# 사이버 안보 국제규범의 세계정치

## 글로벌 질서변환의 프레임 경쟁*

김 상 배 **

❖ 요 약 ❖

최근 사이버 안보의 국제규범을 모색하기 위한 노력이 다양하게 진행되고 있다. 그런데 기존 연구들은 탈린매뉴얼이나 유엔 정부전문가그룹(GGE) 활동 등과 같이, 전통적인 국제법과 국제기구의 틀을 빌어 진행되는 규범 형성의 시도에만 주목하는 아쉬움이 있다. 초국적이고 탈영토적인 속성을 지닌 사이버 위협에 대처하기 위해서는 좀 더 복합적인 시각에서 국제규범의 형성을 보려는 노력이 필요하다. 이러한 문제의식을 바탕으로 이 글은 기존의 '국가간(inter-national)' 프레임이외에도 '정부간(inter-governmental)' 및 '글로벌 거버넌스(global governance)'의 프레임을 기반으로 하여 진행되고 있는 사이버 안보 국제규범의 복합적 형성에 주목하였다. 사이버 안보의 국제규범과 관련하여 원용되는 프레임은 단순히 중립적인 것이 아니라, 이를 통해서 미래 현실을 자신에게 유리한 방향으로 재구성하려는 담론과 이익을 그 바탕에 깔고 있다. 실제로 사이버 안보의 국제규범 형성과정의 이면에는 미국과 서구로 대변되는 서방 진영과 러시아와 중국으로 대변되는 비서방 진영이 글로벌 질서의 미래 구상을 놓고 벌이는 '프레임 경쟁'이 진행되고 있다. 이러한 프레임 경쟁과 거기서 파생되는 질서변환의 양상을 정확히 파악하고 대응하는 일은 한국과 같은 중견국에게 있어서는 더할 나위 없이 중요한 국가전략의 사안이 아닐 수 없다.

**핵심어: 사이버 안보, 국제규범, 세계정치, 글로벌 질서변환, 프레임 경쟁**

# Ⅰ. 머리말

2013년은 사이버 안보의 세계정치 연구에 전기를 안겨준 해로 기억될 것이다. 3월에는 한국의 주요 방송국과 금융기관이 해킹을 당해서 역대 가장 큰 피해를 입은 것으로 알려진 3.20 사이버 테러가 발생했으며, 6월에는 에드워드 스노든의

『국가전략』 2017년 제23권 3호
* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2016S1A3A2924409).
** 서울대학교 정치외교학부 교수

폭로로 미국이 주요국 인사들을 대상으로 광범위한 도청을 벌여왔음이 밝혀지기도 했다. 6월에 열린 미중 정상회담은 국제정치학계에 사이버 공간의 중요성을 각인시키는 사건이 되었다. 두 강대국 정상들이 양국 간의 현안인 북핵과 더불어 사이버 안보를 양대 쟁점으로 선정하고 긴 시간을 할애해서 의견을 나누었던 것이다. 2013년은 사이버 안보 국제규범의 모색이 새로운 전기를 맞았던 해로도 기억될 것이다. 3월에는 기존의 국제법을 사이버 안보에 적용하려는 시도인 탈린매뉴얼이 발표되었고, 6월에는 유엔 정부전문가그룹(GGE)이 오랜 난항 끝에 사이버 안보 관련 권고안을 도출했으며, 10월에는 서울에서 제3차 사이버공간총회가 열려 서울프레임워크를 도출하고 유엔 GGE 권고안을 여러 국가들에게 알리는 계기를 마련했다. 이러한 일련의 사건들이 종합적으로 뜻하는 바는 사이버 안보의 문제가 국제정치학의 논제로서 본격적으로 자리매김했다는 것이다.

사실 사이버 안보는 그 성격상 일국 차원을 넘어서 이해해야 하는 문제이다. 사이버 위협정보를 공유하는 주변국들과의 협력과 글로벌 및 지역 차원의 규범 마련을 위한 외교적 노력이 국내적 차원의 기술역량 강화와 법제도 정비에 못지않게 중요한 문제이다. 일국 차원의 준비가 만병통치약이 될 수 없기 때문에, 피해 당사자들이 스스로 발 벗고 나서서 서로 협력하고 국제적으로 합의할 수 있는 규범을 세우려는 노력이 중요한 분야이다. 이러한 인식은 2010년대에 들어 널리 확산되어 세계 주요국들은 사이버 안보의 국제협력을 위한 전략서를 발간하고 이를 실천하는 정책을 추진하기 시작했으며, 실제로 양자 및 지역 차원의 국제협력을 강화하고 국제기구와 다자외교의 장에서도 국제규범을 도출하기 위한 활발한 논의를 벌였다. 이러한 현실을 반영하여 최근 국제정치학계에서도 다수의 연구들이 사이버 안보 분야의 난제들을 풀어가기 위한 방책으로서 국제규범의 변수에 주목하고 있다 (Stevens, 2012; Schmitt and Vihul, 2014; Forsyth Jr. and Pope, 2014; Kerttunen and Kiisel, 2015).

국내 학계로 눈을 돌려 보면, 그나마 진행된 의미있는 연구들이 대부분 탈린매뉴얼이나 유엔 GGE 활동 등과 같은 전통적인 국제법과 국제기구에만 초점을 맞추고 있어 다소 아쉽다(박노형·정명현, 2014; 박노형·정명현, 2016; 장규현·임종인, 2014; 장노순. 2016). 물론 사이버 안보 문제를 풀어가는 데 있어서 국가간 분쟁을 중재하는 국제법이나 국제기구의 틀을 원용하는 작업의 중요성은 부인할 수 없다. 그러나 초국적으로 작동하는 사이버 공간에서의 안보 문제를 국민국가의 영토적

관할권을 전제로 형성된 기존 국제규범의 틀 안에서만 보는 것은 바람직하지 않다. 다시 말해, 오프라인 공간의 전통안보 분야에서 도출된 국제규범을 온라인 공간의 사이버 안보에 그대로 적용하는 것은 무리가 아닐 수 없다. 다양한 비국가 행위자들이 전면에 나서고 있는 사이버 안보의 게임에서 문제의 책임을 국가 단위로 귀속시키는 기성 국제정치의 단순 발상은 한계가 있을 수밖에 없다. 사이버 안보의 탈영토성과 이에 관여하는 행위자들의 다양성을 고려한 새로운 규범을 모색하는 복합적인 접근이 필요하다.

실제로 1990년대 후반 이후 사이버 안보 분야의 규범형성 문제는 독립적 어젠다로 다루어졌다기보다는, 포괄적 맥락에서 본 글로벌 인터넷 거버넌스의 일부로서 취급되어 왔다. 그러다가 2010년대에 들어서면서 사이버 안보의 전략적 중요성이 부쩍 인식되면서 국가 행위자들이 나서서 국제규범을 모색하는 양상이 나타났던 것이다(Mazanec, 2015). 그럼에도 아직까지 사이버 안보의 규범에 대한 국제적 합의는 마련되지 않았으며, 오히려 최근에는 더 복잡해지는 양상마저 드러내고 있다. 이 글에서 살펴본 바와 같이, 나토의 탈린매뉴얼이나 유엔 GGE 활동이외에도, 사이버공간총회, 유럽사이버범죄협약, 상하이협력기구, OSCE, ARF, ICANN, ITU 등에서도 국제규범들이 모색되고 있다. 이러한 복잡성에 주목하여 일부 국제정치학자들은 이 분야에서 나타나는 규범 모색의 양상을 '레짐 복합체(regime complex)'로 보기도 한다(Choucri, et al., 2014; Nye, 2014). 이 글의 문제의식은 이러한 레짐 복합체에 대한 이론적 논의와 맥이 닿는다. 그러나 레짐 복합체의 개념보다는 한발 더 나아가서, 다양한 국제규범들을 단순히 병렬적으로만 보는 데 그치지 않고, 그들 규범의 구체적인 작동방식과 복합적인 아키텍처를 분석할 수 있어야 한다는 입장을 취한다.

이러한 문제의식을 바탕으로 이 글은 미국의 미디어 학자 토드 기틀린(Todd Gitlin)이 개발하고 미국의 언어학자 조지 레이코프(George Laykoff)에 의해 널리 소개된 '프레임(frame)'의 개념을 원용하여 논의의 실마리를 풀었다(Gitlin, 1980; 레이코프, 2007). 이들의 시각을 사이버 안보의 사례에 적용해서 보면, 현재 국제규범의 형성과정에서 동원되는 프레임은 적어도 다음과 같은 세 가지 차원에서 이해할 수 있다. 첫째, '국가간(inter-national)' 프레임인데, 이는 전쟁법과 같은 국제법을 원용하거나 유엔과 같은 전통 국제기구 모델을 원형으로 한다. 둘째, '정부간(inter-governmental)' 프레임인데, 이는 사이버 공격의 직접 피해 당사자인 서구

선진국들의 정부간협의체 모델 또는 지역적 기반을 공유하는 국가들의 협력체 모델을 원형으로 한다. 끝으로, '글로벌 거버넌스(global governance)' 프레임인데, 이는 국가 행위자이외에도 민간 기업, 학계 전문가, 시민사회 활동가 등과 같은 다양한 비국가 행위자들이 참여하여 만드는 글로벌 거버넌스 모델을 원형으로 한다.

