사이버 안보와 중견국 규범외교 : 네 가지 모델의 국제정치학적 성찰

김 상 배 | 서울대학교

| 목차

| 주제어 사이버 안보, 중견국 외교, 네트워크 이론, 규범외교, 국제규범, Cyber Security, Middle Power Diplomacy, Network Theory, Normative Diplomacy, International Norm

최근 사이버 안보는 21세기 세계정치의 주요 쟁점이 되었다. 각국 차원에서 대응전략을 마련할 뿐만 아니라 주변국과 협력하고 국제규범을 만들기 위한 노력이 한창 진행되고 있다. 이러한 인식을 바탕으로 이 글은 사이버 안보 분야에서 발견되는 중견국 규범외교의 네 가지 모델을 국제정치학적 시각에서 성찰하였다. 특히 이 글은 네트워크 세계정치이론의 시각을 원용하여 각 모델을 개념화하고 체계적인 비교분석을 시도하였다. 이를 통해서 이 글이 제시하는 중견국 규범외교의 네 가지 모델은, 에스토니아가 주도하는 국가동맹 모델로서의 '탈린 프로세스', 네덜란드가 주도하는 정부간레짐 모델로서의 '헤이그 프로세스', 핀란드가 주도하는 지역협력체 모델로서의 '헬싱키 프로세스', 그리고 스위스의 중립국 이미지를 원용하여 마이크로소프트가 제안한 평화윤리 모델로서의 '제네바 프로세스' 등이다. 이들 네 가지 모

* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A3A2924409)

국제정치논총 제59집 2호 (2019), 51-90.

델은 각기 현실주의, 자유주의, 구성주의, 범세계주의 등으로 대변되는 국제정치이론의 시각에서 본 국제규범에 대한 논의의 스펙트럼 전반을 보여주는 의미가 있다. 또한 이들 모델은 최근 사이버 안보 분야에서 새로운 역할을 모색하고 있는 한국의 중견국 규범외교 모델, 즉 이른바 '서울 프로세스'의 개발에 주는 시사점도 크다.

Ⅰ. 머리말

최근 사이버 안보 문제는 국가전략과 세계정치의 현안으로 자리 잡아가고 있다.[1] 각국 차원의 대응전략을 마련하고 주변국과 국제협력을 강화하며 다자외교의 장에서 국제규범을 마련하기 위한 논의가 한창 진행되고 있다. 이러한 맥락에서 이 글은 사이버 안보의 국제규범 형성 과정에서 중견국이 담당할 역할이 무엇인지를 묻는다. 전통안보 분야의 국제규범 형성이 그러했듯이, 사이버 안보의 국제규범도 강대국들이 주도하여 만들 것인가? 아니면 강대국이 아닌 나라들, 특히 중견국도 자신들의 구상을 제시하고 이해관계를 반영하는 역할을 담당할 수 있을까? 중견국 규범외교는 얼마만큼 가능하며 그 내용과 범위는 어디까지인가? 개별 국가의 이익을 반영하는 차원을 넘어서 중견국이 보편적 규범을 주도할 가능성은 얼마나 있을까? 그리고 중견국 한국은 사이버 안보 분야에서 어떠한 규범외교를 추진해야 할 것인가?

이러한 문제의식을 바탕으로 이 글은 최근 사이버 안보 분야에서 활발한 활동으로 주목받고 있는, 에스토니아, 네덜란드, 핀란드, '스위스'[2] 등의 네 가지 사례

1 사이버 안보의 국가전략과 세계정치에 대한 전반적인 논의로는 김상배, 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』(파주: 한울, 2018)을 참조하라.

2 이 글에서 다룬 '스위스'의 사례는, 스위스라는 국가가 일국 차원에서 추구하는 사이버 안보전략의 사례라기보다는, 중립국으로서 스위스의 적십자정신을 상징으로 내걸고 최근 진행되고 있는

를 비교분석하였다. 이들 국가는 사이버 안보의 국제규범과 관련하여 유사한 입장을 갖고 있는 동지국가들이라고 할 수 있다.[3] 그럼에도 자세히 살펴보면 이들 네 가지 사례는 서로 대비되는 중견국 규범외교의 경로를 추구하는 특성을 보여준다. 각 사례는 사이버 안보의 규범외교를 국가동맹, 정부간레짐, 지역협력체, 평화윤리 등으로 각기 다르게 초점을 두어 접근하는데, 일견 상호 경쟁하는 양상을 보이고 있다. 또한 이들 네 가지 사례는 각기 현실주의, 자유주의, 구성주의,[4] 범세계주의 등으로 대변되는 국제정치이론의 시각에서 본 국제규범에 대한 논의의 스펙트럼 전반을 보여주는 사례들이기도 하다.

각국의 사이버 안보전략에 대한 비교분석의 연구는 아직까지 그리 많이 진행되지 못했다. 그나마 진행된 연구도 주로 미 · 중 · 일 · 러와 같은 강대국의 사이버 안보전략과 추진체계에 대한 소개 위주이며, 이들 연구도 일국 전략 위주이지 비교분석을 행한 경우는 많지 않다.[5] 최근 중견국의 사이버 안보 전략에 대한 비교연구가 조금씩 진행되고 있는 상황인데, 에스토니아, 핀란드, 독일, 네덜란드, 노르웨이 등 5개 중견국의 사이버 국방 추진체계[6], 호주, 에스토니아, 이스라엘, 네

중견국들과 민간 기업들의 행보를 염두에 두고 선정하였다.

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

4 이 글에서 다룬 '구성주의'는 엄밀히 보면 '공동체주의'(communitarianism)를 의미하는데, 이 글에서는 '구성주의'라는 용어를 범세계주의(cosmopolitanism)와 구별하여 사용하였다. 규범적 판단의 준거를 국가 행위자에 두느냐 아니면 인류 전체에 두느냐에 따라서 규범이론(또는 넓은 의미의 구성주의) 내에서는 공동체주의와 범세계주의를 구분한다. 자세한 내용은 이 글의 제2장을 참조하라.

5 미 · 중 · 일 · 러의 사이버 안보전략과 추진체계에 대한 연구로는 김상배(2018) 제5장에서 다룬 기존연구 소개를 참조하라.

6 Piret Pernik, *Preparing for Cyber Conflict Case Studies of Cyber Command.* International Centre for Defence and Security Report (December, 2018).

덜란드, 한국 등 5개 중견국의 사이버 안보 대외정책,[7] 비세그라드(Visegrad) 그룹에 속하는 체코, 폴란드, 슬로바키아, 헝가리 등 4개 중견국의 사이버 안보전략,[8] 그리고 브릭스(BRICS) 5개국의 사이버 안보 외교정책[9] 등에 대한 비교연구가 있다. 그러나 이들 연구는 단순 비교나 사례 소개의 수준에 머물고 있어서, 국제정치학의 이론적 시각에서 본격적으로 성찰한 연구가 시급히 필요한 실정이다.[10]

그런데 기존 국제정치이론만으로는 이들 네 가지 중견국 규범외교를 비교분석하는 데 충분한 이론적 자원을 확보하기 어렵다. 우선, 주로 행위자 차원에 초점을 둔 기존 국제정치이론만으로는 이들 사례가 당면하고 있는 각기 다른 성격의 '구조적 상황'과 그 안에서 각 행위자가 차지하는 '구조적 위치'의 의미를 입체적으로 탐구하기 어렵다. 또한 주로 국민국가 단위에 주목하는 기존 국제정치이론만으로는 국가동맹, 정부간레짐, 지역협력체, 초국적 네트워크 등과 같이 일국 단위를 넘어서 활동하는 '중견국'의 복합적 성격을 파악하기 어렵다. 끝으로, 주로 군사력과 경제력과 같은 자원권력의 활용으로서 외교전략을 보는 기존의 국제정치이론만으로는 관계적 맥락의 조율을 통해서 네트워크를 구축하고 규범을 모색해야 하는 중견국 외교의 동학을 설명하기 어렵다. 이러한 문제의식을 반영하여

7 Sico Van der Meer, "Medium-sized States in International Cyber Security Policies," Clingendael, Netherlands Institute of International Relations (2016). 호주 사례연구로는 Frank Smith and Graham Ingram, "Organising Cyber Security in Australia and Beyond," *Australian Journal of International Affairs* 71-6 (2017), pp.642-660도 참조하라.

8 Marek Górka, "The Cybersecurity Strategy of the Visegrad Group," *Politics in Central Europe* 14-2 (2018). pp.75-98.

9 Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34-6 (2013), pp.1054 - 1074.

10 예외적으로 국제정치이론의 시각을 적용하여 뉴질랜드 사례를 살펴본 연구로 Joe Burton, "Small States and Cyber Security: The Case of New Zealand," Political Science 65-2 (2013), pp.216-238가 있다. 또한 사이버 안보전략 자체를 다룬 것은 아니지만, 에스토니아와 핀란드의 대외정책 일반을 국제정치이론 시각에서 비교분석한 연구로 Kristi Raik, "Renaissance of Realism, a New Stage of Europeanization, or Both? Estonia, Finland and EU Foreign Policy," *Cooperation and Conflict* 50-4 (2015), pp.440 - 456를 참조하라.

이 글은 소셜 네트워크 이론, 네트워크 조직 이론, 행위자-네트워크 이론 등으로부터 개념적 자원을 원용하여 중견국 규범외교를 이해하는 국제정치학적 비교분석의 틀을 마련하였다.[11]

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

이러한 네 가지 모델이 한국이 모색할, 이른바 '서울 프로세스'에 주는 실천론적 함의도 크다. 어느 나라 못지않게 복잡한 구조적 상황에 놓인 한국이 추구할 사이버 안보 규범외교의 방향과 내용은 무엇일까? 미 · 중 · 일 · 러 사이에서, 그리고 서방 및 비서방 진영 사이에서 한국이 내세울 프레임의 구도는 무엇이며, 이를 풀어갈 전략적 지향성의 내용은 어떻게 채워야 할까? 탈린 프로세스와 같은 동맹의존 모델인가, 헤이그 프로세스와 같은 정부간레짐 모델인가, 헬싱키 프로세스 같

11 다양한 네트워크 이론의 시각에서 보는 국제정치이론에 대한 논의로는 김상배, 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 (파주: 한울, 2014)를 참조하라. 이를 사이버 안보의 중견국 외교에 적용한 사례로는 Sangbae Kim, "Cyber Security and Middle Power Diplomacy: A Network Perspective," *Korean Journal of International Studies* 12-2 (2014), pp.323-352를 참조하라.

은 지역협력체 모델인가, 아니면 제네바 프로세스와 같은 평화윤리 모델인가? 이 글의 주장은 이들 모델 중에 서울 프로세스가 벤치마킹할 어느 하나의 모델이 있다기보다는, 한국이 처한 구조적 상황을 고려하여 이들 네 가지 모델이 담고 있는 유용한 요소들을 선별적으로 추출해야 한다는 것이다. 결국 서울 프로세스가 지향하는 사이버 안보의 국제규범은 기존 모델을 복합적으로 엮어내는 '메타규범 모델'의 고안에서 찾아져야 할 것이다.

이 글은 다음과 같이 크게 세 부분으로 구성되었다. 제2장은 국제규범에 대한 국제정치이론적 이해의 지평을 소개하고, 네트워크 이론의 시각에서 보는 중견국 규범외교의 비교분석틀을 제시하였다. 제3장은 사이버 안보 분야의 중견국 규범외교를 보여주는, 탈린 프로세스, 헤이그 프로세스, 헬싱키 프로세스, 제네바 프로세스 등의 네 가지 사례를 개괄적으로 살펴보았다. 제4장은 앞서 제시한 네트워크 이론의 분석틀을 원용하여 사이버 안보 규범외교의 네 가지 모델을 비교분석하고, 이들 사례가 서울 프로세스로 개념화될 한국 모델에 주는 이론적 · 실천론적 함의를 도출하였다. 끝으로, 맺음말에서는 이 글의 주장을 종합 · 요약하고, 중견국 규범외교에 대한 비교연구가 지니는 의미와 향후 과제에 대해서 간략히 살펴보았다.

