 인공지능, P2P, 5G 기술 등과 같은 사이버 공간과 관련된 다양한 이슈 및 최신 기술의 발전을 다루어 이목을 끌고 있다.

3. '글로벌 거버넌스 프레임'의 시각

사이버 안보의 국제규범에 대한 논의를 제대로 이해하기 위해서는 사이버 안보 그 자체가 주요 관건으로 부상한 2010년대 이후의 규범 형성에 대한 논의보다 좀 더 넓은 시각에서 접근할 필요가 있다. 이러한 면모를 잘 보여주는 사례가 초창기부터 인터넷을 관리해온 미국 소재 비영리 민간기관인 ICANN이다. 여러모로 보아 ICANN은 개인, 전문가 그룹, 민간기업, 시민사회 등이 다양하게 참여하는 글로벌 인터넷 거버넌스의 실험대라고 할 수 있다. 그러나 초창기부터 ICANN은 지나치게 미국을 중심으로 움직이고 있다는 비판을 받았으며 이른바 'ICANN 개혁' 문제가 줄곧 논란거리가 되어왔다. 인터넷 발전의 초기에는 선발주자로서 미국의 영향력을 인정할 수밖에 없었지만 인터넷이 글로벌하게 확산되고 다양한 국가 간 이해관계의 대립이 첨예해지면서 여태까지 용인되었던 미국 주도의 관리 방식이 지니는 정당성 문제가 의심을 받게 된 것이었다.

이렇게 논란이 벌어지던 와중에 에드워드 스노든의 폭로로 수세에 몰린 미국은 2014년에 ICANN의 감독 권한을 이양할 계획을 발표했으며, 결국 2016년 10월에 46년 만에 그 권한을 내려놓았다. 이러한 과정에서 흥미로운 점은 인터넷할당번호관리기관(Internet Assigned Numbers Authority, IANA)의 권한 이양에 관한 논의를 이른바 '다중이해당사자주의(multistakeholderism)'라는 개념하에 다양한 이해당사자가 동등하게 참여하여 진행하라고 주문했다는 것이다. 이러한 메커니즘은 1국 1표의 원칙하에 국가 간 합의로 의사결정을 하는 유엔과 같은 국제기구의 경우와 사뭇 다르다. 이러한 방식은 조약과 같은 국가 간 합의에 의하여 규범을 형성하는 것이 아니라 정부, 시민사회, 민간이 동등한 자격을 갖고 지속적인 대화와 토론을 통하여 원칙, 규범, 의사결정 절차 등을 형성하는 것이다. 이러한 모델에 대해서 비서방 진영은 국가 행위자들이 좀 더 적극적으로 나서서 전통 국제기구의 틀

을 활용해야 한다는 '국가간다자주의(multilateralism)'의 개념을 제기했다.

국가간다자주의의 움직임을 잘 보여주는 것이 유엔 산하 ITU를 둘러싼 인터넷 거버넌스 논의이다. ITU가 인터넷 거버넌스 분야로 뛰어든 계기는 2003년 제네바와 2005년 튀니스에서 두 차례 열린 바 있는 정보사회세계정상회의(World Summit on Information Society, WSIS)에서 마련되었다. WSIS는 ICANN의 개혁 방안을 마련하는 데까지 이르지 못하고 폐회되었는데, 그 대신 인터넷 관련 정책에 대한 지속적인 토론을 위한 장으로 IGF를 마련했다(김상배 2014, 577-578). IGF는 정부, 민간, 시민단체, 국제기구 등 다양한 이해관계자들이 함께 모여 인터넷 현안에 대하여 논의하는 공개 포럼의 형태로 진행되었다. 2006년 그리스에서의 제1차 IGF 이래 매년 개최되었는데, 2018년 파리 회의에 이르기까지 모두 13회가 개최되면서 인터넷 주소자원, 사이버 안보, 개도국 역량 강화, 인터넷과 인권 등 인터넷 전반의 공공정책 이슈가 폭넓게 논의되었다.

IGF의 최근 행보와 관련하여 2018년 11월 제13회 IGF에서 세계 51개국이 사이버 범죄와 사이버 공격 행위에 대해서 전 세계가 공동 대응을 펼치자고 서명한 이른바 '파리 콜(Paris Call)'에 주목할 필요가 있다. 파리 콜의 정식 명칭은 '사이버 공간에서의 신뢰와 안보를 위한 파리의 요구(Paris Call for Trust and Security in Cyberspace)'로, 마이크로소프트사를 비롯한 여러 조직들이 요구해온 일종의 디지털 버전의 제네바협약을 만들자는 움직임에 해당한다. 즉, 사이버 공간에서의 전쟁 행위와 인권 보호를 위해 모두가 따라야 할 규범을 만들자는 것이다. 전 세계적으로 90개가 넘는 시민단체와 대학, 150여 개의 기술 분야 사기업이 여기에 참여했다. 구글, 마이크로소프트, IBM, 페이스북 등도 여기에 포함된다(『보안뉴스』, 2018. 11. 16). 그러나 러시아, 북한, 중국, 미국 등이 끝내 거절 의사를 표시하면서 파리 콜의 시도는 어쩌면 가장 많은 해킹을 저지르고 있는 대표적인 국가들이 빠져버렸다는 비난을 면키 어렵게 되었다.

