사이버 안보의 국가전략 2.0:
국제규범의 형성과 국제관계의 동학

사이버 안보의 국가전략 2.0:
국제규범의 형성과 국제관계의 동학

2019년 3월 20일 초판 1쇄 인쇄
2019년 3월 29일 초판 1쇄 발행

지은이 김상배, 김소정, 김규동, 정태진, 유인태,
차정미, 이승주, 윤민우, 양정윤, 유지연

편집 김천희
디자인 김진운
마케팅 최민규

펴낸이 윤철호·김천희
펴낸곳 ㈜사회평론아카데미
등록번호 2013-000247(2013년 8월 23일)
전화 02-2191-1133
팩스 02-326-1626
주소 03978 서울특별시 마포구 월드컵북로12길 17

이메일 editor@sapyoung.com
홈페이지 www.sapyoung.com
ISBN 979-11-00000-00000

사이버 안보의 국가전략 2.0:
국제규범의 형성과 국제관계의 동학

김상배 엮음

사회평론아카데미

* 이 저서는 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구입니다 (NRF-2016S1A3A2924409). 이 저서는 2017-2018년도 서울대학교 국제문제연구소의 지원으로 연구를 수행하였습니다. 이 저서는 2018년도 ETRI 부설연구소의 지원을 받아 연구되었습니다.

책머리에

이 책은 2017년 5월에 출간된『사이버 안보의 국가전략: 국제정치학의 시각』의 후속작이다. 2016년 여름 방학을 전후로 시작해 1년여 동안 진행되었던 사이버 안보의 국가전략 연구의 첫 번째 버전은, 사이버 안보 세계정치 일반의 변화를 국제정치학의 시각에서 파악하고, 기술개발이나 인력양성, 법제도 정비의 차원을 넘어서 국제협력과 국제규범 참여전략까지도 포함하는 미래 국가전략 전반을 담아낼 플랫폼의 마련을 목적으로 했었다. 그 이후 어언 2년여의 시간이 지난 지금『사이버 안보의 국가전략 2.0: 국제규범의 형성과 국제관계의 동학』이라는 제목을 달고 두 번째 버전을 내게 되었다.

이 책에 굳이 '웹 2.0'을 연상시키는 '2.0'이라고 제목 붙인 이유는 단순히 두 번째 책이라는 의미를 넘어선다. 무엇보다도 이 책은 '사이버 안보의 국가전략 2.0'을 요구하는 질적 변화의 모멘텀이 2017년 미국 트럼프 행정부의 출범 이후 발생하고 있다는 인식을 바탕에 깔고 있다. 최근 사이버 공격이 양적으로 늘어나는 가운데, 그 목적과 수법

이 다양화되는 질적 변화를 보이고 있다. 게다가 최근 사이버 안보는 단순한 해킹 공격의 문제를 넘어서 통상마찰, 데이터 안보, 심리전 등과 같은 여타 쟁점들과 연계되고 있다. 더 나아가 사이버 안보는 강대국들이 벌이는 지정학적 갈등의 조짐마저도 보이고 있다. 그야말로 이전과는 질적으로 다른 새로운 대응전략을 요구하는 환경의 변화가 발생하고 있다.

이러한 맥락에서 이 책의 필자들은 첫 번째 버전과는 다른 '사이버 안보의 국가전략 2.0'의 배경과 내용을 다음과 같은 세 가지 차원에서 주목하였다. 첫째, 단편적으로 국제규범을 소개했던 '1.0'과는 달리, '2.0'은 '국가 간', '정부 간', '거버넌스' 등의 세 층위 프레임 내에서뿐만 아니라 이들 프레임들을 가로질러 진행되는 규범경쟁의 복합성에 주목했다. 다시 말해, 각각의 '프레임 내(inner-frame) 경쟁'뿐만 아니라 '프레임 간(inter-frame) 경쟁'의 시각에서 사이버 안보 분야 국제규범 형성의 세계정치를 살펴보았다. 이러한 분석이 한국의 전략에 주는 함의는 단순한 국제규범 참여전략에서 더 나아가, 이 분야 국제규범의 구조적 성격을 파악하고, 그 구조 내에서 한국이 차지하는 '구조적 위치'를 읽어냄으로써 중견국으로서 한국의 역할을 모색한다는 데서 찾을 수 있다.