이렇게 세 가지 프레임을 기반으로 한 사이버 안보의 국제규범은 각기 상이한 글로벌 질서상을 상정한다. 이 글은 각 프레임이 지향하는 질서상의 내용적 차이를 좀 더 구체적으로 보여주기 위한 논의를 펼쳤다. 사실 세 가지 프레임의 질서상은 서로 다른 아키텍처와 작동방식을 지니고 있으며 21세기 질서변환의 시대를 맞이하여 서로 경합하는 모습을 보여주고 있다. 이러한 과정에서 이 글이 특히 주목하는 것은 서로 상이하게 주장되는 국제규범 프레임의 기저에 깔린 이익과 이를 구현하기 위한 담론의 경쟁, 즉 '프레임 경쟁'이다. 사실 사이버 안보의 국제규범과 관련하여 제시되는 프레임은 단순히 중립적인 것이 아니라 이를 통해서 미래 현실을 자신에게 유리한 방향으로 재구성하려는 담론과 이익이 반영된 것이다. 실제로 사이버 안보의 국제규범 형성과정의 이면에는 미국과 서구로 대변되는 서방 진영과 러시아와 중국으로 대변되는 비서방 진영이 각기 자신들의 이익을 반영한 프레임을 관철시키기 위한 경쟁을 벌이고 있다. 이렇게 강대국들이 벌이는 프레임 경쟁의 양상을 정확히 파악하는 일은 한국과 같은 중견국의 국가전략에 있어 중요한 사안이 아닐 수 없다.

이 글은 다음과 같이 구성되었다. 제2장은 사이버 안보의 국제규범을 보는 프레임을 이론적으로 구분하고, 이러한 프레임을 현실화시키기 위해서 벌이는 경쟁을 이해하는 플랫폼을 제시하였다. 제3장은 국가간 프레임으로 보는 사이버 안보 국제규범 형성의 사례로서, 국제법을 원용한 탈린매뉴얼과 전통 국제기구인 유엔에서의 GGE 활동을 살펴보았다. 제4장은 정부간 프레임의 사례로서 서방 진영이 주도하는 사이버공간총회와 유럽사이버범죄협약 등을 살펴보았으며, 이에 대항하는 비서방 진영의 시도로서 상하이협력기구와 기타 지역협력체의 사례를 살펴보았다. 제5장은 글로벌 거버넌스 프레임의 사례로서, ICANN의 다중이해당사자주의 모델과 ITU를 중심으로 모색되는 '정부간주의' 모델을 살펴보았다. 끝으로, 맺음말에서는 사이버 안보 국제규범의 세 가지 프레임을 가로지르는 경쟁을 이익, 제도, 관념의 세 가지 측면에서 종합·요약하고, 이러한 프레임 경쟁이 지니는 실천적 함의를 간략히 지적하였다.

## Ⅱ. 사이버 안보 국제규범 경쟁의 분석틀

기존의 국제정치학은 말 그대로 '국(國, nation)'이라는 단위의 성격과 이들의 사이, 즉 제(際, inter)'의 내용을 탐구해왔다. 주류 국제정치학자들도 '국'을 기본 단위로 보는 데 의견이 일치했지만, 그들의 관계, 즉 제(際, inter)의 내용, 즉 구성원리를 무엇으로 보느냐에 대해서는 의견을 달리했다. 근대 국제정치는 주권국가의 권한을 위임받은 세계정부가 없는 상태, 즉 '무정부 상태(anarchy)'인 것은 사실이지만, 그것이 '무질서 상태'를 의미하는 것은 아닐 것이기 때문에 '정부 없는 질서상태'를 좀 더 구체적으로 규정하려는 노력이 제기되어 왔다. 이러한 시도 중의 하나가 국제규범에 대한 논의이다. 국제규범에 대한 논의는 단위들 간 기계적 상호작용을 전제로 한 단순계로서의 '체제(system),' 즉 무정부 상태라고 할 수는 없지만, 단위들 간의 정체성의 공유까지도 전제로 하는 공동체(community)에는 이르지 않은, 그 중간 어디쯤에서 '형성 중인 질서(order-in-making),' 달리 말하면 일종의 국제사회(society)의 요소를 탐구해왔다(전재성, 2011, p.44; 김상배, 2014, pp.319-323).

이러한 국제규범은 단위들 간의 관계를 조율하는 제도화의 의미를 넘어서 국제정치 현상의 도덕성과 당위성을 거론한다. 사실 근대 국제정치에서도 도덕적·윤리적 차원에서 부과되는 규범이 존재했다. 예를 들어, 앤드류 링클레이터(Andrew Linklater)는 국제정치에서 세 가지 측면에서 파악되는 규범이 있음을 주장하였다. 첫째, 남을 죽이지 말아야 하는 의무처럼 상호간에 해야 하는 것이 있는데, 이는 존 롤즈(John Rawls)가 말하는 바처럼 피해를 끼치지 말고 불필요한 고통을 가하지 말아야 할 소극적 의무로서의 자연적 의무를 의미한다. 둘째, 남이 남을 죽이는 것을 막아야 하는 의무처럼 제3자와의 관계에서 해야 하는 것이 있는데, 집단학살과 인권침해 탄압 등과 같은 비인도적 행위를 방관하지 않고 개입해야 하는 의무이다. 끝으로, 죽어가는 사람을 살려야 할 의무처럼 글로벌 차원에서 해야 하는 것이 있는데, 이는 기아 지원과 인도주의적 긴급구호처럼 곤궁에 처한 사람들을 도와야 할 상호원조 의무로서, 롤즈가 말하는 적극적 의무로서의 정의의 의무이다(Linklater, 2005; Rawls, 1999).

이상의 세 가지 개념은 사이버 안보의 국제규범에도 적용 가능하다. 첫째, 남에게

해를 끼치지 말아야 하는 소극적 의무의 관점에서 보면, 타국의 시스템을 해킹하여 지적재산이나 개인정보를 절취하는 자국의 해커를 단속할 의무를 생각해 볼 수 있다. 물론 정치군사적 목적으로 타국의 시스템을 해킹하지 말아야 할 의무도 여기에 해당된다. 둘째, 비인도적 행위를 방관하지 말아야 할 의무라는 관점에서 보면, 자국의 인터넷을 지나치게 통제하며 인권을 침해하는 타국의 행위에 대해서 남의 일이라고 모른 척하지 말아야 할 의무를 설정해 볼 수 있다. 또는 타국의 해커들이 자국의 인프라를 제3국에 대한 사이버 공격의 경유지로 활용하는 것을 거부해야 할 의무도 여기에 해당된다. 끝으로, 어려운 사람을 도와야 하는 적극적 의무라는 관점에서 보면, 글로벌 차원에서 인터넷 환경이 지나치게 낙후되어 해킹의 경유지를 제공하는 취약점이 있는 나라와 지역을 지원해야 할 의무를 생각해 볼 수 있다. 글로벌 디지털 격차 해소의 차원에서 진행되는 개도국의 사이버 안보 역량 지원 사업 등이 여기에 해당된다.

이러한 방식으로 파악되는 도덕적 당위성으로서의 국제규범은 고정불변한 것이 아니라 역사상 나타난 다양한 국제정치의 패권구조 및 구성원리 등과 조응하며 변천해왔다(전재성, 2012). 21세기 세계정치에서도 미국의 패권이 쇠퇴하고 중국이 부상하면서 패권구조가 변화하고 규범의 변화가 논의되고 있으며, 더 나아가 글로벌화와 정보화의 추세 속에 비국가 행위자들이 전면에 나서면서 기존의 국민국가 중심의 질서가 변화를 겪게 되고 이를 반영하는 새로운 규범의 필요성이 제기되고 있다. 전망컨대, 새로운 규범은 기존 국제정치의 테두리를 넘어서 새롭게 부상하는 권력구조와 구성원리를 반영한 규범이 될 가능성이 높다. 특히 사이버 공간을 매개로 부상하는 글로벌 질서에 조응하는 국제규범은 여타 사례들보다 훨씬 더 복합적인 양상으로 출현할 것이다. 여기서 관건은 이렇게 복합적으로 등장할 규범의 내용을 예견하는 것이라고 할 수 있다. 이러한 국제규범 형성의 복합성을 이해하기 위해서 이 글은 국제정치의 이론적 논의에 뿌리를 두는 세 가지의 프레임을 원용하였다.

첫째, '국가간' 프레임으로 보는 국제규범의 형성이다. 이는 주권국가로서 국민국가 행위자를 기본단위로 설정하고 그들의 관계에서 형성되는 규범을 논한다. 이러한 국제규범의 사례로는 헤들리 불(Hedley Bull)이 제기했던 국제사회(international society)와 무정부적 사회(anarchical society)의 개념을 들 수 있다(Bull, 1977). 헤들리 불에 의하면, 정부가 있어야 질서가 형성될 수 있다는 국내정치의 상황과는

달리, 국가를 주요 행위자로 하는 국제정치에서는 무정부 질서 하에서도 상호간에 공유하는 규범과 규칙을 통해서 국가간 사회, 즉 국제사회를 형성하여 질서를 유지할 수 있다고 본다. 구체적으로 근대 국제사회에서 이러한 규범과 규칙은 국가간 권력을 향한 전쟁과 투쟁, 초국적 공감대와 갈등의 요소, 국가간 협력과 규칙에 따른 상호작용의 요소 등을 통해서 형성된다. 전형적인 사례로서 주권국가들의 대표들이 구성하는 유엔과 같은 국제기구나 주권국가들의 합의인 국제법을 들 수 있다. 이러한 국가간 프레임이 궁극적으로 상정하는 질서상은 국민국가들로 구성되는 근대 국제질서이다. 그런데 역설적으로 21세기 세계정치에서 이러한 질서상은 개방적 글로벌화 현상에 저항하여 국가주권의 쇠퇴를 늦춰보려는 보수적인 프레임으로 이용되는 경향이 있다. 실제로 사이버 공간에서의 국가주권을 주장하는 비서방 진영과 개도국들의 주장에서 이러한 국가간 프레임의 반(反) 글로벌화적 경향이 발견된다.

