사이버 안보의 국제정치학적 지평

전략과 외교 및 규범

사이버 안보의 국제정치학적 지평
전략과 외교 및 규범

김상배 · 민병원 엮음

사이버 안보의 국제정치학적 지평
전략과 외교 및 규범

2000년 00월 00일 초판 1쇄 인쇄
2000년 00월 00일 초판 1쇄 발행

지은이 김상배, 민병원, 이상지, 김보라, 고은송, 이진경, 이종진, 유신우, 도호정, 정하연, 황예은

편집 김지산
디자인 김진운
마케팅 강상희

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 academy@sapyoung.com
홈페이지 www.sapyoung.com
ISBN 979-11-88108-00-0 93340

이 저서는 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A3A2924409).

사회평론아카데미

머리말

사이버 안보의 국제정치학적 지평

2017년 5월말과 6월초에 에스토니아 탈린에서 열린 사이콘(CyCon, International Conference on Cyber Conflict)에서 참가자들의 가장 많은 관심을 끈 패널은 국제법 학자인 마이클 슈미트(Michael N. Schmitt)의 대담 코너였다. 2013년 탈린매뉴얼(Tallinn Manuel)을 책임 편집했던 슈미트 교수는, 2017년 2월에는 그 두 번째 버전인 탈린매뉴얼 2.0을 펴낸 바 있었다. '사이버전(cyber warfare)에 적용 가능한 국제법'을 논한 탈린매뉴얼 1.0과는 달리, 탈린매뉴얼 2.0은 각종 사이버 범죄들까지도 포함한 '사이버 작전(cyber operation)에 적용 가능한 국제법'을 논했다. 2017년 사이콘은 사이버 안보 분야 국제법 논의의 지평을 개척하고 있는 슈미트 교수의 작업을 높게 평가하여 두 권에 걸쳐서 출간된 탈린매뉴얼의 뒷얘기를 듣는 시간을 별도로 할애했던 것이다.

2018년이면 10주년을 맞게 될 사이콘은 사이버 안보 연구의 새

로운 지평을 연 회의로 역사에 기록될 것이다. 사이콘은 국제법 외에도 기술공학과 군사전략 분야에서 제기되는 다양한 사이버 안보의 쟁점들을 소개하고 논의하는 노력을 지속해 갈 것으로 전망된다. 그러나 이렇게 기술-전략-법의 세 트랙으로 짜인 사이콘의 패널들을 둘러보면서 새로운 것을 배웠다는 인상보다는 오히려 뭔가 빠진 것이 있다는 느낌이 들었던 이유는 무엇일까? 아마도 정보보안 업계 담당자의 최신 기술에 대한 현란한 소개나 나토 소속 장성들의 군작전 개념에 대한 절도 있는 설명, 그리고 슈미트 교수 패널의 국제법 담론을 넘어서 뭔가 새로운 지평을 보여주어야만 한다는 막연한 책임감이 발동했던 것 같다. 이 책의 제목으로 내건 바와 같이 '사이버 안보의 국제정치학적 지평'을 보여주어야 한다는 국제정치학자의 책임감이라고나 할까?

이 책은 사이버 안보 연구의 국제정치학적 지평을 열어보겠다는 문제의식을 바탕으로 2016년 1학기부터 시작된 두 권의 책 중의 하나이다. 이 책의 자매편은 『사이버 안보의 국가전략: 국제정치학의 시각』(이하 〈국가전략〉)이라는 제목을 내걸고 2017년 5월에 사회평론아카데미에서 출판되었다. 〈국가전략〉이 기성학자들을 중심으로 사이버 안보의 국제정치학적 기본논제들을 다룬 교과서의 성격을 띠었다면, 이 책은 대학원 학생들과 함께 국제정치학이 탐구해야 할 사이버 안보의 응용주제들을 제시한 연구서이다. 사실 이 분야의 학문후속세대인 아홉 명 학생들의 글은, 내용적으로는 여전히 미숙한 부분이 없지 않음에도 불구하고, 그 문제의식의 참신성이라는 측면에서 사이버 안보 연구의 국제정치학적 지평을 넓히는 의미가 충분하다고 판단된다. 특히 국내뿐만 아니라 국제적으로도 아직 연구가 부족한 상황에서 이 책의 필자들은 다음과 같은 세 가지 측면에서 국제정치학적 지평을 보여주고자 했다.