둘째, 한반도 주변4개국과 남북한이라는 '행위자'의 국내체제와 전략의 분석에 머물렀던 '1.0'과는 달리, '2.0'은 이들 국가들의 양자 및 다자 관계가 형성하는 복합적인 관계구도에 주목했다. 미중관계, 미일관계, 미러관계, 중러관계 등이 글로벌 차원과 동북아에서 창출하는, 이른바 주변4망(網)의 지정학적 경쟁구도를 이해하는 것은 매우 중요한 국가전략의 사안이다. 또한 사이버 안보 문제를 둘러싼 미중합의나 중러협약, 미일동맹 등과 같은 당사자 합의나 동맹, 그리고 유사

한 입장을 취하거나 지리적으로 인접한 국가들의 국제적 공조의 형성도 진지하게 고려할 사안이 아닐 수 없다. 이렇게 강대국들이 벌이는 경쟁과 협력의 관계구도를 분석하는 작업이 한국의 전략에 주는 함의는, 일종의 '구조적 공백'을 찾아서 그 빈틈을 공략하는 중견국 외교전략을 모색한다는 데서 찾을 수 있다.

끝으로, 이러한 국제규범의 형성과 국제관계의 구조를 주도하는 강대국들의 전략에 주목했던 '1.0'과는 달리, '2.0'은 이러한 구조의 영향을 받는 중견국의 시각에서 접근하고자 했다. 사이버 안보 분야의 국제규범 형성과 국제관계 동학의 구조적 조건을 파악하고 이를 활용하는 전략을 세우는 것은 모든 나라에게 중요한 일임이 분명하다. 그러나 특히 이러한 구조의 영향 아래 있는 한국과 같은 중견국에게는 더욱 절박한 문제가 아닐 수 없다. 이 책의 작업이 사이버 안보 분야에서 추구되는 한국의 미래 국가전략에 던지는 새로운 의미는 바로 이 지점에서 발견된다. 또한 이러한 문제의식은 이 책 이후를 염두에 두고 진행되고 있는 '사이버 안보의 국가전략 3.0' 작업의 주제와도 밀접히 연결된다.

* * * * *

제1부 '사이버 안보 국제규범의 형성'에는 사이버 안보 분야에서 형성되는 국제규범과 이에 대응하는 한국의 전략에 대한 고민을 담은 다섯 편의 논문을 담았다.

제1장은 사이버 안보의 국제규범과 한국외교의 문제를 주요국 이해갈등의 프레임 경쟁이라는 시각에서 살펴보았다. 제1장은 최근 국제정치학의 논제로 주목을 받고 있는 사이버 안보가 그 성격상 일국

차원을 넘어서 이해해야 하는 초국적인 성격을 지닌 문제라는 지적에서 출발한다. 사이버 위협정보를 공유하는 주변국들과의 협력과 글로벌 및 지역 차원의 규범 마련을 위한 외교적 노력이 국내적 차원의 기술역량 강화와 법제도 정비에 못지않게 중요한 문제이다. 그럼에도 아직까지 사이버 안보의 규범에 대한 국제적 합의는 마련되지 않았으며, 오히려 최근에는 더 복잡해지는 양상마저 드러내고 있다. 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 제1장은 '프레임(frame)'의 시각을 사이버 안보의 사례에 적용하여 현재 국제규범의 형성 과정에 동원되는 프레임을 세 가지 차원에서 이해했다. 첫째, '국가 간(inter-national)' 프레임인데, 이는 전쟁법과 같은 국제법을 원용하거나 유엔과 같은 전통 국제기구 모델을 원형으로 한다. 둘째, '정부 간(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 민간기업, 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.