한편 WSIS의 개최 이전까지 ITU에서는 사이버 안보 의제가 사실상 거론되지 않았다. WSIS의 원칙 선언에서는 정보 네트워크 보안, 인증, 프라이버시 및 소비자 보호 등을 모두 포함하는 '신뢰할 수 있는 프레임워크의 강화'가 정보사회의 발전과 신뢰 구축의 선결 요건이라고 지적하고 특히 모든 이해당사자가 협력하는 사이버 안보 문화의 필요성과 국제협력을 촉구했다. ITU는 2007년에 WSIS 이래 활동을 벌인 'ICT 이용에 있어서 신뢰와 안보 구축'의 촉진자로서의 역할을 다짐하는 차원에서 글로벌사이버안보어젠다(Global Cybersecurity Agenda, GCA)를 제안했다. GCA는 법적 조치, 기술 및 절차 조치, 조직적 구조, 역량 개발, 국제협력 등 5대 과제를 기반으로 하는 국제 프레임워크로, 정보사회의 안보와 신뢰 증진을 목적으로 한다. 이후 ITU는 관련 이해당사자들의 지지와 참여를 통해 사이버 안보와 신뢰를 구축하기 위한 전략과 해결책을 제시하는 역할을 적극적으로 수행하기 위해서 고위전문가그룹(High-Level Experts Group, HLEG)을 설치하여 운영하고 있다(배영자 2017, 120).

요컨대 글로벌 차원의 다양한 프레임에서 사이버 안보의 국제규범에 대한 논의가 진행되고 있으나 아직 그 성과를 기대하기는 이른 단계이다. 가장 기대를 모으고 있는 유엔 GGE의 논의에서도 2017년 제5차 회의에서는 합의문을 도출하지 못했다. 사실 사이버 안보의 기술적·사회적 속성을 염두에 둘 때 유엔 GGE에 대한 지나친 기대는 금물이다. 어쩌면 사이버 안보의 규범 문제는 전통적인 국제법과 국제

기구를 적용해서 해결될 문제가 아닌지도 모른다. 그렇다고 사이버공간총회, 부다페스트협약, 상하이협력기구, 세계인터넷대회 등과 같이 서방 및 비서방 진영이 각기 주도하고 있는 정부간협의체나 지역협력체에서의 사이버 안보 규범에 대한 논의도 아직은 상대 진영을 설득할 정도의 보편성을 획득하지 못하고 있다. ICANN과 ITU, IGF에서의 논의도 진영 간 대립구도가 형성되고 있어 쉽지 않다. 이러한 맥락에서 볼 때 사이버 안보 분야의 국제규범은 당분간 하나의 프레임이 아닌 복수의 프레임이 공존 또는 경쟁하는 구도로 형성될 가능성이 크다.

IV. 동아태 사이버 안보 거버넌스의 모색

현재 글로벌 차원에서 모색되고 있는 국제규범 논의의 연속선상에서 또는 이와는 별도로 동아태 지역에 적합한 국제규범을 마련할 필요가 있다는 문제제기는 계속 있어왔다. 아직 국제규범에까지는 이르지 않았더라도 현실주의 시각에서 파악되는 국가·정부 간 양자합의나 국제공조와 동맹 구축 등의 시도가 발견되며, 자유주의 시각에서 본 지역협력체와 다자제도의 필요성에 대한 논의도 꾸준히 제기되고 있다. 또한 구성주의 시각에서 본 지역정체성과 규범의 새로운 형성에 대한 논의도 발견된다. 이러한 과정에서 동아태 지역의 지정학적 특성은 사이버 안보 거버넌스의 내용과 관련하여 현실주의적 해법에 좀 더 힘을 실어주고 있는 것이 사실이다. 그러나 동아태의 지정학적 구도 안에서도 국가 행위자들 간의 경쟁과 협력의 모델뿐만 아니라 동아태 지역에 적합한 다자적 지역규범을 모색하려는 움직임이 동시에 진행되고 있음을 간과해서는 안 될 것이다.

1. 당사국 간 양자합의의 모색

지정학적 특성을 갖는 동아태 지역의 거버넌스에는 다자적 지역규범의 모색보다는 양자간 타결을 통해서 쟁점을 해소하려는 프레임을 도입하기 위한 시도가 우선 고려될 가능성이 크다. 이러한 현실주의 프레임에서 볼 때 미중관계, 미러관계, 중러관계, 한중관계, 한러관계, 남북관계, 북미관계 등과 같이 당사국 간의 양자합의 가능성에 주목할 필요가 있다. 특히 최근에 동아태 지역에서도 국가 지원 해킹으로 의심되는 사이버 공격이 늘어나는 상황에서 사이버 공격 및 피해의 당사국 정부가 나서서 합의를 도출하려는 시도들이 검토되고 있다. 그러나 일종의 '사이버 불가침 협정'을 연상시키는 이러한 시도들은 전통안보 영역과 달리 사이버 공간 속의 비대칭 관계를 전제로 하는 사이버 안보의 특성상 오프라인 공간에서 관찰되는 국가 간 합의 방식을 통해서 쉽게 제어되지 않는다는 문제점을 안고 있다.

이러한 맥락에서 가장 먼저 눈에 띄는 사례는 미국과 중국 사이에 이루어진 사이버 안보 합의이다. 2010년대 초반에 미국이 우려한 사이버 공간의 안보 위협은 중국의 국가적 지원을 받는 해커 집단들이 미국의 공공기관과 민간시설에 대해 사이버 공격을 가해서 입히는 피해였다. 사이버 안보 문제는 미국과 중국 두 강대국의 주요 현안이 되었으며 결국 2013년 6월에 미중 정상회담의 공식의제로 채택되는 상황까지 이르렀다. 2015년 9월에 미중 사이버 안보 합의를 하면서 양국 정상은 자국 기업들에 경쟁우위를 제공할 목적으로 지적재산에 대한 사이버 절도 행위를 수행하거나 알면서도 지원하는 행위를 하지 않는다는 데 합의했다(조현석 2017).