첫째, 사이버 안보 '전략연구'의 지평을 보여주고자 했다. 사이버 안보의 중요성이 커지면서 세계 주요국들은 국가전략 차원에서 사이버 안보의 문제에 접근하고 있다. 〈국가전략〉에서도 한반도 주변4개국인 미국, 중국, 일본, 러시아의 사이버 안보 국가전략을 다루었으며, 그 연속선상에서 북한과 한국의 사례도 살펴보았다. 이 책에서도 미국과 중국의 사례를 좀 더 심층적으로 분석한 이론적 · 경험적 연구를 진행했다. 이러한 '전략연구'의 지평은 앞으로도 계속 확대되어 가야 할 것이다. 특히 한국의 국가전략에 주는 함의를 염두에 둔다면, 미-중-일-러와 같은 강대국의 사례에 초점을 두는 기존의 발상을 넘어서 영국, 독일, 프랑스 등과 같은 유럽의 선진국들이나 캐나다, 호주, 스웨덴, 노르웨이, 핀란드 등과 같은 전통적 중견국들, 그리고 사이버 안보 분야에서 한국과 비슷한 처지에 있다고 평가되는 에스토니아, 네덜란드, 스위스, 싱가포르, 이스라엘 등과 같은 나라들의 비교연구로 지평을 넓혀가야 할 것이다,

둘째, 사이버 안보 '외교연구'의 지평을 보여주고자 했다. 〈국가전략〉에서도 미국, 중국, 일본, 러시아, 남북한의 사이버 안보 분야 외교전략에 대한 내용을 다룬 바 있다. 이 책에서는 일국 차원의 외교전략 추진을 넘어서 양자관계의 맥락에서 보는 국제협력의 내용과 한계를 검토하였으며, 더 나아가 미국과 중국 두 강대국이 자국 주도의 네트워크를 건설하기 위해 전개한 사이버 안보 분야의 동맹전략에 대해서도 살펴보았다. 특히 핵안보와 사이버 안보 등과 같은 이슈 간 비교연구의 시각을 제시하였다. 이러한 사이버 안보의 외교적 차원에 대한 연구는 북한발 사이버 공격에 대응하기 위해서 한국이 고려해야 하는 국제적 해법을 모색하는 데 주는 의미가 크다. 이러한 '외교연구'는 한반도 주변4개국과 남북한 간에 형성되는 양자 및 삼자 관계 연구로 발

전하고, 더 나아가 동아태 지역협력의 연구로 이어질 필요가 있다.

끝으로, 사이버 안보 '규범연구'의 지평을 보여주고자 했다. 최근 사이버 안보의 양자 및 삼자 협력의 틀을 넘어서 다자간 협력을 통해서 국제규범을 모색하려는 노력이 진행 중이다. 이러한 노력 중의 하나가 전통 국제법을 적용하려는 탈린매뉴얼의 시도이다. 〈국가전략〉에서도 탈린매뉴얼과 같은 국제법 적용의 시도 이외에도 국제기구나 정부간협의체, 그리고 글로벌 거버넌스의 프레임을 활용한 국제규범 형성의 시도들을 살펴보았다. 아울러 이 책에서는 유럽연합 차원에서 추구된 사이버 안보 협력의 사례에 대한 검토를 통해서 새로운 안보 패러다임에 기반을 둔 복원력의 개념과 이를 반영한 새로운 규범의 필요성도 거론하였다. 이러한 점에서 보면 향후 사이버 안보 '규범연구'의 지평은 전통안보와는 질적으로 상이한 사이버 안보의 복합적인 성격을 담아내는 방향으로 펼쳐져야 할 것이다.

앞으로 사이버 공간이 세계정치에 미치는 영향이 커지면서 사이버 안보의 국제정치학적 지평은 점점 더 넓어질 것이다. 비유컨대, 사이버 안보의 국제정치학적 지평은 〈국가전략〉과 이 책에서 제시한 1.0 버전을 넘어서 2.0 버전으로 나아갈 것이다. 사실 벌써 이러한 2.0의 양상이 나타나고 있는데, 탈린매뉴얼 2.0의 출간이나, 포스트-GGE에 대한 논의, 미국의 IANA 권한 이양 이후 포스트-ICANN 체제에 대한 논의 등은 바로 그러한 사례들이다. 이러한 문제의식을 바탕으로 〈국가전략〉의 작업에 참여했던 일부 필자들은 이미 『사이버 안보의 국가전략 2.0』(이하 〈국가전략 2.0〉)에 대한 연구를 시작해서 조만간 선보일 예정으로 진행하고 있다. 이러한 작업에서 〈국가전략 2.0〉이 지향하는 바는 강대국이나 선진국의 전략을 그대로 모방하는 것이 아니라 중견국으로서 한국의 특성을 살리는 경험적 · 이론적 플랫폼의 마련에

있다.