제2장은 사이버 공간의 규범 형성을 위한 유엔의 노력을 살펴보

았다. 제2장은 사이버 공간의 규범 형성을 놓고 국가행위를 규율하고자 하는 각국의 노력이 점점 더 치열해지고 있는 현상에 착목한다. 2013년 제3차 GGE에서 합의한 "오프라인의 국제법이 온라인에도 적용되며, 동일하게 국가주권이 사이버에도 적용된다"는 원칙 합의 이후, 이러한 원칙을 적용할 수 있는 구체적인 규범, 신뢰구축조치 등이 논의되었음에도 불구하고 국제법의 적용방법에 있어 국가 간 이견은 좁혀지지 못한 상황이다. 이러한 상황에서 각국과 각 진영은 국제법의 적용, 보편타당한 적용 가능성을 가진 비강제적·자발적 규범의 형성, 신뢰구축조치의 개발 및 이행, 논의 참여주체의 확장성에 대한 이견 등을 지역별·이슈별·플랫폼별 차별적으로 대응하고 각자의 주장을 강화하고 있다. 그럼에도 불구하고 즉시 적용 가능한 국제사회의 합의 추구는 요원해 보이며, 오히려 대내적으로 구체화된 사례를 통한 공격 행위자 지목, 기소, 제재조치 수행 등을 위한 근거를 마련해 나가고 있다. 그리고 특정 분야에 있어서는 대상국가 간 양자 혹은 소다자 협의를 통해 직접 해결을 위한 규범 마련에 나서고 있다. 사이버는 더 이상 특정 기술의 적용영역으로만 이해되어서는 안 된다. IT 기술을 활용하기 위한 인프라적 측면, 이를 이용해 유통되는 정보, 이를 통해 구성되는 공간으로서의 측면을 모두 고려해야만 한다. 사이버 공간 안전보장은 대외적으로는 다층화된 규범 형성 노력에 대한 이해, 행위자 다변화에 따른 논의 제기의 배경 이해, 국제안보 맥락에서 주요국 정책수행 배경에 대한 이해를 향상시키고 대내적으로는 쟁점에 대한 이해도를 높이고 실제 위정자들이 참고할 수 있는 양질의 사이버 안보 관련 정책판단자료 및 분석결과를 만들어낼 수 있어야 확보될 수 있다. 제2장에서는 사이버 공간에서 규범이 갖는 의미와 국제규범 형성을 위한 유엔의 노력을 되짚어 보고, 국제규범 형성 방향을 전망해보고자 한

다. 이를 통해 한국이 앞으로 취해야 할 입장과 고려해야 할 사항들을 정책제안 하였다.

제3장은 국제사이버법에 관한 경쟁을 탈린매뉴얼의 사례를 중심으로 다루었다. 제3장에서는 사이버 공간을 둘러싼 다양한 측면에서의 규범경쟁 중, 기존에 모든 국가를 구속하고 있던 국제법이 적용되는 방식을 둘러싼 쟁점을 다룬다. 지난 20여 년의 다자간 논의로 사이버 공간에서의 '법의 지배'에 대한 국제사회의 공감대가 형성되었으나, 2015년을 전후하여 그 이후 구체적 내용상의 발전은 답보 상태에 있다. 기존 국제법의 적용범위와 방식, 새로운 법규범의 필요성에 대한 진영 간 입장차를 좁히지 못하고 있기 때문이다. 제3장에서는 이러한 교착의 원인을 정확한 법적 분석을 바탕으로 한 논의의 부재에서 찾는다. 특히 일부 국가들이 규범의 불확실성을 사이버 공간 활용의 기회로 이용하거나, 동시에 기존 국제질서의 구도를 변화시키거나 강화하는 데 이용하고자 하는 정치적 의도의 대립이 존재하며, 한국을 비롯한 다수 국가가 국제사이버법 논의의 복합성과 상호연계성으로 인하여 적극적인 입장을 수립, 표명하지 못하다고 있다는 분석을 제시한다. 이 과정에서 사이버 작업에 대한 현행 국제법 적용방법을 분석한 『탈린매뉴얼 2.0』의 작성 과정과 그 의의를 살핀다. 현재의 규범적 불명성을 해소하기 위한 방법에 대해서도 진영 간의 대립이 이어지고 있는바, 결론적으로 국제법의 쟁점에 대한 논의의 다음 단계로 나아가기 위해서는 현행 국제법 규칙에 대한 정확한 평가와 분석이 불가피하며, 이를 바탕으로 각 국가가 입장을 정하고 실행에 옮기는 것만이 사이버 공간의 평화와 안전을 증대하는 데 규범이 기여할 수 있는 방안이라는 점을 제시한다. 이 과정에서 개별 국가들이 『탈린매뉴얼』과 같은 연구결과의 활용 방안을 제시한다.