Ⅱ. 중견국 규범외교의 분석틀

1. 국제규범의 국제정치이론적 이해

규범(規範, norm)이란 인간이 행동하거나 판단할 때에 마땅히 따르고 지켜야 할 가치판단의 기준이다. 일반적으로 공식적인 법제도의 기저에 깔려 있는 관념의 형태로 나타나는 표준, 원리, 모범, 본보기 등을 의미한다. 최근 국제정치학에서도 기존의 실증주의 인식론을 비판하면서 국제정치 과정에서 도덕과 윤리가 독

자적인 변수로 작동하고 있다고 주장하는 '규범의 국제정치'에 대한 논의가 활발하다. 예를 들어, 국제정치에서 기본적인 규범 또는 옳고 그름의 권리와 의무로서 '정당한' 전쟁의 윤리나 핵무기 윤리, 국제적 차원의 정의, 보편적 인권 등에 대한 탐구가 진행되고 있다. 이러한 규범 연구는 근대 국제정치의 구성원리로서 주권 원칙에 대한 성찰과 연결된다는 점에서 비판이론의 전통에 서 있다. 특히 규범과 주체의 판단 준거, 즉 국제정치적 옳고 그름, 권리와 의무가 국가라는 행위자 개체 차원에 근거를 두느냐, 아니면 인류 전체 차원에 근거를 두느냐 등에 따라서 규범이론의 갈래도 달리 나타난다.[12]

현실주의 전통은 국제규범을 물리력을 행사하지 않고도 원하는 목적을 달성하는 정치적 명분과 정당성 확보의 수단으로 이해한다. 현실주의에서 동맹이나 국제법 등과 같은 규범은 국가이익 추구의 연장선에서 이해되는 전략이다. 자유주의 전통은 국제규범을 행위자들 간의 제도적 합의와 협력의 산물이라는 맥락에서 본다. 규범은 상호 간 약속과 계약으로서 행위를 규제하는 레짐이며, 법보다는 비공식적인 구속과 자발적 제약을 가한다. 구성주의 전통 중에서 공동체주의가 이해하는 규범은 국가 간에 공유된 정체성의 산물에 착안한다. 국가의 주권과 자율성에 제약을 주는 도덕적 가치를 인정하지 않으며, 인류에 대한 의무는 국가의 매개로 이루어진다는 인식을 바탕으로 한다. 이에 비해 범세계주의 전통에서 이해하는 규범론은 국가를 초월하는 전체로서의 인류나 개인에 근거를 두는 윤리와 도덕 기반의 규범을 상정한다. 즉 국가의 자율성에 제약을 주는 당위의 존재를 인정하며 국가도 지켜야 하는 인도주의적 의무가 있다고 주장한다.[13]

이러한 규범의 개념에 입각해서 보면, 중견국의 '규범외교'(normative

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

13 리처드 샵콧, "국제윤리." 존 베일리스, 스티브 스미스, 퍼트리샤 오언스 편, 『세계정치론』, (서울: 을유문화사, 2015), pp.271-289.

diplomacy)를 보는 시각도 다르게 나타날 수밖에 없다. 현실주의 시각은 중견국 규범외교를 상대적으로 물리력이 부족한 중견국이 강대국의 힘에 대응하여 규범 변수를 도구적 또는 거래적(transactional)으로 활용하는 차원에서 이해한다. 이는 주로 강대국의 규범에 참여하여 힘을 얻는 동맹외교의 형태로 나타난다. 자유주의 시각은 중견국 규범외교는 강대국들이 주도하는 규칙 · 제도 · 레짐의 형성 과정에 참여하는(participatory) 활동으로 이해한다. 다양한 국제규범의 형성과정에 적극적으로 참여하여 자국의 이익을 반영하고 자국의 규범을 설파하는 외교라고 할 수 있다. 구성주의나 범세계주의 시각에서 보는 중견국 규범외교는 약자의 담론전략의 차원에서 강력외교에 대항해서 당위론적인 측면을 활용하는 외교이다. 이는 대안적 규범과 정체성의 변환까지도 포함하여 새로운 규범을 제시하는 변환적(transformative) 외교로 볼 수 있다. 이는 실리외교의 차원을 넘어서 보편적인 윤리와 도덕에 기여하는 외교이다.

이러한 규범에 대한 국제정치학적 논의를 사이버 안보 분야에 적용해서 보면, 현재 다양한 시각에서 파악되는 국제규범 형성의 움직임을 좀 더 체계적으로 이해할 수 있다. 최근 주목을 받는 것은, 전통적인 국제법이나 국제기구의 틀에 기대어 사이버 안보의 국제규범을 모색하려는 현실주의적 시도이다. 탈린매뉴얼이나 유엔 정부전문가그룹(Group of Governmental Experts, GGE) 활동, 나토 동맹의 활용 등이 사례이다. 사이버 공격으로부터 피해를 보는 당사국의 정부들이 나서서 국제협력의 레짐을 모색하려는 자유주의적 시도도 눈에 띈다. 정부 간의 양자 및 다자협력이나 사이버공간총회, 유럽사이버범죄협약 등의 사례를 들 수 있다. 구성주의 시각에서 본 국제규범 형성의 움직임으로는 글로벌 인터넷 거버넌스 분야에서 ICANN(Internet Corporation for Assigned Names and Numbers)이나 ITU(International Telecommunication Union) 등이 벌이는 규범형성의 노력이나 유럽연합이나 아세안의 지역차원에서 벌이는 정체성 형성의 시도들을 들 수 있다. 범세계주의 시각에서 본 국제규범의 모색과 관련하여 최근 민간 인터넷 기업들이 주도하고 유럽의 중견국들이 동조하여 모색되고 있는

'디지털 제네바 협정'과 같은 평화윤리의 규범에도 주목할 필요가 있다.

이렇게 상이한 시각에서 이해된 사이버 안보의 국제규범은 각기 상이한 글로벌 질서의 상(像)을 상정한다. 각 글로벌 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 국제규범의 기저에 깔린 이익과 이를 구현하기 위한 담론의 경쟁, 즉 '프레임 경쟁'[14] 이다. 사실 사이버 안보의 국제규범과 관련하여 제시되는 프레임은 단순히 중립적인 것이 아니라 이를 통해서 미래 현실을 자신에게 유리한 방향으로 재구성하려는 담론과 이익이 반영된 것이다. 이러한 복합적인 국제규범 모색의 과정에서 각국은 자국에게 유리한 국제규범을 실현하기 위한 프레임 경쟁을 벌이고 있다.

2. 네트워크로 보는 중견국 규범외교

사이버 안보 분야의 중견국 규범외교를 체계적으로 비교분석하기 위해서는 기존의 국제정치이론을 넘어서는 새로운 분석틀을 마련할 필요가 있다. 각기 다른 규범외교의 전략이 비롯되는 구조의 복합성을 체계적으로 분석하기에는 기존 국제정치이론이 상정하고 있는 '구조'에 대한 이론적 전제가 너무 단순하다. 또한 규범외교를 추진하는 중견국들의 성격도, 주류 국제정치이론이 상정하듯이, 그저 전통적인 국민국가로만 볼 수는 없다. 게다가 그 전략의 내용도 단순히 자원권력

14 이 글에서 사용한 프레임(frame) 경쟁의 개념은 미국의 미디어 학자 토드 기틀린(Todd Gitlin)이 개발하고 미국의 언어학자 조지 레이코프(George Lakoff)에 의해 널리 소개된 논의에서 착안했다; Todd Gitlin, *The Whole World Is Watching: Mass Media in the Making and Unmaking of the New Left.* Berkeley: University of California Press, 1980; 조지 레이코프. 『프레임 전쟁: 보수에 맞서는 진보의 성공전략』 서울: 창비, 2007. 이러한 프레임 경쟁의 시각을 사이버 안보에 운용한 연구로는 김상배(2014)의 제9장을 참조하라.

을 활용하는 세력균형의 권력게임으로만 보기에는 훨씬 더 복잡하다. 결국 구조와 행위자, 그리고 권력게임을 보는 새로운 이론적 시각이 필요하다. 이러한 맥락에서 이 글은 다양한 네트워크 이론, 특히 소셜 네트워크 이론과 네트워크 조직 이론 및 행위자-네트워크 이론 등에서 제기된 개념적 자원을 활용하여 새로운 비교분석의 틀을 마련하였다.[15]

우선, 강대국에 비해서 구조의 영향을 많이 받을 수밖에 없는 중견국의 행동을 설명하기 위해서는 그 중견국이 처한 구조적 상황에 대한 좀 더 면밀한 이해가 필요하다. 다시 말해 그 '구조'는 신현실주의가 상정하는 국가 간의 세력분포라는 맥락에서 이해한 '구조'의 개념보다는 좀 더 복합적이어야 한다. 그 구조는 이익구조이면서 동시에 정체성과 관념의 구조 등을 포괄하는 복합적인 구조이다. 물론 이러한 구조들이 실제로 구성되어 작동하는 복합의 정도는 각 사례마다 다를 것이다. 이러한 복합적인 구조에 대한 정확한 이해는 각 중견국이 처한 구조적 상황을 파악하여 행동하는 출발점이 된다. 이와 관련하여 소셜 네트워크 이론가인 로널드 버트(Ronald Burt)는, '구조적 공백'(structural hole)으로 불리는 네트워크상의 빈틈을 남보다 먼저 찾아서 메움으로써 그 구조적 상황에서 중심적 위치를 장악하고 거기에서 비롯되는 독특한 '위치권력'(positional power)을 발휘하는 것이 중요하다고 지적한다.[16]

둘째, 중견국 규범외교를 벌이는 행위자의 성격을 새롭게 볼 필요가 있다. 사실 전통적인 기준으로만 보면 이들 행위자는 비강대국이어서 새로운 국제규범의 형성과정에서 큰 영향력을 발휘하기 어렵다. 사실 이 글에서 다룬 네 나라는 모두 완전한 주권을 주장하는 전형적인 국민국가 행위자라기보다는 강대국들의 틈

15 이 절에서 원용한 네트워크 세계정치이론에 대한 논의는 김상배 (2014)의 제2부를 기반으로 하였다.

