제1부

사이버 안보 국제규범의 형성

제1장

사이버 안보의 국제규범과 한국외교: 주요국 이해갈등의 프레임 경쟁 사이에서

김상배

I. 머리말

최근 사이버 안보가 국제정치학의 논제로 주목을 받고 있다. 사이버 안보는 그 성격상 일국 차원을 넘어서 이해해야 하는 초국적인 성격을 지닌 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 벌이고 있다.

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 활동 이외에도, 사이버공간총회, 유럽사이버범죄협약, 상하이협력기구, OSCE, ARF, ICANN, ITU 등에서 다양하게 국제규범이 모색되고 있다. 이렇게 복잡한 양상으로 전개되고 있는 규범경쟁을 이해하기 위해서 이 글은 미국의 미디어 학자 토드 기틀린(Todd Gitlin)이 개발하고 미국의 언어학자 조지 레이코프(George Lakoff)에 의해 널리 소개된 '프레임(frame)'의 개념을 원용하였다(Gitlin 1980; 레이코프 2007).

이들의 시각을 사이버 안보의 사례에 적용하면, 현재 국제규범의 형성 과정에 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 협력기구 모델을 원형으로 한다. 끝으로, '글로벌 거버넌스(global governance)' 프레임인데, 이는 국가 행위자 이외에도 민간 기업, 학계 전문가, 시민사회 활동가 등과 같은 다양한 비국가 행위자들이 참여하여 만드는 글로벌 거버넌스 모델을 원형으로 한다. 각기 상이한 미래의 글로벌 질서를 지향하는 이들 세 가지 프레임을 둘러싸고 세계 주요국들은 자신들의 이해관계를 반영할 프레임을 구현시키기 위해서 경쟁을 벌이고 있다.

이러한 프레임 경쟁의 양상을 정확히 파악하는 일은 한국과 같은 중견국에 있어 중요한 사안이 아닐 수 없다. 일차적으로는 아직까지 사이버 안보 분야에 어떠한 규범을 적용하여 제재할지에 대한 합의기반이 마련되지 않은 상황에서 국제규범 형성 과정에 적극적으로 참여하는 것 자체가 중요한 대응방안이 될 수 있다. 그러나 최근 사이버 안보 규범의 구체적 내용에 대한 주요국의 이해관계가 대립하는 상황에서 단순참여를 넘어서는 좀 더 구체적인 방안이 필요하다. 다시 말해, 서방 및 비서방 진영의 이해관계가 갈등을 빚고 있는 상황에서 한국의 선택지는 무엇이 될지에 대해 논의하고, 양자택일이 쉽지 않은 상황이라면 중견국의 시각에서 한국에 적합한 논리를 개발하고 전략적 입장을 선택하는 데까지 나아가야 할 것이다. 이를 통해서 국제규범의 보편성을 강조하면서도 중견국으로서 한국외교의 일관된 원칙과 기조를 투사할 수 있는 전략을 추구해야 할 것이다(김상배 2018).

사실 한국은 최근 진행되고 있는 사이버 안보 관련 국제규범의 논의 과정에 거의 모두 참여하고 있지만, 그 참여의 양상은 다소 파편적이고 분산적인 모습을 보이고 있다. 단순참여의 차원을 넘어서 규범외교의 모색을 위해서는 적어도 다음과 같은 세 가지 구조의 기저에 깔린 주요국 이해갈등의 프레임을 읽어내고, 그 속에서 한국이 차지하는 '구조적 위치'를 파악하는 것이 중요하다. 첫째, 미국, 중국, 일본, 러시아 등 한반도 주변 4국이 형성하는 지정학적 이해갈등의 구조이다. 둘째, 서방 진영과 비서방 진영의 경쟁 사이, 또는 선진국과 개도국 사이에서 형성되는 국제적 이해갈등의 구조이다. 끝으로, 다중이해당사자주의와 '국가간다자주의'의 관념이 경합하는 가운데 형성되는 글로벌 인터넷 거버넌스의 이해갈등 구조이다. 이러한 복합구조를 둘러싸고 펼쳐지는 주요국 이해갈등의 프레임 경쟁 사이에서 한국 나름의 전략적 프레임을 모색하는 것은 중요한 규범외교의 사안이 아닐 수 없다.

이러한 문제의식을 염두에 두고 이 글은 다음과 같이 네 가지 차원에서 논지를 전개하였다. 제2절은 국제법과 국제기구와 같은 '국가간' 프레임의 차원에서 본 사이버 안보 국제규범의 사례로서 탈린매뉴얼과 유엔 GGE 활동을 살펴보았다. 제3절은 정부간협의체와 지역협력기구와 같은 '정부간' 프레임의 차원에서 본 사이버 안보 국제규범의 사례로서 사이버공간총회와 유럽사이버범죄협약, 상하이협력기구와 세계인터넷대회, 그리고 기타 지역협력기구 등을 살펴보았다. 제4절은 글로벌 거버넌스의 프레임에서 본 사이버 안보 국제규범의 사례로서 ICANN의 다중이해당사자주의 모델과 ITU/WSIS/IGF의 '국가간다자주의' 모델을 살펴보았다. 제5절은 앞서 언급한 세 가지 차원의 사이버 안보 국제규범 프레임에서 현재 한국이 처한 한국의 '구조적 위치'와 전략적 과제들을 짚어 보았다. 끝으로 맺음말에서는 이 글의 주장을 종합·요약하고 한국의 사이버 안보 규범외교가 안고 있는 향

후 과제를 짚어 보았다.