제4장은 유럽사이버범죄협약의 사례를 통해서 사이버 범죄 대응을 위한 국제공조의 문제를 살펴보았다. 한국의 유럽사이버범죄협약 가입 필요성에 대한 논의는 지난 몇 년간 끊임없이 제기되었으나 통신비밀보호법 같은 국내법과 상충된다는 이유와 기관마다 견해가 다르고 국내정치 상황 탓에 더 이상 진전을 보이지 못하고 있다. 우리가 이 문제를 해결하지 못하고 있는 동안 국가안보를 위협하는 사이버 범죄는 더욱더 심각하게 발전하여 국제안보를 위협하는 수준의 문제로 인식되어 전 세계 대다수의 국가들이 사이버 범죄 대응에 힘을 쏟고 효과적인 국제공조 체계를 마련하고자 노력하고 있다. 그러나 이 협약에 가입하였을 때, 다른 나라 법집행기관들이 우리나라의 민감한 데이터정보에 접근할 수도 있고 회원국의 요구에 따라 우리 정부가 민감한 데이터정보를 제공해야 한다는 점에서 반대하는 여론도 만만치 않다. 또한 우리나라에 피해를 가장 많이 입히는 나라가 북한이기에 이 협약에 가입하였을 때 얼마나 많은 혜택을 얻을 수 있을지에 대한 의문도 제기되고 있다. 그러나 방글라데시 중앙은행 해킹, 워너크라이, 낫페트야 같은 사이버 공격은 특정국가가 독자적으로 대응하기에는 인적, 기술적, 법률적 자원의 한계에 부딪혀서 불가능하다. 특히나 사이버 범죄가 가지고 있는 특성 중 하나인 국경을 초월하여 발생하는 범죄에 대해서 국제공조 없이는 해결할 수 없다. 국가마다 다른 법률을 가지고 있기에 이 협약에 가입하기 위해서는 국내법 일부 개정이 필요하다. 인접국인 일본도 자국 형사법을 개정하고 이 협약에 가입하였다. 정보통신강국이라고 자타가 공인하는 한국이지만 국가안보를 위협하는 중대한 사이버 범죄는 독자적으로 대응하고 해결할 수 없다.

제5장은 인터넷 거버넌스와 사이버 안보의 문제를 ITU, WSIS,

IGF, ICANN, GCCS 등의 사례에 초점을 맞추어 살펴보았다. 기존의 사이버 안보 분석 연구는 국가 혹은 군사적 관점이 두드러진다. 인터넷 거버넌스의 관점에서의 분석 또한 없지 않으나, 인터넷 거버넌스의 주 참여 국제기구들을 중심으로 한 실증적 조망과 분석은 미미하다. 이러한 맥락에서 제5장은 ITU, WSIS, IGF, ICANN, GCCS에 초점을 맞춘다. 이들에게 초점을 맞추는 이유는 상기된 국제기구/협의체들이 대표적인 인터넷 거버넌스 관련 협의체이기 때문이다. 그뿐 아니라, 이들 협의체 간에는 다양한 축으로 상호 대비될 수 있는 비교 가능성이 존재한다. 우선, 국가 간 다자주의의 거버넌스를 지지하는 ITU와 다중이해당사자주의(Multi-stakeholderism)를 지지하는 WSIS, IGF, ICANN, GCCS은 좋은 대비가 될 것이다. ITU는 정부 간 국제기구임에 비해, WSIS, IGF, GCCS는 국제적인 포럼에 가깝다고 볼 수 있다. 두 번째로, 또 다른 조직 성격의 비교 차원에서 보았을 때, ICANN이 비영리법인 것에 비해 다른 국제 협의체/기구들과는 성격이 다르다고 볼 수 있다. 셋째, 권력구조 차원에서는 ITU가 중국, 러시아와 같은 비민주주의 국가에 의해 활발히 활용되는 장인 것에 비해, 다른 협의체들인 WSIS, IGF, GCCS는 서방 선진국(시민)들이 더욱 적극적으로 참여하고 있는 것으로 볼 수 있다. 넷째, 정부와 비정부 행위자가 참여하는 정도가 다르다. ITU, GCCS는 비교적 국가/정부 행위자들의 비중이 높은 반면, WSIS는 시민사회의 역할이 그들보다 더 강조되기도 한다. IGF는 그보다 더 비정부 행위자들의 영향력이 큰 국제 다자간 협의체로 자리매김해 왔다. 이러한 다양성은, 인터넷 거버넌스 참여 기구들의 사이버 안보에 대한 다양한 접근을 보여주기에 좋다.