둘째, '정부간' 프레임으로 보는 국제규범의 형성이다. 이는 탈냉전 이후 글로벌화의 추세 속에서 초국적 문제의 해결을 위해 구성되는 '정부 간 네트워크'를 통해서 모색되는 규범을 논한다. 예를 들어, 2008년 미국발 금융위기가 세계경제를 강타한 이래 위기극복을 위한 국제공조와 함께 위기 이후 신질서 구축을 위한 제도적 노력의 형태로 부상한 G20 정상회의를 들 수 있다(손열 외, 2010). 이외에도 선진국 정부들 간의 협의체인, OECD나 APEC, ASEAN 등과 같은 지역협력체를 통해서 모색되는 국제규범들도 사례이다. 이러한 규범들은 공식 국제기구는 아니면서 정부간 공식 외교관계를 통해서 발현되며, 이해당사국들이 구성하는 일종의 '클럽 모델'에 기반을 둔다. 이러한 정부간 협의체는, 이전에는 영토국가의 경계 내에 통합되어 있던 행정부, 입법부, 사법부 등의 국가 조직이 각기 초국적 차원에서 행정부의 네트워크, 의회의 네트워크, 사법과 경찰의 네트워크 등과 같이 국가의 기능이 분화되는 형태, 즉 일종의 '해산된 국가(disaggregated state)'의 형태로 진행되기도 한다(Slaughter 2004). 이러한 정부간 프레임이 상정하는 질서상은, 기본적으로는 근대 국제질서이지만, 그 운용과정에는 전세계 모든 국가들이 동등하게 참여하는 것이 아니라 이해당사자인 선진국들이 주도하는 '부분적 국제질서'의 모델이다. G7/8, G20 등과 같은 선진국들의 정부간협의체는 이러한 양상을 반영해 왔으며, 최근에는 초국적 난제들을 해결하는 과정에서 기성 질서를 유지하기 위한 수세적 논리를 대변해 왔다.

끝으로, '글로벌 거버넌스' 프레임으로 보는 국제규범의 형성이다. 이는 탈근대적이고 글로벌한 난제들을 풀기 위해서 국가뿐만 아니라 다양한 비국가 행위자들도 참여하는 규범 형성을 논한다. 다양한 초국적 변화에 직면한 오늘날 다양한 행위자들이 자발적으로 참여해서 만들어내는 수평적이고 분산적인 메커니즘에 대한 관심이 커지고 있다. 이는 거버먼트(Government)로 대변되는 기존의 관리양식을 넘어서는 새로운 관리양식으로 거버넌스(Governance)에 대한 논의와 통한다(Rosenau and Czempiel eds., 1992). 예를 들어, 사이버 안보, 인터넷 거버넌스, 디지털 경제, 글로벌 생태환경 등의 분야에서 비국가 행위자들의 역할이 증대되고, 국가 행위자들은 이러한 변화를 수용할 수밖에 없는 양상이 나타나고 있다. 다양한 형태의 공공-민간 파트너십이나 정부 활동에의 민간 참여 등이 사례이다. 최근 글로벌화와 정보화, 민주화의 맥락에서 제기되는 글로벌 거버넌스에 대한 논의는 이렇게 비국가 행위자들의 역할이 커지고 있는 현상을 전제로 하고 있다. 이러한 글로벌 거버넌스 프레임이 상정하는 질서상은 국가이외도 다국적 기업이나 글로벌 시민사회단체 등과 같은 다양한 비국가 행위자들이 참여하는 탈(脫)국제질서이다. 그러나 21세기 글로벌 거버넌스 모델은 완전한 탈집중적 논리로만 작동하지 않고, 그 이면에는 사실상의 지배를 행사하는 패권국의 힘이 있다는 비판을 받아왔다.

이상에서 살펴본 바와 같이, 세 가지 프레임을 기반으로 한 국제규범의 모색은 각기 상이한 질서관념을 갖고 있으며, 심층적으로 의도하는 바도 다를 뿐만 아니라, 당연히 거기서 파생되는 실천전략적 함의도 다를 수밖에 없다. 이렇게 보면 국제규범과 관련하여 제시되는 프레임은 단순히 중립적인 것이 아니라 이를 통해서 미래현실을 자신에게 유리한 방향으로 재구성하려는 이익이 투영된 것으로 보아야 한다. 각 프레임이 궁극적으로 구현될 경우 자신에게 유리한 구조적 환경으로서 특정한 형태의 국제규범이 도출되는 결과가 예견되기 때문이다. 이를 위해 부단히 자신들의 프레임을 합리화하는 담론을 생산하고 이에 동조하는 세력을 규합하려는, 이른바 '프레임 경쟁'이 벌어진다. 좀 더 구체적으로 말하면, 기존 근대 국제질서에서는 국가간 프레임 '내'에서 벌어진 규범경쟁이었다면, 오늘날 질서변환기의 규범경쟁은 어느 프레임을 플랫폼으로 삼을 것인가의 문제가 우선적 관건이 되는 '프레임 간 경쟁'이 벌어진다. 이러한 문제의식을 가지고, 이하에서는 사이버 안보 분야에서 진행되고 있는 국제규범의 프레임 경쟁의 구체적인 양상을 살펴보겠다.

# Ⅲ. '국가간' 프레임으로 본 사이버 안보 국제규범

## 1. 기존 국제법 원용 시도: 탈린매뉴얼

전통적인 국제법(특히 전쟁법)의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격에 대응하려는 시도의 사례로는 탈린매뉴얼(Tallinn Manuel)이 있다. 탈린매뉴얼은 2013년 3월 나토 CCDCOE(Cooperative Cyber Defence Centre of Excellence)의 총괄 하에 20여명의 국제법 전문가들이 2009년부터 시작하여 3년 동안 공동연구를 거쳐 발표한 총 95개항의 사이버전 지침서이다. 300여 페이지에 달하는 분량의 탈린매뉴얼은 현존 국제법 중에서 특히 '전쟁의 개시에 관한 법(jus ad bellum)'과 '전쟁 수행 중의 법(jus in bello)'이 사이버전에 적용가능한지 여부를 검토했다. 탈린매뉴얼이 언급하고 있는 '사이버전(Cyber Warfare)'은 국가들이 사이버 공간에서 적대적인 군사행위를 하는 사이버 공격, 즉 상대국의 주요 인프라나 명령 통제시스템의 손상 파괴로 인한 인명살상이나 목표물의 손상 등 물리적 타격을 의미한다. 탈린매뉴얼은 새로운 법체계를 구축하기보다는 기존 국제법의 테두리 내에서 사이버 공간에서의 무력행위를 규정하는 방식으로 탐색되었다(Schmitt, ed., 2013; 박노형·정명현, 2014).

탈린매뉴얼의 골자는 사이버 공간에서도 전통적인 교전수칙이 적용될 수 있으며, 사이버 공격으로 인해 인명 피해가 발생할 경우 해당 국가에 대한 군사적 보복이 가능하고, 핵티비스트 등과 같은 비국가 행위자에 대해서도 보복하겠다는 것이었다. 더 나아가 사이버 공격의 배후지를 제공한 국가나 업체에 대해서도 국제법과 전쟁법을 적용하여 책임을 묻겠다는 것이었다(Schimit, 2012). 탈린매뉴얼이 특히 주안점을 둔 이슈는 세 가지였는데, 첫째 물리적 공격에 버금가는 '무력사용(use of force)'의 기준을 어떻게 설정할 것인가, 둘째 사이버 공격에 활용된 인프라의 소재지 및 경유지의 문제를 어떻게 이해할 것인가, 끝으로 두 나라 사이에 이루어진 복잡한 양상의 사이버 공격 행위와 관련하여 '책임소재(attribution)'를 어떻게 가려낼 것인가 등의 문제였다(민병원, 2017, p.33). 탈린매뉴얼은 구속력이 없는 지침서의 형식이지만, 전시 민간인과 포로에 대한 보호를 규정한 제네바 협약처럼, 사이버

전에도 국제법적인 교전수칙을 마련하려는 문제의식을 갖고 있었으며, 이런 점에서 일종의 '정전(正戰, Just War)론'의 시도라고 볼 수 있다.

그러나 탈린매뉴얼은 2007년 에스토니아 사태 이후 미국과 유럽 국가들이 중심이 되고, 게다가 나토 회원국의 전문가들이 참여하여 만들어졌기 때문에, 러시아나 중국 등을 배제한 서방 진영의 시각이 주로 반영되었다는 비판을 받았다. 2015년 소니 해킹 사건 이후 미국이 북한에 대한 '비례적 대응'을 모색하는 과정에서 탈린매뉴얼의 조항들을 원용하려는 조짐을 보여서 국제적으로 주목을 끈 바 있었다. 탈린매뉴얼은 아직까지 사이버 국제법이 존재하지 않는 상황에서 규범을 제시하는 정도의 의미만을 부여받는다. 그러나 한국의 입장에서 볼 때, 기존 국제법의 틀을 적용하여 북한의 사이버 공격을 불법행위로 규정하고 이에 대해 규제할 수 있는 (국제법까지는 아니더라도 국제규범적) 근거기준을 마련하는 의미가 있다. 이로써 중국을 북한으로부터 분리하는 효과도 기대할 수 있기 때문이다. 실제로 이와 관련하여 사이버 공격에 대한 '책임소재'의 원칙을 적용하는 문제가 관건이다. 사이버 공격의 명백한 증거가 제시될 경우 지리적으로 사이버 공격의 근원지 혹은 경유지가 된 국가는 사이버 공격에 대해서 적절한 조치를 취하는 원칙을 마련하자는 것이다. 그러나 이러한 국제법 원칙의 적용문제는 아직까지는 구체화되지 못하고 있다(신맹호, 2016).

