2015).
Kim, Sung. 2015. Special Representative for North Korea Policy, "The North Korean Threat: Nuclear, Missiles and Cyber." Testimony before the House Foreign Affairs Committee, Washington, DC. January 13 2015.
Lewis, James. 2010. "Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace." 38 North, September 7 2010.
Mansourov, Alexandre. 2014. "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance." Academic Paper Series(Korea Economic Institute of America, December 2014).
Technolytics. 2011. "Cyber Commander's eHandbook version 2.0." Technolytics.

제9장

한국의 사이버 안보 전략과 외교*

김상배

* 이 장의 제3절과 제4절은 김상배(2017). "사이버 안보의 주변4망(網)과 한국: 세력망의 구조와 중견국의 전략." 『국제정치논총』, 57(1)의 일부 내용을 수정 보완하여 작성하였음.

I. 머리말

사이버 안보의 문제가 전통안보의 문제만큼이나 중요한 국가안보의 사안으로 새롭게 조명받고 있다. 글로벌 차원에서 벌어지는 해커들의 사이버 공격이나 이를 방지하기 위한 국제협력의 필요성에 대한 세계 각국의 관심도 점점 더 커지고 있다. 한국의 입장에서 보면 사이버 안보의 문제는 추상적인 위협과 대응의 문제가 아니라 엄연히 실재하는 위협이 아닐 수 없다. 그도 그럴 것이 최근 북한의 소행으로 추정되는 사이버 공격이 늘어나면서 이러한 위협이 일단 유사시에 재래식 전쟁이나 핵전쟁의 시나리오와 결합되면 무슨 일이 벌어질까 하는 우려를 낳고 있기 때문이다. 그런데 사이버 공격은 잘 알려지지 않은 컴퓨터 바이러스나 악성코드를 사용할 뿐만 아니라 그 공격의 수법도 점점 더 교묘하게 바뀌고 있어 단순히 기술적으로 방어벽을 쌓는 것만으로는 막아내기 어렵다. 이러한 맥락에서 군사적인 차원에서 방어와 억지의 역량을 구비하고, 좀 더 넓은 의미에서 추진체계의 정비와 법제도적 여건을 정비하려는 노력들이 활발히 이루어지고 있다.

이와 더불어 주변국들과 사이버 공격 관련 위협 정보를 공유하고 더 나아가 글로벌 및 지역 차원에서 협력하기 위한 체제도 가동되고 있다. 사이버 위협에 대한 방어와 억지 역량의 구축이나 추진체계 정비와 법제정의 노력만으로 초국적 사이버 공격에 대한 대응 방안을 충분하게 마련하기 어렵기 때문이다. 사이버 안보 분야의 기술구조적 특성상 기술·전략과 제도·법을 통해서 구축된 '그물망 방패'는 아무래도 빈틈이 있을 수밖에 없다(Deibert 2013). '버추얼(virtual) 창'을 떠올리게 하는 사이버 공간의 보이지 않는 공격을 막아내기 위해서는 국제적인 차원에서 관련 주체들의 협력과 공조가 필요하다. 이러한 관점에서 볼 때, 여태까지 일국적 차원의 대응체계를 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.

사실 인터넷의 보급이 매우 미미하여 보안 층위를 크게 중시하지 않던 초창기에는 컴퓨터 보안이나 정보보호는 컴퓨터 전문가나 소프트웨어 엔지니어들의 몫이었다. 그러나 최근 사이버 안보는 여러 가지 면에서 명실상부하게 국제정치학의 핵심 논제가 되었다.[1] 컴퓨터 해킹 기술이 빠르게 확산되면서 사이버 공격이 물리적 공격만큼 큰 재난을 야기할 가능성을 인식하고 이를 방지하기 위한 국가 간 또는 국제기구 차원의 협력이 모색되고 있다. 최근 새로운 틀을 모색하고 있는 글로벌 인터넷 거버넌스의 과정에서도 사이버 안보는 가장 논쟁적인 어젠다 중의 하나이다. 최근 사이버 안보 문제는 21세기 세계패권을 놓고 다투고 있는 미국과 중국 양국관계에 중요한 현안으로서 거론되기에 이르렀다. 특히 양국은 해킹과 도청 등의 문제를 놓고 갈등의 싹을 점점 키워가고 있다. 사이버 안보는 최근 나타난 신흥이슈임에도 전통적으로 미중 관계를 지배해 온 분야 못지않게 양국의 국가안보를 위협할

1 이 글은 사이버 안보의 세계정치와 국가전략에 대한 논의를 펼침에 있어서 주로 (국제)정치학의 시각을 취하였다. 따라서 기술·전략이나 거버넌스·법에 대한 논의를 하더라고 그러한 대응방안들이 지니는 권력적 함의와 국가전략적 의미를 드러내려는 시각을 취하고 있다. (국제)정치학의 시각에서 사이버 안보를 보는 국내연구로는 이상현(2008), 최인호(2011), 조현석(2012), 장노순·한인택(2013), 김상배(2014a, 제11장; 2014b; 2015a; 2015b; 2015c; 2016), Kim(2014), 민병원(2015), 장노순(2016) 등을 참조하기 바란다.

수 있는 문제로 간주되고 있다.

한국은 이른바 '인터넷 강국'으로서 첨단 정보통신 기기와 글로벌 최고 수준의 인터넷 인프라를 자랑하지만, 북한의 사이버 공격 앞에서는 취약하다. 북한의 사이버 공격을 막기 위한 역량을 키우는 것은 중요한 과제가 아닐 수 없다. 그렇지만 사이버 안보의 게임은 기본적으로 공격이 방어의 우위에 서는 게임이다. 아무리 훌륭한 방어 기술과 전문 인력을 갖추고 있고, 또한 이를 지원하는 법제도를 구비하더라도 사이버 공격의 목표가 되는 빈틈을 모두 막을 수는 없다. 따라서 사이버 공간의 안보를 확보하기 위해서는 기술적·제도적 조치만으로는 안 되고 주변의 관련 국가들과의 협력을 통해서 문제를 정치적·외교적으로 풀어나가려는 노력이 병행되어야 한다. 이러한 맥락에서 이 글은 사이버 안보 분야에서 한국이 모색해야 할 국제안보 및 외교전략의 방향과 이 분야에서 부상하고 있는 국제규범 형성에 참여하는 과정에서 해결해야 할 과제들을 살펴보았다.