이러한 미중 합의의 효과와 관련하여 2017년에 미국의 민간보안업

체인 파이어아이는 "최근 3년간의 중국발 사이버 공격 동향을 분석한 결과 양국 협약이 적어도 미국 산업계에는 긍정적으로 작용했다."고 평가하기도 했다(『ZDNet Korea』, 2017. 5. 11). 그럼에도 미중 합의 이후에도 중국발 해킹 자체가 완전히 사라진 것은 아니어서 사이버 갈등을 겪고 있는 당사국들끼리의 합의에 대한 부분적 실효성만이 인정되고 있다. 게다가 최근에는 양국 정부의 고위 당국자들이 나서서 양국 합의가 지켜지지 않고 있다고 밝히면서 논란이 벌어지기도 했다. 2018년 11월 롭 조이스(Rob Joyce) 미국 국가안보국(NSA) 사이버 안보전략 선임고문은 중국이 2015년에 체결한 사이버 첩보활동 금지 합의의 범위를 넘어선 행동을 하고 있다고 주장했다. 이에 대해 중국은 미국이 제기한 의혹에 근거가 없다고 반박했다(『VOA 뉴스』, 2018. 11. 9).

이러한 미국과 중국의 행보를 이해하는 데 유럽 지역을 배경으로 했던 미국과 러시아의 사이버 합의를 참고할 필요가 있다. 미국과 러시아는 2013년에 사이버 긴장 완화를 한걸음 발전시키고 미래의 사이버 관련 위기를 해소하기 위해서 냉전 시대의 핵 공포에 대해 사용되었던 것과 유사한 사이버 핫라인을 설치하는 협정을 체결했다. 그러나 스노든 사태에도 불구하고 유지되는 듯 보였던 미러 사이버 우호관계는 2014년에 러시아가 우크라이나를 침공하면서 반전되었다(Geers 2015). 2014년 여름에 양국 간의 '사이버 공간의 신뢰조치에 관한 협정'이 폐기되었으며, 아울러 2009년에 메드베데프(Medvedev) 러시아 대통령과 오바마(Obama) 미국 대통령이 선포했던 '사이버 공간에서의 신뢰에 관한 양자간 대통령자문위원회'도 폐지되었다(『Russia Focus』, 2015. 6. 26). 이후 2016년 러시아의 미국 대선 개입으로 긴장을 맞았던 미러 관계는 2017년 7월 G20에서 미러 정상의 사이버 안보 동맹 거론이 와전되는 등 혼란을 겪기도 했다.

이에 비해 중국과 러시아는 사이버 협력을 강화하여 2015년 5월에 중러 사이버 보안 협약을 체결했다. 이 협약은 중국과 러시아가 사이버 공간에서 상호 감시를 지양하고 기술이전과 정보 공유를 하겠다는 내용을 담고 있다. 이는 두 국가가 서로 중대한 정보 인프라만은 건드리지 말자고 암묵적으로 약속했다는 의미이다(『Russia Focus』, 2015. 6. 26). 2016년 4월에 중국 사이버공간안보협회와 러시아 안보사이버연맹이 공동 주최한 제1차 중러 사이버 공간 발전과 안보 포럼이 모스크바에서 개최되었다. 이어 2016년 6월에 중국과 러시아 정상은 공동성명을 내놓고 정보 간섭을 반대하면서 다른 국가들의 고유한 문화전통과 사회이념을 존중하고 인정하자고 주창했다.

이러한 맥락에서 볼 때 최근 한국에 대해서도 사이버 공격을 가하고 있는 것으로 알려진 중국과 러시아를 상대로 하여 한중 또는 한러 사이버 안보 합의를 시도해봄직하다. 현재 진행 중인 한중 사이버 협력은 외교안보적 성격보다는 IT 전담부처가 중심이 된 기술·경제협력의 형태를 띠고 있다. 2015년 10월에 한중 사이버 보안 국장급 협력회의를 개최했으며, 2015년 12월에 제3차 한중 ICT협력 장관급 전략대화도 진행되었다. 한편 한국과 러시아 간에도 2013년 3월에 제1차 한러 정보보안협의회가 개최된 바 있는데, 2013년 10월로 예정되었던 사이버공간총회 직전에 회의 개최를 홍보하기 위해서 마련한 자리가 계기가 되었던 것으로 알려져 있다. 그 후 2014년 5월에 모스크바에서 제2차 한러 정보보안협의회를 개최했으며, 2016년 7월에는 제1차 한러 외교부 국제기구국장 협의회가 개최되었다.

이러한 연속선상에서 볼 때 남북 간에도 사이버 안보 합의를 체결할 가능성을 생각해볼 수 있다. 2018년 4월 27일에 발표된 판문점선언의 조문에서는 "남과 북은 지상과 해상, 공중을 비롯한 모든 공간에서

군사적 긴장과 충돌의 근원으로 되는 상대방에 대한 일체의 적대행위를 전면 중지"하기로 합의했다. 그러나 남북 간의 고질적인 긴장과 갈등을 해소하고 육·해·공 공간에서의 평화를 논한 반면 '제5의 전장'으로 급부상하고 있는 사이버 공간에서의 긴장과 충돌 및 그 해법에 대한 내용은 전혀 포함되지 않았다. 핵 위협이 한창이던 시절에도 사이버 안보가 남북 간의 큰 갈등 요인이었던 것을 떠올리면 사이버 합의 문제는 육·해·공의 갈등 해소 못지않게 중요한 문제임이 분명하다. 언젠가는 남북 정상이 사이버 안보를 현안으로 해서 협상 테이블에 앉게 되는 상황이 벌어질 수도 있을 것이다.

