사이버안보의 국가전략
국제정치학의 시각

사이버안보의 국가전략
국제정치학의 시각

2017년 4월 3일 초판 1쇄 인쇄
2017년 4월 7일 초판 1쇄 발행

지은이 김상배, 민병원, 이상현, 배영자, 신성호, 정종필, 조윤영, 이승주, 신범식, 황지환

편집 김지산
디자인 김진운
마케팅 정세림, 남궁경민

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 979-11-88108-09-1 93340

사이버안보의 국가전략
국제정치학의 시각

김상배 엮음

사회평론

머리말

최근 사이버 안보는 명실상부하게 국제정치학의 핵심적인 논제가 되었다. 무엇보다도 사이버 공격이 물리적 공격만큼이나 국가안보를 위협할 수 있다는 우려가 현장 전문가들뿐만 아니라 국제정치학자들 사이에도 널리 번져가고 있다. 사이버 공격에 대처하기 위해서 일국 차원에서 기술역량을 키우고 법제도를 정비할 뿐만 아니라 외교적으로 관련 국가들의 협력도 활발히 진행되고 있다. 사이버 안보 분야의 국제규범을 모색하기 위한 움직임들이 활발히 진행되고 있으며 그 이면에서는 다양한 행위자들의 이해관계가 충돌하고 있다. 최근 사이버 안보와 관련하여 발생하고 있는 현상들의 면면을 들여다보면 컴퓨터와 인터넷이라는 기술 변수를 매개로 하여 벌어진다 뿐이지 여타 분야에서 볼 수 있는 국제정치의 전형적인 요소들이 발견되고 있다. 그야말로 이제는 국제정치학자들도 기술을 잘 모른다는 핑계로 뒷짐만 지고 있을 수 없는 상황이 되었다.

인터넷의 보급이 미미하여 보안 층위를 크게 중시하지 않던 초창

기에는 컴퓨터 보안이나 정보보호 또는 네트워크 보안, 그리고 이와 관련된 국내정책과 국제협력은 주로 컴퓨터 전문가나 소프트웨어 엔지니어들의 몫이었다. 이들의 논의는 주로 물리적 환경으로서 인터넷 또는 사이버 공간이라는 기술시스템이 작동하는 과정에서 발생하는 내적 오류와 외적 교란 등에 관심을 기울였다. 사정이 이렇다 보니 시스템이 구동되는 이면에 존재하는 국가 및 비국가 행위자들의 인식과 전략, 그리고 이러한 과정에서 발생하는 권력정치의 동학은 상대적으로 소홀히 취급되었다. 게다가 이들의 논의는 간혹 기술시스템 자체에서 발생하는 가능성에만 주목하여 사이버 위협과 공격이 낳을 정치사회적 위험성을 과장하는 경향마저도 있었다. 그러나 최근 사이버 안보의 문제가 더 이상 기술과 공학의 분야에만 머물지 않고 21세기 세계정치의 주요 영역으로 편입된 상황에서 예전의 관성에 의존해서 이 문제를 볼 수만은 없게 되었다.

특히 국가행위자들이 사이버 공격의 주요 주체로서 자리매김하는 현상은 국제정치학자들의 관심을 끌고 있다. 초창기의 사이버 테러와 공격은 체계적으로 조직되지 않은 초국적 핵티비스트나 테러리스트들이 벌이는 게임이었다. 그러나 최근 들어 미국이나 중국, 러시아 등과 같은 강대국들이 사이버 공격과 관련된 논란의 전면에 나섰다. 특히 사이버 공격을 막아내는 대책의 추진에 있어서 국가 행위자는 그 어느 누구보다도 많은 기대를 받고 있다. 한편 사이버 안보가 국제정치학자들의 관심을 끈 배경에는 이 문제를 군사안보론의 시각에서 보기 시작한 변화가 있다. 사이버 공격으로 인해 인명 피해가 발생했을 경우 해당 국가에 대한 군사적 보복이 가능하다는 구상이 정책서클과 학계 일각에서 제기되고 있다. 냉전 시대에 개발된 핵 억지의 개념을 사이버 안보 분야에도 적용하자는 구상도 거론되고 있다. 그 실현 가능성이나 효과성은 별도로 하더라도 이러한 군사안보적 대안들이 거론되기 시작했다는 사실은 사이버 안보가 국가업무의 중요한 축을 이루게 됐다는 점을 보여 준다.