이러한 문제의식을 가지고 볼 때, 현재 한국은 사이버 안보의 전략과 외교를 모색하기 위한 세 가지 과제를 안고 있다. 첫째, 지속되는 사이버 위협에 대응하여 사이버 안보 관련 기술을 개발하고 인력을 양성하려는 노력을 기울일 뿐만 아니라 이를 효과적으로 뒷받침하는 추진체계와 법제도를 정비할 과제를 안고 있다. 이러한 고민과 맥을 같이 하여 최근 다양한 대응방안이 검토 또는 모색되고 있다. 예를 들어, 2014년 말 한국수력원자력(이하 한수원) 사태와 소니 영화사에 대한 북한의 해킹 사건(이하 소니 해킹 사건) 이후 2015년에 접어들면서 청와대 안보특보의 임명, 사이버안보비서관의 신설 등을 포함하여 사이버 안보 추진체계가 정비되었고, 다양한 기술개발과 인력양성을 위한 재정적·제도적 지원책들이 논의되었다. 또한 북한의 해킹 공격을 국가안보에 대한 중대한 위협으로 보고 이를 억지하기 위한 능력을 확보하려는 고민도 깊어 가고 있다. 그러나 전 세계적으로 가장 높은 사이버 공격의 위협에 처해 있음에도 불구하고 사이버 안보 관련 법규 제정이 난항을 겪고 있는 현실은 한국 정치사회가 안고 있는 아이러니컬한 문제가 아닐 수 없다.

둘째, 사이버 방어가 지니는 기술적 난제를 보완하는 차원에서 미국, 중국, 일본, 러시아 등 주변4망(網) 국가들과의 협력과 공조체제를 구축할 과제를 안고 있다. 전통적인 한미동맹을 염두에 둘 때 사이버 안보 분야에서도 한미 간에는 밀접한 협력이 필요함은 물론이다. 그러나 북한과 특수한 관계에 있는 중국과의 협력도 사이버 공격의 진원지를 색출하고 북한에 외교적 압력을 넣는다는 차원에서 필수적이다. 최근에는 사이버 안보 분야에서 갈등의 양상을 보이고 있는 미중 사이에서 한국은 어떠한 노선을 취해야 할까? 또한 미국의 아태전략과 동아시아 지역의 사이버 협력 사이에서 한국이 취할 수 있는 선택지는 무엇일까? 좀 더 구체적으로는 사이버 안보 분야에서 일본이나 러시아와 같은 주변 국가들과의 관계는 어떻게 풀어나가야 할까? 이런 점에서 사이버 안보의 주변4망(網)의 이해관계와 세력구도를 제대로 읽고 그 속에서 한국이 차지하는 위상과 역할을 파악하는 일은 시급한 과제가 아닐 수 없다.

끝으로, 사이버 안보 분야 국제규범 형성에 적극적으로 참여하여 중견국으로서 한국의 외교적 역량을 발휘하는 과제를 안고 있다. 최근 사이버 안보 논의의 장으로 크게 주목받고 있는 유엔 군축 및 국제안보 위원회 산하 정보보안 관련 정부전문가그룹(GGE: Group of Governmental Experts)의 활동뿐만 아니라 사이버공간총회와 같은 선진국들의 정부 간 협의체, 그리고 글로벌 인터넷 거버넌스를 주도해 온

ICANN(Internet Corporation for Assigned Names and Numbers)의 틀에 이르기까지 다층적으로 작동하고 있는 사이버 규범의 모색 과정을 예의주시하고, 그러한 다층적 구조 속에서 한국이 차지하는 위상과 그에 적절한 역할을 찾는 노력이 필요하다. 특히 미국과 서구 국가들로 대변되는 서방 진영과 러시아, 중국 등의 비서방 진영 사이에서, 그리고 선진국 클럽과 개도국 그룹 사이에서 한국이 중견국으로서의 외교적 역할을 적극적으로 수행할 가능성은 얼마나 있을지에 대한 본격적인 고민이 필요하다.

이 글은 크게 세 부분으로 구성되었다. II절은 사이버 위협에 대한 한국의 인식과 이에 대응하기 위해서 펼치는 기술개발과 인력양성 및 전략개발의 문제, 그리고 이러한 연속선상에서 현재까지 추진된 사이버 안보의 추진체계와 법제정을 둘러싼 논란 등을 살펴보았다. III절은 사이버 안보 분야에서 진행되고 있는 주변국들의 협력과 갈등의 현황, 그리고 이에 대처하는 한국의 외교적 과제를 살펴보았다. 북한의 사이버 공격과 한미동맹의 과제, 북중 변수와 미중 사이 한국의 딜레마, 미국의 아태전략과 한일 사이버 협력, 한중일 사이버 협력과 동아시아 담론, 미러경쟁과 중러협약 사이의 한국 등의 주제들을 검토하였다. IV절은 사이버 안보 분야에서 다층적으로 진행되고 있는 국제규범 형성의 움직임과 그 안에서 엿보이는 갈등과 협력의 동학, 그리고 이 분야에 참여하는 과정에서 제기되는 과제들을 중견국 외교론의 시각에서 살펴보았다. 맺음말에서는 이 글에서 제시한 한국의 사이버 안보 전략과 외교에 대한 주장을 종합·요약하고 이러한 과제를 해결하는 것은 21세기를 헤쳐 나가는 미래 국가전략의 사안임을 강조하였다.

II. 사이버 안보의 인식과 역량 및 제도

1. 사이버 위협에 대한 인식

최근 글로벌 및 동아시아 차원에서 사이버 안보에 대한 관심이 정책서클뿐만 아니라 학계와 대중 사이에서도 크게 늘어나고 있다. 한반도에서도 2010년대로 접어들면서 북한의 소행으로 추정되는 사이버 공격이 지속적으로 발생하고 있다. 크게 밝혀진 것만 보아도 2009년 7월 7일 7·7 디도스 공격, 2011년 3월 4일 3·4 디도스 공격, 2011년 4월 12일 농협 전산망 해킹 사건, 2012년 6월 9일 중앙일보 해킹 사건, 2013년 3월 20일 3·20 방송·금융사 침입 사건, 2013년 6월 25일 6·25 디도스 공격 등이 있다. 가장 최근에 사이버 안보에 대한 국내의 관심을 증폭시킨 사례로는 2014년 12월 한수원에 대한 해킹 사건이 있었다. 이상의 사이버 공격들은 한국의 공공기관이나 금융사 및 언론방송사 등의 전산망에 존재하는 빈틈을 노리고 수십만 대의 좀비 PC를 동원하여 분산서비스거부(DDoS: Distributed Denial of Service) 공격을 벌이거나 좀 더 교묘하게 이루어지는 지능형지속위협(APT: Advanced Persistent Threat) 공격을 가하는 방식으로 이루어진 것으로 알려졌다.[2]

한반도 밖에서도 2014년 11월에 발생한 소니 해킹 사건으로 북미 간에 긴장감이 감돌았다. 미국은 북한의 소니 해킹을 자국의 국가안보에 대한 중요한 도전으로 간주하고 즉각적인 반응을 보였다. 오바마

2 북한의 사이버 공격 역량에 대해서는 탈북 컴퓨터 공학자인 김흥광의 증언(김흥광, 2011)과 임종인 외(2013), Mansourov(2014), 그리고 최근 미국의 CSIS(Center for Strategic and International Studies)에서 나온 보고서인 Jun et al(2015)를 참조하기 바란다.