이러한 연속선상에서 보면 한반도 비핵화 문제를 놓고 북미 정상회담이 열렸듯이 사이버 평화를 위한 북미협상이 추진되는 상황도 예상해볼 수 있을 것이다. 다시 말해 2015년 미중 사이버 합의의 전례와 최근 북한의 사이버 공격에 대해 반응하는 미국의 양태를 보면 어느 시점엔가 미국이 북미 양자의 협상 테이블 위에 사이버 안보 문제를 올려놓을 가능성도 없지 않다. 실제로 최근에 미국의 전직 고위관리가 나서서 북미 사이버 합의의 필요성을 거론하기도 했다. 2018년 6월에 크리스토퍼 페인터(Christopher Painter) 전 미국 국무부 사이버정책 조정관은 북한의 핵 위협 다음으로 심각한 문제는 사이버 공격이라고 강조하면서 미국이 북미 정상회담의 후속 협상에 나설 경우에 핵 문제에 이어 북한의 사이버 위협도 의제로 다루어야 한다고 지적한 바 있다(『자유아시아방송』, 2018. 6. 15).

2. 국제공조와 동맹 구축의 모색

동아태 지역의 지정학적 특성에서 볼 때 역내 국가들의 경쟁과 갈등

이 벌어지는 다른 한편에서 우방국들을 중심으로 공조와 협력이 모색되는 현상이 벌어지고 있다. 실제로 동아태 지역에서 발생하는 사이버 공격에 대해 주요 피해 당사국들은 상호 간의 협력체계를 구축하는 방식으로 대응해왔다(김상배 2018, 제8장). 사이버 공격에 대한 예방과 탐지 및 추적의 문제는 일국 차원의 대응만으로는 안 되고 기술협력과 위협정보 공유 등을 포함한 주변국 및 우방국들과의 국제공조와 동맹 구축을 통해서 해결해야 한다. 이렇게 동아태 역내 국가들이 국제적인 협력을 펼쳐나가는 과정에서 유럽에서 나토가 나서서 모색한 바 있는 집단안보나 억지 등과 같은 현실주의적 군사전략의 개념이 많이 원용되고 있다(Burton 2013).

이러한 공조와 동맹의 네트워크 구축에서 가장 적극적인 행보를 보이는 나라는 미국이다. 2010년 초반부터 미국은 아태 지역 사이버 동맹 구축의 차원에서 일본, 호주, 한국 등과 협력해왔다. 이 중에서 가장 눈에 띄는 것은 미일 사이버 안보 협력이다. 2015년 5월에 공개된 미일 양국의 공동성명에 따르면, 미국은 군사기지와 사회기반시설에 대한 사이버 공격에 대처할 수 있도록 일본을 지원하기로 했다. 이러한 미국과의 협력을 배후로 삼아서 일본은 다각적 파트너십의 강화를 목적으로 영국, 인도, 호주, 유럽연합, 아세안 등과 사이버 보안 정책협력회의를 정기적으로 개최하고 있다. 한편 미국은 2011년 9월의 미국·호주 국방·외무장관 합동회의에서 미호동맹을 발전시키면서 사이버 공간도 동맹의 영역에 포함시키기로 합의하는 공동 선언문을 채택했다.

최근 미국은 영국, 캐나다, 호주, 뉴질랜드 등이 구성한 정보공유 네트워크인 '파이브 아이즈(Five Eyes)' 국가들과 공조하고 있다. 쟁점은 중국의 네트워크 장비업체인 화웨이의 약진과 이로 인해 야기되는 공급망 안전 문제이다. 트럼프(Trump) 행정부는 최근 이 동맹국들에

화웨이와의 교류와 협력을 최대한 자제하도록 촉구했다. 화웨이에 대한 견제에 가장 적극적인 곳은 캐나다이다(『글로벌이코노믹』, 2018. 3. 23). 화웨이의 5G 통신장비는 보안 문제를 이유로 영국에서도 제동이 걸렸다(『아주경제』, 2018. 7. 23). 호주 정부도 안보 위험을 이유로 화웨이와 ZTE의 호주 5G 네트워크 시장 진출을 금지했다. 또한 뉴질랜드도 화웨이 규제에 동참하기로 했다(『연합뉴스』, 2018. 10. 4). 이 밖에 파이브 아이즈 동맹국에 소속되어 있지는 않지만 미국의 우방국인 독일, 프랑스 등도 이 대열에 참여했다(『조선일보』, 2018. 10. 12).