탈린매뉴얼로 대변되는 국제법 적용의 프레임은 최근 들어 진전을 보고 있는데, 2017년 2월에는 그 두 번째 버전인 탈린매뉴얼 2.0이 발표되었다(『보안뉴스』, 2017.2.11). '사이버전(cyber warfare)에 적용 가능한 국제법'을 논한 탈린매뉴얼 1.0과는 달리 탈린매뉴얼 2.0은 '사이버 작전(cyber operation)에 적용 가능한 국제법'을 논했다. 여기서 말하는 '사이버전'이란 국가와 국가 사이에 일어나는 사이버 전쟁을 말하는 것이고, '사이버 작전'이란 국경을 넘나드는, 그러나 일국 정부의 의도와는 별개로 일어나는, 각종 사이버 범죄들도 지칭한다. 탈린매뉴얼 1.0의 시도에서 보는 바와 같이, 전쟁법의 적용 문제만을 논한다면, 이에 해당하는 사이버전은 아직까지 발생한 적이 없다고 보아야 할 것이다. 그렇지만 지금도 크고 작은 사이버 공격과 이로 인한 국가사회적 피해는 계속 발생하고 있다. 탈린매뉴얼 2.0은 이러한 상황을 어떻게 이해할 것인가에 대한 부분적 대답을 모색한 작업이라고 평가할 수 있다. 즉 전쟁의 수준에는 미치지 않지만 사회적으로 큰 충격이 있는 공격 행위에 대한 법 적용을 어떻게 하느냐의 문제를 다루고 있다(Schmitt, ed., 2017).

## 2. 전통 국제기구에서의 논의: 유엔 GGE 활동

전통 국제기구인 유엔 차원에서 사이버 안보 문제를 다루려는 움직임도 최근 많은 주목을 받으면서 빠르게 진행되고 있다. 특히 2013년 6월 제3차 유엔 군축 및 국제안보 위원회 산하 정보보안 관련 정부전문가그룹(Group of Governmental Experts, GGE)에서 합의하여 도출한 최종 권고안에 주목할 필요가 있다. 이 안은 1998년 러시아가 제안했는데, 미국은 처음부터 러시아의 제안에 대해 동조하지 않았고, 이후로도 소극적인 자세로 사이버 안보 관련 국제협력에 대응해 왔다. 이후 2004년부터는 제1-2차 GGE의 포맷을 빌어 논의가 진행되었으나 인터넷의 국가통제를 강조하는 러시아나 중국과 같은 비서방 국가들과 이에 반대하는 미국의 입장이 극명히 대립했었다. 그러던 것이 2013년 6월 개최된 제3차 회의에서는 전체 참여국들이 사이버 공간에서도 유엔헌장과 같은 기존 국제법이 적용될 수 있다는 점에 합의하고 이러한 규범을 어떻게 적용할 수 있는지에 대해서 지속적으로 연구하기로 합의하였다(장규현·임종인, 2014, pp.35-38; 장노순, 2016, pp.10-17).

중국과 러시아는 기존의 국제법이 사이버 공간에 적용될 수 없으며, 따라서 새로운 규범에 합의하지 않는 한 사이버 공간에서의 국가 행위에 대한 규율이 존재하지 않는다는 입장이었다. 그러나 제3차 GGE에 이르러서는 종전의 입장을 양보하여 기존 국제법의 사이버 공간 적용 시도에 합의하였다. 한편 미국과 유럽 국가들은 사이버 공간에서 국가주권과 불간섭원칙을 인정하는 것에 반대하였지만 제3차 GGE를 계기로 사이버 공간에서의 국가책임성을 부인하지 않게 되었다. 기존 국제법이 사이버 공간에 적용되는지 여부에 대한 서방과 비서방 진영 간의 논란이 양 진영 모두가 조금씩 양보하는 모양새를 취하게 되었는데, 궁극적으로 최종보고서에 기존 국제법이 사이버 공간에도 적용된다고 기술함으로써 종전의 논란거리들이 일단은 해소되었다. 이외에도 제3차 GGE 보고서는 국가들의 신뢰구축조치(CBM), 정보 교환이나 협의체 구성, 공동대응체계 개발, 역량강화 협력 등의 내용을 담았다(장규현·임종인, 2014, pp.38-42; 이상현, 2017, pp.79-82). 2015년 6월 제4차 GGE에서는 제3차 GGE 권고안을 계승하며, 좀 더 진전된 합의안을 국제법 부문과 규범 부문으로 나누어 도출하였으나, 구체적인으로 국제법이 어떻게 적용되는지에 대해서는 여전히 합의를 보지 못했다(박노형·정명현, 2016, p.173).

2016년 구성된 제5차 GGE에서는 제4차 보고서에서의 합의사항은 그대로 두고, 그 내용을 보다 구체화하고 추가할 사항에 대해서 검토했는데, 서방과 비서방 국가들이 의견을 달리했던 쟁점은 다음의 세 가지였다. 첫째, 자위권과 국제인도법(IHL), 대응조치(counter-measure) 등의 허용을 주장하는 서방측의 주장에 대해, 비서방측(특히 중국)은 반대했다. 둘째, 사이버 테러·범죄를 포함시키는 문제와 관련해서도 중국이 이를 다루는 별도의 국제법 체계를 구성할 것을 주장한 데 대해, 서방측은 국내정치 통제의 수단으로 악용될 것을 우려해 반대했다. 끝으로, 인터넷 거버넌스의 포함 여부와 관련해서 단순한 인터넷 관리 문제로 보고 싶은 서방측에 대해서 비서방측은 이를 국가안보의 문제로 보자고 주장했다. 한편 서방 진영의 국가들 간에도 몇 가지 입장 차이가 있었는데, '제3국의 책임(Due Diligence, DD)'을 국제규범으로 볼 것이냐 아니면 국제법으로 볼 것이냐의 문제, 사이버 기술 수출통제 및 비정부 행위자에 대한 공격적 사이버 무기의 사용금지에 대한 규범을 마련하는 문제, 데이터 관할권 문제를 사이버 안보의 의제로 포함시킬 것이냐의 문제 등이 논의되었다(신맹호, 2016).

이상에서 살펴본 일련의 전개과정에서 유엔 GGE의 임무가 제3차에서 제4차와 제5차 회의로 진행되면서 변화하고 있음에 주목할 필요가 있다. 제3차 GGE 이후 러시아나 중국은 사이버 공간에 새로운 법을 만들어야 한다는 주장을 포기하고, 기존의 국제법을 적용하는 데 합의한 것으로 보인다. 따라서 제4-5차 GGE에서는 사이버 공간의 특별한 성격을 고려했을 때 어떤 국제법을 적용해야 할 것이냐의 문제가 쟁점이었다. 이 문제에 대해서는 서방측은 조심스럽게 접근했는데, 자발적이고 비구속적인 국제 관습법의 개발은 인정하지만, 조약 수준의 국제법을 제정하는 일은 어렵다는 것이 서방측의 기본 입장이었다. 사실 제5차 회의까지 진행되는 동안, GGE의 주요 임무는 사이버 공간에 적용되는 국제법을 새로 제정하는 문제가 아니라, 기존의 국제법을 사이버 공간의 이슈에 적용하면 무엇이 문제인지를 검토하는 데 한정되어 있었다. 이러한 GGE의 논의가 주는 유용성은 국가행동을 규제하는 국제법의 개발과 적용 그 자체보다는 사이버 공간에서의 일탈적 행위와 국가의 책임있는 행동에 대한 규범적 판단의 근거를 마련하는 데 있다고 할 수 있다(김소정, 2016; 박노형, 2017).

# Ⅳ. '정부간' 프레임으로 본 사이버 안보 국제규범

## 1. 사이버공간총회와 유럽사이버범죄협약

2011년에 시작된 사이버공간총회(Conference on Cyberspace)는 사이버 안보의 직접적인 이해당사국의 정부 대표들이 나서 사이버 공간이라는 포괄적 의제를 명시적으로 내건 본격적인 논의의 장이 출현했다는 의미를 가진다. 유엔 GGE 활동이 '국가간'의 틀을 빌어서 '안보' 문제에 주안점을 둔 것과는 달리, 사이버공간총회는 각국 정부가 주도했지만 다양한 민간 행위자들도 참여하였고 안보이외의 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. 현재까지 네 차례에 걸쳐 회의를 진행하는 동안 참여자들도 늘어나고 논의도 활발하게 이루어지고 있지만, 공식적인 국제기구가 아닌 포럼 형식이라는 점, 뚜렷한 주관자가 없이 그때그때 주최국의 구성에 따라 회의가 진행된다는 점 등이 그 위상을 다소 모호하게 만든다는 비판도 없지 않다(배영자, 2017, pp.105-106).

제1차 사이버공간총회는 뮌헨안보회의에서 영국이 그 필요성을 제기한 이후 2011년 런던에서 개최되었다. 런던 회의에서는 '사이버 공간에서 수용할만한 행태를 위한 규범'을 주제로 하여 경제성장과 개발, 사회적 혜택, 사이버 범죄, 안전하고 신뢰할 수 있는 접속, 국제안보 등의 다섯 가지 세부 의제를 논의했다. 제2차 총회는 2012년에 헝가리의 부다페스트에서 열렸는데, 사이버 공간에서 자유, 국가 행위, 인터넷 거버넌스 등 다양한 논의를 펼쳤으나 이렇다 할 결론을 도출하지는 못하고 각국의 입장 차이만을 확인하는 수준에 그쳤다. 제3차 총회는 2013년 10월 서울에서 열렸는데, 총괄 어젠다로 '개방적이고 안전한 사이버 공간을 활용한 글로벌 번영: 기회, 위협, 협력'을 제시했으며, 유엔 GGE의 권고안을 확장한 '사이버 안보에 관한 서울 프레임워크'를 발표했으며, 역량강화 의제 신설이나 러시아나 중국의 참여 등과 같은 성과를 거두었다(김소정, 2016). 제4차 총회는 2015년 네덜란드의 헤이그에서 개최되었는데, 사이버 전문가 글로벌 포럼(Global Forum on Cyber Expertise,

GFCE)의 설립과 글로벌 정보보호센터 지원 사업 등이 제안되는 성과를 거두었다. 제5차 사이버공간총회는 2017년 인도에서 개최될 예정이다(배영자, 2017, pp.116-118).