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

바구니에서 생존을 모색해야 하는 약소국이거나 국가의 존립을 위한 대외적 의존성의 정도가 매우 큰, 일종의 '불완전 주권국가'들이다. 따라서 일국 단위로 단일(unitary) 행위자를 상정하는 기존 국제정치이론의 시각만으로는 그 행위자의 행동이 잘 설명되지 않는다. 특히 이 글에서 다룬 '스위스'의 경우처럼, 국민국가의 경계를 넘나들며 초국적 네트워크 형태로 활동하는 비국가 행위자들과 유럽연합의 국가들과 기타 글로벌 중견국의 연대를 설명하기 어렵다. 이 글은 네트워크 조직 이론에서 말하는 '네트워크 국가'(network state)의 개념을 원용하여 이들 네트워크 행위자의 성격을 이해하였다.[17]

끝으로, 네트워크 국가로서 이들 중견국이 구조적 공백을 장악하기 위해서 벌이는 전략의 과정을 기존 국제정치이론이 상정하는 것처럼 자원권력의 추구라는 관점에서 본 세력균형의 권력게임으로만 볼 수는 없다. 사실 이들 중견국의 규범외교 전략이 그 의미를 발휘하는 대목은, 군사력과 경제력과 같은 자원권력은 부족하더라도, 이들이 구성하는 네트워크를 활용하여 새로운 권력게임, 즉 '네트워크 권력'(network power)의 게임을 벌일 수 있다는 데서 발견된다. 이러한 중견국의 네트워크 전략을 구체적으로 비교분석하기 위해서 이 글은 프랑스의 행위자-네트워크 이론가인 미셸 칼롱(Michel Callon)이 제시한 네트워크 전략의 네 단계를 외교전략 분야에 맞게 개작하여 원용하였다.[18]

중견국 네트워크 전략의 첫 번째 단계는 '프레임 짜기'이다. 이는 행위자들의 이

17 Martin Carnoy and Manuel Castells, "Globalization, the Knowledge Society, and the Network State: Poulantzas at the Millennium," *Global Networks* 1-1 (2001), pp.1-18; 하영선 · 김상배 편, 『네트워크 지식국가: 21세기 세계정치의 변환』 (서울: 을유문화사, 2006).

18 Michel Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay," in John Law ed. Power, *Action and Belief: A New Sociology of Knowledge*. London: Routledge and Kegan Paul, 1986, pp.196-233; 행위자-네트워크 이론의 국제정치학적 적용에 대한 좀 더 자세한 논의를 보기 위해서는 김상배 (2014), pp.370-399를 참조하라. 한편 이하에서 서술한 네트워크 전략의 네 단계, 즉 프레임 짜기-맺고 끊기-내편 모으기-표준 세우기에 대한 논의는 김상배(2018) pp.330-332의 내용을 요약하였다.

해관계를 정의하고 네트워크 전체의 구도를 파악하는 단계이다. 이 단계에서 이루어지는 외교전략은 마치 언론이 뉴스의 프레임을 짜는 것을 연상시킨다. 이는 행위자들이 놓여 있는 네트워크의 상황을 재구성하여 인식하고 이러한 상황에서 자국의 위치를 설정하여 그 역할을 정당화하는 방향으로 프레임을 짠다는 의미이다. 이러한 프레임 짜기의 단계에서는 세계정치를 둘러싼 사고와 행동의 플랫폼을 제시하려는 담론의 경쟁이 벌어진다. 중견국의 입장에서 볼 때, 강대국들이 주도하는 세계정치 현실에서 중견국의 입지를 부각시키는 방식으로 상황을 인식하게 만들 수 있느냐가 관건이 된다.

두 번째 단계는 '맺고 끊기'이다. 이는 기존에 형성되어 있던 관계를 해체하고 새로운 관계를 수립하기 위한 기초를 세우는 단계이다. 이 단계의 전략은 주로 네트워크상에서 끊어진 선을 잇고 새로운 선을 긋는 방식으로 나타나는데, 이러한 과정에서 집중과 선택의 비대칭적인 관계조율이 발생한다. 이러한 관계조율의 과정은 보통 기존의 네트워크를 끊고 새로운 네트워크를 맺거나 구조적 공백을 메우려고 사회적 자본을 활용하는 전략으로 나타나는데, 이러한 과정은 기회비용이 발생하는 전략적 선택의 영역이다. 주위의 행위자들과 될 수 있는 한 많은 관계를 맺어 모두와 좋은 관계를 유지하는 것이 최선이겠지만, 만약에 이것이 가능하지 않다면 이른바 중심성(centrality)을 극대화하는 방향으로 맺고 끊기를 할 수밖에 없다.

세 번째 단계는 '내편 모으기'이다. 이는 맺고 끊기를 통해 해체되고 재편된 관계를 다시 수습하여 자신의 주위에 새로운 네트워크를 건설하는 단계이다. 이전 단계들의 네트워킹 과정을 통해서 불러 모은 동지집단의 행위자들에게 새로운 역할을 부여하고 여럿이 함께 할 수 있는 둥지를 만드는 것이라고 볼 수 있다. 그리고 이러한 둥지 안에, 단순히 연결망을 치는 차원을 넘어서, 나를 지지하는 편을 얼마나 많이 끌어 모아 세(勢)를 형성하는 단계에까지 나아갈 것이냐가 관건이다. 따라서 이 단계의 과제는 네트워크상에서 일단 관계를 맺은 상대방을 끌어들이는 방법과 자원을 다각적으로 활용하는 데 있다. 연대외교나 협업외교 등은 외교 분

야에서 나타나는 내편 모으기의 대표적 사례들이다.

마지막 단계는 '표준 세우기'이다. 이는 새로이 만들어진 네트워크에 일반적 보편성을 부여하는 단계이다. 이 단계에서는 단순히 관계를 연결한 행위자들의 숫자를 늘리는 차원을 넘어서 일단 형성된 관계를 지속성 있는 네트워크로 계속 유지할 수 있느냐의 문제가 관건이다. 다시 말해 이는 몇 개의 특수한 성공사례의 샘플을 넘어서 표준 설정의 과정을 통해 세계정치의 '게임의 규칙'을 장악하느냐의 문제이다. 실제로 성공적으로 네트워크를 구축한 소수 행위자는 자신이 마련한 플랫폼 위에 동원된 다수 행위자들을 '대변'하는 권리를 갖게 됨으로써 세계정치라는 네트워크의 프로그램을 설계하는 권력을 행사하게 된다.

Ⅲ. 중견국 규범외교의 네 가지 모델

1. 탈린 프로세스: 현실주의 국가동맹 모델

구소련 연방 국가였던 에스토니아가 탈냉전 이후 직면한 가장 큰 안보위협은 여전히 러시아였다.[19] 군사적 약소국인 에스토니아의 입장에서는 중립을 유지하는 것도 쉽지 않았다. 이러한 구조적 상황을 타개하는 에스토니아의 선택은 나토 가입에 맞춰졌다.[20] 투마스 일베스(Toomas Ilves) 대통령의 주도 하에 에스토니아 정부는 나토 가입의 요건을 충족시킬 국가역량을 확보하기 위해 사회경제적

19 Eric Noreen and Roxana Sjöstedt, "Estonian Identity Formations and Threat Framing in the Post-Cold War Era." *Journal of Peace Research* 41-6 (2004), pp.733 - 750.

20 Erik Männik, "Small States: Invited to NATO-Able to Contribute?" *Defense & Security Analysis* 20-1 (2004), pp.21 - 37; Henric Praks, "Estonia's First Steps in the Direction of NATO and National Defence," *Estonian Yearbook of Military History* 4 (2014), pp.113-140.

발전과 행정 시스템의 개혁에 착수했다. 대표적인 사례가 바로 1996년부터 시작한 '호랑이 도약'(Tiger Leap)이라는 이름의 정보화 프로젝트였다.[21] 이러한 에스토니아의 시도는 일정한 성과를 거두었는데, 유럽 내에서도 상대적으로 높은 인터넷 보급률, 전자정부와 온라인 투표 도입 등의 성과를 바탕으로 'e-Stonia'라는 별명을 얻기까지 했다. 이러한 일련의 시도를 통해서 에스토니아는 미개발된 동유럽 국가의 이미지를 탈피하는 계기를 마련하였다.[22]

이러한 과정에서 2007년 4월 발생한 러시아의 사이버 공격은 에스토니아의 사이버 안보전략을 도약시키는 직접적인 계기를 제공하였다. 2007년 총선에서 반(反) 러시아계 정당이 집권한 후 구성된 에스토니아 정부가 2차 대전 참전을 기념해서 수도 탈린에 세운 옛 소련 군인의 동상을 수도 외곽지역으로 이전하려는 계획이 빌미를 제공했다. 러시아발 사이버 공격의 충격은 매우 컸는데, 에스토니아 정부의 전산망에 연결된 수만 대의 컴퓨터들이 디도스 공격을 받아 3주가 넘는 기간 동안 주요 국가기능이 마비될 정도였다. 나토 회원국인 에스토니아에 대한 재래식 공격이 나토의 집단 방위권을 발동시킬 우려가 있는 상황에서, 러시아가 에스토니아에 대한 직접적인 물리적 충돌 대신 사이버 공격 행위를 통해 에스토니아 내부의 갈등에 개입한 것으로 평가되었다.[23]

21 Pille Runnel, Pille Pruulmann-Vengerfeldt and Kristina Reinsalu, "The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice," *Journal of Baltic Studies* 40-1 (2009), pp.29-51; 알리나 쉬만스카, "구소련의 약소국에서 유럽 규범의 주도국으로 진화: 에스토니아의 사이버 안보 중견국 외교 중심으로." 한국국제정치학회 연례학술대회 발표논문 (2018)

22 Riina Kaljurand, "Security Challenges of a Small State: The Case of Estonia." in Raimonds Rublovskis, Margarita Šešelgyte and Riina Kaljurand. *Defence and Security for The Small: Perspectives from the Baltic States.* Centre for Small State Studies Institute of International Affairs, (2013), pp.55 - 81.

23 Christian Czosseck, Rain Ottis and Anna-Maria Taliharm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *International Journal of Cyber Warfare and Terrorism* 1-1 (2011), pp.24-34; Matthew Crandall, "Soft Security Threats and Small States: the Case of Estonia." *Defence Studies* 14-1 (2014), pp.30-55; 김상배 (2018), pp.126-127.

그러나 이러한 사이버 공격 행위에 대하여 에스토니아는 나토에 집단방위를 규정한 나토조약 제5조를 적용하여 러시아에 대항해 줄 것을 요구했다. 사이버 공격에 대한 명확한 국제규범이 부재한 상황에서 나토가 직접 개입하지는 않았지만, 2007년 사태는 이전부터 사이버 안보 분야에서 나토 회원국 내에서 자국의 역할을 찾고 있던 에스토니아에게 일종의 '구조적 공백'으로 작용했다. 일찌감치 사이버 안보 분야는 물리적 군사력이 취약한 에스토니아가 나토에 기여할 수 있는 영역으로 물색되어 있었다. 마침 에스토니아는 1990년대 말부터 추진한 '호랑이 도약 프로젝트'의 성과로 ICT분야의 역량도 갖추고 있었다. 게다가 에스토니아 정부는 2003-2004년에 이미 나토에 CCDCOE(Cooperative Cyber Defence Centre of Excellence)의 설치를 제안했고 2006년에는 그에 대한 승인을 받은 상황이었다. 2007년 사태는 CCDCOE를 주도하려던 에스토니아에게 '구조적 공백'의 기회를 제공했다.[24]

이렇게 에스토니아가 추진한 사이버 안보전략의 기저에는 러시아에 대항하기 위해 나토라는 서방 진영의 정치군사 동맹을 활용하려는 전략적 프레임이 깔려 있었다. 다시 말해 구소련 연방에서 탈피하여 독자적인 발전전략을 추구하는 과정에서 친서방적인 노선을 취해야만 했던 구조적 상황이 에스토니아 사이버 안보전략의 프레임에 반영되었다. 이러한 일련의 과정에서 에스토니아가 취하고 있는 사이버 안보 분야 국제협력의 정향성은 전통안보의 경험에서 추출된 동맹모델을 적용하려는 현실주의적 접근이었다. 다시 말해, 에스토니아의 대내외 정책지향성은 기본적으로는 국가주권 프레임에 기반으로 두고 국가안보를 보장하기 위해서 동맹국들과의 국제협력을 모색하는 모습으로 이해할 수 있었다.[25]

정치군사동맹의 관점에서 사이버 안보에 접근한 에스토니아의 행보는 오프

24 알리나 쉬만스카 (2018), pp.12-13.