미국은 이러한 구상을 일본과 한국으로 이전시키려는 의도를 갖고 있다. 2018년 8월에 일본 정부는 중국의 스마트폰 제조업체인 화웨이와 ZTE를 정보 시스템 관련 입찰 대상에서 제외하기로 했다. 일본 정부의 이러한 결정은 미국 및 파이브 아이즈 국가들의 움직임에 보조를 같이하는 것으로, 국제적 위협이 되는 사이버 공격과 국가기밀 누설 등을 방지하려는 목적을 지니고 있다. 한편 미국 의회는 한국이 5G 장비로 화웨이를 선택하지 못하도록 압박해야 한다는 입장을 보이고 있다. 사실 미국의 견제는 한국의 화웨이 장비 도입 문제와도 연관되면서 한국에 대한 미국의 압력 요인으로 작동했다. 2014년 초에는 LG유플러스가 화웨이 네트워크 장비를 도입하려고 했을 때 미국이 나서서 만류하는 상황이 발생했다. 2017년에는 한국이 화웨이 장비로 5G 네트워크를 구축하는 것에 대한 미국의 견제가 미 하원의 서한 형태로 전달되었다.

이러한 와중에도 한국과 미국은 사이버 안보 분야의 협력을 진행해왔다. 2014년 4월과 2015년 10월 두 차례에 걸친 정상회담에서 한국과 미국은 사이버 안보를 포함한 포괄적 동맹관계를 더욱 공고히 하는 데 합의했다. 정부 차원에서도 한미 사이버정책협의회가 개최되었는데, 2012년 9월에 제1차 회의가 열린 이후 2018년 6월의 제5차 회의에

이르기까지 양자 간의 사이버 협력 방안이 논의되었다. 한편 한국과 호주 간에도 사이버 안보 협력이 진행 중이다. 2014년 8월에 외교부 국제안보대사를 수석대표로 하는 제1차 한국·호주 사이버정책 대화를 열었고, 2014년 4월에는 한국과 호주 양국 정상이 합의한 사이버 분야 협력 강화의 후속조치로 아태 지역체제 내에서의 협력과 양국 간 국방 사이버 협력, 사이버 범죄에 대한 공동 대응 등의 다양한 의제에 대해 협의했다.

이렇게 강화되고 있는 미국 주도의 아태 사이버 지역동맹의 틀 중에서 상대적으로 가장 빈 부분은 한일 사이버 협력이다. 그런데 2012년 6월의 한일 정보보호협정(GSOMIA)을 둘러싼 논란을 보면 한일 사이버 안보 협력의 전망은 그리 밝지 않다. 2016년 3월에 워싱턴에서 열린 한·미·일 3국 정상회의에서도 미일 양국은 GSOMIA 체결의 필요성을 거듭 강조했지만 한국 측은 국내정치의 부담감을 이유로 일본과 거리를 두고 속도를 조절하려는 태도를 보인 바 있다. 그럼에도 2016년 10월에 한일 간에 처음으로 사이버정책협의회를 열고 사이버 분야에서의 협력 방안, 사이버 공간상의 국제규범 및 신뢰 구축 조치 등에 대해 의견을 나누는 자리를 마련했다(『연합뉴스』, 2016. 10. 28). 한·미·일 간에도 사이버 안보 협력채널이 가동되고 있는데, 2016년 1월의 제2차 한·미·일 차관급 협의 당시에 미국이 3국 간의 사이버 안보 분야 협력을 제안한 이후 구체적인 협력 방안을 논의하고 있다.

한국의 입장에서 볼 때 관건은 이렇게 미국이 주도하는 아태 지역동맹체제의 구축 과정에 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 유럽

수준으로 강화하려고 할 경우 한국은 어떠한 선택을 할 것인가가 쟁점이 될 가능성이 있다. 유럽에서 나토가 상정하는 적 개념에서 주요 위협으로 러시아의 사이버 공격을 상정하고 있다면, 아태 지역에서 미국 주도의 사이버 동맹이 상정하는 적 개념은 무엇이며 이러한 대결구도에서 한국이 취할 수 있는 입장은 무엇인지에 대한 고민이 필요할 것이다.

3. 지역협력체와 다자규범의 모색

이상에서 살펴본 현실주의 시각에서 이해된 국제협력의 모색 이외에 자유주의 시각에서 보는 동아태 지역 국가들 간의 역내 협력의 모색에도 주목할 필요가 있다. 이러한 노력은 사이버 안보 문제를 다루는 새로운 제도적 틀을 고안하는 것일 수 있겠지만, 아세안, 아세안지역안보포럼(ARF), 아시아태평양경제협력체(APEC) 등과 같은 기존의 제도적 틀 안에서 사이버 안보 문제를 다루는 구체적인 협력 방안을 모색하는 것일 수도 있다. 이러한 정부 간 협력과 제도화의 시도는 구성주의 시각에서 보는 역내 구성원의 지역안보 정체성 및 규범 형성에 대한 논의로 연결된다. 이러한 정체성과 규범에 대한 논의는 유럽 지역에서 진행되는 논의와 구별되는 동아태 지역의 지정학적 특성을 고려하는 것이어야 한다(Burton 2013; Sleat 2017).

이와 관련하여 최근에 아세안 국가들이 제기하고 있는 사이버 안보 협력과 규범에 대한 논의에 주목할 필요가 있다. 예를 들어, 2018년 4월 27일에 싱가포르에서 열린 제32차 아세안 정상회담에서 사이버 위협의 긴박성에 공감하면서 역내 국가들의 복원 역량 및 협력 방안을 강화하는 것이 논의되었을 뿐만 아니라 책임 있는 국가 행동을 보장하기 위한 국제규범의 필요성도 거론되었다(『HaninPost Indonesia』, 2018. 5. 7). 2018년 10월에는 아세안 10개국이 모두 합류하여 동남아시아 역내 테러에 대응하는 정보공유 네트워크인 '아워 아이즈(Our Eyes)'를 결성하기도 했다. 아워 아이즈는 파이브 아이즈를 벤치마킹한 것으로, 2018년 1월에 인도네시아가 제안하여 1차로 아세안 6개국이 모여 발족한 이래 동년 10월에 이르러 10개국이 모두 참여하게 되었다. 아워 아이즈는 지역 평화 및 대테러 협조 강화, 공해 안전 및 사이버 안보를 위해 협력하는 것을 목표로 내걸었다(『아시아경제』, 2018, 10. 21).