II. 사이버 안보의 국제규범(1): 국제법과 국제기구

1. 기존 국제법 원용 시도: 탈린매뉴얼

전통적인 국제법(특히 전쟁법)의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격에 대응하려는 시도의 사례로는 탈린매뉴얼(Tallinn Manual)이 있다. 탈린매뉴얼은 2013년 3월 나토 CCDCOE(Cooperative Cyber Defence Centre of Excellence)의 총괄 하에 20여 명의 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 적용 가능한지 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 교전 수칙이 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(Schmitt 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: 33). 탈린매뉴얼은 구속력이 없는 지침서의 형식이지만, 전시 민간인과 포로에 대한 보호를 규정한 제네바협약처럼, 사이버전에도 국제법적인 교전 수칙을 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 사

이버 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 적용 문제는 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. '사이버전(Cyber Warfare)에 적용 가능한 국제법'을 논한 탈린매뉴얼 1.0과는 달리 탈린매뉴얼 2.0은 '사이버 작전(Cyber Operations)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 움직

임도 최근 많은 주목을 받으면서 빠르게 진행되고 있다. 특히 2013년 6월 제3차 유엔 군축 및 국제안보 위원회 산하 정보보안 관련 정부전문가그룹(GGE: Group of Governmental Experts)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: 35-38; 장노순 2016: 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. 요컨대, 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: 38-42; 이상현 2017: 79-82).

2015년 6월 제4차 GGE에서는 제3차 GGE 권고안을 계승하며, 좀 더 진전된 합의안을 도출하였다. 최종보고서는 사이버 공간의 국제규범에 관한 논의를 국제법 부문과 규범 부문으로 나누어 담았다. 국제법 부문에서는, 주권평등, 국제분쟁의 평화적 해결, 국제관계에서 무력사용의 자제, 인권과 기본적 자유의 존중 및 국내문제 불간섭 등과 같은 유엔헌장과 국제법의 기본원칙이 사이버 공간에도 적용됨을 확인했다. 또한 예시적인 견해로 관할권, 국제법 원칙, 자위권, 국제인도법(IHL: international humanitarian law), 대리자 및 국가책임에 관한 6개 항목을 제시했다. 그러나 이들 국제법 원칙의 선택에 대하여 서방 국가들과 비서방 국가들의 다툼이 커서 국제법이 어떻게 적용되는지에 대한 구체적 논의는 제대로 이루어지지 않았다. 한편 규범 부문에서는, 자발적이고 비구속적인 규범, 규칙 또는 원칙을 국가들이 고려하도록 국제협력, ICT사고, 제3국의 책임, 정보 교류 및 사법공조, 인권 존중, 핵심 기반시설의 보호, 공급망의 완전성 보장, 악의적 ICT 이용 확산 방지, ICT 취약성 보고, 긴급대응팀의 활동, 개도국 상황 고려에 대하여 권고사항 등을 제시하였다(박노형·정명현 2016: 173).

2016년 구성된 제5차 GGE에서는 제4차 보고서에서의 합의사항은 그대로 두고, 그 내용을 보다 구체화하고 추가사항을 검토하였다. 서방과 비서방 국가들 간에는 자위권, 국제인도법(IHL), 대응조치(counter-measure)의 허용, 사이버 테러·범죄와 인터넷 거버넌스의 의제 포함 여부 등과 같은 세 가지 쟁점에서 합의 도출에 어려움을 겪

었다. 한편 제5차 GGE에서는 서방 진영의 국가들 간에도 입장이 일치하지 않는 내용들이 다수 제기되었는데, 이른바 '적절한 성의(DD: Due Diligence)'의 성격 규정 문제, 사이버 기술 수출통제 및 비정부 행위자에 대한 공격적 사이버 무기의 사용금지 규범 제정, 데이터 관할권의 문제 등이 사례이다(신맹호 2016). 결국 2017년 6월 최종 4세션에서 두 의제 사이의 거래를 통해 타협점이 모색될 수 있을 것이라는 예측과는 달리, 양측의 의견이 지속적으로 대립하여 보고서 채택에 실패하였다. 최종회의에서 합의 도출에 실패한 핵심 의제는 국제법 적용 및 향후 계획이었는데, 특히 미국은 이미 2015년 보고서를 근거로 자국에 유리하게 국제법 해석을 할 수 있는 상황에서 중국과 러시아 등이 주장하는 개방형 워킹그룹 창설 및 유엔의 역할 확대를 수용할 의지가 없었으며, 중국과 러시아도 상세화된 국제법적 요소를 수용할 의지가 없는 상황이었다. 현재 2019년부터 제6차 GGE를 재개한다는 정도의 내용만 합의한 상태이다.

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 대해서 서방 측은 조심스럽게 접근했는데, 자발적이고 비구속적인 국제 관습법의 개발은 인정하지만, 조약 수준의 국제법을 제정하는 일은 어렵다는 것이 서방 측의 기본 입장이었다. 서방 측은 아직 창발 중인 이슈에 대해서 전 세계 190여 개 국가들이 무엇을 합의할 수 있겠느냐는 회의론을 제시하였다. 사실 제5차 회의

까지 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. 초국적이고 탈영토적인 성격을 지닌 사이버 공간에서의 일탈적 문제를 근대적인 영토적 관할권의 개념을 기반으로 하여 성립된 국제법(전쟁법)을 실증적으로 적용하는 것에 여러 가지 문제가 표출되고 있는 실정이 반영된 기대라고 할 수 있다(김소정 2016; 박노형 2017).

III. 사이버 안보의 국제규범(2): 정부간협의체와 지역협력기구

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 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 지향

했다. 현재까지 다섯 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: 105-106).

제1차 사이버공간총회는 뮌헨안보회의에서 영국이 그 필요성을 제기한 이후 2011년 런던에서 개최되었다. 런던 회의에서는 '사이버 공간에서 수용할 만한 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(GFCE: Global Forum on Cyber Expertise)의 설립과 글로벌 정보보호센터 지원 사업 등이 제안되는 성과를 거두었다(배영자 2017: 116-118). 제5차 사이버공간총회는 2017년 인도 뉴델리에서 개최되었다.