대통령은 북한의 해킹 공격을 '사이버 반달리즘'이라고 비판하며 이른바 '비례적 대응'을 천명했다. 이후 북한의 인터넷 접속이 전면 불통되고 이동통신망이 마비되는 일이 벌어졌으며, 북한에 대한 금융제재를 위한 행정명령이 내려지기도 했다. 이런 와중에도 미국은 중국 해커들에 의한 자국 정보인프라와 지적재산에 대한 공격에 맞서 단호한 대응의 자세를 보였다. 게다가 미중 양국은 모두 사이버 안보와 관련된 국내법을 제정하려는 움직임에도 박차를 가하고 있어 그 경쟁의 양상이 21세기 패권경쟁의 한 단면을 보는듯한 모습으로 발전하고 있다. 사이버 안보 분야의 특성상 제한된 정보만이 공개되고 있음에도, 현재 미국과 중국 사이에서 보이지 않는 사이버 공방이 벌어지고 있는 것을 미루어 짐작하는 일은 어렵지 않다.

이러한 일련의 사태 전개 속에서 한국 정부는 북한의 사이버 공격을 심각한 위협으로 인식하고 있다. 정부는 통일부 대변인 성명을 통해 "북한이 다양한 경로를 통해 한수원 관련 자료를 절취한 후 우리 국민의 생명과 안전을 볼모로 원전을 파괴하겠다고 위협하고 관련 자료를 여러 차례 나누어 공개함으로써 우리 사회의 혼란을 야기하려 한 것은 우리 안보에 대한 명백한 도발"이라는 수사결과를 발표했다. 정부는 "이번 사건을 포함해 북한이 우리와 국제사회에 대해 사이버 테러를 지속적으로 감행하고 있는 것에 대해 규탄하며 즉각 중단할 것을 촉구한다"고 밝혔다. 이에 앞서 정부 합동수사단은 한수원 공격에 쓰인 악성코드가 북한 해커 조직이 쓰는 것과 구성 및 동작 방식이 비슷하고 범행에 사용된 IP가 북한과 연관된 점 등을 들어 이 사건이 북한 해커조직의 소행으로 보인다는 내용의 중간 수사결과를 발표한 바 있었다(아주경제 2015.03.17). 이러한 위협인식은 그 후 사이버 공격에 대한 체계적인 대응 및 대비 체제를 갖추는 차원에서 사이버 안보비서관의 신설로 이어지기도 했다.

북한의 사이버 위협에 대응하는 한국 정부는 기술적인 대책을 포함하여 동원 가능한 모든 수단과 방법을 적절히 원용하겠다는 입장을 취하고 있다. 특히 사이버 공격이 갖는 기술적 특성이나 한반도 및 동북아의 지정학적 특성을 고려할 때, 주변국가 및 국제사회와의 긴밀한 협력이 필요하다는 인식을 갖고 있다. 예를 들어, 한수원 사태가 발생하기 1년여 전인 2013년 10월 서울에서 열린 사이버공간총회 개회식 축사에서 박근혜 대통령은 "인터넷 환경이 발달할수록 개인정보 유출과 스팸, 악성코드 유포를 비롯한 사이버 보안에 대한 위협도 갈수록 커지고 있다"며 "사이버 공간의 개방성을 최대한 보장하면서도 이런 위험을 방지할 수 있는 국제적 규범과 원칙을 함께 만들어야 한다"고 주장했다. 또한 "우리가 직면한 이러한 도전과제들은 어느 한 국가 차원을 넘어 전 세계가 함께 글로벌 협력과 네트워크를 통해 해결책을 찾아야 할 것"이라며 "이번 서울총회를 계기로 사이버 공간의 건전한 발전을 위한 국제협력과 행동을 구체화하게 되기를 기대한다"고 말한 바 있다(경향비즈 2013.10.17).

2. 사이버 방어의 역량과 전략

실질적으로 한국이 취할 수 있는 사이버 공격에 대한 대응의 첫 단계는 기술적인 측면에서 방어의 역량을 강화하는 데 있을 수밖에 없다. 북한의 사이버 공격에 대해서 한국이 선제공격 또는 보복공격 등을 통해서 방어의 효과를 올리기에는 정보 인프라 면에서 너무나도 큰 '비대칭적 취약성'이 한국 측에 존재하기 때문이다. 북한에는 공격할 정보 인프라도 없을 뿐만 아니라 자칫 잘못 공격하다가는 물리적 전쟁으

로 비화할 가능성이 있는데다가, 한국의 발달된 정보 인프라로 인해 손해 볼 것이 너무 많다. 이런 맥락에서 볼 때, 북한의 사이버 공격에 대처하는 방안의 핵심은 기술적인 차원에서 방패를 짜서 방어력을 키우는 것이다. 그런데 여기서 문제가 되는 것은 그 방패가 '비닐막'이 아니라 '그물망'이라는 데 있다. 이러한 그물망은 아무리 잘 만들더라도 빈틈을 없앨 수 없다. 그럼에도 그물망 방패를 만드는 것 이외에는 딱히 다른 묘책이 없는 상황이라면, 일단은 그러한 방패를 가능한 한 촘촘히 짜서 사이버 공격을 막아내려는 노력을 벌일 수밖에 없을 것이다.

이렇게 사이버 공격을 막아낼 방패를 만들기 위해서 필요한 것은 기술역량의 증대를 위한 재정적·제도적 지원이다. 이러한 인식을 바탕으로 최근 연구개발을 위한 예산지원을 늘리고, 정보보호 산업의 육성을 위한 민간 및 정부 지원사업의 확대를 위한 대책들이 강구되고 있다. 이러한 맥락에서 2015년 6월 22일 공포된 '정보보호 산업의 진흥에 관한 법률안'이 낳을 효과가 기대되고 있다. 이 법률에는 정보보호 제품에 대한 제값 주기, 보안성 지속 대가 신설, 가격 대신 성능 중심 제품 선택, 정보보호 투자 기업에 대한 인센티브 제공 등 정보보호 산업을 위한 다양한 경제적 지원책이 담겨 있다. 물론 이 법률만으로 정보보호 산업이 갑자기 활황을 맞으리라는 기대를 하지는 않더라도, 이 조치가 국내 정보보호 시장 확대와 정보보호 산업의 융합 촉진에 크게 기여할 "최소한의 마중물 역할은 해 줄 수 있지 않나"라는 것이 전문가들의 기대이다(디지털타임즈 2015.5.13; 아이티비즈 2015.7.2).