아세안이 한목소리로 사이버 안보 규범의 필요성을 강조한 반면 동북아 3국인 한·중·일의 사이버 안보 분야 협력은 지지부진하지만 협의의 틀은 계속 유지해오고 있다. 사실 역사적으로 볼 때 동북아에서 한·중·일 3국은 IT장관회의를 통해 협력해온 경험을 갖고 있다. 제1차 한·중·일 IT장관회의가 2002년에 모로코에서 개최된 이후 2003년에 제주에서 제2차 회의, 2004년에 일본 삿포로에서 제3차 회의, 2006년 3월에 중국 샤먼에서 제4차 회의가 개최된 바 있다(Thomas 2009). 그러던 것이 2000년대 후반 3국 간 IT협력이 다소 소강상태를 거치고 난 후 최근에 사이버 위협에 대한 공동 대응 차원에서 협력에 대한 논의가 다시 이루어지고 있다. 2014년 10월에 베이징에서 사이버 안보 분야의 3국 간 첫 고위급 회의로 제1차 한·중·일 사이버정책협의회가 열린 이후에 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 논의가 펼쳐졌다.

아울러 아태 지역 국가들이 역내 안정을 추구하기 위해 1994년에 출범시킨 다자간 정치·안보 협의체인 ARF 차원에서 진행되는 사이버 협력에도 주목할 필요가 있다(김상배 2018, 281). ARF에는 아세안 10

개국, 아세안 대화상대국 10개국, 기타 아시아 지역 7개국이 회원국으로 가입했으며 2000년대 중반 이후 중국의 적극적 참여와 2010년 미국의 참여로 영향력이 확대되고 있다. 2007년에는 한국의 주최로 ARF 사이버 테러 세미나를 서울에서 개최했으며, 2012년 제19차 프놈펜 회의에서는 중국의 주도하에 사이버 위협에 공동 대처하기 위한 합동전략의 개발 협력에 합의했다. 2013년 7월에 브루나이에서 열린 제20회 ARF에서는 대테러 작전과 초국가 범죄와 관련된 사이버 안보 이슈가 핵심 의제로 논의되었다. 2015년 8월의 ARF 외교장관회담에서는 회원국 간의 신뢰 구축을 통해 분쟁을 방지하고 상호 이해를 제고하기 위해 사이버 안보 작업계획을 채택했다. 2018년 8월에 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 없다는 것도 알아야 한다. 우선 유사한 생각을 가진 국가들의 정부가 나서서 원칙과 관행을 개발하고 역내 국가들이 준수할 규범을 만드는 것이 중요하다. 민간 부문이나 시민사회가 나서서 규범의 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 있다(외교부 2015). 동평구는 동북아 지역의 공동 위협요인인 원자력 안전, 에너지

안보, 기후변화와 환경, 재난관리, 사이버 공간, 마약 및 보건 분야에서의 협력 사업을 지속적으로 진전시켜 참여 국가들 간에 공감대가 형성되면 점진적으로 정치군사적 갈등이 주류를 이루는 전통안보 의제로 논의를 확대시켜나간다는 것이었다. 동평구는 안보 개념을 신흥안보 분야로 확장하여 동북아 협력을 제안했다는 점에서 기존에 전통안보를 중심으로 진행되어온 한국 외교의 새로운 지평을 연 것으로 평가되기도 한다. 이는 문재인 정부의 '동북아 평화협력 플랫폼' 구상으로 이어진다. 동북아 평화협력 플랫폼은 문재인 정부 100대 국정과제인 '동북아플러스 책임공동체 형성'의 세부 실천과제 중 하나로, 테러, 전염병, 자연재난, 사이버 범죄 등과 같은 초국가적 위협에 효율적으로 대응하기 위한 협력의 모색을 명시하고 있다

이러한 논의의 연속선상에서 볼 때 동아태 지역에서 한국이 주도하는 사이버 안보 분야의 다자규범 형성이 얼마나 가능할 것인지를 묻지 않을 수 없다. 예를 들어, 그 형태는 상이하더라도 유럽 지역의 탈린매뉴얼과 같은 규범, 굳이 이름을 붙이자면 한국이 주도한다는 의미에서 '서울매뉴얼'의 모색은 얼마나 가능할까? 탈린매뉴얼의 형성과 그 이후의 과정에서 발트 해 연안의 작은 나라인 에스토니아의 외교적 리더십이 주목을 받았다. 이를 보면 한국이 동아태 지역에서 외교적 리더십을 발휘하지 못할 이유가 없다. 물론 서울매뉴얼의 내용은 유럽 지역에 기반을 두는 탈린매뉴얼과는 달라야 한다. 사실 탈린매뉴얼은 2007년 에스토니아 사태 이후 미국과 나토 회원국들을 중심으로 만들어져서 서방 진영의 시각이 주로 반영되었다는 비판을 받았다. 근대적 영토 공간의 전쟁법을 원용해서 초국적 사이버 공간의 안보 문제를 다룬다는 한계도 지적되었다. 이를 염두에 두면 중견국인 한국이 구상하는 서울매뉴얼에는 탈린매뉴얼의 전략론 발상을 넘어서는 탈냉전과 탈근대의 평화담론

이 담겨야 할 것이다.