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 작업을 진행하였다. 2015년에는 '경제적 사회적 번영을 위한 디지털 안보 위험의 관리'에 대한 OECD 권고안이 발표되었다(김상배 2014: 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(COC: European Convention on Cybercrime), 즉 일명 부다페스트협약이 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 이 중에서 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 국내 절차를 마련하였는데, 절차적으로 어떤 사이버 범죄이든 이와 연루된 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 120여 국에 사이버 범죄 관련법과 제도개혁을 권고하였다. 유엔총회에서도 사이버 범죄 수사와 기소를 위한 법제도의 모범사례로서 부다페스트협약이 언급되기도 했다. 그러나 부다페스트협약은 가입조건이 까다로운데다가 서방 중심의 규범설정이라는 비판을 받고 있어, 전 세계 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 있는 데 비해, 러시아나 중국 등이 미온적 반응을 보이고 있다. 게다가 부다페스트협약의 노력은 국가가 중심이 되다보니 민간 행위자들을 참여자로 끌어들이는 데 있어 한계가 있다

는 지적도 제기된다(장윤식 2017).

2. 상하이협력기구와 세계인터넷대회

상하이협력기구(SCO: Shanghai Cooperation Organization)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 러시아 예카테린부르크에서 열린 상하이협력기구 정상회담에서 '국제정보보안강화 협력에 대한 협정(일명 예카테린부르크협정)'을 체결했는데, 사이버 공간의 주요 위협에 대한 정의, 국가이익과 관련된 ICT의 사용, 사이버 안보에 관한 포괄적 지역협정의 청사진 제시 등의 내용을 담고 있다(조성렬 2016: 389-90; 방송통신위원회 외 2012).

2011년 9월에는 러시아, 중국, 타지키스탄, 우즈베키스탄 4개국의 유엔 대표들이 유럽사이버범죄협약에 반대하면서 제66차 유엔총회에서 '국제정보보안행동규약(International Code of Conduct for Information Security)' 초안을 유엔총회에 제출하였다. 이 제안은 예카테린부르크 협정에서 제기된 주장을 계승했는데, ICT를 국제평화나 안보에 대한 위협, 침해, 적대적 행위에 사용하는 것을 제한하기 위해 국가가 인터넷을 통제해야 한다는 주장을 담고 있다. 사이버 안보의 주된 위협을 사이버 무기 개발 및 사용을 통한 정보전 준비와 실행으로 규정했다. 다른 국가들의 정치·경제 체제, 사회·문화 환경을 불안정하게 만드는 행위를 위협으로 간주하고 이를 막기 위해 노력해야 한다고 주장했다(정종필·조윤영 2017: 193).

이후 2015년 1월에는 카자흐스탄과 키르기스스탄이 추가로 참여해 6개국이 합의한 '국제정보보안행동규약' 개정안을 제69차 유엔총회에 제출했다. 이는 2011년에 유엔총회에 제출한 행동규약을 수정·보완한 것으로 사이버 공간에서의 국가의 역할 강화를 강조했으며, 사이버 공간에 대한 국가주권의 적용범위를 확장하여 검열 및 정보차단의 여지를 남기고 인권 제한의 가능성을 명시했다. 국제법 적용 문제와 관련하여 이 안은 2013년 제3차 GGE 최종보고서에서 합의된 기존 국제법, 특히 유엔헌장의 적용이라는 문구를 생략한 채, 기존 국제법과 관련된 규범만을 언급함으로써 기존 국제법의 직접 적용보다는 새로운 국제법의 채택을 염두에 두고 있는 속내를 드러내기도 했다. 러시아는 2015년 브릭스(BRICS) 정상회의와 상하이협력기구 정상회의에서도 이러한 행동규약을 제출함으로써 사이버 안보 및 거버넌스를 포괄하는 형태의 새로운 국제법 창출을 지속적으로 주장하였다(배영자 2017: 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. 이 중에서 특히 CIS의 경우, 러시아 정부는 사이버 테러 및 컴퓨터 범죄와 관련하여 CIS 구성원들과 협력하여 관련법의 정비를 진행하였는데, 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 통

하여 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.

한편 이러한 국가주권의 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 바탕에 깔고 있었다. 특히 2013년 스노든 사건 이후 중국은 글로벌 인터넷 거버넌스를 주도하는 미국을 견제하며, 중국이 중심이 되는 사이버 진영 건설을 목표로 국제협력을 강화하고 있다. 서방 진영이 주도하고 있는 현행 체제 하에서는 중국이 독자적인 국제규범을 제시하는 데 한계가 있다는 판단을 바탕으로 한 행보였다. 개별 국가의 정치·사회의 다양성이 인정되고 국가주권이 보장되는 사이버 환경을 구축해야 한다는 것이 주된 논리였다. 시진핑 중국 국가주석은 축사에서 "중국은 세계 각국과 손잡고 노력하여 상호존중, 상호신임의 원칙 아래 국제협력을 심화시키고, 사이버 주권을 존중하며 사이버 안보를 보장받는, 공동으로 평화, 안전, 개방, 협력적인 사이버 공간을 건설해야 한다"고 주장했다.

세계인터넷대회는 규모와 행사 면에서 확대되고 있으며 사이버 안보, 공유경제, 인터넷플러스, 사물인터넷, 가상현실, 빅데이터, 인공지능, P2P, 5G 기술 등 다양한 사이버 공간과 관련된 이슈 및 최신 기술 발전을 다루어 이목을 끌고 있다. 세계인터넷대회는 2018년 11월까지 총 5회 개최되었는데, 정부관계자, 국제단체인, 기업, 민간단체인, 인터넷 엘리트 등이 참석하는 것으로 알려져 있으며, 디지털 경제, 첨단기술, 인터넷과 사회, 웹 공간 거버넌스, 교류 협력 등을 주제로 하여 사이버 주권 존중, 사이버 공간의 평화안전 유지, 사이버 공간의 개방협력 촉진, 사이버 공간 내 질서구축, 인터넷 거버넌스 체계 구축에 대한 토론의 장을 마련하는 것을 목적으로 한다. 이러한 기조는 2017년 초 발표된 『사이버 공간국제협력전략(网络空间国际合作战略)』으로 이어졌다(国家互联网信息办公室 2017).