이 밖에도 전통적인 국제법, 특히 전쟁법의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격을 이해하고 제어하려는 움직임도 진행되고 있다. 해커나 테러리스트 등과 같은 비국가 행위자뿐만 아니라 사이버 공격의 배후지를 제공한 국가나 업체에 대해서도 전쟁법을 적용하여 책임을 묻겠다는 것이다. 전통적인 정치군사 분야의 국제기구인 유엔 차원에서 사이버 안보 문제를 다루려는 시도도 최근 빠르게 진행되고 있다. 물론 사이버 안보라는 새로운 안보위협의 문제를 지나치게 전통적인 인식 틀에만 의거해서 풀어 간다는 비판도 만만치 않다. 전통적인 국가행위자 중심의 안보담론이나 군사담론 또는 정치담론이 야기할 과잉담론(hyper-discourse)의 출현 가능성도 우려되고 있다. 이러한 맥락에서 양자 및 다자 간 협력이나 글로벌 거버넌스의 맥락에서 보는 사이버 안보의 국제규범 형성에 대한 기대도 출현하고 있다. 그러나 아직까지 현실주의, 자유주의, 구성주의 등으로 대변되는 기존의 국제정치이론은 사이버 안보의 세계정치에 대한 제대로 된 분석과 처방을 내놓고 있지 못하다.

이러한 문제의식을 바탕으로 이 책의 필자들은 사이버 안보의 세계정치를 보는 국제정치학의 여러 접근법들을 정리하고 이를 통해서 한반도의 주변 네 나라들, 즉 미국, 중국, 일본, 러시아의 국내외 전략을 이해함으로써 북한의 사이버 공격에 대응하는 한국의 전략과 외교를 고민하는 기초 작업을 펼쳤다. 이러한 과정에서 이 책의 필자들이 염두에 두었던 논제는 사이버 안보의 기술공학적인 문제들을 구체적으로 다루고 있는 여타 분야의 전문가들에게 국제정치학적 시각의 필

요성과 유용성을 제대로 설파하는 문제였다. 전통안보와는 질적으로 성격이 다른 사이버 안보의 논리를 인정하면서도 거기에 중첩되는 국제정치의 고유 논리가 독자적으로 자리매김하고 있음을 보여주고 이를 바탕으로 사이버 안보 국가전략의 실천적 방향을 제시하는 것이었다. 이를 위해서 필자들이 착안한 것은, 이 책의 제목에 담긴 네 가지 표제어, 즉 '사이버,' '안보,' '국가,' '전략' 등의 의미가 기존 전통안보론에서 이해하던 그것들과는 크게 다르다는 사실을 보여 주는 것이었다.

첫째, '사이버'로 대변되는 분야의 특성이 군사안보 영역과는 다르다는 것을 보여 주고자 하였다. 사이버 공격은 전통안보 공간과는 다른 사이버 공간을 배경으로 해서 발생한다. 사이버 공간의 확장 속도가 예상을 뛰어넘고 그 확장 범위가 지구 곳곳에 미치는 것만큼, 이에 비례해서 사이버 공간의 범죄와 테러의 위협도 점점 더 복잡한 양상으로 전개되고 있다. 따라서 자신의 컴퓨터와 네트워크에 대해서 아무리 철저한 보안 조치를 취하더라도, 보이지 않는 공격으로부터 완전히 자유로울 수는 없다. 특히 네트워크상의 빈틈을 의미하는 착취혈(exploit)의 존재는 방어하는 측에 비해 공격자에게 훨씬 유리한 조건을 제공한다. 이밖에도 사이버 공간의 기반을 이루는 네트워크 시스템의 복잡계적 특성은 사이버 위협의 잠재적 위력을 더욱 강화한다. 게다가 컴퓨터 바이러스나 악성코드, 경우에 따라서는 네트워크 그 자체와 같은, 이른바 비인간 행위자(non-human actor)의 활동은 사이버 테러와 공격에 독특한 성격을 부여하는 변수로 작동한다. 이렇듯 전통 군사영역과는 다른 메커니즘으로 움직이는 사이버 공간의 구조와 동학을 이해하는 것은 그 안에서 벌어지는 국제정치를 이해하는 기초 작업임에 틀림없다.

둘째, 사이버 안보에서 논하는 '안보'의 의미도 전통안보의 그것과는 다르다는 것을 보여 주고자 했다. 사이버 안보는 단순계의 논리

에 입각해서 발생하는 전통안보의 경우와는 달리, 이른바 신흥안보(emerging security)의 대표적 사례이다. 신흥안보란 미시적 차원에서는 단순히 소규모 단위의 안전(安全, safety)의 문제였는데 그 이슈 자체의 양이 크게 늘어나거나 또는 다른 이슈들과 연계되면서 국가적 차원의 안보(安保, security) 문제로 창발(創發, emergence)하는 현상을 의미한다. 다시 말해, 평소에는 개별 단위 차원의 안전이 문제시될 정도의 미미한 사건들이었지만, 그 발생 숫자가 늘어나서 상호작용이 복잡해지고 그 와중에 새로운 패턴이 출현하는 지점, 이른바 양질전화(量質轉化)의 임계점을 넘게 되면 국가안보를 위협하는 심각한 문제가 되는 현상이 발생한다는 것이다. 예를 들어, 우리의 컴퓨터 한두 대에서 발견된 악성코드는 그냥 무시될 수도 있겠지만, 전 국민의 컴퓨터가 바이러스에 감염되거나, 더 나아가 국가 기반시설을 통제하는 컴퓨터 시스템이 해킹을 당한다면 이는 국가적 차원에서 그냥 지나칠 수 없는 중대한 위험이 되는 이치이다.