사이버공간총회와 유사한 프레임을 지닌 선진국 정부간협의체인 OECD에서의 인터넷 거버넌스와 사이버 안보, 특히 개인정보보호 논의에도 주목해야 한다. 31개국을 회원국으로 하는 OECD는 1980년 사생활 및 개인정보의 국경 간 이동 보호에 관한 지침을 채택하는 등 정보사회의 새로운 문제들을 논의하기 시작했다. 1982년 4월 정보통신정책위원회를 설립하였고 통신 인프라 및 서비스정책 작업반, 정보경제작업반, 정보보호 작업반, 정보사회 지표작업반 등 산하 작업반을 중심으로 정보사회의 문제들을 다루어 왔다. 특히 정보보호 작업반은 사이버 공간의 안전과 보안, 개인정보 보호, 회원국의 사이버 안보 전략 등의 관련 이슈를 중점적으로 논의해 왔다. 최근에는 사이버 안보에 대한 국가별 전략비교 작업과 2002년 만들어진 정보보호 가이드라인에 대한 검토 작업이 진행하였다. 2015년에는 '경제적 사회적 번영을 위한 디지털 안보 위험의 관리'에 대한 OECD 권고안이 발표되었다(김상배, 2014, p.578).

사실 이렇게 서방 선진국들이 중심이 되어 사이버 공간의 범죄나 위협에 공동으로 대처하려는 사례의 역사는 좀 더 길다. 초창기 사이버 범죄에 대응해서 각국 정부들이 나서서 상호 간의 법제도를 조율하는 정부간 네트워크를 구성한 초기 사례로는 미국과 유럽평의회(Council of Europe)의 주도로 2001년 조인된, 유럽사이버범죄협약(European Convention on Cybercrime, COC), 즉 일명 부다페스트 협약이 있다. 부다페스트협약은 2001년 11월 23일 48개국의 서명으로 시작되었으며 2004년 7월 1일에 발효되었다. 2017년 5월 현재 유럽 국가들 이외에 미국, 캐나다, 일본 등을 포함한 59개국이 가입되어 있고 이중에서 55개국이 비준했으나, 러시아나 중국 등은 미온적 반응을 보이고 있으며, 한국은 아직 가입하지 않고 있다(Council of Europe, 2017).

부다페스트협약은 사이버 범죄와 관련된 종합적인 내용을 포괄하고 있으며, 법적으로 구속력을 갖는 최초의 국제협약으로서 범죄행위 규정, 절차법, 국제협력 등에 대한 내용을 담고 있다. 첫째, 범죄행위 규정과 관련하여, 4개 유형 컴퓨터 범죄인 사기와 위조, 아동포르노, 지적재산권 침해, 해킹과 자료절취 등에 대해 국내법으로 규정해 제재를 부과했다. 둘째, 절차법과 관련하여, 컴퓨터 범죄를 탐지·수사·기소하기 위한 국내절차를 마련하였는데, 절차적으로 어떤 사이버 범죄이든 이와 연루

된 개인들로부터 협력을 강제할 수 있는, 소송, 증거보존, 수색 및 압수 등과 관련된 권한을 협약국에 부여했다. 끝으로, 사이버 범죄 대응을 위해 각국 국내법의 조화 및 국제 수사공조 강화를 규정하였다. 여러 나라의 사이버 범죄 조목을 일관되게 함으로써 사이버 범죄와 관련하여 피해를 본 국가가 범죄자가 있는 국가에 이를 고발하면 해당 국가가 처벌할 수 있도록 하자는 취지인데, 상호사법공조협약, POC (Point of Contact) 공유 등의 내용을 담았다(장윤식, 2017).

부다페스트협약은 각국의 사이버 범죄에 대한 법제도 개혁을 유발하는 계기를 제공했다. 2006년을 기점으로 유럽평의회는 부다페스트협약을 내실화하기 위해 '사이버 범죄에 대한 글로벌 프로젝트'를 출범시켜 120여국에 사이버 범죄 관련법과 제도개혁을 권고하였다. 유엔 총회에서도 사이버 범죄 수사와 기소를 위한 법제도의 모범사례로서 부다페스트협약이 언급되기도 했다. 그러나 부다페스트협약은 가입조건이 까다로운데다가 서방 중심의 규범설정이라는 비판을 받고 있어, 전세계 59개국이 참여하고 있음에도 불구하고, 아직까지 보편적인 국제규범의 역할을 하고 있지는 못하다. 미국과 서구 국가들이 사이버 공간의 자유로운 정보 유통을 보호하기 위해서 사이버 범죄를 통제하자는 입장을 취하고 있는데 비해, 러시아나 중국 등이 미온적 반응을 보이고 있다. 게다가 부다페스트협약의 노력은 국가가 중심이 되다보니 민간 행위자들을 참여자로 끌어들이는 데 있어 한계가 있다는 지적도 제기된다(장윤식, 2017).

## 2. 상하이협력기구와 기타 지역협력기구

상하이협력기구(Shanghai Cooperation Organization, SCO)는 중국, 러시아, 우즈베키스탄, 카자흐스탄, 키르기스스탄, 타지키스탄 6개국 정상들이 2001년 7월에 설립한 지역협력기구이다. 사이버 안보의 국제규범 과정에서 상하이협력기구에 주목하는 이유는 미국과 유럽 국가들의 입장에 반론을 제기하는 러시아나 중국 등의 프레임을 대변하기 때문이다. 실제로 상하이협력기구는 2000년대 중반부터 사이버 안보를 위한 지역협력을 강조하고 있다. 2009년 6월에는 '국제정보보안강화 협력합의'를 체결했으며, 2011년 9월 12일에는 러시아, 중국, 타지키스탄, 우즈베키스탄 4개국의 유엔대표들이 유럽사이버범죄협약에 반대하면서 제66차 유엔총회에서 '국제정보보안행동규약(International Code of Conduct for Information Security)'

초안을 유엔총회에 제출하였다. 이 제안은 ICT를 국제평화나 안보에 대한 위협, 침해, 적대적 행위에 사용하는 것을 제한하기 위해 국가가 인터넷을 통제해야 한다는 주장을 담고 있다(정종필·조윤영. 2017, p.193).

이후 2011년 9월에는 52개 국가의 정보기관 지도부가 러시아 예카테린부르크에 모여서 개최한 '제2차 고위급 안보회의'에서도 러시아는 국제정보보안협정(Convention on International Information Security, CIIS)을 제안했다(조성렬, 2016, pp.389-90). CIIS는 인터넷에 대한 회원국의 주권을 보장하고 안정된 글로벌 사이버 안보 문화를 형성해야 한다고 강조하였다(방송통신위원회 외, 2012). 당시 러시아 외교부는 "우리가 먼저 선제적으로 대응하여 서방의 수중에서 주도권을 뺏어왔다. 전 세계는 우리가 제정한 규칙에 대하여 논의하게 될 것이고 영국은 대회(2011년 영국 런던에서 열린 사이버공간총회를 의미)의 의제를 바꿀 수밖에 없을 것"이라고 논평했다(『参考消息网』 2011.11.2). 이후 2015년 1월에는 카자흐스탄과 키르기스스탄이 추가로 참여해 6개국이 합의한 '국제정보보안행동규약' 개정안을 제69차 유엔총회에 제출했다. 또한 러시아는 2015년 브릭스(BRICS) 정상회의와 상하이협력기구 정상회의에서도 CIIS를 제출함으로써 사이버 안보 및 거버넌스를 포괄하는 형태의 새로운 국제법 창출을 지속적으로 주장하였다(배영자, 2017, pp.124-125).

이밖에도 CIS(Commonwealth of Independent States)와 CSTO(Collective Security Treaty Organization)와 같이 러시아가 주도하는 지역협력기구 차원에서 이루어지는 사이버 안보에 대한 논의에 주목할 필요가 있다. 1996년 2월 제7차 CIS 연합의회 전체회의에서는 기본형법을 채택하는 과정에서 컴퓨터 범죄에 대한 형사상의 책임을 적시하였고, 2001년 6월 컴퓨터 정보영역에서의 범죄에 대한 CIS 국가들 간의 협력협정을 벨라루스의 수도인 민스크에서 맺었다. 이를 통하여 러시아와 우크라이나, 벨라루스, 카자흐스탄 등 CIS 주요국들이 관련 법령을 통합하여 사이버 테러와 컴퓨터 관련 범죄에 힘을 모아 대응하는 새로운 체제를 구축하였다(신범식, 2017). CIS협정은 사이버 범죄 중심의 규범 형성을 논의하고 있는데, 이는 테러리즘과 사이버전 등을 포함하는 정보보안의 문제까지도 다루는 상하이협력기구 차원의 규범 형성과 대비된다. 한편, CSTO 국가들 간에는 정보보안 증진 체제의 구축을 위한 연합행동 프로그램이 실행되고 있다.