V. 맺음말

최근 양적으로 늘어났을 뿐만 아니라 질적인 패턴도 변화하고 있는 사이버 공격에 대한 대응책 마련이 일국 차원뿐만 아니라 글로벌 및 동아태 거버넌스 차원에서도 큰 관심사로 부상하고 있다. 이 장에서는 사이버 안보 거버넌스를 보는 이론적 논의를 바탕으로 동아태 지역 사이버 안보 거버넌스 모색의 현황과 과제를 짚어보았다. 이러한 과정에서 사이버 공격과 방어의 배경이 되는 기술 시스템의 성격에 대한 검토와 사회적 공간으로서 사이버 공간의 복합 네트워크적 성격에 대한 논의를 일반론적 배경으로 하여 동아태 지역의 고유한 지정학적 특성까지도 고려한 적합한 거버넌스의 내용을 탐색하고자 시도했다. 더 나아가 이러한 분석틀을 원용하여 향후 한국이 모색해야 할 동아태 사이버 거버넌스의 전략적 과제까지도 가늠해보고자 했다.

최근 늘어나고 있는 국가 지원 해킹에 대한 동아태 지역 국가들의 대응은 일차적으로는 피해 당사국들이 나서서 양자간 또는 다자간의 국제협력을 모색하는 것으로 나타나고 있다. 우선 눈에 띄는 것은 공격과 피해의 당사국들이 양자협의를 통해서 사이버 안보 갈등을 조율하려는 시도이다. 대표적인 사례는 2015년 9월 미중 사이버 안보 합의인데, 미중 양국은 적어도 민간시설과 지적재산은 공격하지 않겠다는 양자간 합의가 사이버 안보 분야에서도 어느 정도 가능함을 보여주었다. 조만간 북미관계나 한중관계, 한러관계, 남북관계에서도 이러한 양자합의가 시도될 가능성이 없지 않다. 그러나 비국가 행위자인 해커들이 활동하는 사이버 안보 분야에서 전통적인 현실주의 국가 간 프레임에 기반을 둔 이러한 양자합의 모델의 효과성에 대해서는 논란의 여지가 있다.

이에 비해 현재 동아태 지역에서 주목을 끌고 있는 거버넌스의 양식은 사이버 공격의 피해를 보는 나라들이 나서서 국제공조와 동맹협력을 벌이는 모델이다. 최근 이 국가들은 사이버 공격을 공식적으로 지목(attribution)하는 데 한목소리를 내고 위협정보를 공유하거나 사이버 방어 태세를 더욱 공고히 하고 있다. 이러한 사이버 방패 구축의 허브에 미국이 있다. 최근 미국의 행보를 보면 기존에 아태 지역에서 구축한 오프라인 동맹의 구도를 온라인 공간으로 옮겨오려는 전략을 펼치고 있는 것으로 판단된다. 미국은 중국 기업인 화웨이와 관련된 공급망 안전 문제 등을 내세워 파이브 아이즈 국가들과 공동전선을 펼치고 있으며 일본, 한국 등과도 긴밀한 협력체계를 구축하고 있다. 이러한 미국의 아태 지역 행보는 나토를 통해서 유럽 지역에서 추구했던 사이버 안보 구상을 떠올리게 한다.

그러나 사이버 안보의 기술적·사회적 특성에 대한 이론적 논의는 국가 행위자가 나서는 해법만으로는 사각지대가 있음을 보여준다. 비국가 행위자들이 나서서 초국적으로 감행하는 보이지 않는 공격을 국가 행위자들이 나서서 가시적으로 약속하거나 제재하려는 발상에는 기본적인 한계가 있을 수밖에 없다. 이러한 맥락에서 사이버 안보 문제를 정체성의 형성이나 제도적·당위적 규범의 마련이라는 관점에서 풀어보려는 시도가 힘을 얻는다. 이러한 문제의식을 가지고 볼 때 실제로 글로벌 차원에서 국제법과 국제기구 및 민간 참여의 글로벌 거버넌스 등의 다양한 프레임을 내세운 국제규범의 모색이 진행되고 있다. 그러나 이러한 사이버 안보 국제규범의 모색은 아직 시작단계일 뿐만

아니라 다소 교착상태에 빠져 있기까지 하다. 동아태 지역 차원에서도 국제규범을 마련하는 문제는 아세안이나 ARF의 사례에서 보는 바와 같이 아직은 다소 선언적인 차원에 머물러 있다.

결국 사이버 안보의 기술적·사회적 속성을 반영하면서도 동아태 지역의 지정학적 특성을 고려한 거버넌스 모델의 개발이 필요하다. 다시 말해 동아태 사이버 안보 거버넌스에는 어떠한 프레임이 적합한지에 대한 좀 더 체계적인 연구가 뒤따라야 할 것이다. 이 과정에서 한 가지 확실한 것은 전통안보 분야에서 도출된 거버넌스 모델을 사이버 안보 분야에 그대로 적용할 수는 없다는 사실이다. 동아태 지역의 특성상 국가 행위자들이 나서는 의미는 매우 크다. 그러나 아무리 국가의 지원을 받는 해커 집단의 활동이라고 하더라도 이를 정부 간 합의를 통해서 완전히 통제하기는 어렵다. 정부 간 합의의 차원을 넘어서 관련 행위자들을 규율하는 국제규범의 필요성이 논의되는 것은 바로 이러한 맥락에서이다. 결국 동아태 사이버 안보 거버넌스의 내용은 국가 행위자들이 나서는 양자협력 모델과 비국가 행위자들의 초국적 활동을 규율하는 지역 차원의 다자규범 모델을 복합하는 방식으로 채워져야 할 것이다.