25 Matthew Crandall and Collin Allan, "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36-2 (2015), pp.346-368.

라인 공간의 국제법, 특히 전쟁법 규범을 사이버 공격 행위에 적용하여 일종의 사이버전 교전수칙을 마련하려는 시도로 나타났다. 그 대표적인 사례가 나토 CCDCOE의 총괄 하에 20여명의 국제법 전문가들이 2009년부터 시작하여 3년 동안 공동연구를 거쳐 2013년에 발표한 총 95개항의 사이버전 지침서인 '탈린매뉴얼'(Tallinn Manual)이다. 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. 이러한 탈린 매뉴얼은 그 실제 적용가능성 등을 놓고 논란이 되기도 했지만, 사이버 안보 분야에서 나름대로의 '표준'을 설정하는 효과를 보기도 했다.[26] 이후 에스토니아는 싸이콘(Cycon)으로 알려진 사이버 분쟁에 관한 국제회의를 매년 개최하며 나토 차원의 사이버 안보담론을 주도하고 있다.

2. 헤이그 프로세스: 자유주의 정부간레짐 모델

사이버전에 대한 대응을 강조한 에스토니아의 경우와는 달리, 네덜란드는 사이버 안보를 외교의 문제로 접근한다.[27] 이러한 네덜란드의 접근은 북해 연안 지역의 물류중심지로 발전하면서 국제평화와 질서확립을 위한 국제법과 다자외교의 추진을 국익증진의 통로로 여겨온 역사적 · 구조적 상황과 밀접히 관련된다. 이는 기후변화, 개발협력, 인권, 군축 등의 분야뿐만 아니라 사이버 안보 분야에서도 나타난 바 있다. 사실 네덜란드는 인터넷 보급률이나 ICT 인프라에 대한 투자,

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

27 Alexander Claver, "Governance of Cyber Warfare in the Netherlands: An Exploratory Investigation," *The International Journal of Intelligence, Security, and Public Affairs* 20-2 (2018), pp.155-180.

전자정부 시스템 도입, 데이터 센터의 보유 등에 있어서 유럽 국가들 중에서도 가장 앞선 나라 중의 하나이다. 이렇듯 고도로 디지털화된 시스템을 보유한 네덜란드와 같은 나라에게 사이버 공격은 치명적인 위협이 될 수밖에 없다. 이러한 이유로 네덜란드는 사이버 공간이 반드시 안전하게 지켜져야 함을 강조해 왔으며, 사이버 안보를 확보하기 위한 이해당사자들의 국제협력과 국제규범의 수립활동에 앞장서 왔다.[28]

이러한 네덜란드의 외교적 접근은 미국과 영국으로 대변되는 서방 진영과 러시아와 중국으로 대변되는 비서방 진영의 사이에서 친(親)서방 외교선봉대의 역할을 담당하는 것으로 나타났다. 네덜란드는 다자외교에 적합한 환경을 활용하여 다양한 사이버 안보 분야의 국제협력과 연합형성 활동에서 중개자의 역할을 적극적으로 수행했으며, 서방 진영의 규범 전파자 또는 촉진자 역할을 수행하려는 의지를 표방해 왔다. 특히 사이버 안보의 국제규범 형성에 대한 국제적 합의를 현행 국제법에서 시작해야 한다는 서방 진영의 입장을 대변했으며, 이러한 규범 형성의 과정을 인터넷 분야의 이해당사자들이 주도해야 한다는 입장을 취해왔다. 특히 네덜란드는 사이버 안보 분야에서 민관협력을 강조하는 대표적인 나라로 알려져 있다.

네덜란드는 영국과 헝가리, 한국에 이어 2015년에 제4차 사이버공간총회를 헤이그에서 개최한 바 있다. '런던 프로세스'로 불리는 사이버공간총회는 사이버 안보의 직접적인 이해당사국의 정부 대표들이 나서 사이버 공간이라는 포괄적 의제를 명시적으로 내건 본격적인 논의의 장을 출현시켰다는 의미를 가진다. 이러한 사이버공간총회는 서방 국가들이 표방하는 이른바 '다중이해당사자주의'(multistakeholderism)를 대변하는데, 이는 러시아와 중국을 중심

28 양정윤, "중견국의 사이버 안보 전략 연구: 네덜란드의 규범외교 사례를 중심으로." 한국국제정치학회 연례학술대회 발표논문 (2018).

으로 한 비서방 진영이 주도하는 국가 행위자 주도의 접근, 즉 '국가간 다자주의'(multilateralism)와 대비된다. 이러한 서방과 비서방 진영의 경쟁 구도는 2010년대 초반 무렵부터 구체화되며 각기 상이한 국제규범을 모색하고 있는데, 네덜란드는 서방 진영의 담론 형성을 중개하는 허브의 역할을 자처하고 있다.

제4차 헤이그 총회의 가장 큰 결실로는 42개의 정부와 국제기구 및 기업이 참여한 CFCE(Global Forum on Cyber Expertise)의 설립과 글로벌정보보호센터 지원 사업의 제안을 들 수 있다. 초기 런던 프로세스가 서방 진영의 청사진에 따라서 진행되었다면, 헤이그 총회 이후 네덜란드가 서방 진영의 구도 속에서도 나름대로의 주도권을 가지고 규범외교를 진행하는 모습이 나타났다. 런던 프로세스에서 만들어진 사이버공간총회의 포맷에 국제법과 다자외교를 중시하는 네덜란드의 색채가 가미되면서 '헤이그 프로세스'로 업그레이드되며 발전할 가능성을 내비쳤다는 평가를 받는 대목이다. 이밖에도 네덜란드는 유럽, 미국, 중동, 아시아, 아프리카 등의 30개국이 참여하는 정부간그룹인 자유온라인연합(Freedom Online Coalition, FOC)을 2011년 11월 헤이그에 창설한 바 있다. FOC는 자유로운 온라인을 기치로 내걸고 기본인권과 표현의 자유를 옹호하며 민주적 가치의 수호를 목적으로 한다.[29)]

네덜란드는 헤이그 프로세스의 추진을 통해서 (평화)국제법을 사이버 공간에 적용하는 데 앞장서겠다는 입장이다. 기본적으로 네덜란드가 취하는 접근법은 전쟁(국제)법의 관점에서 접근한 에스토니아의 기조와는 다소 차이가 있다. 이러한 네덜란드의 입장은 '탈린매뉴얼 2.0'의 발간을 후원하여, 세 차례에 걸쳐 매뉴얼 초안을 각국 정부에 회람하고 의견을 수렴하는 재검토 작업과정에서 드러났다.[30)]

29 양정윤 (2018), p.18.

30 ASSR Institute, "The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime." Center for International and European Law (2016); ASSR Institute, "The International Law of Peacetime Cyber Operations: The Hague Launch of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and a

'사이버전(cyber warfare)에 적용 가능한 국제법'을 논한 '탈린매뉴얼 1.0'과는 달리 '탈린매뉴얼 2.0'은 평시의 사이버 범죄까지도 포함하는 '사이버 작전(cyber operation)에 적용 가능한 국제법'을 논했다.[31] 이러한 헤이그 프로세스의 진행을 통해 네덜란드는 기존 에스토니아 소재 나토 CCDCOE를 중심으로 이루어졌던, 사이버 안보에 관한 국제법 규범 형성과정에 끼어들어 새로운 프레임을 제시하는 모습을 보여주었다.

3. 헬싱키 프로세스: 구성주의 지역협력체 모델

핀란드의 사이버 안보 전략은 국방이나 외교의 관점보다는 사회의 필수기능을 안전하게 유지한다는 포괄안보의 관점에서 접근한다. 이러한 비(非)정치적 접근은 유럽과 러시아 사이에서 핀란드가 차지하고 있는 구조적 상황에서 기인하는 바가 크다. 강대국 러시아를 마주보고 있는 지정학적 위치와 두 번의 전쟁을 통해 얻은 역사적 경험을 토대로 핀란드는 냉전시기 '친(親)소련의 중립정책'을 시행했다. 소련과의 갈등 상황을 피하고자 노력했던 핀란드의 중립정책은 유럽 국가들로부터 '핀란드화'(Finlandization)라는 비판과 비웃음을 사기도 하였다. 그러나 소련의 눈치를 보는 상황에서 나토와 유럽연합과의 협력은 어려웠다. 따라서 '핀란드화'라는 비판을 무마하기 위해 유엔 평화유지 활동에 참여하며 국가 브랜드 이미지 개선을 꾀해왔으며, 나토와는 위기관리 대응차원에서 협력하면서 유럽적 정체성을 유지하고자 했다.[32]

Panel Discussion." Center for International and European Law (2017).

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

32 김진호 · 강병철, "스웨덴과 핀란드의 중립화의 정치: 국제-지역-국내정치의 다이내믹스," 『유럽연구』 제25집 3호 (2007), pp.49-87; Ulrika Möller and Ulf Bjereld, "From Nordic Neutrals to Post-neutral Europeans: Differences in Finnish and Swedish Policy Transformation," *Cooperation and Conflict,* 45(4), (2010), pp.363-386; 안상욱, "핀란드 외교정책 변화: 러시

냉전이 종식되면서 이전보다 러시아의 위협을 덜 받는 상황이 되면서 핀란드는 좀 더 자유롭게 서방 국가들과의 안보 협력을 추진하게 되었다. 핀란드는 1995년 유럽연합에 가입하였으며, 1999년에는 유로화를 도입하였다. 소련 붕괴 이후 심각한 경제 위기를 겪었던 핀란드는 위기 타개책의 일환으로 유럽연합과의 관계 개선을 모색하게 되었다. 유럽연합 가입은 핀란드로 하여금 유럽연합의 CFSP(Common Foreign and Security Policy)를 준수할 의무를 발생시켰으며, 이러한 과정에서 핀란드는 점점 더 '유럽화'(Europinization)의 길을 걷게 되었다.[33] 핀란드는 나토의 회원국은 아니지만 1994년 '평화를 위한 동반자 관계'(Partner for Peace, PfP)'에 가입하였으며, 2014년 9월에는 나토와 협정 체결을 통해서 위기관리 활동을 벌이며 이미지 제고와 서방 국제기구와의 협력을 점차 증진시켰다.

이러한 핀란드의 전략은 사이버 안보 분야에도 반영되었다. 사실 핀란드는 노키아의 성공에서 보는 바와 같이 ICT분야에서 성공한 나라인데, 유럽연합 내에서 디지털 인프라가 발달한 대표적인 국가 중의 하나이다. 이러한 성과를 바탕으로 핀란드는 전통적인 비(非)나토 노선을 넘어서 나토 회원국들과의 양자간 파트너십을 늘려왔다. 핀란드는 아직까지도 나토에 참여하지 않고 있지만 나토와 다양한 모의훈련을 매년 수행하고 있다. 나토 CCDCOE는 2010년부터 매년 나토 회원국 및 파트너 국가와 함께 '락쉴드'(Locked Shields)라는 사이버 사고 대응 모의훈련을 실시하고 있는데, 2012년 이후 핀란드는 나토의 파트너로서 이 훈련에 참여하고 있다. 또한 나토는 회원국 및 파트너국의 사이버보안 전문가들과 '사이

아 의존성 약화를 중심으로." 『유럽연구』 제35집 4호 (2017), pp.65-88; 김인춘, "20세기 핀란드의 사회적 분리와 정치적 통합: '사회적인 것'의 민주주의적 구성과 '정치계획'," 『스칸디나비아연구』 20 (2017), pp.137-180.

33 Kristi Raik, "Renaissance of Realism, a New Stage of Europeanization, or Both? Estonia, Finland and EU Foreign Policy," *Cooperation and Conflict* 50-4 (2015), pp.440 - 456.