사이버 보안기술 전문가들에 의하면, 그물망 방패의 구축은 크게 세 가지 역량의 증대에 초점이 맞춰져야 한다고 한다. 첫째, 공격을 미리 예측하고 사고 발생을 최소화하는 예방력을 키우는 것이다. 이와 관련해서 이른바 '사이버 보안 인텔리전스 네트워크 기반의 국가 통신망 모니터링 체계'의 구축이 거론된다. 둘째, 해킹 공격 루트에 대해 수사하고 공격자를 확인하는 탐지력을 키우는 것이다. 이는 근원지를 역추적하고 공격자의 신원을 식별하며, 사이버 공격 증거들을 확보하고 공격 원점을 타격하거나 동일한 수준의 목표물에 대해 부수적 피해 없이 동일한 수준의 대응공격을 할 수 있는 능력을 증대시키는 것이다. 끝으로, 공격이 발생했을 때 최단시간 내에 차단하여 피해를 최소화하고 빠르고 원활하게 복구하는 복원력(resilience)을 키우는 것이다. 그동안 보안 분야의 주된 관심과 투자가 사이버 공격을 막거나 예방하는 데 있었다면, 앞으로는 공격을 당하더라도 피해를 최소화하자는 것이다(임종인 외 2013; 전자신문 2013.3.26).

이러한 방어기술의 역량을 강화하는 데 있어 인력양성은 중요한 이슈가 아닐 수 없다. 사이버 보안기술 전문가들은 효과적인 사전 예방과 사후 대응을 위해서는 하드웨어, 소프트웨어, 네트워크, 정보보호, 디지털 포렌식 등의 지식을 두루 갖춘 고도의 전문가가 필요하다고 역설해 왔다. 그러나 현재 국내 상황은 이들 인력이 부족한 상황이다. 다시 말해, "사이버 전사를 양성하기 위한 국가적인 차원의 체계적인 계획이 부족하고 이들에 대한 활용계획과 적절한 대우와 포상정책 또한 없으며, 사이버 전사들을 효과적으로 활용하기 위한 사이버 병과도 없는 상황"이라는 것이다(임종인 외, 2013). 민간 영역에서도 주요 기반시설의 보안관리와 정보보호 산업에 종사할 전문 인력 육성의 필요성도 강력하게 제기되고 있다. 그러나 현재는 정보보호 전문기업 대부분이 중소업체 위주로 되어 있고, 대학의 전문인력 배출도 미흡한 상황이다. 이러한 상황을 인식하고 정부는 공공 및 민간 부문에서 이른바 '화이트 해커'로 알려진 사이버 전문인력을 양성하기 위한 대책들을 내놓고 있다(조선닷컴 2015.7.25).

한편, 사이버 공격과 방어 전략을 마련하는 차원에서, 적극적으로 맞받아치는 공격은 아니더라도 상대방이 공격하려고 해도 반격이 두려워 공격하지 못하게 하는 억지력의 보유가 필요하다는 주장이 제기되었다. 최근 냉전기의 핵억지 개념에서 유추한 '사이버 억지' 개념을 원용하자는 것이다(Morgan 2010; Lupovici 2011; Singer and Shachtman 2011; Nye 2011; 2013; 장노순·한인택 2013). 2012년 5월 미 국무부는 이러한 억지 개념에 입각하여 사이버 공격의 배후지를 제공한 국가의 주요시설에 대해서 사이버 보복을 가하거나 또는 그 가능성이 있는 국가에 대해서 사이버 선제공격을 가하겠다고 엄포를 놓은 바 있다. 또한 2014년 12월 북한의 소니 해킹 이후 미국은 북한의 통신망을 마비시키거나 금융제재 조치를 단행한 것으로도 알려졌는데, 이는 복합적인 대응을 통해서 미국에 대한 사이버 공격이 어떠한 보복을 야기할 수 있는지를 보여주려 한 것으로 해석된다. 최근 한국에서도 이러한 사이버 억지의 개념을 원용하는 방안이 거론되고 있다. 그러나 냉전기의 지정학적 핵억지 개념에서 유추한 사이버 억지의 개념을 원용하는 것은 어느 정도까지 가능할 것인가의 문제는 여전히 논란거리이다.

3. 사이버 안보의 추진체계와 법제도

국내 인프라와 정보자산을 대상으로 이루어지는 사이버 공격에 효과적으로 대응하기 위해서는 이상에서 지적한 기술개발과 인력양성 및 억지능력을 뒷받침하는 추진체계의 정비와 관련법을 마련하는 것은 필요하다. 앞서 언급한 바와 같이, 2014년 말 한수원 해킹 사건을 계기로 남북관계뿐만 아니라 북미관계에서도 사이버 안보의 중요성이 크게 강조되면서 사이버 안보 추진체계의 정비가 급물살을 타고 진행

된 바 있다. 특히 2015년 들어 청와대는 사이버 보안기술 전문가를 대통령 안보특보로 임용하여 이 문제의 중요성을 적시하였으며, 이어서 청와대 국가안보실 산하에 사이버안보비서관을 신설하여 청와대가 실질적인 사이버 안보 컨트롤타워 역할을 수행함으로써 이를 기반으로 공공기관들의 협력체계가 실질적으로 가동할 추진체계를 갖춘 바 있다. 이러한 추진체계에는 최상위에 위치한 컨트롤타워(청와대 국가안보실)를 주축으로 국가정보원(이하 국정원), 미래창조과학부(이하 미래부), 국방부, 경찰청, 검찰청 등이 기타 정부기관들과 협력하는 이른바 '국가사이버안전체계'를 이루었다.

이러한 추진체계의 운영과 관련하여 국정원의 위상과 역할을 어떻게 설정할 것인가의 문제는 아직도 해결되지 않은 논란거리 중의 하나이다. 또한 국무조정실이 관장하는 주요 기반시설 보호체계와 청와대 국가안보실 주도의 국가사이버안전체계를 조율하는 문제도 지적되고 있다. 중앙행정기관, 지자체와 주요 기반시설 관리기관의 보안능력 확충을 위해 사이버 보안 전담조직을 신설·확대하자는 안도 거론된다. 또한 효율적인 민·관·군 사이버위협 정보공유 및 공동 대응체계를 확립해야 한다는 주장도 제기된다. 이러한 위협정보 공유체계를 구축하기 위해서는 공공 부문의 대책 마련과 더불어 정부와 민간 부문의 긴밀한 협력이 필요하다. 사이버 안보의 중장기 국가전략을 수립하여 공표할 필요성도 지속적으로 거론되고 있다. 그 동안 정부는 북한의 사이버 공격이 있을 때마다 종합대책, 마스터 플랜, 강화 방안 등의 형태로 대책을 마련해 왔지만 단기적인 수습 방안에 주안점을 두었던 것이 사실이기 때문이다.