이상에서 언급한 프레임 이외에도 유럽과 아태 지역협력기구 차원에서 진행되는 사이버 안보 국제규범이나 사이버 범죄 관련 협약에도 주목할 필요가 있다. 먼저

OSCE(Organization for Security and Cooperation in Europe) 차원에서 진행되는 국제규범에 대한 논의이다. OSCE는 냉전기 동서간의 신뢰구축을 통해 유럽의 공동 안보와 협력을 추구한 경험을 살려 사이버 공간에서의 위협요소 감축과 신뢰구축에 활용하려는 노력을 진행 중이다. 2012년 4월 이래 비공식 워킹그룹을 설립하고 정보통신과 사이버 분야의 신뢰구축방안에 관하여 논의하였다. 2013년 12월에는 첫 번째 조치로 회원국 간에 사이버 안보 분야의 신뢰구축을 위한 기본 11개 원칙에 대한 합의안을 내기도 했다. 그러나 핵안보 분야의 군축과 사이버 안보는 본질적인 측면에서 다르기 때문에 일방적인 군축 개념을 사이버 안보 분야에 적용시키기 어렵다는 회의적인 시각도 존재한다(신성호, 2017, pp.165-166).

아태지역에서 ARF(ASEAN Regional Forum)는 역내 안정을 위해 1994년 출범한 다자간 정치·안보 협의체이다. 2012년 캄보디아에서 열린 제19회 ARF에서 각국의 외교부 장관들이 사이버 안보 증진을 위한 공동선언을 채택한 후, 각종 사이버 안보 현안에 대해서 논의했다. 한편 2013년 7월 브루나이에서 열린 제20회 ARF에서는 대테러 작전과 초국가 범죄와 관련해 사이버 안보 이슈가 핵심 의제로 논의되었다. 특히 정보공유와 능력 배양을 바탕으로 한 역내 정부간 협력강화의 중요성을 재확인했다. 2013년 9월에는 사이버 안보 강화 조치에 관한 제1차 ARF 신뢰구축조치 워크숍이 중국과 말레이시아의 주최로 베이징에서 열려서, 인터넷 발전을 위한 법제도와 문화적 다양성 존중의 필요성에 대해 논의하고 ARF 회원국 간 협력의 필요성을 강조하였다. 2014년 3월에는 제2차 ARF 신뢰구축조치 워크숍 개최되었는데, 컨택 포인트의 설정, 국내 사이버 조정체제와 기술적 능력의 하한선 규정, 향후 지속적인 신뢰구축의 노력 약속 등을 다루었다(정종필·조윤영, 2017, pp.195-196).

유럽이나 아시아 지역 이외의 기타 지역협력기구에서도 사이버 안보의 국제규범에 대한 논의가 진행되고 있음에 주목할 필요가 있다. 미주 지역에서 OAS(Organization of American States) 차원에서도 사이버 범죄와 기타 조직범죄를 다루는 공동의 틀을 만들기 위한 노력을 벌이고 있다. 중동 지역의 LAS(League of Arab States)에서도 사이버 범죄에 대한 규범 형성이 협의되어 LAS 협정을 체결했다. AU(African Union)도 아프리카의 맥락에서 AU 협정 초안을 마련하였는데, 사이버 범죄이외에도 사이버 안보 이슈 일반을 다루지만 국제협력과 관련된 내용은 부재하다. 그러나 이들 협약의 대부분은 범죄화, 절차권한, 전자증거, 관할, 국제공조, 서비스 제공자

의 책무 등과 같은 사이버 범죄 관련 규정에 초점을 맞추고 있어서, 상하이협력기구 등과 같이 러시아가 주도하는 지역협력기구가 서방 진영에 대한 대항의 차원에서 국제정보보안 문제에 대한 논의를 펼치는 것과 대비된다(김소정, 2016).

# Ⅴ. '글로벌 거버넌스' 프레임으로 본 사이버 안보 국제규범

## 1. 다중이해당사자주의 모델: ICANN

사이버 안보의 국제규범에 대한 논의를 제대로 이해하기 위해서는 사이버 안보 그 자체가 주요 관건으로 부상한 2010년대 이후의 규범 형성에 대한 논의보다 좀 더 장기적인 시각에서 문제를 보아야 한다. 사이버 안보 문제는 지난 수 년 동안 국가간 분쟁과 정부간 협력의 이슈로 부상하기 전에는 민간 행위자들이 나서서 글로벌 인터넷 거버넌스의 일부로서 다루던 문제였다. 사실 인터넷 거버넌스의 기본골격은 국제기구의 장에서 정부 대표들의 합의에 의해서 이루어진 것이 아니라 시민사회, 인터넷 전문가들과 민간사업자, 학계, 국제기구 전문가들이 자율적으로 구축한 메커니즘을 통해서 이루어졌다. 그러던 중 러시아의 문제제기로 2010년대 초반부터 국가간 포맷인 유엔 GGE에서 사이버 안보 문제를 논하고 사이버공간총회와 같은 정부간협의체가 본격적인 조명을 받게 되었던 것이다. 이러한 맥락에서 보면, 다양한 경로를 통해서 복합적으로 진행되고 있는 사이버 안보 분야의 글로벌 거버넌스 과정을 면밀히 살펴보는 것이 필요할 것이다.

미국을 중심으로 시작된 초기 인터넷 분야의 제도 형성 과정에는 자율적 거버넌스를 옹호하는 비국가 행위자들이 중요한 역할을 담당했다. 이러한 면모를 잘 보여주는 사례가, 초창기부터 인터넷을 관리해온 미국 소재 비영리 민간기관인 ICANN (Internet Corporation for Assigned Names and Numbers)이다. ICANN의 주요 업무로는 도메인이름체계(DNS), 루트서버 관리, 최상위도메인 생성 및 관리기관 위임, DNS루트서버, 도메인 및 IP주소 관련 정책개발 등이 있다. 여러모로 보아 ICANN은 개인, 전문가 그룹, 민간 기업, 시민사회 등이 다양하게 참여하는 글로벌 거버넌스의 실험대라고 할 수 있다. ICANN은 1998년에 미국 상무성 주도로 비영리

민간법인으로 설립되었지만, 2009년에 이르러 미 상무성과 인터넷주소관리체계에 자율성을 부여하는 AOC(Affirmation of Commitments)를 체결함으로써 다수의 이해관계자가 참여하는 글로벌 관리체제로 전환했었다(박윤정, 2016).

그러나 초창기부터 ICANN은 지나치게 미국을 중심으로 움직이고 있다는 비판을 받았으며, 따라서 이른바 ICANN 개혁 문제는 줄곧 논란거리가 되어 왔다. 예를 들어, 중국, 브라질, 이란, 사우디아라비아 등은 인터넷 거버넌스 분야에 새로운 국제기구가 필요하다는 주장을 펼쳤다. 이들 주장의 핵심은 미국 정부의 관리와 감독을 받을 수밖에 없는 기존 ICANN 체제의 개혁을 요구하는 데 있었다. 인터넷 발전의 초기에는 선발주자로서 미국의 영향력을 인정할 수밖에 없었지만 인터넷이 글로벌하게 확산되고 다양한 국가간 이해관계의 대립이 첨예해지면서 여태까지 용인되었던 관리방식의 정당성을 문제 삼을 수밖에 없게 되었다는 것이었다. 특히 이러한 움직임은 인터넷 초창기에는 상대적으로 뒤로 물러서 있던 전통적인 국가 행위자들이 인터넷 거버넌스의 전면으로 나서려는 문제의식과 밀접히 맞물렸다. 다시 말해, 인터넷 거버넌스의 진행 과정에 국가 행위자들이 영토적 주권을 좀 더 적극적으로 주창해야 된다는 것이었다(김상배, 2014, pp.567-577).

이렇게 논란이 벌어지던 와중에 에드워드 스노든의 폭로로 수세에 몰린 미국은 2014년 ICANN 감독 권한을 각국 정부와 아무런 관계가 없는 이해당사자들로 구성된 감시기구에 넘길 계획을 발표하기에 이르렀다. 미국 정부가 ICANN 대한 감독권한을 넘긴다고 하는 경우 가장 큰 쟁점은 IANA(Internet Assigned Numbers Authority) 관리권한의 이양 문제였는데 결국 2016년 10월에 미국 정부가 인터넷 주소에 대한 관리권한을 46년 만에 내려놓았다. IANA는 크게 보아 IP주소, 도메인네임, 프로토콜 파라미터 분야에 대한 관리기능을 의미하는데, IP주소나 프로토콜 파라미터 분야는 기술적이고 비정치적인 분야로 보아 권한이전에 관하여 큰 논란은 없으나, 도메인이름은 일반적인 이용자가 인터넷에 접속하는 수단이고 상표권, 표현의 자유 등의 법률적 이슈도 존재하기 때문에 각국 정부도 국가적인 이해관계를 가지고 접근하였다. 결국 미국은 이러한 IANA 관리권한을 민간에 이양하고 다중이해당사자 커뮤니티에서 그에 관한 논의를 하라고 주문했다(배영자, 2017, pp.126-127; 『경향비즈』 2014.3.15).

이러한 논의과정에서 흥미로운 것은 IANA 권한 이양에 관한 논의를 이른바 '다중이해당사자주의(multistakeholderism)'라는 개념 하에 다양한 이해당사자가 동등

한 참여하여 진행하라고 주문했다는 점이다. 이러한 메커니즘은 1국1표의 원칙 하에서 국가간 합의로 의사결정을 하는 유엔과 같은 국제기구의 경우와 사뭇 다르다. 이러한 방식은 조약과 같은 국가간 합의에 의하여 규범을 형성하는 것이 아니라 정부, 시민사회, 민간이 동등한 자격에서 지속적인 대화와 토론을 통하여 원칙, 규범, 의사결정 절차 등을 형성하는 것이다. 따라서 이러한 거버넌스 체계에서는 평소 인터넷 커뮤니티에 대한 관심과 기여가 중요하게 평가되고 커뮤니티의 의견형성 과정에 꾸준하고도 적극적인 참여가 필요하게 된다. 그런데 이러한 모델은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판을 받아왔다. 이러한 모델에 대해서 인터넷 초창기에는 상대적으로 뒤로 물러서 있던 국가 행위자들이 좀 더 적극적으로 나서 전통 국제기구의 틀을 활용해야만 한다는 '정부간주의(inter-governmentalism),' 좀 더 엄격하게 말하면 '기존 국제기구의 외연확대 모델'이 대두되었던 것이다.