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 Co-operation in Europe) 차원에서도 사이버 안보 국제규범에 대한 논의가 진행되고 있다. 최근 아세안(ASEAN) 국가들도 제기하고 있는 사이버 안보 협력과 규범에 대한 논의를 벌이고 있으며, 아태지역 국가들이 역내 안정을 추구하기 위해 1994년 출범시킨 다자간 정치·안보 협의체인 ARF(ASEAN Regional Forum) 차원에서 진행되는 사이버 협력에도 주목할 필요가 있다. 이외에 미주 지역은 OAS(Organization of American States)가 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 범죄 이외에도 사이버 안보 이슈 일반을 다루지만 국제협력과 관련된 내용은 부재하다(김소정 2016).

IV. 사이버 안보의 국제규범(3): 글로벌 거버넌스

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 수년 동안 국가 간 분쟁과 정부 간 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 국가 간 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, 민간기업, 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 국가 간 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: 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 감독 권한을 넘긴다고 하는 경우 가장 큰 쟁점은 IANA(Internet Assigned Numbers Authority) 관리권

한의 이양 문제였는데 결국 2016년 10월에 미국 정부가 인터넷 주소에 대한 관리 권한을 46년 만에 내려놓았다. IANA는 크게 보아 IP주소, 도메인네임, 프로토콜 파라미터 분야에 대한 관리 기능을 의미하는데, IP주소나 프로토콜 파라미터 분야는 기술적이고 비정치적인 분야로 보아 권한 이전에 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 관리 권한을 민간에 이양하고 다중이해당사자 커뮤니티에서 그에 관한 논의를 하라고 주문했다(배영자 2017: 126-127).

이러한 논의 과정에서 흥미로운 것은 IANA 권한 이양에 관한 논의를 이른바 다중이해당사자주의(multistakeholderism)라는 개념 하에 다양한 이해당사자가 동등하게 참여하여 진행하라고 주문했다는 점이다. 이러한 메커니즘은 1국1표의 원칙 하에서 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 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 국가간다자주의(multilateralism), 좀 더 엄격하게 말하면 '기존 국제기구의 외연확대 모델'이 대두되었던 것이다(DeNardis 2013).

2. 국가간다자주의 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 준비 과정과 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: 577-578).

IGF는 2005년 튀니지 WSIS 합의에 따라 2006년 설립된 유엔 산하 국제포럼이다. 미국 주도의 인터넷 주소 관리에 불만을 가진 국가들을 위해 인터넷 전반의 공공정책 이슈를 한시적으로 논의하기 위한 장으로 설립되었다. 정부, 민간, 시민단체, 국제기구 등 다양한 이해관

계자들이 함께 모여 인터넷 현안에 대하여 논의하는 공개 포럼의 형태로 진행되었다. 2006년 그리스 제1차 IGF 이래, 매년 개최되었는데, 2016년 멕시코 과달라하라 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 ITU 내 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 법적 조치, 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, 고위전문가그룹(High-Level Experts Group, HLEG)을 설치하여 그 임무 수행을 구체화하고 있다(배영자 2017: 120). 한편 GCA와 HLEG 등과 더불어 IMPACT(International Multilateral Partnership Against Cyber Threat)의 활동도 진행되고 있다.

한편, 사이버 안보의 국제규범보다는 좀 더 포괄적인 의미에서 진행된 인터넷 거버넌스의 사례로서, 2012년 12월 WCIT(World Conference on International Telecommunication)에서 시도된 ITRs(International Telecommunication Regulations)의 개정은 ITU의 프레임에서 벌어졌던 중요한 사건이었다. ITRs은 전기통신 업무의 일반 원칙과 규정을 담고 있었는데, 그 내용이 너무 포괄적이고 모호해서 오랫동안 유명무실한 문서로만 남아 있었다. 게다가 ITRs은 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 ITRs의 폐기를 주장하는 선진국들의 입장과 ITRs의 개정과 강화를 주장하는 개도국들의 입장이 대립하는 양상이 나타났다. 이러한 과정에서 개도국들은 ITRs을 통해 개별 국가 차원의 규제정책의 기조를 유지하려 했는데, 특히 인터넷에 대한 규제권한을

확보하려 했다. ITRs의 규제조항이 급변하는 기술환경에 부합하지 않으므로 폐기해야 한다는 선진국들의 입장과 ITRs의 개정과 강화를 통해 개별 국가 차원의 규제정책의 기조를 유지하려는 개도국들의 입장이 맞섰으나 일단 개도국의 입장이 관철되는 것으로 마무리되었다(김상배 2014: 574-575).

V. 한국의 사이버 안보 규범외교

1. 탈린매뉴얼과 유엔 GGE 활동

최근 사이버 공격이 국가 간 분쟁의 주요 사안으로 부상하면서 전통적인 전쟁법에 의존하여 이러한 행위를 규제할 것인지, 아니면 새로운 국제법을 만들 것인지의 문제가 관건이 되었다. 그 중에서 나토의 CCDCOE의 총괄 하에 발표된 사이버전 교전 수칙인 탈린매뉴얼은 기존의 국제법 체계를 적용하여 새로운 사이버 안보 문제를 다루려는 대표적인 사례이다. 그러나 2007년 에스토니아 사태 이후 미국과 유럽 국가들이 중심이 되고, 게다가 NATO 회원국의 전문가들이 참여하여 러시아의 사이버 위협에 대응하는 성격을 띰으로써 탈린매뉴얼의 시도는 러시아나 중국 등과 같은 구 사회주의권 국가들의 외면을 받고 있다. 러시아는 말할 것도 없거니와 중국도 탈린매뉴얼은 국제법적으로나 정치군사적으로나 미국의 속내가 너무 많이 반영된 가이드라인이라고 비판하면서, 기존에 발표된 미국의 사이버 안보 관련 군사문서나 전략서와 다를 바가 없다는 불만을 토로했다.