한편 사이버 위기 발생 시 체계적이고 효율적인 대응을 위한 법적 근거를 마련해야 한다는 주장도 주기적으로 제기되고 있다. 현재 한국

의 사이버 안보 관련 법제는 대통령 훈령으로 만든 '국가사이버안전관리규정'이 전부인데, 그나마 사이버 위기가 발생했을 때 상황 전파 등에 관한 내용만을 다루고 있다는 평가가 있어 왔다. 또한 전자정부법, 정보통신기반보호법, 정보통신망법 등에 사이버 안전 관련 규정이 산재해 있지만, 이는 일상적인 정보 보호에 중점을 둔 것이어서 사이버 공격에 대응하기에는 역부족이라는 우려도 제기되어 왔다(조선닷컴 2015.7.25). 이러한 법제정의 필요성에 동조하여 국회 차원에서 '국가사이버테러 방지에 관한 법률안'(서상기 의원 발의), '국가 사이버안전관리에 관한 법률안'(하태경 의원 발의), '사이버위협정보 공유에 관한 법률안'(이철우 의원 발의) 등이 발의되었지만 국정원의 권력남용이나 프라이버시 침해에 대한 우려 등을 이유로 그 처리가 지연되었다.

이러한 사이버 안보 관련 법률 제정 과정에서 관건이 되는 것은 국정원의 위상과 역할이다. 찬성하는 측의 주장은, 1) 국가차원의 사이버 위기관리 등을 위한 법제가 시급히 요구된다는 점, 2) 현재 사이버안보마스터플랜과 훈령에 따라 국정원이 실제 컨트롤타워 역할을 수행하고 있는 부분을 법률에 규정함으로써 그 기능을 강화할 수 있다는 점, 3) 국정원은 국내에서 사이버 공격 등에 대한 분석 및 대응에 있어 최고의 기술력과 노하우가 있다는 점 등을 강조하고 있다. 이에 비해 반대하는 측의 주장은 1) 국정원의 사이버 공간에 대한 통제력이 과도하게 될 위험이 있다는 점, 2) 국정원의 활동이 민간의 영역에까지 개입하게 되는 빌미를 제공할 수 있다는 점, 3) 민간과 공공 간의 정보공유 과정에서 개인정보가 유출되어 프라이버시가 침해될 수 있다는 점 등을 들고 있다(허영호, 2014). 그런데 최근 국정원이 정부 입법으로 제정을 추진하고 있는 '사이버안보기본법'에는 그 동안 논란이 되어왔던 '사이버위협정보공유센터'를 국정원이 아닌 국무조정실 소속으로 두는 안이 담겨있다(중앙일보 2016.8.3).

사이버 안보의 추진체계를 정비하고 법제도를 제정할 필요성을 충분히 인정하더라도 그 과정에서 지나친 기술효율성의 논리나 사이버 공간의 군사화 담론으로 경도되거나 국가안보 담론을 과장하고 정파적 이해관계를 투영하여 지나치게 정치화될 가능성은 경계되어야 한다. 다시 말해, 사이버 안보의 국가전략을 모색하는 과정에서 나타날 수 있는 과잉 안보담론(hyper security discourse)의 출현을 경계해야 한다(Hansen and Nissenbaum 2009; Rid 2013). 이런 맥락에서 김상배(2015c)는 네 가지 과잉 안보담론의 위험성을 지적하였다. 첫째, 기술합리성과 효율성의 논리에 지나치게 매몰되는 과잉 안보화, 둘째, 사이버 공간의 활동을 지나친 냉전논리와 군사논리로 이해하는 과잉 군사화, 셋째, 사이버 안보 문제를 지나친 정치적 논리, 특히 국가권력의 논리나 좌우이념의 논리로 몰고 가는 과잉 정치화, 끝으로 국가 행위자들이 벌이는 제로섬 게임의 양상을 과장하는 과잉 현실주의 담론 등이 그것이다. 이러한 과잉담론들은 모두 사이버 안보의 문제가 지니는 복합적인 성격을 간과하고 단순 발상에 입각해서 추진되는 정책들의 소산이라는 것이다.

III. 사이버 안보 주변4망(網) 속의 한국

사이버 안보의 대응 전략을 마련하는 데 있어 국내적으로 기술과 전략 및 법제도 대책을 마련하는 문제를 넘어서 주변 국가들과의 외교적으로 협력하는 것은 중요한 과제이다. 특히 한국의 경우에는 전통적으로 이른바 주변4강(强)으로 불려온 미국, 중국, 일본, 러시아 등과의 양자

및 다자 간 협력이 중요한 변수가 될 수밖에 없다. 그러나 사이버 안보 분야에서 이들 네 나라는, 자원권력의 잣대로 본 '강(强)'이라는 표현보다는 네트워크 권력 개념을 원용해서 보는 주변4망(網)으로 파악하는 것이 좀 더 적절하다. 사이버 안보 분야에서 이들 국가들이 생성하는 구조는, 물질권력의 분포로서의 '구조'라기보다는 행위자들의 상호작용이 생성하는 관계구도, 즉 네트워크 구조라고 할 수 있다. 특히 탈(脫)지정학적 공간으로서 사이버 공간을 배경으로 벌어지는 사이버 안보 이슈의 성격을 보건대 더욱 그러하다. 이 장에서는 사이버 안보의 관계구도로서의 세력망(NoP: network of powers)의 내용을 살펴보고, 이 네트워크 안에서 한국이 처해 있는 위상과 역할에 대한 논의를 펼쳐보고자 한다.[3]

1. 한미 사이버 안보 협력의 과제

사이버 안보 주변4망 중에서도 사이버 선진국이자 우방국인 미국과의 기술과 정보공유 및 협력체계를 구축하는 문제가 핵심이다. 2014년 11월 북한의 소니 해킹 사건이 발생했을 때에도 미국이 북한의 소행을 밝혀내는 과정에서 한국의 기술적인 협조가 있었던 것으로 알려져 있다(보안뉴스 2015.7.17), 미국은 사이버 공격에 동원된 수단이 2013년 3월 20일 발생했던 한국의 금융기관과 언론사에 대한 공격 수법과 유사하다는 사실을 밝혀냈는데, 이는 수사단계에서 한미 간에 정

3 이 글에서 탐구하는 사이버 안보의 네트워크 구조에 대한 연구와 맥이 닿는 소셜 네트워크 분석(SNA, social network analysis)을 행한 연구로는 Kim et al(2015)을 참조하기 바란다. Kim et al(2015)은 2009년부터 2014년까지의 동북아 5개국(미-일-중-러-한국) 간의 신뢰구축조치(CBMs)를 중심으로 세력망 구도를 엿보게 하는 작업을 했다.

보공유가 이루어졌음을 보여준다. 그럼에도 한국은 미국으로부터 충분한 기술과 정보를 제공받는 것이 원활하지 못하다는 비판이 일각에서 제기되기도 했다. 한 언론매체에 의하면, "미국 상무부의 산업보안국(Bureau of Industry & Security)은 미국 내 최고(最高) 해킹 관련 업체인 이뮤니티가 해킹 프로그램을 한국에 팔 때 반드시 허가를 거치도록 하고 있다"며, 이는 사이버 전쟁에서 미사일과 같은 무기인 최고급 해킹 프로그램을 한국에게 팔지 못하도록 제한한 것"이라고 주장했다. 한국이 해당 해킹 프로그램을 도입하려면 2-6개월가량 허가를 기다려야 하는 것으로 알려졌다(조선일보 2015.7.24).