셋째, 사이버 안보 분야에서 논하는 '국가'는 전통안보의 주체로서 상정되었던 국가와 그 성격이 다르다는 것을 보여 주고자 했다. 국가안보에 대한 사이버 공격의 잠재적 충격이 예상되면서 많은 국가들이 사이버 군사력을 확대하기 시작했다. 사이버 공격을 행하는 주요 주체는 국민국가의 정부라기보다는 애당초 해커 집단이나 테러리스트와 같은 비국가 행위자들이었다. 그러나 최근에는 국가의 비호를 받는 사이버 부대원들이 암약하거나 정부가 사이버 갈등의 전면에 나서고 있다. 사이버 방어를 위한 국내외 거버넌스의 주체로서 국가는 여전히 대표적인 행위자일 수밖에 없다. 그러나 사이버 안보 게임에 임하는 주체로서 국가 및 비국가 행위자 간의 경계는 점차로 희미해지고 있다. 초국적으로 발생하는 사이버 위협과 공격은 전통안보의 경계로

간주되었던 국민국가의 영토 단위가 지니는 의미를 허물어 가고 있다. 이러한 맥락에서 볼 때, 사이버 안보의 세계정치는 국민국가를 주요 단위로 하는 전통적인 국제정치의 반복이라기보다는 사이버 공간이라는 복합 네트워크 환경을 기반으로 다양한 행위자들이 참여하는 새로운 양식으로 이해해야 할 것이다.

끝으로, 사이버 안보 분야에서 원용되는 '전략'은 전통안보 분야의 단순전략이 아니라는 것을 보여주고자 했다. 앞서 언급한 바와 같이, 사이버 공간의 기술적 특성은 사이버 공격을 막기 위해서는 촘촘한 방어막을 구축하는 것만이 능사가 아님을 보여준다. 다시 말해, 공격이 우위에 서는 사이버 안보 분야의 특성상 이 분야의 전문가들이나 이른바 '화이트 해커'들이 나서서 기술적 방어와 군사적 역량을 구축하는 것만으로는 효과적인 대응 방안을 마련할 수 없다. 이를 뒷받침하는 사이버 안보의 추진체계 정비와 법 제정의 노력도 중요할 뿐만 아니라 주변 국가들과의 정보 공유 네트워크를 구축하고, 사법 공조를 위한 외교적 노력을 펼치거나, 국제사회에 호소하고 도움을 요청하는 외교력의 발휘도 병행되어야 한다. 더 나아가 사이버 안보의 국제규범 형성 과정에 적극적으로 참여하는 것 자체가 중요한 대응 방안이 될 수 있다. 진화하는 사이버 공격에 대응하는 바람직한 방안은 사이버 안보 분야의 어느 일면만을 강조하는 접근이 아니라 기술과 전략, 국가와 사회, 일국적 대응과 외교적 대응, 양자적 해법과 다자적 해법 등을 다층위적으로 아우르는 복합적인 전략에서 찾아야 한다.

이상의 문제의식을 바탕으로 이 책은 국제정치학의 시각에서 본 사이버 안보의 국가전략을 모색하기 위한 이론적·경험적 논의를 크게 세 부분으로 나누어 전개하였다. 먼저 제1부 '국제정치학으로 보는 사이버 안보'에서는 사이버 안보를 보는 국제정치학의 시각으로서 군사전략론, 국제규범론, 글로벌 거버넌스론 등의 세 가지를 소개하였다.

제1장 '군사전략론으로 보는 사이버 안보(민병원)'는 오늘날 사이버 공간 속에서 국가가 사이버 공격 또는 사이버 위협에 대응하기 위해 택할 수 있는 전략에 대한 논의를 펼쳤다. 전통적인 억지 전략이 가상의 공간에서 더 이상 작동하지 않는다면, 새로운 사이버 억지 전략은 어떻게 수립되어야 하는 것인가? 사이버 공격이 이전의 분쟁과 전혀 다른 속성을 가진 것이라면, 이를 어떻게 이해하고 활용할 것인가? 제1장은 이러한 질문을 바탕으로 하여 사이버 억지의 새로운 패러다임을 논의하고 정리하였다. 이를 위해 사이버 공간의 분쟁과 갈등이 갖는 특징을 논의하고, 기존의 국제법 규범이 이러한 새로운 환경에 어떻게 적용될 수 있는가에 관한 지금까지의 노력들을 개괄적으로 살펴보았다. 또한 사이버 억지의 개념이 적용 범위와 방식에 있어 더 확대되고 있으며, 억지 전략을 둘러싼 논의도 일반억지와 긴급억지, 단계적 억지와 맞춤형 억지 등 세부적인 개념화를 통해 진화하고 있음을 소개하다. 이러한 논의의 연속선상에서 사이버 억지 전략이 과거와 같은 보복 또는 방어의 차원을 뛰어넘어 국가들 사이의 상호의존성을 동시에 고려한 협력적 관계를 지향해야 한다는 점을 부각시키고 이를 응용한 전략적 재보장의 패러다임을 살펴보았다. 결론적으로 사람들의 일상생활에 깊숙하게 연동된 사이버 공간의 특성상 억지 전략에 일정한 제약이 따르며, 자원의 한계를 고려한 선택과 집중의 원칙에 따라 적정한 수준의 억지를 지향해야 한다는 점을 강조하였다.