이 책은 크게 세 부로 구성되었다. 제1부 '사이버 안보의 전략'에는 세 개의 논문이 실렸는데, 제1장 "미국의 사이버 안보 정치와 정책: 안보화 이론의 시각(이상지)"은, 2008년 이후 오바마 행정부하에서 다양한 국가안보 문제 중에서 사이버 안보가 가장 우선순위를 차지하게 되는 과정을 코펜하겐학파의 안보화 이론을 원용하여 살펴보았다. 제1장은 현재 미국 내 안보화 담론의 수사를 정부 · 군사 담론, 경제 · 기술 담론, 그리고 시민사회 담론으로 구분하였는데, 안보화의 과정을 둘러싼 정치적 긴장과 갈등은 각 담론이 묘사하는 위협을 대처하는 데 있어 세 가지 논점을 바탕으로 전개되었다고 주장한다. 다시 말해, 연방정부가 주요 사회기반시설 보호에 있어서 어떠한 역할을 할 것인지, 어떤 연방기관이 중점적으로 조정 체계를 마련하고 리더십을 발휘할 것인지, 정보 공유의 확대와 심화는 어떠한 범위로 규정할 것인지 등이 그것이다. 제1장은 이러한 논쟁의 과정에서 이해관계자들의 상당수가 정부와 민간 주도의 양 극단 사이에서 관련 행위자들의 자발적인 협력을 강조하는 접근을 지지했다는 결론을 내린다. 더 나아가 이러한 담론과 정치적 논쟁이 정부 주도의 주요 기반시설 보호조치의 시행과 개입 강화, 네트워크상의 정보보안 역량 개선, 그리고 국토안보부 중심의 범국가적 조정체계의 마련이라는 정책수단으로 구체화되었다고 주장한다.

제2장 "미국의 대테러 전쟁과 거시안보화: 스노든파일 사례를 중심으로(김보라)"는 미국 주도의 지구적 감시 체계가 작동하고 있다는 에드워드 스노든의 폭로가 야기한 파장을 코펜하겐학파의 거시안보화 이론의 시각에서 분석하였다. 2001년 9 · 11 테러 이후 부시 정권이 천

명한 '테러와의 전쟁'은 미국 대외정책의 중요한 기조로 작동해왔다. 비록 오바마 정권의 출범과 함께 '테러와의 전쟁'은 종적을 감추는 듯 했으나 상존하는 거대한 테러 위협 앞에 영역을 막론하고 모든 자원과 제도가 언제든 동원되어야 한다는 위협인식은 수정되지 않았다. 제2장은 스노든의 폭로가 '테러와의 전쟁'을 중심으로 구축되어온 미 정부의 대외 인식에 내재한 모순을 비판적으로 조명한 사건이었다고 평가한다. 다시 말해, 스노든 폭로 사건은 테러와의 전쟁이 조장한 전 지구적 공포와 그로 인한 위협이 실제보다 부풀려진 허상이었으며, 전 세계가 공유하는 것이 아닌 미국의 특수한 이익을 대변하기 위해 전략적으로 이용되었다는 것이다. 결론적으로 부시 정권이 천명한 '테러와의 전쟁'은 거시안보화의 전형적 사례였으며, 이는 안보대상을 국가 차원 이상의 것인 자유민주주의로 설정해 사회 기능 전체를 포괄할 안보 논리를 창출해냄으로써 가능했다고 해석한다.