실무 차원에서 진행되는 한미 사이버 협력의 굴곡과는 별개로 한미 정상 차원에서는 사이버 안보 분야의 협력관계 구축 및 확대를 위한 합의가 이루어져왔다. 한미 정상은 두 차례에 걸친 회담에서 사이버 안보 문제를 논의한 바 있는데, 2014년 4월 한미 정상회담에서는 개방적이고 상호 운용이 가능하며 안전하고 신뢰 가능한 사이버 공간이라는 공동의 비전을 촉진해 나갈 것에 합의하였다. 2015년 10월 한미 정상회담에서는 사이버 안보를 포함한 포괄적 동맹관계를 더욱 공고히 하는 차원에서 청와대와 백악관 사이에 '사이버안보 협력채널'을 신설하고 국제사회에서 사이버안보 관련 국제규범을 선도하기로 합의하였다. 특히 사이버위협 정보공유, 사이버범죄 수사공조, 군사적 사이버협력 심화 등의 문제에 대해서 동맹 차원에서 협력하고 사이버 역량 강화를 위해 공동연구, 교육, 기술협력에 나서기로 했다(연합뉴스 2015.10.17).

정부 차원에서도 외교부, 국방부, 미래부 등이 주도하는 사이버 안보 협의가 진행되고 있다. 먼저, 외교부 국제안보대사가 참여하는 한미 사이버정책협의회가 2012년 9월 제1차 회의가 열린 이후 2013

년 7월 제2차, 2014년 8월 제3차에 이어서 2016년 6월에는 제4차 회의를 열어 사이버 안보 등 관련 정책에 대한 의견을 교환하였으며, 국가 정보통신망 보호, 사이버 공간에서의 신뢰구축조치, 사이버 범죄 대처 방안 및 북한에 의한 사이버 테러 대비 방안 등을 협의하였다. 한편 국방부 차원에서도 정책기획관급이 참여하는 국방사이버정책실무협의회가 2014년 2월 제1차 회의가 서울에서 열렸으며, 2015년 2-3월에는 제2차(워싱턴), 2015년 10월에는 제3차 회의를 갖고 한미 간 공조체계를 강화하고 사이버 위협 관련 정보를 공유하는 방안 등을 논의하였다. 이외에도 미래부 차원의 한미 사이버 협의도 진행되었는데, 2013년 양국 정상회담의 합의사항에 따른 후속조치 차원에서 제1차 한미 ICT정책포럼이 2013년 11월 워싱턴에서 열렸으며, 2015년 10월에는 서울에서 제2차 포럼이 열려 양국의 ICT 정책과 미래 유망기술 교류·협력을 활성화하기 위한 다양한 협력방안 등을 논의했다.

이러한 과정에서 한미 사이버 협력의 쟁점은 북한에 대한 사이버 억지력을 보강하는 차원에서 한미 상호방위조약의 틀 내에 사이버 안보의 문제를 포함시켜 미국의 이른바 '사이버 우산'을 빌려 쓸 것이냐의 문제이다. 국내 일각에서는 오프라인 동맹의 경우처럼 온라인에서도 한미 사이버 동맹을 구축하는 차원에까지 협력을 강화해 나가야 한다는 주장이 제기되기도 하였다. 그러나 탈냉전 이후 세계정치의 시대적 상황과 사이버 안보 문제가 지니는 쟁점의 교유한 성격, 그리고 지정학적 문제가 복합적으로 작용하는 주변4망(網)과의 관계 등을 고려할 때, 한국의 입장에서 한미 사이버 협력을 무조건 동맹 수준으로 격상시키는 것만이 능사가 아님을 명심할 필요가 있다.

기존 한미동맹의 맥락에서 사이버 협력을 적극적으로 자리매김하는 것은 맞지만, 이를 정치군사동맹으로서 한미동맹, 그것도 한미 상호방위조약의 틀에 넣는 것에 대해서는 좀 더 깊은 고민이 필요하다. 한미 사이버 협력은 냉전기의 단순동맹의 틀이 아니라 탈냉전 이후 새롭게 모색되고 있는 복합동맹의 맥락에서 이해해야하기 때문이다. 더욱이 사이버 공간의 복합 네트워크를 바탕으로 해서 발생하는 사이버 안보 분야의 고유한 특성은 양국 간의 협력도 복합적인 시각에서 보게 만든다. 그도 그럴 것이 한미 양국이 재래식 공격이나 핵공격을 받았을 때 서로 돕는다는 것의 의미와 사이버 공격을 받았을 때 서로 돕는다는 것, 그것도 오프라인의 상호방위조약을 준수하는 차원에서 돕는다는 것의 의미는 사뭇 다를 수밖에 없다. 그야말로 협력영역, 협력주체, 협력정도 등이 복합화되는 비대칭 복합동맹이라는 맥락에서 한미 사이버 안보 협력에 접근할 필요가 있다.

이러한 복합동맹의 접근은, 국내 일각에서 제기하는 바와 같이, 한미 사이버 협력을 저층위 협력에서 시작해서 고층위 협력으로 발전시켜 가자는 이른바 기능주의적 접근과는 그 성격이 다르다. 사실 이러한 기능주의적 접근은 이른바 '아시아 패러독스'를 해소하기 위한 방안으로 연성안보 영역의 협력에서 시작해서 경성안보의 협력으로 가자는 '동북아평화협력구상'의 고민과 맞닿는다. 그렇지만 사이버 안보 분야의 협력은 저층위에서 고층위로 나아가는 일방향 모델을 설정할 성질의 것이 아닐 뿐만 아니라, 만약에 가능하더라도 무작정 정치군사 동맹 수준의 고층위 협력모델을 지향할 문제도 아니다. 오히려 다층위에서 복합적인 협력의 틀을 만들어내는 것이 더 유용할 수도 있다. 네트워크 이론에서 말하는 바처럼, 네트워크상에서는 강한 고리(strong ties)만이 능사가 아니라 경우에 따라서는 약한 고리(weak ties)가 더 유용할 수도 있다. 다른 말로 하면 사이버 안보 분야에서는 근접중심성을 강화하는 시도이외에도 연결 중심성과 매개 중심성의

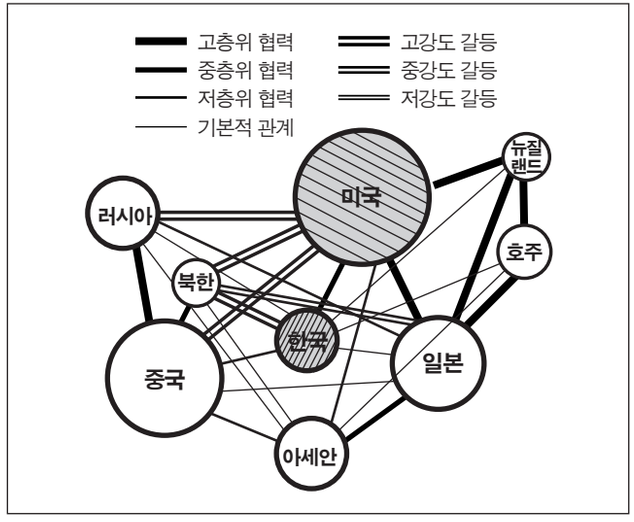

그림 1. 사이버 안보 세력망 속의 한미동맹 (가상도)[4]

강화를 복합적으로 고려하는 발상이 필요하다. 이러한 맥락에서 보면, 한미 사이버 협력은 〈그림 1〉에서 가상도를 그려본 바와 같이, 동아시아 사이버 안보 세력망의 복합적인 맥락 속에서 그 미래를 설정해야 하는 문제라고 할 수 있다.