제2부 '사이버 안보 국제관계의 동학'에서 한반도 주변4망(網)이 형성하는 국제관계의 구도와 유럽연합 차원의 국제협력 전략의 사례

를 다룬 네 편의 논문을 담았다.

제6장은 미중 사이버 군사력 경쟁과 북한위협의 부상이 한국 사이버 안보에 주는 함의를 다루었다. 사이버 공간은 육지, 바다, 항공, 우주에 이어 강대국 간의 군사력 경쟁이 전개되는 다섯 번째의 전장이 되고 있다. 미중 패권경쟁 속에서 양국은 사이버 안보를 위한 군대의 역할을 강화하고 있으며, 사이버사령부를 별도로 설치하는 것은 물론 최근 사이버사령부의 위상과 통합역량을 강화하기 위한 제도적 조치들을 취하고 있다. 또한 사이버 공간에서의 공격력과 억지력을 강화하기 위한 기술적 노력, 그리고 민관협력의 필요한 구조들을 발전시키고 있다. 사이버 공간의 미중 군사력 경쟁이 첨예화되는 한편으로 북한의 사이버 공격력은 세계안보의 최대 위협이라고 지적될 만큼 급격히 강화되고 있고 또 대담해지고 있다. 2017년 랜섬웨어의 배후로 북한이 지목된 이후 사이버 공간에서 북한은 대표적인 불량국가로 부상하면서 세계의 우려와 경계가 높아지고, 이에 대한 제재와 적극적 대응의 필요성들이 논의되고 있다. 주요 강대국들의 사이버 군사력 경쟁과 함께 사이버 공간에서의 불량국가 북한의 부상은 한국의 안보환경에 주요한 영향변수이다. 한국에서 사이버 안보에 대한 관심과 필요성이 증대됨에도 불구하고 여전히 한국이 어떠한 사이버 위협에 처해 있는지, 어떠한 방향에서 사이버 안보를 강화해야 하는지에 대한 구체적인 논의와 대안이 취약한 것이 사실이다. 이에 제6장은 미중 간 사이버 경쟁을 군사안보적 측면, 즉 미중 양국 간 사이버 군비경쟁에 초점을 두고 분석하는 한편, 북한 사이버 위협의 부상과 이를 둘러싼 미중 경쟁 구도를 함께 분석한다. 제6장은 사이버 공간에서 한국이 처한 안보정세가 북핵문제와 미중 경쟁에 직면해 있는 전통적인 안보정세를 닮아가고 있다는 점에 주목한다. 미중 사이버 군사력경쟁과 북한위협의

부상에 따른 한국 사이버 안보 위협의 증대와 사이버 안보 협력의 제약을 살펴보고, 한국 사이버 안보정책에 주는 함의와 정책적 과제를 제시한다. 미중 패권경쟁의 강화 속에서 한미동맹과 한중협력을 병행 발전시켜야 하는 과제, 그리고 비핵화와 함께 한반도 평화안정의 문제를 동시에 해결해야 하는 과제가 사이버 공간에서도 유사하게 적용되고 있다는 점을 보여주고 이에 대한 전략적 접근의 필요성을 제기한다.