버 코얼리션'(Cyber Coalition)이라는 모의훈련도 매년 개최하고 있는데, 핀란드는 여기에도 참여하고 있다.[34]

이러한 행보는 구체적으로 유럽연합 차원에서 2017년 10월 헬싱키에 유럽하이브리드위협대응센터가 설립되면서도 나타났다. 하이브리드 위협이란 경제 · 산업 · 군사 및 정보 도메인 등 전방에 걸쳐서 일어날 수 있는 위협을 의미한다. 2017년 8월 스웨덴, 프랑스, 독일, 영국, 미국, 폴란드, 라트비아 및 리투아니아 등이 참여하여 헬싱키에 유럽하이브리드위협대응센터를 개설하는 양해각서에 서명하고, 10월에 개설하여 현재 헬싱키에서 운영 중이다. 이 센터를 통해 핀란드는 나토와 유럽연합 간의 협력을 더욱 강화하고 새로운 정보기구 설립 및 훈련 강화 등을 추진하고 있다. 그럼에도 핀란드가 취하고 있는 사이버 안보전략은 에스토니아와 같은 사이버 국방의 맥락이라기보다는 사이버 범죄나 기술 등 분야에서 유럽 국가들과 협력하는 형태로 나타났음에 주목할 필요가 있다.

이러한 과정에서 드러나는 핀란드의 사이버 안보 규범외교는 사이버 위협에 대응하는 범유럽 차원의 지역협력에 적극 참여하는 형태이다. 앞서 살펴본 바와 같이 핀란드는 냉전기 이래로 핀란드화의 오명을 씻는 국가 브랜드 이미지의 개선을 모색해 왔는데, 서방 국가와의 협력 강화는 물론 범유럽 차원의 포괄안보를 추구하는 과정에서 이른바 '헬싱키 프로세스'로 알려진 나름대로의 중립적 역할을 자처해 왔다. 핀란드는 냉전기인 1972년 미국과 캐나다를 포함한 35개 유럽국가들 간의 다자간 협상과정을 통해 산출된 1975년 헬싱키 의정서 체결과 CSCE(Conference on Security and Cooperation in Europe)로의 이행 과정에서 평화 조정의 중립허브 역할을 담당했었다.[35] 최근 핀란드는 사이버 안보 분야

34 홍지영, "중견국 외교로서의 핀란드 사이버 보안 전략 및 체계 분석," 한국국제정치학회 연례학술대회 발표논문 (2018), p.13.

35 홍기준, "헬싱키 프로세스의 경로창발성: 동북아에의 시사점."『유럽연구』제32집 1호 (2014), pp.109-132.

에서도 CSCE 과정에서 나타났던 또 다른 버전의 '중립적 역할'을 염두에 두는 것으로 평가할 수 있다.[36]

4. 제네바 프로세스: 범세계주의 평화윤리 모델

이상에서 살펴본 세 모델과는 달리, 제네바 프로세스는 중견국으로서 스위스가 주도하는 사이버 안보 분야의 규범외교를 의미하는 것은 아니다. 스위스가 명시적 역할을 한 것은 아니고, 다만 스위스(또는 제네바)가 지니는 중립국 이미지를 차용하여 진행되고 있는 일련의 규범외교를 제네바 프로세스라고 명명해 보았다. 특히 이는 마이크로소프트가 주창한 '디지털 제네바 협정'(Digital Geneva Convention)의 제안에서 착안했다. 2017년 2월 마이크로소프트의 브래드 스미스(Brad Smith) 사장은 미국 샌프란시스코에서 개최된 RSA 2017 컨퍼런스에서, 2차 대전 이후 전시에 민간인과 비전투원을 보호하기 위해서 1949년 서명된 제네바 협정과 스위스의 오래된 중립의 전통에서 영감을 받아 국가지원 사이버 공격으로부터 민간인을 보호하기 위한 목적으로 디지털 제네바 협정을 제안하였다.[37]

36 소련을 위시한 동유럽 국가들이 참여했던 1970년대의 헬싱키 프로세스 모델과는 달리, 2010년대의 모델은 러시아의 사이버 공격에 대한 대응을 전제로 한다는 점에서 차이가 있다. 다시 말해, 1975년 채택된 헬싱키 의정서의 경우, 유럽에서 핵전쟁이 일어나면 동서유럽 모두 공멸한다는 위협인식 하에 북유럽 중립국인 핀란드의 주도로 서유럽의 나토진영 국가들과 소련을 위시한 동유럽의 바르샤바조약기구 참가국들이 모두 당사국으로 참여하였으며, 이에 따라 공동안보의 인식에 입각한 다자안보협의체인 CSCE가 결성되었다. 이러한 시각에서 보면, 러시아가 불참하고 대부분의 회원국이 나토 진영 국가들인 유럽하이브리드위협대응센터가 2017년 헬싱키에 설립되었다고 해서 이것을 디지털 시대의 CSCE 또는 구성주의에 의한 범유럽 차원의 지역안보협력기구의 모색으로 보기에는 아직까지는 다소 조심스러운 부분이 있다. 그럼에도 이 글은 사이버 안보 분야에서 핀란드가 내보이고 있는 행보가 정치군사적 성격을 탈색하고 기술협력과 범죄예방과 관련된 범유럽 지역의 협력에 치중하고 있다는 점에서 향후 러시아까지도 포괄하는 '디지털 헬싱키 프로세스'의 가능성을 지니고 있다고 해석한다.

37 Microsoft, "A Digital Geneva Convention to Protect Cyberspace," Policy Paper, (2017); Maria Gurova, "The Proposed 'Digital Geneva' Convention: Towards an Inclusive Public–

스미스 사장은 민간 부문과 기반시설 같은 핵심 인프라를 겨냥한 사이버 공격을 하지 말아야 한다고 주장했다. 적십자와 국제원자력기구(IAEA)와 같은 역할을 수행하는 독립기구를 공공 · 민간 부문에 걸쳐 설립하여 사이버 위협에 대처하고 특정 공격이 발생하면 조사해서 증거를 확보 · 공유할 수 있어야 한다는 것이다. 특히 사이버 안보를 위해서 마이크로소프트 등 기술기업들의 역할이 중요하다고 강조했다. 스미스 사장은 "제4차 제네바 조약이 전시에 민간인을 보호하기 위해 적십자에 의존하는 것처럼, 국가 지원 사이버 공격으로부터 보호하기 위해서는 기술 부문의 적극적인 지원이 필요하다"고 강조했다. 그에 의하면, 민간 보안 기업들이 불법 사이버 공격 행위에 가담하지 말아야 할 뿐만 아니라 "중립국으로 자리한 스위스와 같은 역할을 해야 한다"는 것이다.[38]

최근 민간 보안 기업들은 사이버 공격으로부터 민간인을 보호하기 위한 공동행동에 실제로 나서고 있음에 주목할 필요가 있다. 2018년 4월 RSA 2018 컨퍼런스에서는 마이크로소프트, 페이스북, 시스코, 오라클 등 34개 주요 기업들은 사이버 공격으로부터 사용자를 보호하기 위한 '사이버안보기술협약(Cybersecurity Tech Accord)'에 서명했다. 마이크로소프트가 주도한 이 협약은 참여 기업들이 정부가 무고한 시민과 기업에게 사이버 공격을 가하지 못하도록 관련 국가와 협력하지 않는다는 원칙을 담았다. 사이버안보기술협약에 참여한 기업들은 "모든 사용자와 고객을 보호하고, 무고한 시민과 기업에 대한 사이버 공격을 반대하며, 사용자와 고객, 개발자가 사이버 보안을 강화할 수 있도록 지원하고, 사이버 보안을 강화하기 위해 같은 생각을 가진 그룹과 파트너가 된다"는 네 가지 원칙에 합의했다.[39]

Private Agreement on Cyberspace?" Geneva Centre for Security Policy(GCSP). No.4. (July, 2017).

38 Microsoft (2017); 『보안뉴스』 "마이크로소프트, 보안 업계에 '제네바 협약' 도입 주장." (2017. 2. 15).

39 『바이라인네트워크』, "사이버보안 위해 IT기업들이 뭉쳤다…'디지털제네바조약' 실현 첫 발." (2018. 4. 19).

이러한 민간 기업들의 노력은 스위스 다보스에서 열린 세계경제포럼(World Economic Forum, WEF) 또는 다보스 포럼으로도 이어졌다. 2018년 3월 세계경제포럼은 20여명의 직원을 고용하여 제네바에 글로벌사이버보안센터(GCCS, Global Centre for Cybersecurity)를 개소하고, 사이버 안보에 대처할 것임을 밝혔다.[40] GCCS는 정부와 기업, 국제기구가 함께 사이버 안보 문제를 해결하는 글로벌 플랫폼의 역할을 수행하며, 인터폴과도 협력한다. 사이버 공격은 혼자서 방어할 수 없는 형태로 변화했기 때문에 국제사회가 정보를 교환하고 협업하지 않으면 안 된다는 것이 GCCS 개소의 문제의식이다. GCCS는 그동안 세계경제포럼에서 다루었던 사이버 보안 이니셔티브를 통합하여, 사이버 모범 사례를 모은 독립 도서관을 설립하고, 사이버 안보 관련 지식을 널리 확산할 뿐만 아니라 각종 사이버 위협을 조기 경보하는 싱크탱크 역할 수행을 목표로 내세웠다.[41]

한편 2018년 11월에는 프랑스에서 열린 파리평화포럼에서 '사이버 공간의 신뢰와 안보를 위한 파리의 요구', 즉 '파리 콜'(Paris Call)이 발표되었다. 파리 콜에는 유럽연합 회원국 전체와 세계 주요국들이 참여했고, 218개 컴퓨터 관련 기업과 93개 시민단체도 참여했다. 그러나 미국, 러시아, 중국, 북한, 이스라엘 등 사이버 공격의 배후로 의심받는 국가들은 불참했다. 그럼에도 파리 콜 참여국과 기업 · 시민단체들은 앞으로 국가 지원 사이버 공격의 형태와 범위를 규정하고, 공격을 가한 상대국에 대한 반격 범위와 민간 피해의 최소화에 대한 방안을 수립할 계획이라고 밝혔다.[42] 파리 콜은 민간 기업들이 시작한 디지털 제네바 협정의 프로세스에 국가 행위자들이 동참하는 의미를 갖는다. 또한 그 발표과정에서 프랑스가 파리평화포럼과 인터넷 거버넌스 포럼(IGF) 활동의 일환으로 주도적 역할

40 『MK경제』, "다보스의 사이버 공격 경고…WEF, 연내 사이버보안센터 만든다." (2018. 1. 16).
41 『전자신문』, "WEF 사이버보안센터 3월 가동…사이버 위협 공동 대응." (2018. 1. 29).
42 『서울신문』, "미 · 러 · 北 빠진 채… 세계 51개국 '디지털 제네바협약' 합의." (2018. 11. 13).