4 〈그림 1〉은 노드와 링크에 대한 엄밀한 데이터를 대입해서 그린 것이라기보다는 대략의 데이터를 염두에 두고 직관적으로 그린 가상도이다. 다른 크기의 원으로 그려진 노드들은 국가 행위자들을 의미하는데, 군사력이나 경제력, 기술력 등과 같은 대략적인 국력의 크기를 염두에 두고 그려 보았다. 〈그림 1〉에서 좀 더 중요한 것은 굵기의 차이로 표현된 링크의 속성인데, 이는 각국 간에 벌어지고 있는 사이버 안보 관련 협력과 갈등의 정도를 표시했다. 사이버 안보 분야의 협력을 고층위, 중층위, 저층위의 셋으로 나누었으며, 사이버 갈등도 고강도, 중강도, 저강도의 셋으로 나누었다. 특별한 협력과 갈등의 양상을 보이지 않는 기본적 관계는 그냥 실선으로 표시하였다. 아쉽게도 〈그림 1〉에서 링크의 길이는, 이른바 근접중심성을 가능한 한 표현하는 방향으로 그렸지만, 평면에 그림을 그리는 제약 때문에 이를 엄밀하게 반영하지는 못했다.

2. 미중경쟁의 구도에서 한국의 딜레마

이렇게 복합적 시각에서 한미 사이버 협력의 문제를 풀어나가는 데 있어서 제일 큰 고민거리는 중국이다(Lindsay et al(eds.) 2015). 최근 미국이 사이버전 능력을 강화하면서 한국과 일본, 호주 등 전통적 동맹국에 사이버 협력을 요청했을 때 한국 정부는 머뭇거리면서 적극적인 참여를 유보했던 것으로 알려져 있는데, "미국과 사이버 동맹을 맺으면 중국이 반발할 것이란 우려 탓에 제대로 판단하지 못했다"는 지적이 제기되었다(조선닷컴 2015.7.24). 북한이 사이버 거점으로 활용하는 국가라는 점에서 중국 변수는 사이버 안보 분야에서도 한국이 무시할 수 없는 변수이다. 전 대통령 안보특보 임종인 교수에 의하면, "2014년 말 한수원 사태 때 정부 합동수사단은 해커의 공격 IP가 중국 선양지역이라는 것을 찾아냈지만 중국 정부의 협조를 얻지 못해 더 이상 수사를 하지 못하고 중단했다. 중국 선양에서 무슨 일이 있었는지 원격 수사를 할 수 있는 역량도 없었고, 중국 정부의 협조를 이끌어낼 만한 사이버 외교력도 부족했다. 그러니 공격의 배후를 북한이라고 '추정'만 할 뿐 증거도 찾지 못하고 더 이상의 후속조치도 취하지 못했다"고 한다(디지털타임즈 2015.5.13).

이러한 맥락에서 볼 때, 한중 양국 간 사이버 수사공조와 사이버 안보 협력을 성사시키는 것은 중요할 수밖에 없다. 이러한 외교적 고려에서 진행되는 것은 아니지만, 현재 다양한 채널을 통해서 한중 사이버 협력이 진행 중이다. 그러나 한미 사이버 협력의 경우와는 달리 군사적 차원보다는 미래부가 중심이 되어 기술·경제적 협력의 형태를 띠고 있다. 예를 들어, 2015년 10월 중국 베이징에서 미래부와 중국의 공업신식화부(공신부)는 '한중 사이버보안 국장급 협력회의'를 개최했

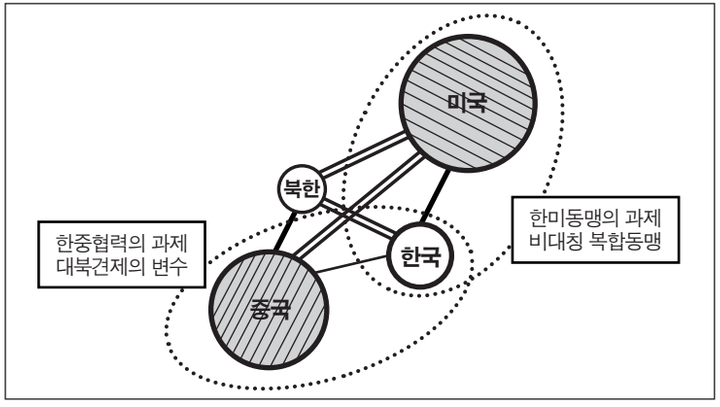

그림 2. 한미동맹과 한중협력 사이의 한국(가상도)

는데, 이는 2014년 10월 미래부와 공신부가 체결한 '사이버보안 협력 강화를 위한 양해각서'의 실질적 이행을 위해 첫걸음을 떼는 자리로서, 사이버 보안 정책, 사이버 침해사고 대응 및 정보공유, 주요 기반시설 보호, 보안산업 진흥 등 주요 정책과 공동 관심 현안에 대한 협력 강화방안을 논의했다. 한편 2015년 12월에 열린 제3차 한중 ICT협력 장관급 전략대화에서도 해킹 등 인터넷 안전에 위협이 되는 정보를 공유하고 대처하기 위한 플랫폼 구축에 합의했으며, 사이버 위협에 대한 대응력을 높이기 위해 사이버 위협 관련 URL, IP, 악성코드 샘플 등 구체적 정보도 공유하기로 했다.