이러한 탈린매뉴얼의 시도가 앞으로 국제사회에서 얼마나 넓은

공감대를 확보할지는 알 수 없는 상황에서, 한국은 전략적 이해관계를 고려하여 적절한 자리매김을 해나가는 노력이 요구된다. 예를 들어 한국은 미국과 유럽 중심의 탈린매뉴얼 체제에 동참할 것인지, 아니면 새로운 국제레짐이나 관련 국제규범을 창출하는 노력에 더 집중할 것인지에 대한 국가전략적 입장을 설정할 필요가 있다. 미국이나 유럽이 기존 국제법을 원용하는 담론에서 앞서고 있기는 하지만, 러시아와 중국, 개도국들을 중심으로 새로운 법체계의 도입을 주장하는 도전도 만만찮은 상황이라는 점을 알아야 한다. 그런데 현재까지 한국은 탈린매뉴얼을 둘러싼 담론 형성 과정을 소극적으로 관망하는 자세를 취해왔는데, 향후 탈린매뉴얼의 시도가 동아시아 또는 아태 지역에서도 적용가능한지의 여부에 대한 검토 등을 포함한 적극적 대응이 필요하다. 그러나 "현재 여타 포괄적인 사이버 안보 규범 형성 노력이 부재한 상태에서 탈린매뉴얼은 사이버 공간의 교전과 관련된 일정정도 준거점으로 활용될 가능성이 크다"(Noor 2015: 156).

기존의 전쟁법을 사이버 안보 분야에 적용하려는 시도인 탈린매뉴얼에 대한 국제적 합의가 쉽게 이뤄지지 않는 것처럼, 전통적인 국제기구인 유엔의 정부전문가그룹(GGE)에서 국제법의 적용 여부를 검토하는 시도도 난항을 겪기는 마찬가지였다. 유엔 GGE는 그동안 2004년, 2009년, 2012년, 2014년, 2016년 등 5차례에 걸쳐서 구성되었다. 2016-17년에 진행된 제5차 GGE회의에까지 이르면서 국내적, 지역·국제적 차원의 신뢰구축조치 이행방안 제시, 역량강화를 위한 협력적 조치의 개발, 기존 GGE에서 권고된 자발적 규범·규칙·원칙의 구체적 적용방법에 대한 권고 등의 사안과 관련해서는 나름대로의 진전을 이루었지만, 기존 국제법을 사이버 공간에 적용하는 문제와 향후 사이버 안보 관련 논의의 발전을 위해 개방형 워킹그룹을 구성하는

문제에 대한 이견으로 인하여 최종합의에 실패하였다.

한국은 우주분과로 가느라고 불참했던 2012-13년의 제3차 GGE 회의를 제외하고 나머지 4차례의 GGE회의에 모두 참여했다. 유엔 GGE에서 한국의 입장은 기본적으로 사이버 공간은 피해국이 일방적으로 불리한 구조이므로, 피해국에 유리한 방향으로 국제법의 해석 및 규범의 창출이 필요하다고 강조하였다. 이러한 주장의 이면에 존재하는 한국의 주 관심사는 북한의 사이버 공격을 막고, 북한의 공격이 경유국으로 거치는 국가, 특히 중국의 협조를 확보하는 데 있었다. 따라서 한국은 북한발 사이버 공격의 주요 피해국으로서 국제법 적용에 있어 피해국의 권리를 보장하기 위한 국제법의 상세화가 필요하다는 기본 입장을 취했다. 이밖에 유엔 GGE에서 거론되는 글로벌 이슈와 관련해서 한국은 대체로 서방 측의 주장을 지지하였는데, 적절한 범위에서 서방 측과 같은 입장을 유지하는 것이 국익에 부합한다는 판단이었다. 예를 들어, 한국은 자위권, 국제인도법, 대응조치의 필요성과 관련하여 서방 측과 입장을 같이했다.

'적절한 성의(DD)'가 국제법으로 성립되었는지의 여부와 관련하여 한국은 일부 서방 국가들(일본, 핀란드, 네덜란드, 스위스, 에스토니아 등)과 공조를 펼쳤다. 그러나 DD에 대해서 강대국들은 모두 반대하였다. 특히 중국이 반대했는데, 북한의 사이버 공격이 중국을 경유할 경우 이를 방지할 부담이 있기 때문인 것으로 판단된다. 전반적으로 강대국들의 입장은 DD는 국제법이 아니라 비구속적(non-binding) 규범이라는 것이었다. 한편 한국은 사이버 테러가 중대한 국제안보 이슈로 여러 계기에 논의되고 있다는 점을 '유의'한다는 문안을 제안하여 중국의 입장을 일부 인정했다. 이밖에 한국이 추가로 제안한 내용으로는 자국 영토가 특정국에 대한 사이버 공격에 활용된 경우, 피해국이 통보하는 시점부터 피해국에 협조해야 할 의무가 발생하는 것으로 보자고 제안하기도 했으며, 경유 국가들은 피해국이 협조 요청 시 '지체 없이' 반응을 보여줄 의무를 지자고 했다(신맹호 2016).

한편 한국은 상대적으로 진영 간 이견이 적은 내용을 제안하여 보고서의 상세화에 기여했다. 제5차 GGE회의 4세션에서 한국은 국가를 대신하거나 국가 목적의 달성을 위한 악성 ICT 활동에 있어 프록시 서버의 사용을 제한할 필요성을 제기했으며, 사이버 범죄의 심각성을 지적하고 이에 대한 대응의 필요성을 지적했다. 또한 ICT 침해사고 시 국가 간 협조를 위한 통지 템플릿을 마련할 필요성과 사이버 공격에 활용된 경유국의 상당주의 의무, 주요 기반시설에 대한 공격 발생 시 피해국에 대한 협조 규정의 상세화, 사이버 공간의 규범을 준수하겠다는 국가 간 선언을 통한 안전한 사이버 공간 구축 필요성 등을 강조하였다. 5차 GGE회의에서는 비록 최종보고서의 채택이 무산되었으나, 진영간 이견 대립에도 불구하고 한국이 제안한 사항들이 양 진영의 지지를 모두 확보하여 최종 초안에 충실히 반영되기도 하였다.