제3장 "중국의 '인터넷 안전' 정책과 국가의 역할(고은송)"은 중국에서 인터넷 안전 전략을 구축하고, 인터넷 안전에 대한 국민들의 인식을 이끌어내며 발전을 거듭하는 과정에서 관찰되는 국가의 역할에 대해서 논했다. 최근 중국이 사이버 안보의 확보 및 강화를 통한 자국 체제 방어에 대해서 강한 열의를 내비치고 있음은 주지하는 사실이다. 21세기를 맞이하여 국가가 혼자서는 해결할 수 없는 새로운 국제정치 이슈와 안보위협 등이 등장하고 이의 해결을 위해 비국가 행위자들의 개입이 필요해지면서 근대 국민국가의 영향력이 상대적으로 퇴보하였다는 주장이 제기되어 왔다. 그러나 중국에서는 여전히 사이버 안보와 같은 새로운 문제에도 정부가 최전선에 나서 대응하고 있어, 이와 같은 이론적 논의는 중국의 사례에 적용되지 않는 것처럼 보인다는 것이다. 특히 중국의 인터넷 검열은 철저히 국가의 통제하에 이루어지고 있는바, 인터넷의 발전이 중국 사회에 가져다주는 긍정적 변화는 무시할 수 없으나 중국 정부로서는 해야 할 일이 늘어난 셈이다. 제3장은 이러한 일련의 세계정치 변화에 발맞추어, 새로이 등장한 이슈인 인터넷 안전을 모색하는 중국 국가의 역할을 정부(government), 국가(state), 네이션(nation) 등의 세 가지 개념을 원용하여 논의하였다.

제2부 '사이버 안보의 외교'에는 세 개의 논문이 실렸는데, 제4장 "미국과 유럽연합의 동맹 안보딜레마: 핵안보와 사이버 안보 비교(이진경)"는 핵안보 분야에서 도출된 '동맹안보 딜레마'의 개념을 사이버 안보에 원용하여 나토 내의 동맹인 미국과 유럽연합의 관계를 살펴보았다. 핵안보 시기 미국과 유럽연합이 겪었던 동맹안보 딜레마 현상이 사이버 안보의 시기에서도 크게 다르지 않게 나타날 가능성이 있다는 것이다. 사이버 안보의 영역에서는 나토의 2010년 '신전략구상'을 통해 동맹국들이 나토에서 가장 강력한 행위자인 미국의 사이버 공간의 안보화 시도에 연루되어갈 가능성이 증가되었다. 또한 2013년 스노든 사건으로 증명되는 사이버 공간에서 생성된 데이터 자원에 대한 도청이나 해킹과 같은 방기의 대응으로, 미국과 유럽연합의 데이터 자원 교류에 대한 조약인 세이프하버 원칙은 폐기되고 데이터 보안을 강화한 프라이버시 쉴드가 체결되었다. 동시에 미국 정보기관의 데이터 접근을 제한하는 제도적 장치도 만들었다. 제4장의 주장에 의하면, 핵안보와 사이버 안보같이 파급효과가 큰 자원에 대해서 미국과 유럽연합은 동맹관계이지만 끊임없이 경쟁을 계속하는 '동맹안보 딜레마'의 관계에 놓여 있으며 이러한 관계는 냉전시기로 대변되는 핵안보 시기나 현재의 사이버 안보의 시기에 동일하게 나타난다고 한다.

제5장 "미국의 사이버 안보 국제협력 전략: 아태지역 전략과 미일협력(이종진)"은 미국의 아태 전략이라는 맥락에서 미국의 '사이버 우

산'의 보호대상을 일본 전역까지 연장한 미일 사이버 안보 협력의 의미를 분석했다. 한층 강력해진 미일 사이버 안보 협력 배경에는 일본이 여타 국가에 비해 발전된 사이버 기술 수준을 보유하고 있음에도, 사이버 안보 측면에서 상대적으로 취약한 '비대칭적 상황'이 있다. 따라서 일본은 미국의 '사이버 우산'을 빌려서 악의적 사이버 공격에 대응하는 방안을 모색했다. 또한 미국도 전통적 군사동맹 속에서 사이버 안보 이슈를 복합화하고 이를 확산하는 사이버 안보 전략을 추구하였다. 특히 아태 지역에서 일본과의 사이버 안보 협력을 강화하며, 이 지역에서 일본에게 교두보이자 '린치핀'으로서 사이버 안보 전략에서의 적극적 역할을 요구하였다. 그러나 미국의 적극적 사이버 안보 협력은 전통안보 측면에서도 미일동맹을 강화시켰고 결국 일본의 보통국가화를 위한 발판을 마련해 주었다. 이러한 변화는 중국, 북한 및 러시아에 대한 미국의 견제와 함께 보통국가를 향한 일본의 속내와 맞물리면서 더욱 더 가속화되고 있다. 이는 일본의 우경화에 대한 중국, 북한과 러시아 등의 의혹을 증폭시키면서 지역안보의 불안정성은 높아질 가능성이 있다.