제2장 '국제규범론으로 보는 사이버 안보(이상현)'는 사이버 공간을 둘러싼 강대국들의 이해가 충돌하고 민간의 우려가 커지는 가운데 최근 주목받고 있는 유엔 등 다자무대에서 벌어지는 국제협력의 양상을 살펴보았다. 사이버 범죄나 안보는 이미 국제적으로 중요한 사안으

로 부상했지만 국제규범이나 법적 통제는 미약하다. 사이버 공간에 관한 국제적 논란의 핵심은 인터넷 자유와 사이버 안보의 적절할 균형을 어떻게 설정할 것인지에 집중된다. 사이버 안보의 국제적 논의에서 최근의 진전은 몇 가지 중요한 이정표를 거쳐 발전해 왔다. 그중 대표적인 것으로는 유럽평의회의 사이버 범죄에 관한 글로벌 프로젝트의 일환으로 탄생한 부다페스트 협약과 탈린매뉴얼을 들 수 있다. 국제기구 차원에서는 대표적으로 유엔 정보안보 정부전문가 그룹(GGE)을 통해 사이버 안보 확보를 위한 국가 간 규범 문제를 논의 중이다. GGE의 주요 내용 중 일부 쟁점에서 괄목할 만한 진전을 기록한 것은 제3차 GGE 보고서(2013)에서였다. 3차 권고안에서는 사이버 공간의 주권이 인정되고, 사이버 공격에 대한 자위권 차원의 무력 사용이 인정되며, 비국가 행위자의 사이버 위협에 대한 국가의 책임 소재를 분명히 하는 등의 진전이 이뤄졌다. 한국은 2013년 서울 사이버 공간 총회를 주최하는 등 사이버 공간의 규범 확립을 위한 국제적 움직임에 적극 참여하고 있다. 제2장이 주장하는 바에 따르면, 향후 사이버 안보 관련 국제규범은 국제사회의 논의를 거쳐 서서히 규범화되는 과정을 거칠 것으로 예상되는 바, GGE 및 사이버 공간총회 등 국제적 행사를 계기로 '지속 가능한' 국제적 협력의 규범과 틀을 제도화하는 방향으로 후속 조치를 강화해야 할 것이다.

제3장 '글로벌 거버넌스론으로 보는 사이버 안보(배영자)'는 사이버 안보에 관한 국제협력 가운데 국제규범 마련과 관련된 노력을 글로벌 거버넌스의 관점에서 살펴보았다. 현재 진행 중인 사이버 안보 국제규범에 관한 논의 중에서 부다페스트 협약, 사이버 공간 총회, 국제전기통신연합(ITU), 상하이협력기구(SCO), 인터넷주소관리기구(ICANN) 등에서 진행되고 있는 사이버 안보 국제규범에 관한 논의에

초점을 맞추었다. 현재 사이버 안보 국제규범에 관한 논의는 크게 사이버 공간의 국가주권 인정과 기존 국제법 적용 여부를 둘러싸고 서방 측과 러시아·중국 측이 대립하고 있는 가운데 양측의 지속적인 협상이 다양한 장에서 진행 중이다. 부다페스트협약과 사이버 공간총회에서는 서방 측 이해가, SCO와 ITU에서는 러시아와 중국 측 이해가 두드러지고 있음을 확인할 수 있다. 아울러 참여자 측면에서 볼 때 부다페스트협약, ITU, SCO는 국가들이 중심이 되어 진행되고 사이버 공간총회나 ICANN은 기업이나 관련 시민사회단체나 기업도 함께 하는 장으로 발전해 왔다. 전반적으로 볼 때 시민사회의 참여는 아직 부족한 편이고 국가 주도로 논의가 이루어지고 있음을 알 수 있다. 현재 점증하는 사이버 위협에 대한 일치된 우려와 국제협력의 필요성에 대해서는 공감대가 형성되어 있음을 확인할 수 있다. 비록 현재까지 범세계적으로 강제력을 가지는 합의된 국제조약은 마련되지 못했지만 그동안의 지속적인 노력을 통해 각 국가 간 입장의 차이가 분명히 드러나고 서로 협력할 수 있는 선이 어디까지인지를 알게 된 것은 큰 의미를 가지는 성과로 평가된다. 다만 국가 간의 입장 차이가 단시일 내에 좁혀지거나 조정될 수 있는 수준이 아니어서 이에 대해서는 지속적인 대화와 협력이 요구되는 상황이다.