2. 사이버공간총회와 유럽사이버범죄협약

사이버공간총회는 사이버 공간이라는 포괄적 의제를 명시적으로 내건 본격적인 논의의 장이며, 사이버 안보에 구체적으로 이해관계가 걸린 당사국들을 중심으로 구성되었다는 의미가 있다. 한국은 2013년 10월 서울에서 제3차 총회를 개최하여 유엔 GGE의 권고안을 확장한 '사이버 안보에 관한 서울 프레임워크' 발표하였으며 역량강화 의제를 신설하는 등의 성과를 거두었다. 사이버공간총회가 서방 국가들의 주도 하에 이루어져서 러시아나 중국과 같은 비서방 국가들의 호응을 얻어내

는 것이 큰 과제로 남아 있었는데, 서울 총회에서는 러시아와 중국이 모두 참여하는 성과를 거두었다. 2013년 6월에 마무리된 제3차 유엔 GGE회의에 뒤이어 개최된 회의라는 시기상의 이점도 있었지만 참가국의 저변을 넓히려는 한국의 노력도 주효했던 것으로 평가된다. 여하튼 한국의 입장에서 볼 때, 서울이 런던과 부다페스트 등의 유럽 국가들의 수도에 이어 세 번째로 사이버공간총회를 유치하여 성공적으로 개최했다는 사실은 사이버 외교의 의미 있는 성과라고 할 수 있다.

한국은 이후 2015년 헤이그에서 열린 제4차 사이버공간총회에서도 글로벌 정보보호센터 사업 등에 적극 참여하는 등 활발한 활동을 보였다. 당시 한국은 외교부 장관이 참석하여 네트워크 연계성이 초래한 사이버 위협에 대한 취약성은 모든 국가, 기업, 개인이 직면한 공통의 과제가 되고 있다면서 국가 간 협력의 필요성을 강조했다. 특히 사이버 공간이 기회와 잠재력의 원천이자 혁신과 성장의 동력이 되고 있는 반면 사이버 공격도 다양화, 빈번화되고 있음을 상기시키며, 전세계적으로 인터넷 연계성이 가장 높은 사회이자 분단 상황에 처해 있는 한국은 특히 이러한 위협의 심각성을 절실히 인식하고 있다고 소개했다. 한수원 및 소니 영화사 해킹 사건은 이러한 사이버 위협의 대표적 사례로서 거론됐는데, 특히 한수원 해킹사건과 같이 핵심 기반시설을 대상으로 한 사이버 공격에 대해서는 관련 국가들이 공격세력을 규명하기 위한 수사공조와 정보공유에 적극 협조해야 함을 제기했다.

당시 한국은 사이버 공간을 규율할 국제규범이 부재한 상황에서 국가 간 사이버 신뢰구축조치(CBMs: Confidence-Building Measures)를 통해 불신과 오인으로 인한 국가 간 긴장 가능성을 줄이고 상호 협력의 기반을 만드는 것이 중요함을 강조했다. 아울러, 개발도상국의 사이버 안보 취약성이 전체 사이버 생태계의 안전성을 위협하고 있음을 감안하여, 개도국의 역량강화를 위한 국제협력이 중요함을 강조하고, 한국이 2015년 중 설립 예정인 글로벌정보보호센터(GCCD: Global Cybersecurity Center for Development)를 통해 개도국의 사이버 안보 역량강화를 지원할 계획임을 소개했다. 한국은 2013년 서울 사이버공간총회에서 의장국으로서 총회 프로세스에 역량강화를 주요의제로 삽입하였는데, 2015년 사이버공간총회에서 출범한 글로벌 사이버 전문역량 포럼(GFCE: Global Forum on Cyber Expertise)은 이러한 의제에 기반을 제공한 국제적 이니셔티브의 좋은 사례라 할 수 있다.

2017년 5월 현재 유럽사이버범죄협약, 즉 부다페스트협약에는 59개국이 가입되어 있고 이 중에서 55개국이 비준했다. 그런데 한국은 아직 가입하지 않고 있다. 따라서 정보공유 등 여러 가지 면에서 제약을 받고 있다. 미가입의 가장 큰 원인은 사이버 범죄의 감청 문제, ISP의 정보 보존의무 등이 국내의 기존 법제와 충돌하기 때문인 것으로 알려져 있다. 특히 감청 문제가 관건인데, 사이버 범죄를 예방하기 위해서 감청을 허용할 것이냐 또는 해킹이 감청을 허용할 정도로 중범죄이냐의 문제에 대해 이견이 존재한다. 다시 말해, 사이버 위협에 대응하기 위한 정보의 자유로운 접근 문제와 어떠한 경우에도 감청은 안 된다는 입장이 대립하고 있다. 또한 보존의무 제도도 관건이다. 외국에서는 사이버 범죄에 사용된 로그정보 등의 보존유지가 허용되지만, 국내에서는 권고사항일 뿐 현행법상으로는 허용되지 않기 때문에 절차법적인 차원에서 수사에 필요한 유용한 수단의 활용이 제약받고 있다(장윤식 2017).