을 담당하여 주목을 끌었다.[43]

Ⅳ. 네 가지 모델의 비교분석과 함의도출

1. 네 가지 모델의 비교분석

이상에서 살펴본 사이버 안보 분야 중견국 규범외교의 네 가지 프로세스는, 물론 그 내용은 모두 다르지만, 상호 대립 또는 경합하는 두 세력 사이에서 형성되는 구조적 딜레마(동시에 구조적 공백)를 배경으로 출발하였다. 에스토니아가 주도한 탈린 프로세스는 러시아와 나토 사이의 대립구도 속에서 생존과 번영의 전략을 모색하려는 약소국의 국가안보에 대한 관심에서 비롯되었다. 네덜란드가 주도한 헤이그 프로세스는 서방 진영과 비서방 진영의 경쟁구조 사이에 서방의 다자포럼외교를 주도하려는 상업국가의 관심사에서 추동되었다. 핀란드가 주도한 헬싱키 프로세스는 유럽 지역과 러시아 사이에서 새로운 정체성을 모색하는 '탈핀란드화'의 고충을 담고 있었다. 제네바 프로세스는 국가 행위자들이 벌이는 사이버 안보의 군사화 경쟁을 넘어서 사이버 공간에서 민간인의 안전을 확보하려는 민간 보안 기업들의 평화윤리 담론을 바탕에 깔고 있었다. 이러한 구조적 상황의 제약과 거기서 발생하는 차이는 구조적 공백을 공략하는 각 프로세스의 전략적 방향을 규정하였다.

무엇보다도 각 프로세스가 제시한 '프레임 짜기'의 성격을 다르게 규정하였다. 사실 각 프로세스는 사고와 행동의 플랫폼을 규정하는 이론적 기반과 안보관이 다르고, 이에 입각한 프레임의 설정이 달랐다. 탈린 프로세스는 지정학적 구조에

43 『엠아이앤뉴스』"정부, 사이버 보안원칙에 관한 국제협약 발표." (2018. 11. 20).

서 잉태되는 현실주의 발상과 국가안보 중심의 안보관을 바탕으로 사이버전에 대응하는 군사적 프레임을 제시하였다. 헤이그 프로세스는 글로벌 차원에서 형성되는 사회경제적 이익구조의 공백을 제도적 협력을 통해서 메우려는 자유주의 발상을 바탕으로 이해당사자들의 안전을 중시하며 정부간레짐을 구축하기 위한 외교적 프레임을 원용하였다. 헬싱키 프로세스는 글로벌 차원의 국가 브랜드를 다듬고 지역 차원의 정체성을 구성하려는 구성주의 발상에 입각해서 범유럽 차원의 포괄안보를 해치는 사이버 위협에 대응하는 실무협력의 프레임을 제시하였다. 제네바 프로세스는 사이버 공간의 군사적 편향성을 지적하고 인도주의적 중립성을 주창하는 범세계주의 발상과 세계사회의 안보관에 입각해서 전시 민간인 보호를 위한 평화윤리의 프레임을 제시하였다.

각기 상이한 프레임 짜기에 입각해서 진행된 각 프로세스의 '맺고 끊기' 전략이 상이하게 제시되고 있음은 물론이다. 특히 각국이 처한 구조적 위치에 따라서 끊기와 맺기를 수행하는 비대칭 관계조율 전략의 내용과 그 과정에서 담당할 중개자의 역할이 달랐다. 탈린 프로세스에서 나타난 에스토니아의 전략은 러시아를 방어하기 위해서 취한 나토 가입의 노력을 핵심으로 하며, 이 과정에서 나토 내 사이버 안보의 '동맹허브'를 추구했다. 헤이그 프로세스에서 나타나는 네덜란드의 전략은 비서방 진영에 대응하는 서방 진영 내 협력을 강화하는 동시에 서방 진영 내에서도 차별화된 접근을 모색하는 다자포럼외교의 '중개허브'를 모색했다. 헬싱키 프로세스에서 나타나는 핀란드의 전략은 핀란드화의 오명을 벗고 유럽국가의 정체성을 회복하는 과정에서 러시아와의 갈등을 피하기 위해 '비나토 유럽화'를 추구하는 '중립허브'를 지향했다. 제네바 프로세스의 과정에서 마이크로소프트로 대변되는 초국가적 민간 네트워크는 군사-민간 분리의 명분을 바탕으로 사이버 공간의 군사화 담론에 대항하여 민간인 보호를 위한 기술적십자형 '평화허브' 역할을 강조하였다.

각 프로세스가 동원하는 '내편 모으기'의 메커니즘도 구체적인 메커니즘과 추상적인 원칙이라는 점에서 각기 달랐는데, 동지그룹을 모으기 위한 사실상 네트워

크 구축이나 법률상의 기구설치 등에서 상이한 접근을 보였다. 탈린 프로세스의 내편 모으기 메커니즘은 주로 나토CCDCOE 활동을 중심으로 진행되었으며 나토 국가들의 반(反)러 동맹을 결속시키는 새로운 전쟁법 규범을 지향했다. 아울러 싸이콘(CyCon)과 같은 컨퍼런스의 개최도 큰 몫을 담당했다. 헤이그 프로세스는 사이버공간총회나 자유온라인연합(FOC) 등과 같은 다자포럼을 활용하여 서방 선진국 진영의 공조와 연대를 모색했다. 헬싱키 프로세스는 나토나 유럽연합 차원에서 진행되는 사이버 모의훈련 참여나 유럽하이브리드위협대응센터의 설립 등을 통한 지역차원의 협력을 지향했으며, 유엔 차원의 평화유지활동 참여로 국가 브랜드의 개선을 꾸준히 꾀했다. 제네바 프로세스는 민간 기업들의 '사이버안보 기술협약' 서명이나 세계경제포럼의 글로벌사이버보안센터(GCCS) 설치, 그리고 이른바 파리 콜 등과 같은 메커니즘을 활용하여 사이버 평화윤리의 담론을 전파함으로써 밑으로부터 세력을 규합하고자 했다.

이상에서 살펴본 네트워크 전략은 각기 상이한 '표준 세우기'를 지향했는데, 이는 사이버 안보 국제규범의 네 가지 상이한 모델로 나타났다. 탈린 프로세스는 기존의 전쟁법 규범을 사이버전에 적용하려했던 '탈린매뉴얼 1.0'에서 보는 바와 같이 이른바 사이버 정전론의 개념에 입각한 사이버 교전수칙의 수립을 목적으로 했다. 헤이그 프로세스는 사이버공간총회와 같은 정부간 다자포럼의 개최 및 참여 등을 통해서 사실상 협력의 레짐을 주도하고자 했는데 이는 '탈린매뉴얼 2.0의 회람과정에서도 나타났다. 헬싱키 프로세스는 유럽지역에서 진행되는 실무 협력 메커니즘의 구축 차원에서 CSCE와 같은 범유럽 지역안보협력체를 디지털 분야에서도 모색하는 데 앞장서는 모델이었다. 제네바 프로세스는 2차 대전 직후 체결된 제네바 협정과 같은 모델을 사이버 안보 분야에도 도입하여 초국가적 윤리 규범을 수립하려는 디지털 적십자모델이라고 할 수 있다. 이러한 네 가지 모델의 내용을 요약하면 〈도표-1〉과 같다.

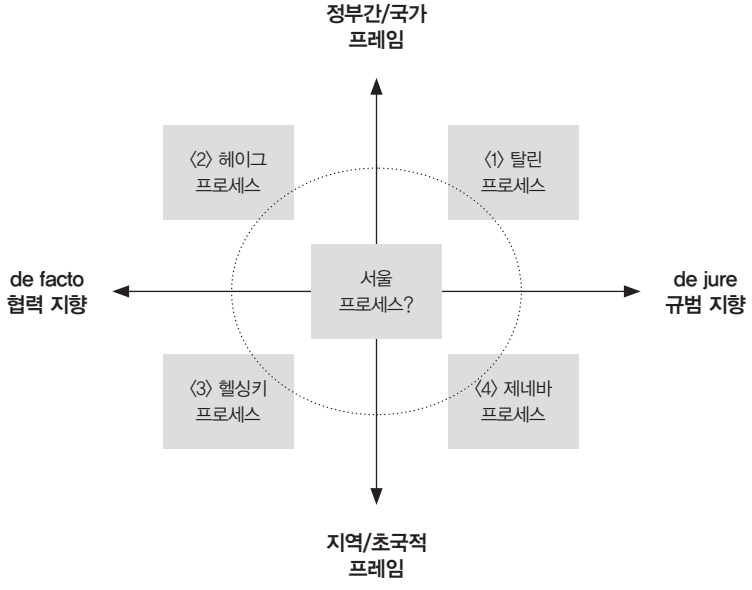
〈도표-1〉 중견국 규범외교의 네 가지 모델

	탈린 프로세스 (현실주의 국가동맹 모델)	헤이그 프로세스 (자유주의 정부간레짐 모델)	헬싱키 프로세스 (구성주의 지역협력체 모델)	제네바 프로세스 (범세계주의 평화윤리 모델)
구조적 상황	– 러시아 vs. 나토 – 약소국, ICT강국	– 서방 vs. 비서방 – 상업국가	– 유럽 vs. 러시아 – 탈핀란드화 정체성	– 국가 vs. 민간 – 초국가적 네트워크
프레임 짜기	– 현실주의 발상 – 국가 안보관 – 사이버전 대응의 군사 프레임	– 자유주의 발상 – 이해당사자 안전관 – 사이버 안보협력의 외교 프레임	– 구성주의 발상 – 범유럽 포괄안보관 – 사이버 위협대응의 실무협력 프레임	– 범세계주의 발상 – 세계사회 안보관 – 민간인 보호의 평화윤리 프레임
맺고 끊기	– 러시아 방어 위한 나토가입 – 나토 가입의 노력 – 사이버 안보의 동맹허브	– 친서방 확대를 통한 대(對) 비서방 – 서방진영내 차별화 – 다자포럼외교의 중개허브	– 러시아와의 갈등을 피하는 비(非)나토 유럽화 전략 – 디지털 탈핀란드화 중립허브	– 군사-민간의 분리 접근 – 초국적 민간협력 – 기술 적십자형 평화허브
내편 모으기	– 나토CCDCOE – 싸이콘(CyCon) – 반(反) 러시아 동맹의 결속	– 사이버공간총회 – 자유온라인연합 – 서방 선진국 진영의 연대	– 나토, EU 등과 사이버 모의훈련 – 유럽하이브리드위협 대응센터	– 사이버안보기술협약 – 다보스포럼 GCCS – 파리 콜
표준 세우기	– 탈린매뉴얼 1.0 – 사이버 정전론 – 사이버 교전수칙	– 탈린매뉴얼 2.0 – 이해당사국 포럼 – 정부간 다자레짐	– 범유럽 차원의 지역안보협력기구 – 디지털 시대 CSCE	– 디지털 제네바협정 – 디지털 적십자모델 – 초국가적 윤리규범

이 글은 중견국 규범외교의 네 가지 모델을 좀 더 체계적으로 비교하기 위해서, 〈그림-1〉에서 보는 바와 같이, 이상에서 살펴본 내용을 응축한 두 가지 잣대에 의거해서 유형을 구분하였다. 첫 번째 잣대는 각 모델이 처해 있는 구조적 상황과 거기서 비롯되는 프레임 짜기의 차이인데, 이는 각 프로세스가 설정한 프레임이 정부간/국가 프레임이냐 아니면 지역/초국적 프레임이냐에 따라서 구분된다. 이러한 프레임의 차이는 현실주의-자유주의-구성주의-범세계주의 발상의 스펙트럼을 타고 나타난다. 두 번째 잣대는 각 모델이 추구하는 네트워크 전략의 양상, 특히 맺고 끊기와 내편 모으기에서 나타나는 차이인데, 이는 각 프로세스가 채택한 전략이 사실상 협력 지향이냐, 아니면 법률상 규범 지향이냐에 따라서 구분된다. 이러한 전략적 지향성의 차이는 국가동맹-정부간포럼-지역협력체-초국적 네트워크 또는 국제법-다자레짐-지역정체성-윤리규범의 스펙트럼을 타고 나타난다.