제6장 "중국의 사이버 안보 전략과 외교: 중국의 시각(유신우)"은 중국의 사이버 안보 정책을 미중경쟁과 중국이 펼치는 국제협력 전략의 맥락에서 살펴보았다. 중국의 시각을 원용해서 집필된 제6장의 인식에 의하면, 중국은 사이버 주권을 강조하면서 '자주혁신'을 통해서 민관협력의 실현을 목표로 '중앙 인터넷 안전 정보화 영도소조'를 중심으로 하는 사이버 안보 추진체제를 만들었으며, 그 연속선상에서 2016년 7월 〈인터넷안전법〉을 통과시키는 행보를 보이고 있다고 한다. 미중 양국은 사이버 공간에서 서로 다른 인식을 갖고 있기 때문에 양국 간에는 지속적으로 갈등과 경쟁이 존재하고 있다. 미국은 중국이

사이버 공간에서 공격적이거나 억지전략을 취하고 있다고 지적하는 반면에, 중국은 자신들이 방어적인 대책을 우선시하고 있다고 주장한다. 그렇지만 양국은 서로 다른 규범을 추구하고 있음에도 공존할 공간이 없지 않다는 것이 제6장의 주장이다. 중국은 중국 내에서 기술개발과 인재양성에 집중함으로써 미국과 공정한 경쟁을 벌이도록 노력하고 있을 뿐만 아니라, 양국은 글로벌 차원에서 발생하는 사이버 범죄와 테러에 대처하기 위해 대화와 협력을 시도하고 있다는 것이다. 다시 말해 중국은 향후 미국과 '역적역우(亦敵亦友)'적인 '신형 강대국 관계'를 모색할 것이라고 주장한다.

제3부 "사이버 안보의 규범"에는 세 편의 논문이 실렸는데, 제7장 "핵과 사이버 안보레짐에서 미국과 러시아의 역할(도호정)"은 냉전기 미국과 소련 간의 핵안보 레짐형성의 사례를 바탕으로 최근 사이버 안보 분야에서 모색되는 국제레짐의 한계에 대해서 살펴보았다. 이를 위해서 제7장이 주목한 것은 핵안보와 사이버 안보의 질적 차이이다. 핵안보의 사례와는 달리 사이버 공간에서는 국가 행위자뿐만 아니라 비국가 행위자들의 활동이 활발하게 이루어지고 있다. 또한 핵무기와 달리 사이버 공격은 상대적으로 비용이 저렴하며, 전문적인 지식이 없더라도 상대방에게 큰 타격을 입힐 수 있기 때문에 국가 간 공격도 발생하지만, 비국가 행위자가 국가를 공격하기도 한다. 특히나 사이버 공간에서는 공격자의 신원이 불분명하기 때문에, 미국과 러시아는 핵무기와 달리 사이버 공격이 자국에게만 상당한 피해를 불러일으킨다는 사실을 서로 인지하기가 어렵다. 즉, 사이버 공간의 기술적 특성과 미국과 러시아의 상이한 안보이익은 사이버 공간에서 강대국의 협력을 이끌어내려는 유엔 정부전문가그룹(GGE)의 노력의 한계를 보여준다. 그럼에도 제7장은 미국과 러시아와 같은 강대국의 협력이 이 분야의

안보레짐 형성에서 중요한 변수로 작용할 것이라고 인정한다.

제8장 "사이버 공격의 개념적 적용과 함의: 탈린매뉴얼을 중심으로(정하연)"는 탈린매뉴얼에서 제기된, 사이버전에의 국제법 적용에 대한 논의를 바탕으로 국가 간 갈등이 사이버 공간으로 표출된 사례들에 어떻게 적용될 수 있는지, 그리고 그러한 사건에 대해 어떠한 적절한 대응이 있을 수 있는지에 대해 탐구하였다. 아울러 탈린매뉴얼에서 제기된 논의의 장점과 한계, 그리고 그 국제정치적 함의도 살펴보았다. 제8장은 단순히 개인이나 집단의 차원에서 발발하는 사이버 범죄 행위가 아니라, 기존에 국가 간 갈등이 있던 상황에서 혹은 적대관계에 놓인 행위자들 사이에 발생한 대표적인 사건을 분석하기 위해서, 탈린매뉴얼의 주요 규칙과 주석들을 바탕으로 하여 공격의 행위자, 성격, 대상을 중심으로 한 분석틀을 마련하였다. 이를 바탕으로 에스토니아, 조지아, 이란에 가해진 사이버 공격의 사례에 대해 탈린매뉴얼을 적용하여 분석하였다. 이를 통해 향후 사이버 공간에서 표출되는 국가 간 갈등 문제에 대해 접근 및 해석할 수 있는 기준을 고찰하고 기존의 탈린매뉴얼의 유용성과 한계를 짚어보았다.