제2부 '사이버 안보의 주변4망(網): 전략과 외교'에서는 한반도의 사이버 안보 문제에 영향은 미치는 주변의 네 나라, 즉 미국, 중국, 일본, 러시아의 전략과 외교에 주목하였다. 전통안보 분야에서는 한반도 주변의 네 강대국이라는 의미로 주변4강(强)이라는 표현을 주로 쓰지만 이 책에서는 네 개의 네트워크 또는 네트워크 국가라는 의미로 주변4망(網)이라는 개념에 입각해서 논의를 전개하였다.

제4장 '미국의 사이버 안보 전략과 외교(신성호)'는 사이버 공간

의 가장 큰 기술적 리더이자 수혜자이며, 또한 각종 사이버 공격의 가장 큰 대상이기도 한 미국의 사례를 살펴보았다. 미국은 정보의 자유로운 소통과 접근, 개인의 의사 표현과 정보 습득 권한 보장, 열린 사이버 공간을 통한 개인과 민간, 국가 이익의 증진 등을 목표로 사이버 범죄로부터 이들 가치와 원칙을 지키기 위한 국내정책, 국제협력, 국제규범 창출에 노력하고 있다. 특히 미국은 사이버 안보 관련 국제규범과 통치제도의 창출을 위해 다음과 같은 원칙을 가지고 노력을 경주하고 있다. 첫째, 사이버 공간과 인터넷 표현의 자유, 개방, 신뢰 등 기본 원칙이 존중되어야 한다. 둘째, 사이버 공간을 사용하고 있는 개인, 산업계, 시민사회 및 정부기관 등 다양한 구성원들의 의견이 수렴된 국제적 규범을 제정해야 한다. 셋째, 인터넷 및 사이버 공간에도 규범 원칙을 설정함에서 그 출발은 유엔헌장과 같은 기존의 국제규범과 법을 토대로 하여야 한다. 넷째, 상호 간 사이버 공간상의 위협 요소 감축 및 신뢰 증진을 위한 사이버 공간에 적용 가능한 신뢰구축조치(CBMs: Confidence Building Measures)의 이행이 필요하다. 그러나 미국의 노력은 이에 대한 다른 이해관계와 접근을 추구하는 중국이나 러시아와의 갈등을 야기하기도 한다. 그럼에도 미국의 사이버 안보 전략은 향후 한국을 비롯한 각국의 사이버 안보 전략은 물론 글로벌 사이버 질서 확립에서도 많은 시사점을 줄 것이라고 전망한다.

제5장 '일본의 사이버 안보 전략과 외교(이승주)'는 2014년 사이버안보기본법을 제정한 이후 정책의 기본 방향을 제시한 일본의 사례를 다루었다. 제5장은 일본이 사이버 안보 전략과 외교를 강화하게 된 원인을 네 가지 차원에서 설명하였다. 첫째, 일본은 사이버 위협이 빈발함에 따라, 사이버 위협이 경제 및 사회에 미치는 영향을 새롭게 인식하게 되었다. 일본 정부는 규제와 프라이버시 보호의 균형을 유지하면서 질서를 유지하는 자율 거버넌스 형성에 주안점을 두고 있다. 둘째, 일본의 사이버 전략과 외교는 일본 외교안보 정책과의 연계라는 관점에서 이해할 필요가 있다. 이는 일본의 새로운 국가안보전략 변화와 연계되어 진행되는 경향이 있으며, 더 나아가 중국의 부상에 대응하고, 이 과정에서 역내 국가들과의 협력을 강화하는 수단이라는 의미가 있다. 셋째, 일본은 사이버 안보 전략과 외교에서 국제협력을 강조하는 대표적인 국가이다. 일본은 특히 사이버 안보 외교를 다양한 차원에서 추진하는 가운데 가치를 공유하는 국가들과 사이버 분야의 국제질서와 규범을 확립하는 데 주도적 역할을 하겠다는 의지를 반복적으로 천명한 바 있다. 넷째, 일본의 사이버 안보 전략과 외교는 민관협력을 강조하고 있다. 일본이 기업들이 초국적 공급 사슬을 형성하고 있기 때문에, 국내 기업뿐만 아니라 그 대상을 외국에 위치한 자국 기업으로 사이버 안보의 대상을 확대해야 할 현실적 필요성이 커졌다. 또한 일본 정부는 아시아의 개도국들과 사이버 안보를 위한 국제협력을 심화, 확대하는 가운데 일본 IT기업의 해외 진출을 측면 지원하려는 의도를 내보이고 있다.