이러한 두 가지 잣대로 적용하면, 〈그림-1〉에서 보는 바와 같은 네 가지 유형의 중견국 규범외교 모델을 설정해 볼 수 있다. 〈1-영역〉의 탈린 프로세스는 국가 프레임에 입각해서 법률상 규범을 지향하는 에스토니아 모델이다. 〈2-영역〉의 헤이그 프로세스는 정부간 프레임에 입각해서 사실상 협력을 지향하는 네덜란드 모델이다. 〈3-영역〉의 헬싱키 프로세스는 지역 프레임에 기초하여 사실상 협력을 지향하는 핀란드 모델이다. 〈4-영역〉의 제네바 프로세스는 초국적 프레임에 근거하여 법률상 규범을 지향하는 디지털 제네바 협정 모델이다. 이들 모델은 각기 다른 문제의식을 기반으로 하여 각각의 이익을 반영하고 있으며 각기 상이한 표준을 지향한다. 그러나 아직까지는 어느 것도 표준의 지위를 획득하지 못한 상태에서 규범경쟁을 벌이고 있는 상황이다. 그렇다면 이러한 네 가지 모델에 대한 고찰이 사이버 안보 분야에서 펼칠 한국의 중견국 규범외교, 이른바 '서울 프로세스'에 주는 함의는 무엇일까?

〈그림 1〉 중견국 규범외교의 유형구분



2. 서울 프로세스의 모색에 주는 함의

이상에서 살펴본 네 가지 사례의 비교분석이 주는 함의를 논하기 전에, 한국이 이상의 국가들과는 상이한 구조적 상황에 처해 있음을 명심해야 한다. 이들 국가에 비해서 한국의 사이버 안보 중견국 규범외교가 헤쳐 나가야 할 구조적 딜레마의 상황은 좀 더 복잡하다. 우선, 동북아 지역 차원에서 보면 한국은 패권경쟁을 벌이는 미국과 중국 사이에 놓여 있다. 이러한 미중경쟁은 최근 사이버 안보 분야에서도 치열하게 벌어지고 있다. 동아태 지역 차원에서 벌어지는 지역규범 모색에 있어서도 한국은 한미관계에 기반을 둔 미국 주도 아태동맹 정체성과 한중일과 아세안 지역협력을 기반으로 하는 동아시아 정체성 사이에서 껴 있는 양상이다. 또한 글로벌 차원에서도 한국은 서방 진영과 비서방 진영 사이에서 또는 선진국 진영과 개도국 진영 사이에 껴 있는 중견국의 신세이다.

이렇게 복합적으로 펼쳐지는 구조적 딜레마에 직면하여 한국은 한미동맹이냐 한중협력이냐, 아태 국가냐 동아시아 국가냐, 선진국 편이냐 개도국 편이냐 등의 선택을 요구받고 있다. 게다가 한국은 'ICT강국'으로서 역량은 있으면서도 사이버 공격에 대한 대비 정도는 상대적으로 낮은 나라이면서, 외부로부터의 사이버 위협은 상존하지만 법제도는 제대로 정비하지 못하는 나라라는 이중의 패러독스를 안고 있다. 이러한 상황에서 한국이 추구할 사이버 안보 중견국 외교의 방향은 어디인가? 예컨대, 만약에 '서울 프로세스'를 진행한다면, 프레임과 지향성의 잣대로 볼 때 한국 모델은 〈그림-1〉에서 어디에 위치시켜야 할까? 좀 더 구체적으로 서울 프로세스에 담길 내용은 무엇인가? 그리고 이상에서 살펴본 네 가지 프로세스가 주는 함의와 이를 실제로 한국의 사례에 적용할 경우 발생할 문제점은 무엇일까? 사실 이러한 문제제기는 지난 5-6년 동안 한국이 추구해온 사이버 안보전략의 고민과정에서 나타났으며, 앞으로의 전략 모색과정에서도 제기될 문제이기도 하다.

첫째, 에스토니아가 추진한 탈린 프로세스의 현실주의 처방이 한국에 주는 함

의는, 북한(또는 중국)의 사이버 위협이 엄존하는 상황에서 강대국 정치군사 동맹규범에 의지하는 모델이 가장 쉬운 처방임을 보여줬다는 데 있다. 이는 한미동맹의 강화나 미국이 주도하는 아태동맹, 한미일 협력, 또는 파이브 아이즈(Five Eyes) 네트워크 등에 적극적으로 편입하는 모델이다. 한국에 나토 CCDCOE와 같은 성격의 '아태 CCDCOE'를 설립하는 방안도 고려될 수 있다. 사실 한국이 외부로부터 당한 사이버 피해나 ICT강국으로서의 역량을 고려하면 충분히 추구해 봄직한 대안이며, 실제로 박근혜 정부 초반에 제기된 전략안이기도 하다. 그러나 이 모델은 한중관계의 특수성 때문에 현실적 대안이 되기는 쉽지 않다. 냉전 이후 러시아 변수가 에스토니아에 주는 의미와 최근 중국 변수가 한국에 주는 의미는 큰 차이가 있을 수밖에 없다. 사드(THAAD)의 한반도 배치 사태에서 경험한 바와 같이, 경제 분야에서 한중협력이 긴밀하게 진행되고 있는 상황에서 대미 편중의 노선은 한국에 예기치 않은 피해를 초래할 가능성이 있다. 이와 더불어 이 모델이 갖는 한계는 복합적인 네트워크 환경에서 사이버 정전론의 국제법적 적용과 같은 전통적인 발상이 얼마나 실효성이 있겠느냐는 의구심에서도 발견된다.[44]

둘째, 네덜란드가 추진한 헤이그 프로세스의 자유주의 처방이 한국에 주는 함의는, ICT 강국이자 서방 국가들과 활발한 온라인 · 오프라인 교역을 벌이고 있는 한국이 사이버 공간을 안전한 환경으로 만들기 위해 친서방 외교를 펼치는 데 참고가 되는 모델이라는 데 있다. 실제로 한국은 2013년 제3차 사이버공간총회를 개최한 바 있으며, OECD차원에서도 다양한 사이버 안보 분야의 협력을 주도한 바 있기 때문에, 이 모델의 적극적 채택을 통해서 동지국가들의 내편 모으기를 모색하고 선진국들의 자유주의적 규범을 확산하는 계기를 마련하는 효과가 있을 것이다. 그러나 외부로부터의 사이버 위협이 엄연히 존재하는 상황에서 한국에

44 Matt Sleat, "Just Cyber War?: *Casus belli*, Information Ethics, and the Human Perspective." *Review of International Studies* 44-2 (2017), pp.324 - 342.

게는 사이버 공간에서의 안전한 환경의 조성을 단순히 경제적 관심을 우선시하는 민간 주도 질서구축의 문제로만 볼 수 없는 속사정이 있다. 실제로 한국의 인터넷 및 사이버 안보 정책은 국가가 주도적인 역할을 담당했던 역사적 유산이 있어서 사이버 공간에서의 다중이해당사자들의 무제한적인 자유를 옹호하기에는 어려운 상황이 존재한다. 게다가 서방 진영이 표방하는 다중이해당사자주의 모델을 그대로 수용하기에는 국내적으로 한국의 민간 기업이나 시민사회의 역량이 얼마나 성숙했는가의 문제도 존재한다. 다중이해당사자주의가 한국과 같은 나라에는 이데올로기일 수도 있다는 비판이 나오는 것은 바로 이러한 이유 때문이다.

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

끝으로, 제네바 프로세스의 범세계주의 처방이 한국에 주는 함의는, 강대국들이 추구하는 힘의 논리에 기반을 둔 사이버 공간의 군사화 담론에 문제를 제기하

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

Ⅴ. 맺음말

이 글이 다룬 사이버 안보 분야의 중견국 규범외교 연구는 21세기 세계정치에서 국제규범의 중요성에 대한 인식을 바탕에 깔고 있다. 강대국이 만드는 '힘의 규범'에 대한 논의를 넘어서 비강대국도 의지할 수 있는 '규범의 힘'에 대한 기대가 늘어났다. 국제정치학에서 국제규범을 보는 이론적 시각은 명분과 제도 그리고 정체성과 윤리 등에 이르기까지 다양하게 나타난다. 물론 21세기 세계정치에서도 물리적 힘의 행사는 사라지지 않겠지만, 이를 넘어서는 국제규범이라는 변수에 대한 관심은 계속 늘어날 것이다. 특히 국제정치의 전통무대보다는 미래 세계정치의 신흥무대에서 국제규범의 존재감은 더 두드러질 것으로 예견된다. 이 글에서 다룬 사이버 안보는 그 대표적인 사례 중의 하나이다. 무엇보다도 이 분야

국제규범의 형성과정에서는 강대국의 힘의 논리만이 아닌 중견국의 규범외교가 주목을 받고 있다.

이러한 인식을 바탕으로 이 글은 사이버 안보 분야에서 발견되는 중견국 규범외교의 네 가지 모델을 이론적 시각에서 비교분석하였다. 특히 이 글은 네트워크 세계정치이론의 시각을 원용하여 체계적인 개념화를 시도하였다. 복합적인 구조적 상황 아래에서 각 행위자가 차지하는 위치에 대한 논의에서부터 시작해서 그 구조의 공백을 공략하는 행위자들의 전략을 구체적으로 비교분석하기 위해서 네트워크 이론의 개념적 자원들을 활용하였다. 이를 통해서 이 글이 발굴하고 개념화한, 중견국 규범외교의 네 가지 모델은 에스토니아가 주도하는 현실주의 국가동맹 모델로서의 탈린 프로세스, 네덜란드가 주도하는 자유주의 정부간레짐 모델로서의 헤이그 프로세스, 핀란드가 주도하는 구성주의 지역협력체 모델로서의 헬싱키 프로세스, 그리고 스위스의 중립국 이미지를 차용하여 마이크로소프트가 제안한 범세계주의 윤리규범 모델로서의 제네바 프로세스 등이다.

이러한 네 가지 모델의 개념화는 다소 도식적으로 보일 수도 있지만, 그 유형구분의 국제정치학적 유용성은 매우 크다. 무엇보다도 이들 네 가지 모델은 각기 다른 이론적 기반을 바탕으로 한 실천적 처방의 시나리오를 담고 있다는 점에서 사이버 안보 분야에서 나타날 수 있는 중견국 규범외교의 스펙트럼 전반을 보여준다. 또한 이들 네 가지 모델은 최근 사이버 안보 분야에서 새로운 역할을 모색하고 있는 한국의 중견국 규범외교, 즉 서울 프로세스의 모델에 주는 시사점이 크다. 실제로 각 모델이 담고 있는 전략적 요소들이 한국의 사이버 안보전략 모색의 과정에서 일부 나타나기도 했었다. 그러나 이 글에서 비교분석한 네 가지 모델은 그 자체로는 어느 것도 서울 프로세스가 벤치마킹할 대상은 아니며, 다만 서울 프로세스의 모델을 개발하는 데 유용한 힌트를 제공할 뿐이다. 결국 서울 프로세스는 이들 네 가지 모델의 다양한 요소들을 한국의 상황에 복합적으로 응용하는 과정에서 개발될 것이다.