제7장은 미일 사이버 안보 협력을 양자, 소다자, 지역 협력 전략의 결합이라는 시각에서 다루었다. 미국과 일본은 기존 미일동맹을 바탕으로 사이버 안보 분야에서도 협력을 강화하고 있다. 미일 양국의 사이버 안보 협력의 진화는 미일동맹의 변환, 사이버 안보 협력을 매개로 한 지역 협력의 강화, 도쿄 올림픽에 대비한 협력 강화 등 세 가지 차원에서 이루어지고 있다. 이를 위해 미일 양국은 새로이 대두되고 있는 사이버 위협의 증대에 효과적으로 대처하기 위해 양자 협력을 확대·강화하고 있으며, 이를 기반으로 소다자 및 지역 차원의 협력으로 확대해 나가는 접근법을 취하고 있다. 미일 사이버 안보 협력의 확대 및 강화는 아베 정부의 보통국가화를 위한 노력과 미일동맹의 변환이라는 두 가지 요소가 함께 작용한 결과이다. 미국의 입장에서 부상하는 중국에 대응하는 차원에서 미일동맹을 강화해야 할 상황에 직면하고 있다. 한편 아베 정부는 보통국가를 지향하는 과정에서 헌법의 개정을 추구하는 가운데 과도기적 조치로서 헌법에 대한 재해석을 통해 집단적 자위권을 추구하고 있다. 사이버 안보 협력은 미국의 중국에 대한 견제 필요성과 일본의 보통국가화의 필요성을 연결하는 접합점으로서 역할을 하고 있다. 이러한 측면에서 볼 때, 미국과 일본의 사이버 안보 협력을 이해하기 위해서는 사이버 위협에 대한 실체적 인식

과 공동 대응의 필요성뿐 아니라 중국의 부상과 미일동맹의 재조정이라는 거시적 변화에 대한 이해가 병행될 필요가 있다. 미국과 일본은 양자 차원의 협력을 기반으로 사이버 안보 협력을 지역 차원으로 확대하고 있다. 지역 차원의 미일 사이버 안보 협력은 사이버 위협이 초국적으로 가해지는 데 따른 대응과 부상하는 중국의 영향력이 아시아 지역으로 심화·확대되는 데 대한 대응이라는 두 가지 측면이 결합되어 있다. 미국과 일본은 중국에 대한 대응 차원에서 호주와 미·일·호주 삼각 사이버 안보 협력을 강화하는 한편, 동남아시아 국가들의 사이버 안보 역량 강화를 위한 지원을 확대하고 있다.

제8장은 미러 사이버 안보 경쟁과 중러 협력의 주제를 다루었다. 제8장은 오늘날 사이버 공간상에서 벌어지고 있는 미러 사이버 안보 경쟁과 중러 협력의 양상을 기술한다. 미국과 러시아-중국 간의 안보 경쟁은 기본적으로 미국이 주창하는 다중이해당사자주의와 러시아와 중국이 주창하는 국가간다자주의 간의 충돌이다. 이러한 미국과 러시아 간의 근본적인 차이는 양 당사자 간에서 나타나는 기술과 문화적 간극과 다른 정치체제에서 비롯된다. 러시아와 중국의 협력은 공동의 이해관계에서 비롯된다. 먼저 미국이라는 공동의 위협이자 동시에 반패권 연대의 대상이 존재하기 때문이며, 또한 동시에 이들이 갖는 권위주의 정체의 특성 때문이다. 사이버 안보 경쟁과 협력은 냉전시기의 핵안보 경쟁과 서방과 공산 진영의 지정학적 충돌과 대치와는 다른 양상을 띤다. 사이버 안보 경쟁은 미국과 러시아-중국의 패권충돌과 정치, 군사, 경제적 이해관계의 충돌이라는 지정학적 양상을 보이지만 동시에 자신들의 담론과 프레임이 국제질서의 표준이 되기 위해 경쟁하고 더 많은 내편을 끌어 모으기 위한 매력 경쟁의 요소를 갖고 있다. 흥미로운 점은 사이버 안보 경쟁이 이처럼 복합 지정학적 특성

을 가지기 때문에 오히려 과거 냉전시기 핵 안보 경쟁보다 더욱 위험할 수 있다는 것이다. 이는 사이버 공간이 가지는 이중적 성격과 은밀성과 책임소재의 불분명성, 그리고 사이버 안보의 대상의 모호성 등과 같은 고유한 속성들 때문이다. 이러한 주요한 속성들은 경쟁의 당사자로 하여금 공세적, 공격적 전략과 전술을 채택하도록 만든다. 때문에 경쟁 당사국이자 주요 강대국인 미국과 러시아, 그리고 중국 간의 상호 신뢰 구축과 협력의 강화는 사이버 안보뿐만 아니라 보편적인 국제 안보질서를 위해서도 매우 중요하다. 미국과 러시아-중국 간의 직접적인 경쟁을 완화하고 협력과 신뢰를 구축하기 위해 글로벌 패권추구 의지와 능력이 없으면서 국제적으로 역량을 갖춘 제3국들의 네트워크적 역할을 강화하는 것이 제안될 수 있다. 중견국가로서 한국은 미국과 러시아의 사이버 안보 경쟁에서 경쟁을 조절하고 협력과 신뢰를 증진시키는 매개역할을 수행할 수 있다.