끝으로, 글로벌 차원의 사이버 안보 규범이 부재한 가운데 동아태 차원에서 사이버 안보의 국제협력을 진행하고 지역규범을 모색하는 독자적 여정의 의미를 되새겨볼 필요가 있다. 한 가지 대전제는 기존에 유럽 지역에서 논의되었던 거버넌스 모델을 동아태 지역에 그대로 적용할 수는 없다는 것이다. 그러나 전통안보와는 달리 사이버 안보가 지니는 고유한 속성을 무시할 수도 없다. 결국 이는 글로벌 차원에서 논의되는 국제규범의 보편성을 수용하는 문제인 동시에 지역 차원에서 역내 국가들 간의 신뢰를 구축하고 협력을 유발하는 문제로 통

한다. 이러한 과정에서 동아태 국가들은 공동의 언어를 개발하고 정책을 조율하며 정보 교환을 촉진함으로써 사이버 안보 문제를 다루는 인식과 정책의 플랫폼을 마련해야 할 것이다. 궁극적으로 이러한 동아태 사이버 거버넌스 모델을 개발하는 문제는 이 장에서 살펴본 다양한 요소들을 복합적으로 고려하는 이론적 상상력의 문제와 연결된다.

참고문헌

김상배(2016), "신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해", 『한국정치학회보』, 50(1), pp.75-102.

_____(2018), 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』, 한울엠플러스.

김상배·신범식 편(2017), 『한반도 신흥안보의 세계정치: 복합지정학의 시각』, 사회평론.

외교부(2015), "동북아 평화협력구상", 외교부 홍보책자.

조현석(2017), "미중 사이버 안보 협약 연구", 『21세기정치학회보』, 27(2), pp.211-232.

페르 박(2012), 『자연은 어떻게 움직이는가?: 복잡계로 설명하는 자연의 원리』, 한승.

"'중국 화웨이는 위험한 기업' 교류·협력 중단 전 세계 확산…미국+캐나다 호주 영국 등 '화웨이주의보'", 『글로벌이코노믹』, 2018. 3. 23.

"중국, 러시아, 북한에 이어 미국도 '파리 콜'에서 빠지기로 결정", 『보안뉴스』, 2018. 11. 16.

"대테러연합 '아워아이즈', 아세안 10개국 모두 뭉쳤다", 『아시아경제』, 2018. 10. 21.

"中 5G 굴기…보안 문제로 꺾이나", 『아주경제』, 2018. 7. 23.

"한일, 28일 북한발 사이버 공격 대응 첫 양자협의", 『연합뉴스』, 2016. 10. 28.

"전 미 관리 '미북 협상에서 사이버 공격도 논의해야'", 『자유아시아방송』, 2018. 6. 15.

"서방 정보동맹 'Five Eyes' 세력 확대…中 정보 스파이戰 대응", 『조선일보』, 2018. 10. 12.

"아세안정상회담 '사이버 보안협력' '남북정상회담 지지'", 『HaninPost Indonesia』, 2018. 5. 7.

"'세계는 사이버전쟁 중'…러, 스마트 무기 기반 준비태세 강화", 『Russia Focus』, 2015. 6. 26.

"미국 '중국, 사이버안보 합의 위반'…중국 '근거 없는 주장'", 『VOA 뉴스』, 2018. 11. 9.

"정부간 사이버스파이 중단 합의, 효과 있나", 『ZDNet Korea』, 2017. 5. 11.

Access Partnership(2017), "Norms for Cybersecurity: Policy Options for Collaborative Security in the Southeast Asian Region", Consulting Paper.

Burt, Ronald S.(1992), *Structural Holes: The Social Structure of Competition,* Cambridge, MA: Harvard University Press.

Geers, Kenneth(2015), *Cyber War in Perspective: Russian Aggression against Ukraine,* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence(CCDCOE).

Burton, Joe(2013), "Small States and Cyber Security: The Case of New Zealand", *Political Science,* 65(2), pp.216-238.

Kitschelt, Herbert(1991), "Industrial Governance Structures, Innovation Strategies and the Case of Japan: Sectoral or Cross-National Comparative Analysis", *International Organization,* 45(4), pp.453-493.

Lee, Kyu-Young and Yoo-Joung Kim(2013), "Cyber Security for the Construction of Northeast Asian Community", 『아태연구』, 20(3), pp.301-330.

Noor, Elina(2015), "Strategic Governance of Cyber Security: Implications for East Asia", Rizal Sukma and Yoshihide Soeya eds., *Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance,* Tokyo: Japan Center for International Exchange, pp.150-163.

Schmitt, Michael N.(2012), "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", *Harvard International Law Journal,* 54, pp.13-37.

Sleat, Matt(2017), "Just cyber war?: Casus belli, information ethics, and the human perspective", *Review of International Studies,* 44(2), pp.324－342.

Thomas, Nicholas(2009), "Cyber Security in East Asia: Governing Anarchy", *Asian Security,* 5(1), pp.3-23.

Yoon, J.(2015), "Indonesia's Crisis Response Strategies: The Indian Ocean Tsunami of 2004", *Global Journal on Humanites & Social Sciences*(Online), 2, pp.195-202.