## 2. '정부간주의' 모델: ITU/WSIS/IGF

ICANN의 대안을 모색하려는 움직임은 기존 국제기구들이 인터넷 거버넌스 분야에 진출하면서 새로운 국면을 맞았다. 특히 전통적으로 전기통신 분야의 국제기구로 활동해온 유엔 산하의 ITU가 민첩하게 움직였다. ITU는 1932년 유선전신에 대한 국제 협력을 도모하기 위해 설립되었으며, 기술이 발달하면서 영역이 유무선 전기통신뿐만 아니라 전파통신, 위성, 방송 분야 전반으로 확장되어 왔다. ITU가 인터넷 거버넌스 분야로 뛰어든 계기는 2003년에 제네바와 2005년에 튀니스에서 두 차례에 걸쳐서 열린 바 있는 WSIS(World Summit on Information Society)에서 마련되었다. WSIS의 준비과정과 본 회의에서는 다양한 이슈가 제기되었는데, 그 중에서도 향후 인터넷을 누가 어떻게 관리할 것이냐의 문제와 함께 미국의 영향력 아래 놓여 있는 ICANN의 개혁이 가장 큰 쟁점이었다. 주로 네트워크 보안의 신뢰성 강화, 프라이버시 및 고객보호, 범죄와 테러 목적의 사용 예방, 스팸대응 등이 다루어졌다. 그러나 WSIS는 ICANN의 개혁방안을 마련하는 데까지는 이르지 못하고 폐회되었는데, 그 대신 인터넷 관련 정책에 대한 지속적인 토론을 위한 장으로서 IGF(Internet Governance Forum)를 마련했다(김상배, 2014, pp.577-578).

IGF는 2005년 튀니지 WSIS 합의에 따라 2006년 설립된 유엔 산하 국제포럼이다. 미국 주도의 인터넷 주소관리에 불만을 가진 국가들을 위해 인터넷 전반의 공공정

책 이슈를 한시적으로 논의하기 위한 장으로 설립되었다. 정부, 민간, 시민단체, 국제기구 등 다양한 이해관계자들이 함께 모여 인터넷 현안에 대하여 논의하는 공개 포럼의 형태로 진행되었다. 2006년 그리스 제1차 IGF 이래, 매년 개최되었는데, 2016년 멕시코 과탈라하라 회의에 이르기까지 모두 11회가 개최되면서 인터넷 주소자원, 사이버 안보, 개도국 역량강화, 인터넷과 인권 등 인터넷 전반의 공공정책 이슈가 폭넓게 논의되고 있다. 그러나 워크숍 등이 동시다발적으로 진행되는 등 다루는 이슈가 다소 광범위하며, 포럼을 통해 도출되는 결과물의 구속력이 없다는 지적이 지속적으로 제기되었다.

한편, 사이버 공간과 관련한 ITU의 활동은 크게 인터넷 거버넌스와 사이버 안보 의제를 중심으로 전개되었다. 특히 2003년 ITU가 WSIS를 개최한 이래 사이버 공간의 안보와 관련된 ITU의 역할은 계속 확장되어 왔다. WSIS 개최 이전까지 ITU에서는 사이버 안보 의제가 사실상 거론되지 않았으며, 인터넷 주소자원인 도메인이름의 등록과 할당 및 기술발전 정책 및 표준에 논의가 집중되었다. 그러던 것이 2003년 제네바에서 WSIS를 개최하면서 ITU내 사이버 안보에 대한 논의가 본격화되기 시작되었다. WSIS 원칙선언에서 정보 네트워크 보안, 인증, 프라이버시 및 소비자 보호 등을 모두 포함하는 '신뢰할 수 있는 프레임워크의 강화'가 정보사회의 발전과 신뢰구축의 선결요건이라고 지적하고 특히 모든 이해당사자가 협력하는 사이버 안보 문화의 필요성과 국제협력을 촉구하였다.

2007년 ITU는 WSIS 이래 활동을 벌인 'ICT 이용에 있어서 신뢰와 안보 구축'의 촉진자로서 역할을 다짐하는 차원에서 GCA(Global Cybersecurity Agenda)를 제안했다. GCA는 법적조치, 기술 및 절차 조치, 조직적 구조, 역량개발, 국제협력 등 5대 과제를 기반으로 하는 국제 프레임워크로 정보사회의 안보와 신뢰 증진을 목적으로 했다. ITU는 GCA를 통해 각 회원국이 채택할 수 있는 법안 모델의 발전을 기대할 수 있을 것이라 전망했다. 국가 내 사이버 안보 침해사고대응팀(CERT)의 설치 및 운영 여부 등 조직 구조에 기반을 둔 '사이버 안보 준비 지수(Cybersecurity Readiness Index)' 제정 등이 제안되었다. 이후 ITU는 단순히 당면한 과제들을 나열하는 데 그치지 않고 관련 이해당사자들의 지지와 참여를 통해 사이버 안보와 신뢰를 구축하기 위한 전략과 해결책을 제시하는 역할을 적극적으로 수행해 왔으며, 고위전문가그룹을 설치하여 그 임무수행을 구체화하고 있다(배영자, 2017, p.120).

한편, 사이버 안보의 국제규범보다는 좀 더 포괄적인 의미에서 진행된 인터넷 거버넌스의 사례로서, 2012년 12월 WCIT(World Conference on International Telecommunication)에서 시도된 ITR(International Telecommunications Regulation)의 개정은 ITU의 프레임에서 벌어졌던 중요한 사건이었다. ITR은 전기통신 업무의 일반 원칙과 규정을 담고 있었는데, 그 내용이 너무 포괄적이고 모호해서 오랫동안 유명무실한 문서로만 남아 있었다. 게다가 ITR은 회원국들로 하여금 자신들의 사정에 맞추어 규제정책을 추진할 재량권을 너무 많이 부여하고 있었기 때문에 급변하는 기술환경을 따라잡기에는 미흡하다는 지적이 선진국들을 중심으로 제기되었다. 이러한 맥락에서 2012년 WCIT에서 ITR의 폐기를 주장하는 선진국들의 입장과 ITR의 개정과 강화를 주장하는 개도국들의 입장이 대립하는 양상이 나타났다. 이러한 과정에서 개도국들은 ITR을 통해 개별 국가 차원의 규제정책의 기조를 유지하려 했는데, 특히 인터넷에 대한 규제권한을 확보하려 했다. ITR의 규제조항이 급변하는 기술환경에 부합하지 않으므로 폐기해야 한다는 선진국들의 입장과 ITR의 개정과 강화를 통해 개별 국가 차원의 규제정책의 기조를 유지하려는 개도국들의 입장이 맞섰으나 일단 개도국의 입장이 관철되는 것으로 마무리되었다(김상배, 2014, pp.574-575).

## Ⅵ. 맺음말

이 글은 국가간, 정부간, 글로벌 거버넌스 등의 세 가지 프레임을 원용하여 현재 복합적인 양상으로 진행되고 있는 사이버 안보 분야의 국제규범 형성을 살펴보았다. 최근 주목을 받는 것은, 2013년 이후 근대 국제질서에서 잉태된 국가간 프레임으로 사이버 안보의 국제규범을 보려는 시도이다. 그러나 전통적인 국제법의 적용을 실험하는 탈린매뉴얼이나 유엔 GGE 활동에서 보는 바와 같은 전통 국제기구의 틀 안에만 초국적이고 탈영토적인 사이버 위협에 대응하는 적절한 해법을 찾기란 쉽지 않을 것이다. 이러한 점에서 사이버 공격으로부터 피해를 보는 당사국의 정부들이 나서서 해법을 찾아보려는 정부간 프레임의 시도들이 좀 더 현실성이 있어 보인다. 실제로 2010년대에 들어서 서방국들이 주도한 사이버공간총회나 유럽사이

버범죄협약과 같은 정부간협의체 모델, 그리고 비서방 국가들이 공을 들이고 있는 상하이협력기구와 같은 지역협력기구 모델이 사이버 안보 국제규범 논의의 전면으로 치고 들어온 바 있다. 그러나 좀 더 넓은 시각에서 본 글로벌 인터넷 거버넌스 분야의 규범 형성 노력도 간과해서는 안 된다. 글로벌 거버넌스의 프레임에서 본 ICANN 주도의 인터넷 거버넌스 체제의 변환과 ITU의 새로운 관할권 주장의 과정에서도 사이버 안보의 국제규범을 모색하기 위한 움직임들이 진행되고 있기 때문이다.

이러한 복합적인 국제규범 모색의 과정에서 각국은 자국에게 유리한 국제규범을 실현하기 위한 프레임 경쟁을 벌이고 있다. 이 글에서 파악한 사이버 안보 분야 프레임 경쟁의 양상은 세 가지 층위로 나누어 살펴본 각각의 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. 다시말해, 서방 진영이 정부간 프레임과 글로벌 거버넌스 프레임을 결합한 복합 아키텍처의 국제규범을 모색한다면, 비서방 진영의 시도는 근대 국제질서의 아키텍처를 기반으로 하는 국가간 프레임에 입각해 있다.