최근 국내에서도 유럽사이버범죄협약에의 가입을 주장하는 목소리가 높아지는 가운데, 최근 외교부를 중심으로 법무부, 경찰청 등이 가입 여부를 검토 중이다. 그러나 이는 여러 가지 기존 법제도 정비의

문제 및 〈국가사이버 안보법〉 제정 문제 등과 연관되어 있다. 2012년 8월 관계부처 협의 시 유럽사이버범죄협약 가입 문제를 논의하였으나 부처 간 이견이 노정되었다. 유럽평의회와 미 법무부 등은 다양한 창구를 통해서 한국의 가입을 요청하고 있다(신맹호 2016). 2016년 6월 제4차 한미 사이버 정책협의회에서 미 법무부 측은 협약 가입 및 이행 관련 미국 전문가를 한국에 파견해 관계부처 대상 설명회를 갖는 방안을 제안하기도 했다. 외교부 차원에서도 유럽사이버범죄협약의 이행성과 등에 대한 평가를 바탕으로, 협약 가입 필요성을 협의하고 있다. 최근 한국의 가입을 가로막았던 통신비밀보호법이 위헌확인을 받아 새로운 전기를 맞게 될 것으로 보인다.

한편 대검찰청 과학수사부는 임시 옵서버 자격으로 2016년 11월 스트라스부르/바르샤바에서 개최된, 유럽사이버범죄협약위원회(T-CY: The Cybercrime Convention Committee)에 참석했다. T-CY는 유럽사이버범죄협약의 효과적 활용과 이행 촉진을 목적으로 운영되는 가입국 참석 위원회로, 옵서버 참석 시 협약에 대한 이해를 제고하고 국내 사이버 범죄와 관련하여 협약을 이행하기 위한 입법안을 마련하는 데 실질적 도움을 얻을 것으로 기대되었다. 2017년 11월에는 스트라스부르에서 열린 사이버범죄협약총회에 외교부, 대검찰청, 경찰청, 과기정통부 담당자들이 참석하였다. 사이버 안보 문제에 대한 입장이 유사한 국가들로 구성된 사이버범죄협약총회는 유엔 GGE 등에 비해 국가 간 논의 과정이 순조롭고 합의 수준도 높은 것으로 평가된다. 이미 상당수 국가에서 사이버범죄협약과 연계하여 사이버 범죄 관련 역량강화 프로그램을 진행하고 있으며, 또한 온라인 상의 외국인 혐오와 사이버 범죄 증거 관련 보전 조치 등의 개선방안에 대한 다양한 논의가 사이버범죄협약 가입국 간에 진행 중이다.

3. ICANN과 ITU/WSIS/IGF

현재 한국은 ICANN의 3개 지원기구 중에서 ccNSO(Country Code Names Supporting Organization)와 ASO(Address Supporting Organization)의 논의에 한국인터넷진흥원(KISA)이 참여하고 있으나, GNSO(Generic Names Supporting Organization)에는 참여하지 않고 있다. ICANN의 4개 자문위원회 중에서는 GAC(Government Advisory Committee, KISA가 참여)과 ALAC(At-Large Advisory Committee, ISOC Korea, OSIA 참여)에는 참여하나, SSAC(Security & Stability Advisory Committee)와 RSSAC(Root Server System Advisory Committee)에는 참여하지 않고 있다. 한편, 2014년 1월 KISA 내에 ICANN 서울사무소 개소 이후, 인터넷 거버넌스 교육 프로그램을 개설하고, ICANN의 주요 정책문서에 대한 한글번역 서비스를 제공하고 있으며, ICANN 공인 도메인 등록대행자 대상의 고객서비스를 제공할 뿐만 아니라 관련 정보교환의 장을 마련하는 사업을 벌이고 있다. 또한 2016-17년에는 아태지역 역량강화를 위한 '인터넷 거버넌스 아카데미'를 공동으로 추진하고 있다.

이러한 한국의 ICANN 활동과 관련하여 주목할 것은, 주로 과기정통부와 그 산하기관인 KISA를 중심으로 참여하고 있는데, 이러한 정부 중심의 참여가 다소 소극적 참여와 관망적 자세로 나타나고 있다는 점이다. 이는 다중이해당사자주의를 내세우며 주로 민간전문가들이 ICANN 활동에 참여하는 서방 국가들의 경우와 대비된다. 역으로 뒤집어 보면, 과연 다중이해당사자주의 모델 자체가 한국의 실정에 적합한지에 대한 검토가 필요한 것은 사실이다. 관념으로서의 다중이해

당사자주의와 이를 실천할 사회경제적 기반으로 나누어 보았을 때, 관념으로서 다중이해당사자주의는 인터넷 초창기부터 모색되어 왔던 이상과 일맥상통하는 것으로서 한국의 입장에서도 그 자체를 부인할 이유는 없다. '인터넷 강국'으로서 한국의 명성에 걸맞게 민간이 주도하는 자유로운 사이버 공간의 활동과 질서를 중장기적으로 모색하는 것은 바람직하다고 볼 수 있기 때문이다.

그러나 국내외적으로 다중이해당사자주의 모델을 실천할 사회경제적 기반이라는 관점에서 보았을 때 현재 한국의 현실은 매우 빈약하다고 평가하지 않을 수 없다. 사실 한국에는 인터넷 거버넌스와 관련하여 다중이해당사자주의를 논할 정도로 이해당사자(stakeholder)들이 결속되어 있지도 못했으며, 만약에 있더라도 그 층이 매우 얇다. 게다가 미국의 경우처럼 정부와 기업 및 시민사회 등을 오고가며 활동하는 공공 및 민간 전문가들이 거의 없다. 따라서 국내업계의 이해당사자들이 충분히 성숙되지 않은 상황에서 다중이해당사주의의 추구는 한국의 현실에 근거한다기보다는 다소 이상적이라는 지적이 나오기도 한다. 그렇지만 사정이 이러하다고 대외적으로 글로벌 인터넷 거버넌스의 장에서 공공연히 러시아와 중국이 내세우는 바와 같은 국가간다자주의를 지지하기에는, 한국에게는 미국과의 관계에서 파생되는 '안보 변수'가 일종의 제약요인으로 작용한다.