제6장 '중국의 사이버 안보 전략과 외교(정종필·조윤영)'는 최근 인터넷과 사이버 공간에 대한 정책적 행보가 주목을 끌고 있는 중국의 사례를 다루었다. 중국은 2000년대에 들어와 전자·정보 산업 발전에 따른 인터넷 보급 확대와 국내외 정보 교류가 활발해졌다. 하지만 이로 인해 오히려 사이버 안보의 취약성은 심화되었다고 평가받는다. 따라서 사이버 공간의 보호를 위해 정보화 전략을 바탕으로 국방·군사 시스템 개선을 추구하고 나아가 사회 안정을 유지하고자 한다. 이를 위해 2014년부터 정치·사회 사이버 안보 정책 수립과 집행 업무를 '중앙네트워크안전·정보화영도소조'와 '국가인터넷정보판공실'로 일

원화 했다. 또한 사이버 군사 전략은 공산당 중앙군사위원회에서 담당하기 시작했다. 사이버 안보 강화를 위한 중국의 정책은 다른 나라와 유사하다. 국가 안보, 기업·개인 경제활동 등에 악영향을 미치는 활동을 차단해 인터넷을 보호하고자 하는 것이다. 하지만 중국은 국내 인터넷 보호를 위해 국가의 주도적 역할을 강조하는 국가 중심적 전략을 취한다는 점에서 미국을 포함한 서구 국가와 큰 차이를 보인다. 특히 중국은 사이버 공간의 개방성, 포괄성, 상업성에도 불구하고 각 국가의 특수성은 우선돼야 한다고 주장한다. 이 같은 인식은 미국과의 마찰을 불러일으키고 있다. 그럼에도 전략경제대화를 통한 미국과의 사이버 안보 협력을 위해 노력하고 있다. 또한 SCO와 아세안지역포럼(ARF) 내에서의 역내 국가들과 사이버 안보 의제를 논의하기 위해 주도적 역할을 하고 있다. 나아가 유엔 내 GGE 활동에 적극적으로 참여하고, ITU을 통한 인터넷 거버넌스 개혁을 위해 노력하고 있다.

제7장 '러시아의 사이버 안보 전략과 외교(신범식)'는 사이버 안보 분야에서 미국 중심의 서구 질서에 대항하면서도 제한적인 협력을 펼치는 러시아의 전략과 외교의 사례를 다루었다. 러시아의 사이버 안보 전략의 가장 큰 특징은 크게 세 가지이다. 첫째, 서방과는 다른 '사이버 공간'에 대한 인식이 투영되어 있다는 점이다. 즉 서방이 자유로운 정보의 흐름을 강조하는 것과 달리, 러시아는 사이버 공간도 분명히 주권국가의 관할권이 행사되는 영역임에 상당한 방점을 두고 있다. 둘째, 사이버 역량을 디지털 시대에 국익을 제고할 수 있는 분명한 수단으로 본다는 점이다. 이러한 관점에는 외부의 러시아 사이버 공간에 대한 공격 가능성은 상존하고, 국가에 미치는 타격이 엄청나다는 인식이 반영되어 있다. 이를 뒷받침하기 위해 러시아 정부는 적극적으로 관련 입법 절차를 실시하여 왔다. 셋째, 사이버 보안 업무 소관 부서를 기존의 정보기관에서 군으로 전환시키고 있다는 점이다. 주어진 위협을 분석하는 수동적인 업무가 아닌 공세적으로 사이버 역량을 신장시키겠다는 러시아의 의도가 담겨있다. 동시에 재래전과 사이버전은 상호 병행될 수 있음이 암시되고 있다. 이러한 러시아의 전략은 서방과 갈등을 겪을 소지를 다분히 갖고 있다. 실제로 러시아는 중국과의 협력은 강화하였지만, 미러관계는 개선되지 못 하는 등 반(反) 서방 진영의 선두주자 이미지를 굳혀가고 있다. 향후 러시아는 자유로운 정보의 흐름을 강조하는 서방에 대항하여 주권적 요소를 부각시키는 '인터넷 거버넌스의 국제화'를 추진할 것으로 보인다.

제3부 '한반도의 사이버 안보: 현황과 과제'에서는 앞서의 장들이 제기한 국제정치학의 이론적 논의와 주변4망(網)의 전략과 외교에 대한 경험적 논의를 바탕으로 북한의 지속적인 사이버 공격에 대응하는 한국의 사이버 안보 전략을 국내적인 차원에서 기술과 인력의 양성 및 법제도의 정비, 그리고 대외적인 차원에서 양자 및 다자 협력의 필요성을 강조하였다.