이 글에서 살펴본 사례들은 이러한 '프레임 내 경쟁'과 '프레임 간 경쟁'의 양상이 중층적으로 겹치면서 서로 치고받는 모습을 보여주었다. 예를 들어, 국가간 프레임 내에서 벌어지는 경쟁의 양상을 보면, 미국과 나토가 탈린매뉴얼을 내세워 국제법 프레임에 입각한 공세를 펼치는 데 대해서 러시아는 유엔 GGE에서의 사이버 안보 규범의 논의라는 국제기구 프레임을 관철시키기 위해 유럽 지역 밖으로 목소리를 높였으며 끝내는 미국으로 하여금 유엔이라는 전통 국제기구의 프레임을 수용케 하는 성과를 거두어냈다. 한편 유엔 GGE에서의 국가간 프레임을 활용한 안보 우선의 논의에 대해서 영국을 비롯한 서구 국가들은 사이버공간총회라는 좀 더 포괄적이고 다양한 이슈를 다루는 정부간 프레임으로 맞불을 놓았다. 다른 한편으로 서방 선진국들이 세운 사이버 범죄 분야의 '표준'이라고 할 수 있는 유럽사이버범죄협약의 확산에 대항하는 방책을 모색하는 과정에서, 러시아와 중국이 주도하는 상하이

협력기구의 행보가 박차를 가하게 된 측면이 없지 않다. 이러한 구도와 중첩되면서 사이버공간총회와 상하이협력기구 간에도 프레임 경쟁의 양상이 진행되었음을 무시할 수 없다.

이러한 프레임 경쟁의 면모가 가장 극명하면서도 복합적으로 나타나는 분야는 글로벌 인터넷 거버넌스의 영역이다. 미국이 초창기부터 주도한 ICANN체제 중심의 글로벌 거버넌스 프레임에 대해서 러시아와 중국, 개도국들은 ITU와 같은 전통 국제기구의 프레임을 원용해서 반론을 제기했다. 이러한 프레임 경쟁의 구도는 민간 사업자와 비영리기구의 주도권에 대한 국가세력과 국제기구의 도전일 수도 있으며, 인터넷 거버넌스의 사실상 메커니즘에 대한 법률상 메커니즘의 도전이기도 했다. 사실 이러한 대립은 크게 두 차례 걸쳐서 두드러지게 발생했는데, 그 하나는 2003-2005년 WSIS 추진과정에서 미국을 비롯한 서방 진영이 종전의 좁은 의미의 인터넷 거버넌스 프레임을 넘어서 사이버 안보나 정보격차 해소 등과 같은 포괄적 이슈를 포함한 국가간 프레임을 수용하는 과정에서 발생했다. 다른 하나는 2012년 ITU WCIT에서 서방 진영의 ITR개정 필요성에 대한 문제제기에 대항하여 개도국과 비서방 진영이 이견을 표출했던 사건에서 발견할 수 있었다.

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 국제연대 담론을 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.

요컨대, 사이버 안보의 국제규범 형성의 사례에서 볼 수 있는 세계 주요국들의 경쟁양상은 여태까지 알고 있던 근대 국제질서 내에서 자국의 이익을 모색하는 단순경쟁이 아니라, 미래의 국제규범을 자신들에게 유리한 방향으로 유도하기 위한 프레임 경쟁으로 나타나고 있다. 이러한 프레임 경쟁에 적응하기 위해서는 전통적

인 국가간 프레임에만 갇혀 있을 것이 아니라, 좀 더 복합적인 프레임에서 이 분야의 규범형성을 보는 노력이 필요하다. 특히 강대국들이 벌이는 프레임 경쟁이라는 구조변화에 대응하는 중견국의 입장에서는 이러한 프레임들이 누구의 이익을 대변하는지, 그리고 각 프레임이 궁극적으로 지향하는 질서상이 무엇인지를 제대로 파악하는 일 자체가 국가전략의 사안이라고 할 수 있기 때문이다. 이러한 프레임 경쟁에 대비하는 국가전략의 모색은 아직까지 국제적으로 합의된 국제규범이 형성되지 않은 사이버 안보 분야의 특성을 고려할 때 더욱 필요하다고 할 수 있다.

투고일 : 2017.05.31.
심사완료일 : 2017.06.21.
게재일 : 2017.08.30.

# 참고문헌

김상배. 2014.『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 한울.

김소정. 2016. “사이버 안보의 국제협력.” 사이버 안보와 세계정치 공부모임 세미나 발표문, 서울대학교 국제문제연구소. 8월 8일.

레이코프, 조지. 2007.『프레임 전쟁: 보수에 맞서는 진보의 성공전략』, 창비.

민병원. 2017. “군사전략론으로 보는 사이버 안보.”『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.26-64.

박노형. 2017. “사이버 안보의 국제법적 접근.” 사이버 안보와 세계정치 공부모임 세미나 발표문, 서울대학교 국제문제연구소. 1월 17일.

박노형·정명현. 2014. “사이버전의 국제법적 분석을 위한 기본개념의 연구: Tallinn Manual의 논의를 중심으로.”『국제법학회논총』 59(2), pp.65-93

박노형·정명현. 2016. “제4차 정보안보에 대한 유엔정부전문가그룹 논의 분석과 국제사이버법의 발전 전망.”『국가전략』 22(3), pp.173-198.

박윤정. 2016. “글로벌 인터넷 가버넌스와 사이버 안보: 한국의 시각과 역할.” 사이버 안보와 세계정치 공부모임 세미나 발표문, 서울대학교 국제문제연구소. 9월 5일.

방송통신위원회·행정안전부·지식경제부. 2012.『국가정보보호백서』, 국가보안기술연구소·한국인터넷진흥원.

배영자, 2017. “글로벌 거버넌스론으로 보는 사이버 안보.”『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.96-135.

손열 외. 2010. “신세계질서의 구축과 한국의 G20 전략.” EAI Special Report.

신맹호. 2016. “외교부 사이버안보 업무 현황.” 사이버 안보와 세계정치 공부모임 세미나 발표문, 서울대학교 국제문제연구소. 12월 16일.

신범식. 2017. “러시아의 사이버 안보 전략과 외교.” 김상배 편.『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.241-277.

신성호. 2017. “미국의 사이버 안보 전략과 외교.” 김상배 편.『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.138-176.

이상현. 2017. “국제규범으로 보는 사이버 안보.”『사이버 안보의 국가전략: 국제정치학의 시각』 사회평론, pp.65-95.

장규현·임종인, 2014. “국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고

안을 중심으로.”『정보통신방송정책』 26(5), pp. 21-52.

장노순. 2016. “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로.”『정치·정보연구』 19(1), pp. 1-28.

장윤식. 2017. “사이버 범죄와 국제공조.” 사이버 안보와 세계정치 공부모임 세미나 발표문, 서울대학교 국제문제연구소. 1월 9일.

전재성. 2011.『동아시아 국제정치: 역사에서 이론으로』동아시아연구원.

전재성. 2012. “동아시아의 복합네트워크 규범론과 한국 전략의 규범적 기초.” 하영선·김상배. 편. 2012.『복합세계정치론: 전략과 원리, 그리고 새로운 질서』한울. pp. 310-340

정종필·조윤영. 2017. “중국의 사이버 안보 전략과 외교.” 김상배 편.『사이버 안보의 국가전략: 국제정치학의 시각』사회평론, pp. 177-210.

조성렬. 2016.『전략공간의 국제정치: 핵·우주·사이버 군비경쟁과 국가안보』서강대학교출판부.

Bull, Hedley. 1977. *The Anarchical Society: A Study of Order in World Politics*. New York: Columbia University Press.

Choucri, Nazli, Stuart Madnick and Jeremy Ferwerd. 2014. “Institutions for Cyber Security: International Responses and Global Imperatives.” *Information Technology for Development,* 20(2), pp. 96-121.

Council of Europe, 2017. “Chart of Signatures and Ratifications of Treaty 185, Convention on Cybercrime, Status as of 28/05/2017.” http://www.coe.int/en/web/conventions/bi-or-multilateral-agreements (검색일: 2017년 5월 28일).

Forsyth Jr., James Wood and Maj Billy E. Pope. 2014. “Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace.” *Strategic Studies Quarterly,* Winter, pp. 113-130.

Gitlin, Todd. 1980. *The Whole World Is Watching: Mass Media in the Making and Unmaking of the New Left.* Berkeley: University of California Press.

Kerttunen, Mika and Saskia Kiisel. 2015. “Norms for International Peace and Security: The Normative Frameworks of International Cyber Cooperation.” *ICT4Peace Norms Project Draft Working Paper*. April. ICT for Peace Foundation.

Linklater, Andrew. 2005. “The Harm Principle and Global Ethics.” *Global Society,* 20(3), pp. 329-343.

Mazanec, Brian M. 2015. *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons.* Potomac Books.

Nye, Joseph S. 2014. "The Regime Complex for Managing Global Cyber Activities." CIGI Paper Series No. 1, May.

Rawls, John. 1999. *The Law of Peoples*. Cambridge, MA: Harvard University Press.

Rosenau, James N. and Ernst-Otto Czempiel. 1992. *Governance Without Government: Order and Change in World Politics,* Cambridge: Cambridge University Press.

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

Schmitt, Michael N. and Liis Vihul. 2014. "The Nature of International Law Cyber Norms." *Tallinn Papers*, No. 5.

Schmitt, Michael N. ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge, MA: Cambridge University Press.

Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge, MA: Cambridge University Press.

Slaughter, Anne-Marie. 2004. *A New World Order,* Princeton and Oxford: Princeton University Press.

Stevens, Tim. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy,* 33(1), pp. 148-170.