제9장 "유럽 정보 네트워크와 사이버 안보: EU INTCEN과 ENISA의 사례(황예은)"는 유럽연합의 사이버 안보 전략과 안보 위협 관련 정보 네트워크 간 연결 지점을 살펴봄으로써, 유럽의 지역차원에서 형성되고 있는 사이버 협력 거버넌스 모델을 살펴보았다. 사이버 안보를 포함한 신흥안보 분야에서는 다양한 이해당사자들 간에 존재하는 위계적 질서와 수평적 관계를 아울러 적절히 관리할 수 있는 메타 거버넌스 체제가 요구된다. 유럽연합의 사이버 정책의 발전 과정은 일국 차원에서 수립되는 정보 및 사이버 안보 대응책과 지역적 메커니즘이 때때로 상충하면서도, 다른 한편으로는 상호보완적으로 발전하는

구도를 보여주었다. 여기에 관여하는 다양한 행위자 중에서 안보 이슈 관련 정보 수집 및 공유를 담당하는 유럽연합 정보분석센터(EU INTCEN)와 네트워크 및 정보 보안 유지와 관련된 활동을 주도하는 유럽네트워크정보보호청(ENISA)은 유럽 내 사이버 안보를 위한 협력 강화에서 중요한 역할을 하였다. 제9장은 두 기관의 성격과 활동에 대한 분석을 통해 사이버 안보 이슈를 관리하기 위해 요구되는 지역적 차원의 접근법을 검토하였다.

이 책이 나오기까지 많은 분들의 도움을 얻었다. 특히 이 책의 작업에 공동저자로 참여한 서울대학교 정치외교학부(외교학 전공) 대학원과 이화여자대학교 정치외교학과 대학원의 아홉 명 학생들의 노고를 치하하고 싶다. 2016년 1학기와 여름방학 기간에 걸쳐서 연구주제들을 구상하고 이를 발전시켜서 2016년 12월 초 한국국제정치학회 연례대회에서 대학원생 패널을 구성하여 초고를 발표하고 이후 집중세미나를 통해서 수정작업을 반복하면서 글들을 다듬어 가는 동안, 이들 학생들의 젊은 학구욕이 없었다면 이 책을 끝까지 마무리하기는 힘들었을 것이다. 학생들의 초고를 평균 예닐곱 번이나 읽으면서도 지치지 않았던 것은 아마도 코멘트를 기다리는 학생들의 기대감 때문이었던 것 같다. 이러한 과정에서 공동편집자로 학생들의 논문들을 지도해 주신 민병원 교수님에 대한 감사의 마음도 빼놓을 수 없다.

이 책의 작업은 한국연구재단의 한국사회기반연구사업(Social Science Korea, 일명 SSK)의 지원을 받아 2016년 9월에 시작된 대형연구센터 프로젝트인, '신흥권력의 부상과 중견국 미래전략'의 학문후속세대 네트워킹 사업의 일환으로 진행되었다. 이전에도 여러 번 이러한 네트워킹 사업을 진행했지만, 이 책이 지닌 특별한 의미는 지난 수

년 동안 서울대학교 학생들만으로 시도했던 지적 탐구의 외연을 확장하여 이화여자대학교 학생들과 공동작품을 내놓게 되었다는 데 있다. 이 책의 모태가 된 대학원생 세미나와 병행하여 진행된 '사이버 안보의 세계정치 공부모임(일명 사세공)'에 참여하셨던 선생님들께도 감사의 마음을 전한다. 여러 차례의 세미나 준비와 이 책의 교정 작업을 총괄해 준 이종진 군의 헌신에도 감사한다. 끝으로 학생들이 벌이는 지적 도전의 취지를 알아주시고 흔쾌히 출판을 맡아 주신 사회평론아카데미의 관계자들께도 감사의 말씀을 전한다.

2017년 6월 1일
에스토니아 탈린에서
김상배

차례

제2부 사이버 안보의 외교

제3부 사이버 안보의 규범