제8장 '북한의 사이버 안보 역량과 전략(황지환)'은 사이버 안보의 국가전략에 대한 논의에서 주관심사가 될 수밖에 없는 북한의 사례를 재래식 전략과 핵전략의 연속선상에서 다루었다. 북한에서 사이버 능력은 핵, 미사일과 함께 인민군의 3대 수단으로 간주되며, 사이버 전력은 핵·미사일, 게릴라전과 함께 북한의 3대 비대칭 전력으로 평가받고 있다. 이러한 관점에서 북한의 김정은 노동당 제1비서는 "사이버전이 핵, 미사일과 함께 인민군대의 무자비한 타격능력을 담보하는 만능의 보검"이라고 언급하며 사이버전의 중요성을 강조하였다. 한국에 대한 사이버 공격 활동은 2009년 7월의 디도스 공격 이후 최근의 정부 주요 인사 스마트 폰 해킹까지 다양하게 진행되어 왔다. 사이버

전 활동의 특성상 한국에 대한 모든 사이버 공격 활동이 북한에 의한 것이라고 단정할 수는 없다. 하지만 공격의 대상과 형태 및 방식 등에서 북한의 대남 사이버전 활동이라고 추정할 수 있는 근거는 많다. 해킹 공격의 중국 선양 경유지 IP, 범행에 사용된 악성코드의 구성과 동작방식, 협박 이메일의 표현 등을 고려하면, 상당수가 북한이나 북한 추종 세력들에 의한 공격으로 추정된다. 남북한 관계가 불안정하고 북한의 핵과 미사일 위협이 가중되는 상황에서 북한의 사이버 안보 역량은 우리에게 또 하나의 커다란 위협요인을 제공해 주고 있다. 미국 역시 소니 픽쳐스 해킹 사건 이후 북한의 사이버 역량과 공격에 대해 커다란 관심을 가지고 있다.

제9장 '한국의 사이버 안보 전략과 외교(김상배)'은 최근 지속적으로 발생하고 있는 북한발 사이버 공격에 대응하는 과정에서 제기되는 한국의 사이버 안보 전략과 외교의 과제를 짚어 보았다. 사실 한국의 입장에서 보면 사이버 안보의 문제는 추상적인 위협과 대응의 문제가 아니라 엄연히 실재하는 위협이 아닐 수 없다. 최근 북한의 소행으로 추정되는 사이버 공격이 늘어나면서 이러한 위협이 일단 유사시에 재래식 전쟁이나 핵전쟁의 시나리오와 결합되면 무슨 일이 벌어질까 하는 우려를 낳고 있기 때문이다. 이러한 맥락에서 한국은 기술적인 차원에서 방어 역량을 구비하고, 사이버 안보의 추진체계와 법제도적 여건을 정비하려는 노력들을 벌이고 있다. 이와 더불어 주변국들과 사이버 공격 관련 위협 정보를 공유하고 더 나아가 글로벌 및 지역 차원에서 협력하기 위한 체제도 가동하고 있다. 그런데, 제9장이 주장하는 바에 따르면, 여태까지 일국적 차원의 대응 체계를 마련하는 데 주안점을 두었던 한국의 대응 방안도 이제는 좀 더 적극적으로 미국, 중국, 일본, 러시아 등과 같은 주변국들과의 협력을 벌일 필요가 있다. 이러한 모색의 과정에서 관건이 되는 것은 주변국들과 정보공유체계를 만들고, 사법공조를 위한 외교적 노력을 펼치거나, 사이버 안보의 국제규범 형성에 참여하고, 국제사회에 호소하고 도움을 요청하는 외교적 역량의 발휘이다. 이러한 문제의식을 바탕으로 제9장은 사이버 안보 분야에서 한국이 모색해야 할 국제안보 및 외교전략의 방향과 이 분야에서 부상하고 있는 국제규범 형성에 참여하는 과정에서 해결해야 할 과제들을 상세히 검토하였다.

끝으로, 제10장 '사이버 안보 국가전략의 과제'는 이 책에 실린 논문들의 최종원고발표회를 겸해서 열린 컨퍼런스에서 가진 종합토론의 내용을 이 책의 결론을 대신해서 담았다. 종합토론에서 다룬 가장 큰 주제는 사이버 안보의 연구와 실천 전략의 모색 과정에서 여타 전공 분야와 비교해서 국제정치학이 기여할 수 있는 바는 무엇인가의 문제였다. 그리고 이러한 시각에서 입각해서 볼 때 한국이 사이버 안보 분야에서 추구할 전략과 외교의 방향과 내용은 무엇인지를 규명하는 것이었다. 이러한 문제의식을 바탕으로 크게 세 가지 그룹으로 대별되는 주제들을 탐구하였다. 첫째, 북한의 사이버 공격을 어떻게 볼 것인가의 문제였다. 북한은 어느 정도의 역량을 지니고 있고, 이를 뒷받침하는 조직과 제도의 현황은 어떠한가? 북한의 사이버 공격을 포함한 초국적 사이버 공격을 보는 한국의 인식은 어떠한가? 둘째, 북한의 사이버 공격에 대응하는 한국의 전략과 제도에 대한 문제였다. 사이버 방어와 억지를 수행하는 한국의 기술역량과 인력 현황은 어느 정도의 수준인가? 사이버 위협에 대응하는 추 진체계와 법제를 구축해 가는 차원에서 현재 한국이 해야 할 일은 무엇인가? 끝으로, 사이버 안보 분야에서 한국이 추구할 외교에 대한 문제였다. 사이버 위협에 대응하는 차원에서 한국이 주변 국가들과의 국제협력을 풀어가기 위해서 당면