제9장은 상하이협력기구의 사이버 안보 논의를 러시아와 중국의 역할에 초점을 맞추어 다루었다. 제9장에서는 사이버 공간상 미국 중심의 서방국가와 다른 방향으로 자국의 이익을 확대하기 위한 러시아와 중국의 노력을 상하이협력기구(이하 SCO)의 활동을 통해 살펴본다. 제9장은 크게 세 부분으로 구성된다. 먼저, 사이버 안보 논의의 발달에서는 SCO에서의 사이버 안보 논의 발단과 전개 과정을 주요 합의문건을 중심으로 검토한다. 둘째, 사이버 안보에 관한 SCO 내 러시아와 중국의 역할에서는 사이버 공간에서의 러시아와 중국의 공동 이익으로 중국과 러시아가 SCO를 통해 수립하고자 하는 사이버 안보 규범의 특징이 사이버 공간에서의 국가주권강화, 국가의 정보통제권 인정, 국제 인터넷 거버넌스 체제 변경임을 확인한다. 그러나 SCO의 강력한 양 주도국이 SCO에 대한 동일한 비전을 공유하지는 않음으로 이익

갈등이 발생할 수 있음을 분석한다. 셋째, SCO의 사이버 안보 전망에서는 SCO 플랫폼에서 러시아와 중국이 주장하는 사이버 안보 의제의 지속 발전 가능성을 분석한다. 분석을 통해 중단기적으로 SCO를 통한 양국의 협력은 지속될 것이나, 2017년 6월 인도와 파키스탄의 SCO 가입에 따라 사이버 안보 의제의 변화 가능성이 존재함을 확인한다. 끝으로, SCO에서의 러시아와 중국의 활동을 통한 국제 사이버 안보 규범 형성 가능성을 타진하고 SCO 사례를 통해 한국도 지역 국제기구 등을 통해 사이버 안보 협력 및 국제규범 형성 노력이 필요함을 주장한다.

제10장은 유럽연합(EU)의 사이버 안보 국제협력 전략을 다루었다. 유럽연합은 사이버 공간에서도 EU 핵심 가치(인간 존엄성, 자유, 민주주의, 평등, 법, 인권)를 추구하며 글로벌 행위자로서 사이버 공간에서의 시민 안전과 디지털 시장 보호를 위한 규범 생성 및 협력자 역할을 수행하고자 한다. 이에 제10장에서는 EU가 추진하고 있는 사이버 안보 전략과 국제협력 관계에 대해 살펴봄으로써 사이버 안보에 있어서 EU의 위치와 유럽이 형성하고 있는 사이버 안보 지형을 파악해 보고자 한다. 또한 사이버 공간에서의 신뢰 증진과 협력을 위한 한국의 협력적 방안에 대해 살펴보고자 한다. EU의 사이버 안보 전략은 초기에 개별 국가 차원의 임무와 권리로 접근되어 네트워크 및 정보시스템 보호와 사이버 범죄에 대해서만 논의되었다. 이후 사이버 안보 위협이 글로벌 전체의 위협(systemic cyber risk)으로 인식되고 확산되면서 EU는 보다 강력하고 방어적인 사이버 안보 전략을 마련하게 된다. 그리고 EU는 조약 및 전략적 파트너십, 대화 및 워킹 그룹 등을 통해 미국, 브라질, 아시아를 포함한 다양한 국가들과 협력을 추진하고 있다. 이와 같은 EU의 사이버 안보 전략과 국제협력 추진은 초국가적 특

성과 내외부적인 문제점을 고려해 통합적으로 추진됨으로써 한국의 사이버 안보 전략 추진 및 국제협력에도 시사하는 바가 있다.