이상의 내용을 종합해서 볼 때, 한국이 추구할 중견국 규범외교의 모델로서 '서

울 프로세스'는, 이상의 네 가지 모델 중에서 어느 하나를 선택하기보다는, 각 모델이 지니고 있는 유용한 요소들을 추출하여 복합적으로 구성한 모델일 가능성이 크다. 예를 들어, 서울 프로세스 발상은 현실주의, 자유주의, 구성주의, 범세계주의 중에서 어느 하나에만 근거할 수는 없다. 맺고 끊기를 추구하는 관계조율의 전략도 동맹허브, 중개허브, 중립허브, 평화허브 등을 포괄하는 복합 기능허브이어야 한다. 내편 모으기의 메커니즘도 동맹국가, 선진국정부, 동아시아 이웃국가, 글로벌 시민사회 등을 모두 대상으로 진행되어야 할 것이다. 결국 서울 프로세스 모델은 동맹규범 모델이며 협력레짐 모델이고 지역협력 모델이며 초국적 윤리담론 모델을 모두 포괄하는 '메타규범 모델'이어야 한다. 이러한 서울 프로세스 모델을 〈그림-1〉에 자리매김한다면, 아마도 그 한복판에 위치지울 수 있을 것이다.

그러나 이러한 '메타규범 모델'에 대한 논의는 한국이 추구할 전략의 방향성을 제시하는 데는 유용하지만, 그 내용적 요소들을 충분히 제시하지 못하는 한계를 안고 있다. 이 지점에서 이 글에서 수행한 사이버 안보 분야 중견국 규범외교 연구의 향후 과제가 제기된다. 다시 말해, 이 글에서 서울 프로세스가 지향할 모델로서 제시한 '메타규범 모델'의 형성 조건과 내용 및 구체적인 정책방안에 대한 좀 더 구체적인 연구가 필요하다. 사실 실천적 정책을 수립하는 관점에서 볼 때 '메타 모델'이라는 개념적 범주의 설정은 다소 막연하게 들릴 수도 있다. 구체적으로 발생하는 구조적 상황에 맞추어 그 대응 모델의 내용을 채우고 실제로 실천하는 데 원용할 수 있는 정책방안에 대한 논의를 도출할 수 있어야 할 것이다. 한국 모델이 '서울 프로세스'가 되기 위해서는 '형식'뿐만 아니라 '내용'을 제시하는 노력이 수반되어야 한다.

요컨대, 최근 사이버 안보 분야에서는, 기존 국제정치의 규칙 하에서 자국의 이익을 추구하는 단순경쟁이 아니라, 게임의 규칙 자체를 자신들에게 유리하게 설정하려는 복합경쟁이 벌어지고 있다. 이 글에서 다룬 중견국 규범외교는 이러한 복합경쟁으로서 규범경쟁 또는 프레임 경쟁이 진행되고 있음을 보여주는 사례이다. 중견국의 입장에서 이러한 규범경쟁에서 뒤지지 않고 적응하기 위해서는, 전

통적인 국민국가나 동맹의 프레임에만 갇혀 있어서는 안 되며, 좀 더 복합적인 프레임에서 규범형성의 양상을 이해하고 대응하려는 노력이 필요하다. 아울러 새로운 프레임을 수용하기 위한 인식론적 발상 전환도 병행되어야 할 것이다. 이러한 맥락에서 볼 때, 이 글에서 살펴본 네 가지 모델은 한국이 이러한 복합적인 프레임을 개발하는 데 큰 시사점을 주는 사례가 아닐 수 없다.

참고문헌

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

_____. 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 파주: 한울, 2018.

김인춘. "20세기 핀란드의 사회적 분리와 정치적 통합: '사회적인 것'의 민주주의적 구성과 '정치계획'," 『스칸디나비아연구』 20 (2017), pp.137-180.

김진호 · 강병철. "스웨덴과 핀란드의 중립화의 정치: 국제-지역-국내정치의 다이내믹스," 『유럽연구』 제25집 3호 (2007), pp.49-87.

레이코프, 조지(Lakoff, George). 『프레임 전쟁: 보수에 맞서는 진보의 성공전략』 서울: 창비, 2007.

『바이라인네트워크』, "사이버보안 위해 IT기업들이 뭉쳤다…'디지털제네바조약' 실현 첫 발." (2018. 4. 19).

『보안뉴스』, "마이크로소프트, 보안 업계에 '제네바 협약' 도입 주장." (2017. 2. 15).

샵콧, 리처드(Shapcott, Richard). "국제윤리." 존 베일리스, 스티브 스미스, 퍼트리샤 오언스 편. 『세계정치론』 서울: 을유문화사, 2015, pp.271-289.

『서울신문』, "미 · 러 · 北 빠진 채… 세계 51개국 '디지털 제네바협약' 합의." (2018. 11. 13).

쉬만스카, 알리나. "구소련의 약소국에서 유럽 규범의 주도국으로 진화: 에스토니아의 사이버 안보 중견국 외교 중심으로." 한국국제정치학회 연례학술대회 발표논문. (2018).

안상욱. "핀란드 외교정책 변화: 러시아 의존성 약화를 중심으로." 『유럽연구』 제35집 4호 (2017), pp.65-88.

양정윤. "중견국의 사이버 안보 전략 연구: 네덜란드의 규범외교 사례를 중심으로." 한국국제정치학회 연례학술대회 발표논문, (2018).

『엠아이앤뉴스』, "정부, 사이버 보안원칙에 관한 국제협약 발표." (2018. 11. 20).
『전자신문』, "WEF 사이버보안센터 3월 가동...사이버 위협 공동 대응." (2018. 1. 29).
전재성. "동아시아의 복합네트워크 규범론과 한국 전략의 규범적 기초." 하영선 · 김상배. 편. 『복합세계정치론: 전략과 원리, 그리고 새로운 질서』 파주: 한울, 2012, pp.310-340.
하영선 · 김상배 편, 『네트워크 지식국가: 21세기 세계정치의 변환』 서울: 을유문화사, 2006.
홍기준. "헬싱키 프로세스의 경로창발성: 동북아에의 시사점." 『유럽연구』 제32집 1호 (2014), pp.109-132.
홍지영. "중견국 외교로서의 핀란드 사이버 보안 전략 및 체계 분석." 한국국제정치학회 연례학술대회 발표논문. (2018).
『MK경제』, "다보스의 사이버 공격 경고…WEF, 연내 사이버보안센터 만든다." (2018. 1. 16).
ASSR Institute, "The International Law of Peacetime Cyber Operations: The Hague Launch of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and a Panel Discussion." Center for International and European Law. (2017).
_____. "The Tallinn Manual 2.0 and The Hague Process: From Cyber Warfare to Peacetime Regime." Center for International and European Law. (2016).
Burt, Ronald S., Structural Holes: *The Social Structure of Competition.* Cambridge, MA: Harvard University Press, 1992.
Burton, Joe. "Small States and Cyber Security: The Case of New Zealand," *Political Science* 65-2 (2013), pp.216-238.
Callon, Michel. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay." in John Law ed. *Power, Action and Belief: A New Sociology of Knowledge.* London: Routledge and Kegan Paul, 1986, pp.196-233
Carnoy, Martin, and Manuel Castells. "Globalization, the Knowledge Society, and the Network State: Poulantzas at the Millennium." *Global Networks* 1-1 (2001), pp.1-18.
Claver, Alexander. "Governance of Cyber Warfare in the Netherlands: an Exploratory Investigation," *The International Journal of Intelligence, Security, and Public Affairs* 20-2 (2018), pp.155-180.

Crandall, Matthew and Collin Allan. "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." *Contemporary Security Policy* 36-2 (2015), pp.346-368.

Crandall, Matthew. "Soft Security Threats and Small States: the Case of Estonia." *Defence Studies* 14-1 (2014), pp.30-55.

Czosseck, Christian, Rain Ottis and Anna-Maria Taliharm. "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *International Journal of Cyber Warfare and Terrorism* 1-1 (2011), pp.24-34.

Ebert, Hannes, and Tim Maurer. "Contested Cyberspace and Rising Powers." *Third World Quarterly* 34-6 (2013), pp.1054 - 1074.

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

Górka, Marek. "The Cybersecurity Strategy of the Visegrad Group," *Politics in Central Europe* 14-2 (2018), pp.75-98.

Gurova, Maria. "The Proposed 'Digital Geneva' Convention: Towards an Inclusive Public-Private Agreement on Cyberspace?" Geneva Centre for Security Policy(GCSP). No.4, (July, 2017).

Kaljurand, Riina. "Security Challenges of a Small State: The Case of Estonia." in Raimonds Rublovskis, Margarita Šešelgyte and Riina Kaljurand. *Defence and Security for The Small: Perspectives from the Baltic States.* Centre for Small State Studies Institute of International Affairs, (2013), pp.55 - 81.

Kim, Sangbae. "Cyber Security and Middle Power Diplomacy: A Network Perspective." *Korean Journal of International Studies* 12-2 (2014), pp.323-352.

Männik, Erik. "Small States: Invited to NATO-Able to Contribute?" *Defense & Security Analysis* 20-1 (2004), pp.21 - 37.

Microsoft. "A Digital Geneva Convention to Protect Cyberspace." Policy Paper. (2017).

Möller, Ulrika and Ulf Bjereld. "From Nordic Neutrals to Post-neutral Europeans: Differences in Finnish and Swedish Policy Transformation," *Cooperation and Conflict,* 45(4), (2010), pp.363-386.

Noreen, Eric and Roxana Sjöstedt. "Estonian Identity Formations and Threat Framing in the Post-Cold War Era." *Journal of Peace Research* 41-6 (2004), pp.733 - 750.

Pernik, Piret. *Preparing for Cyber Conflict Case Studies of Cyber Command.* International Centre for Defence and Security Report. (December, 2018).

Praks, Henric. "Estonia's First Steps in the Direction of NATO and National Defence," *Estonian Yearbook of Military History* 4 (2014), pp.113-140.

Raik, Kristi. "Renaissance of Realism, a New Stage of Europeanization, or Both? Estonia, Finland and EU Foreign Policy." *Cooperation and Conflict* 50-4 (2015), pp.440 - 456.

Runnel, Pille, Pille Pruulmann-Vengerfeldt and Kristina Reinsalu. "The Estonian Tiger Leap from Post-Communism to the Information Society: From Policy to Practice," *Journal of Baltic Studies* 40-1, (2009), pp.29-51.

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

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

Sleat, Matt. "Just Cyber War?: Casus belli, Information Ethics, and the Human Perspective." *Review of International Studies* 44-2 (2017), pp.324 - 342.

Smith, Frank and Graham Ingram. "Organising Cyber Security in Australia and Beyond," *Australian Journal of International Affairs* 71-6 (2017), pp.642-660.

Van der Meer, Sico. "Medium-sized States in International Cyber Security Policies." Clingendael, Netherlands Institute of International Relations. (2016).

Cyber Security and Normative Diplomacy of Middle Powers : Reflections of Four Models from the Perspective of International Relations

Sangbae Kim | Seoul National University

Recently, cyber security has become a major issue of world politics in the 21st century. Countries around the world are developing strategies for responding to cyber threats, cooperating with neighboring countries, and participating in creating international norms for cyber security. Based on these perceptions, this paper examines four models of normative diplomacy in middle powers found in the arena of cyber security from the perspective of International Relations. In particular, relying on the Network Theory of World Politics, this paper conceptualizes four models of middle power's normative diplomacy for cyber security, and attempts a systematic comparative analysis: the "Tallinn Process" as a national alliance model led by Estonia, the "Hague Process" as an inter-governmental regime model led by the Netherlands, the "Helsinki Process" as a regional cooperation model led by Finland, and the "Geneva Process" as a peace-ethics model proposed by Microsoft utilizing the neutrality image of Switzerland. These four models have implications for showing the overall spectrum of international norms from the perspective of International Relations theories, each represented by realism, liberalism, constructivism and cosmopolitanism. These models also have significant implications for developing the "Seoul Process" as a South Korea's model of normative diplomacy in the cyber security arena.

투고일: 2019년 3월 31일 | 심사일: 2019년 4월 15일 | 심사완료일: 2019년 5월 20일