이렇듯 글로벌 인터넷 거버넌스의 장으로서 ICANN에의 참여는 정부의 소극적 자세와 국내 사회경제적 기반의 취약성으로 인해서 그리 활발하게 이루어지지 못하고 있다. 이에 비해 한국 정부는, ICANN 활동에의 참여보다는, 전통 국제기구 모델 또는 국가간다자주의에 기반을 둔 글로벌 인터넷 거버넌스의 활동에 좀 더 중점을 두고 있는 것으로 보인다. 예를 들어, 한국은 인터넷 시대를 맞이하여 전통적인 전

기통신 분야의 관할권을 확장하는 데 주력하고 있는 ITU 활동에 적극 참여하고 있다. 한국은 과기정통부와 정보통신정책연구원(KISDI)을 중심으로 ITU와 APT 등에서 개최하는 주요 회의의 의제를 분석하고 이에 대응함으로써 국내의 관련 정책협의를 이끌어가고 있다. 또한 이 분야의 국제협력을 위한 국내적 기반을 강화함으로써 국제기구 활동의 지원체계를 구축해 왔다. 이를 바탕으로 최근에는 2014년 ITU 전권회의(부산)와 ITU 전기통신개발총회(WTDC) 및 정보사회세계정상회의(WSIS)+10 고위급행사, 그리고 APT 총회 등을 개최하거나 참여한 바 있다.

인터넷 거버넌스와 관련해서는 이 중에서 2015년 12월 유엔에서 개최된 WSIS+10 고위급회의 참여에 주목할 필요가 있다. 유엔은 디지털 정보격차 해소를 위해 2003년과 2005년에 걸쳐서 WSIS를 개최했는데 그 이후 10년 후인 2015년 총회에서 그동안의 의제 이행과 관련된 검토 작업을 벌이기로 결정했는데, 여기에 미래부(현 과기정통부), KISDI, KISA, 외교부 등에서 참여했다. 2016년 5월에는 KISDI가 스위스 제네바에서 개최된 WSIS 포럼에 참여했는데, 이 포럼은 WSIS의 결과 이행을 위해 2009년 이후 매년 개최되고 있다. 2015년 12월의 WSIS+10 고위급회의에서 모든 이해관계자가 WSIS의 이행현황을 논의하고 모범 사례를 공유하는 플랫폼으로서 WSIS 포럼을 지속하기로 결정한 바 있다. 한편 한국은 2006년 이후 IGF에도 계속 참여해 왔는데, 현재 IGF의 운영 제반 사항을 논의하는 IGF MAG(Multistakeholder Advisory Group)에 참여 중이다.

VI. 맺음말

이 글은 국가간, 정부간, 글로벌 거버넌스 등의 세 가지 프레임을 원용하여 현재 복합적인 양상으로 진행되고 있는 사이버 안보 분야의 국제규범 형성과 그 기저에 깔려 있는 주요국들의 이해갈등 구도를 살펴보았다. 최근 주목을 받는 것은, 2013년 이후 근대 국제질서에서 잉태된 국가 간 프레임으로 사이버 안보의 국제규범을 보려는 시도이다. 그러나 전통적인 국제법의 적용을 실험하는 탈린매뉴얼이나 유엔 GGE 활동에서 보는 바와 같은 전통 국제기구의 틀 안에서만 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 유럽사이버범죄협약과 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 규범 경쟁인 동시에, 더 중요하게는 세 가지 층위를 가로질러서 나타나는 '프레임 간 규범 경쟁'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 국가 간 프레임을 고수하는 모양새를 나타내고 있다. 양 진영이 벌이고 있는 프레임 경쟁의 차이를 요약하면, 서방 진영이 정부간 프레임과 글로벌 거버넌스 프레임을 결합한 복합 아키텍처의 국제규범을 모색한다면, 비서방 진영의 시도는 근대 국제질서의 아키텍처를 기반으로 하는 국가 간 프레임에 입각해 있다고 볼 수 있다.

이 글에서 살펴본 사례들은 이러한 '프레임 내 경쟁'과 '프레임 간 경쟁'의 양상이 중층적으로 겹치면서 서로 치고받는 모습을 보여주었다. 예를 들어, 국가 간 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 국가 간 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 과정에서, 러시아와 중국이 주도하는 상하이협력기구의 행보가 박차를 가하게 된 측면이 없지 않다. 이러한 구도와

중첩되면서 사이버공간총회와 상하이협력기구 간에도 프레임 경쟁의 양상이 진행되었음을 무시할 수 없다.

이러한 프레임 경쟁의 가장 밑바닥에는 글로벌 질서의 미래상과 관련하여 서방 진영과 비서방 진영이 지닌 근본적으로 상이한 관념이 자리 잡고 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 필요 시 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 국가간다자주의 프레임으로 요약해 볼 수 있다.

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 전통적인 국가 간 프레임에만 갇혀 있을 것이 아니라, 좀 더 복합적인 프레임에서 이 분야의 규범 형성을 보는 노력이 필요하다. 특히 강대국들이 벌이는 프레임 경쟁이라는 구조변화에 대응하는 중견국의 입장에서는 이러한 프레임들이 누구의 이해관계를 대변하는지, 그리고 각 프레임이 궁극적으로 지향하는 질서상이 무엇인지를 제대로 파악하는 일 자체가 국가전략의 사안이라

고 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.

참고문헌

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

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

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

_____. 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.

신맹호. 2016. "외교부 사이버 안보 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.

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

장규현·임종인. 2014. "국제 사이버 보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로."『정보통신방송정책』26(5), pp. 21-52.

장노순. 2016. "사이버 안보와 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.

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.

Brenner, Susan W. 2007. "Council of Europe's Convention on Cybercrime." J.M. Balkin and Information Society Project, Yale Law School, *Cybercrime: Digital Cops in a Networked Environment*. New York: New York University Press, pp. 207-220.

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).

DeNardis, Laura. 2013. *The Global War for Internet Governance*. New Heaven, CN: Yale University Press.

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

Noor, Elina. 2015. "Strategic Governance of Cyber Security: Implications for East Asia." in 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.

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

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

国家互联网信息办公室(국가인터넷정보판공실). 2017.『网络空间国际合作战略(사이버 공간국제협력 전략)』3月 1日.