제11장은 '사이버 안보의 국가전략 2.0, 무엇을 연구할 것인가?'이라는 제목으로 진행된 종합토론의 내용을 담았다. 이 책의 작업이 진행되는 중에 필자들은 사이버 안보 국가전략의 의미와 향후과제에 대해서 활발한 토론을 벌였다. 이 책의 연구가 지니는 의미가 무엇인지, 앞으로 어떤 방향으로 가면 좋겠는지, 그런 면에서 연구의 좌표를 어떻게 설정하는 것이 좋겠는지 등의 문제를 놓고 토론을 벌였다. 이러한 종합토론은 세 가지의 주제에 초점을 두어 진행되었다. 첫째로는 총론 차원에서 2018년 현재 '사이버 안보의 국가전략 2.0'을 논하는 의미와 필요성이 무엇인가에 대해서 논의했다. 둘째, 각 필자가 담당한 장에 대한 내용 소개를 겸해서, 해당 분야에서 현재 제기되는 사이버 안보의 세계정치와 국가전략의 현황과 과제를 정리하였다. 그리고 마지막으로 앞으로 우리가 사이버 안보의 국가전략에 대한 연구를 계속 해나간다고 할 경우에, 현 단계에서 우리가 생각해볼 수 있는 연구주제들이 무엇인가에 대해서도 이야기를 나누었다.

* * * * *

이 책이 나오기까지 많은 분들의 도움을 받아서 일일이 감사의 말씀을 드려야 할 분들은 너무나도 많다. 2017년 여름부터 시작된 공동작업에 참여하여 귀한 글을 집필해 주신 필자 선생님들께 깊은 감사의 말씀을 전하고 싶다. 동시에 진행되었던 여러 공부모임 중에서도 유난히 유쾌하고 생산적인 분위기에서 진행되었던 세미나였던 것 같다. 그 생생했던 세미나의 장면 중에서 2018년 2월 1일(목) 16:00~18:00 충남 대전에 위치한 국가보안기술연구소 회의실에서 진행되었던 필자들의 종합토론 내용은 이 책의 제11장에 담았다. 이 책의 준비세미나 과정에서 2017년 2학기와 2018년 1학기의 두 차례에 걸쳐서 '사이버 안보의 국제규범'과 '사이버 안보의 외교전략'이라는 제목으로 진행된 사이버 안보 포럼에 토론자로 참여해 주신 유준구 교수(국립외교원), 정명현 교수(고려대학교), 이정석 소령(합참), 류동주 대표(비트레스), 윤재석 팀장(한국인터넷진흥원), 이영음 교수(방송통신대학교), 신성호 교수(서울대학교), 황지환 교수(서울시립대학교), 이기태 박사(통일연구원), 신범식 교수(서울대학교), 송은지 연구원(한국인터넷진흥원), 김주희 박사(경희대학교)께 감사드린다. 2018년 9월 20일 이 책에 실린 원고들의 최종발표회를 겸해서 열렸던 학술회의에서 축하의 말씀을 주신 조현숙 국가보안기술연구소장, 이내영 국회입법조사처장, 문덕호 외교부 국제안보대사께 감사드린다. 당일 학술회의에서 사회를 맡아주신 김유향 팀장(국회입법조사처), 채재병 박사(국가안보전략연구원), 배영자 교수(건국대학교)께도 감사한다. 또한 당일 토론을 맡아주신 조현석 교수(서울과학기술대), 유준구 교수, 신용우 박사(국회입법조사처), 황지환 교수, 이기태 박사, 신범식 교수, 장노순 교수(한라대학교), 오일석 박사(국가안보전략연구원), 김도승 교수(목포대학교)께도 감사드린다. 당일 행사 진행을 맡아 주었던 서울대학교 석박사과정의 최용호, 김화경, 알리나, 장성일 그리고 서울대학교 국제문제연구소의 하가영 주임께도 감사한다. 특히 이 책의 작업이 진행되는 동안 총괄을 맡아 준 서울대학교 박사과정의 이종진에 대한 고마움도 빼놓을 수 없다. 이 책의 작업이 진행되는 동안 한국연구재단의 한국사회기반연구사업(SSK)과 서울대학교 국제문제연구소, ETRI 부설 국가보안기술연구소에서 제공해 주신 재정적 지원에도 감사의 마음을 전

한다. 항상 묵묵한 후원자의 마음으로 출판을 맡아 주시는 사회평론아카데미의 관계자들께도 감사의 말씀을 전한다.

2018년 10월의 마지막 밤
김상배

차례

제2부 사이버 안보 국제관계의 동학

제1부

사이버 안보 국제규범의 형성