한 외교적 과제는 무엇인가? 최근 다층적으로 진행되고 있는 사이버 안보의 국제규범 형성 과정에 한국은 어떻게 참여해야 하는가?

이 책이 나오기까지 많은 분들의 도움을 얻었다. 무엇보다도 국제정치학계에는 아직 생소한 주제인 사이버 안보에 대한 연구에 기꺼이 동참해 주신 필자 선생님들께 감사드린다. 이 책에 담긴 글들은 몇 가지 계기를 통해서 기획되어 준비되었다. 특히 2016년 여름 방학을 전후하여 진행된 공부모임을 통해서 그 형체를 갖추어 나갔다. 이 공부모임은 몇 차례의 세미나를 거치면서 '사이버 안보의 세계정치 공부모임(일명 사세공)'이라는 이름까지 얻게 되었다. 사세공을 통해서 이루어진 발표와 토론은 사이버 안보의 국제정치학 연구를 위한 화두를 던지려는 필자들의 문제의식을 무르익게 하였으며, 이 책을 학계에 내놓게 되는 지적 토양을 제공하였다.

사세공 세미나에 참여하여 함께 토론의 시간을 가진 서울대학교 정치외교학부와 이화여자대학교 정치외교학과의 대학원생들에게도 감사의 마음을 전한다. 이 책에 담긴 기성 학자들의 글 모음과는 별도로 이들 대학원생들의 작업은 2016년 12월 한국국제정치학회 연례학술회의에서 대학원생 패널을 구성하여 학계에 소개되었으며 곧이어 별도의 단행본으로 묶어내려고 준비하는 중에 있다.

이 책에 담긴 논문의 초고들은 2016년 10월 13일(목) 한국프레스센터에서 서울대학교 국제문제연구소(소장: 김상배)와 국가보안기술연구소(소장: 김광호)의 공동주최로 열린 〈사이버 안보의 국가전략: 국제정치학의 시각〉이라는 제목의 학술회의에서 발표되었다. 귀중한 시간을 내어 환영사와 기조연설의 말씀을 주신 김광호 소장님과 임종인 전 대통령 안보특보께 감사드린다. 당일 불가피한 일정으로 참석은 못하셨지만 따로 축하의 말씀을 전해주신 신맹호 외교부 국제안보대사께도 고마움을 전하고 싶다.

또한 학술회의 당일, 사회와 발표 및 토론을 맡아주신 임종인(고려대), 신욱희(서울대), 전혜원(국립외교원), 박노형(고려대), 박윤정(한국뉴욕주립대), 도종윤(제주평화연구원), 박민형(국방대학교), 전재성(서울대), 김웅희(인하대), 이민자(서울디지털대) 선생님께 감사의 말씀을 드린다. 특히 종합토론을 벌인 제3부에서 사회 및 토론을 맡아주신 조현석(서울과학기술대), 류석진(서강대), 장노순(한라대), 조화순(연세대), 김소정(국가보안기술연구소), 권헌영(고려대), 이원태(정보통신정책연구원), 유지연(상명대), 강하연(정보통신정책연구원) 선생님께 심심한 감사의 말씀을 드리고 싶다. 그날 진행된 종합토론의 내용은 녹취되어 이 책의 제10장에 담겼다.

이밖에 사세공 세미나와 학술회의의 원활한 진행을 위해서 도움을 준 서울대학교 국제문제연구소의 이종진, 조문규, 이은솔 연구원, 그리고 한국연구재단의 한국사회기반연구사업(SSK: Social Science Korea) 대형센터의 전임연구원인 송태은, 이헌미, 차태서 박사와 참여연구원인 최은실, 김유정, 문영란, 김지훈, 이요셉 연구원 등에게도 감사의 마음을 전하고 싶다. 끝으로 성심껏 이 책의 출판을 맡아주신 사회평론아카데미의 관계자들께도 감사의 말씀을 전한다. 또한 이 책의 원고 교정 작업을 도와준 ooo에게도 고마움을 전한다.

2016년 12월 24일

김 상 배

제3부 한반도의 사이버 안보: 현황과 과제

국제정치학으로 보는 사이버 안보