현재 미국과 중국이 사이버 안보 분야에서 갈등하고 경쟁하는 상황에서 한국은, 〈그림 2〉에서 보는 바와 같이, 한미동맹과 한중협력의 사이에서 형성되는 이 분야의 구조적 조건을 파악하고 그 안에서 전략적으로 적절한 위치를 설정해야 하는 과제를 안고 있다. 그러한 과제가 쉽지 않은 것은 두 강대국 사이에서 중견국 외교의 딜레마가 발생할 가능성이 있기 때문이다. 예를 들어 한국은 사이버 안보 분야에서

경합하는 미국과 중국의 상이한 기술표준 사이에서 기회와 도전을 동시에 경험할 가능성이 있다. 중국이 사이버 안보 분야에서 기술표준의 공세를 벌일 경우 마이크로소프트의 운영체계와 인터넷 익스플로러, 시스코의 네트워크 장비 등과 같은 미국의 기술표준에 크게 의존하고 있는 한국은 어떠한 결정을 내려야 할까? 실제로 이와 유사한 사태가 2014년 초 중국의 통신업체인 화웨이로부터 한국의 정보통신기업인 LG 유플러스가 네트워크 장비를 도입하려 했을 때 미국이 나서서 만류했을 때 나타난 바 있다. 이러한 상황은 양국의 인터넷 관련 정책과 규제제도, 즉 인터넷 거버넌스 상의 차이와 관련하여 미국의 민간 주도 모델과 중국의 국가 개입 모델 사이에서 한국이 어떠한 선택을 해야 하는 상황을 창출할 수도 있다. 더 나아가서는 글로벌 인터넷 거버넌스와 과정에서 나타나고 있는 양국의 입장 사이에서의 고민으로 발전할 수도 있다.

3. 아태 지역동맹과 동아 지역협력 사이의 한국

미국이나 중국 변수와 함께 한국이 사이버 안보 분야의 국제협력을 고민하는 데 있어서 빼놓을 수 없는 변수가 일본이다. 그런데 일본은 그 특성상 최근 사이버 안보 분야에서도 협력체계를 갖추어 가고 있는 미일동맹의 맥락에서 보아야 한다. 미국과 일본은 2015년 4월 양자동맹을 사이버 공간과 우주까지 확대하는 방위협력지침 개정안을 발표하였다. 2015년 5월 공개된 미일 양국의 공동성명에 의하면, 미국은 군사 기지와 사회 기반시설에 대한 사이버 공격에 대처할 수 있도록 일본을 지원하기로 했다. 이밖에도 미일 간에 사이버위협안보그룹의 설치, 사이버 합동훈련 실시, 사이버 훈련 기술협력과 인적교류 등에 이

르기까지 다양한 협력과 공조가 진행 중이다(Lewis 2015).

이러한 미일동맹의 변화는 미국이 사이버 안보를 포함하여 새로이 강화하고 있는 아태 지역동맹 전략의 연속선상에서 이해해야 한다. 2015년 5월 애슈턴 카터(Ashton B. Carter) 미 국방장관은 기후, 북한, 사이버 안보 등 불안정 요인들을 예시하며 군사·경제 차원에서 한국, 일본, 호주, 인도, 필리핀, 베트남, 말레시아 등 역내 동맹 및 파트너 국가들과의 협력강화를 통한 재균형 정책의 실천의지를 표명한 바 있다(한국일보 2015.6.4). 2015년 7월 마틴 뎀프시(Martin. E. Dempsey) 미국 합참의장은 '2015 군사전략보고서'를 통해 러시아, 이란, 북한, 중국 등 4대 위협국을 거론하며, 나토, 호주, 일본, 한국과 같은 파트너들과의 '하이브리드 분쟁'에 대한 억지와 대응을 강조하였다. 특히 북한에 의한 핵과 미사일 위협뿐만 아니라 한국과 일본, 미국 본토에 대한 사이버 공격에 대한 강력한 대응을 언급하였다(문화일보 2015.7.2). 이러한 맥락에서 미국은 일본 이외에도 호주와도 사이버 협력을 진행하고 있는데, 2011년 9월 '호주·미국 국방·외무장관 합동회의(AUSMIN)'에서는 양국이 미·호 동맹을 무역 및 개발 분야까지 포괄하는 다원적 동맹으로 발전시키고 사이버 공간까지 범위를 확대시키기로 합의하는 공동 선언문을 발표한 바 있다.

이렇게 강화되고 있는 미국 주도의 아태 사이버 지역동맹의 틀 중에서 상대적으로 가장 미미한 고리는 한일 사이버 협력이다. 현재 동아시아 주변4망(網)의 구도에서 한일관계는 일종의 '구조적 공백(structural hole)'이라고 할 수 있다. 그러나 전통적인 한미관계나 최근 활발해 지고 있는 한중관계의 맥락에서 볼 때 일본은 중요한 변수가 아닐 수 없다. 또한 아세안이나 아태 지역공간을 활용한다는 차원에서도 일본이 지니는 의미는 크다. 그러나 2012년 6월 한일 정보보호협정(GSOMIA)을 둘러싼 논란을 보면, 사이버 안보 분야에서의 한일협력에 대한 전망이 그리 밝지 않다. 2016년 3월 워싱턴에서 열린 한미일 3국 정상회의에서도 미일 양국은 GSOMIA 체결 필요성을 거듭 강조했지만, 한국 측은 국내정치의 부담감을 이유로 일본과 거리를 두고 속도를 조절하려는 태도를 보인 바 있다(조선일보 2016.4.4). 그럼에도 2016년 10월 한일 간에 처음으로 사이버정책협의회를 열고 사이버 분야에서의 협력 방안, 사이버 공간상 국제규범 및 신뢰구축조치 등에 대해 의견을 나누는 자리를 마련해 귀추가 주목된다(연합뉴스 2016.10.28).

궁극적으로 한국의 입장에서 볼 때 관건은 이렇게 미국이 주도하는 아태지역 동맹체제의 구축과정에 한미동맹이라는 양자 협력 차원을 넘어서 얼마나 더 적극적으로 참여할 것이냐의 문제일 것이다. 우선은 미국이 주도하여 아태지역에 건설하려는 질서의 성격이 무엇인지를 정확히 이해할 필요가 있다. 유럽지역에서 탈린매뉴얼(Tallinn Manual)의 사례에서 보는 바와 같이, 미국은 나토와 같은 집단적 자위 모델을 아태지역에 도입하려는 것은 아닌지 예의주시할 필요가 있다. 다시 말해, 탈린매뉴얼에서 보이는 나토의 실험은 기본적으로는 오프라인 냉전동맹 모델의 온라인으로의 확장이라는 점에서, 만약에 미국이 이러한 나토 모델을 원형으로 하여 아태지역에서 사이버 협력체제를 구축하려 시도한다면 북한과 대치하고 있는 특수한 상황에 처한 한국의 입장에서는 조심스러운 일이 아닐 수 없기 때문이다. 유럽에서 나토가 상정하는 적 개념이 러시아의 사이버 공격이라면 아태 지역에 상정하는 적 개념은 무엇이며, 그리고 대결의 구도에서 한국이 취할 수 있는 입장은 무엇인지에 대한 고민이 필요할 것이다.

그럼에도 한국이 사이버 안보 전략을 모색함에 있어서 아태지역

에서의 협력은 중요하지 않을 수 없다. 그리고 실제로 한국은 아태지역 국가들과의 협력을 추진하거나 APEC 차원의 사이버 협력을 주도하고 있다. 예를 들어, 한국과 호주 간에는 사이버 안보 협력이 진행 중인데, 2014년 8월에는 외교부 국제안보대사를 수석대표로 하는 제1차 한-호주 사이버정책 대화를 가졌고, 2014년 4월 한-호주 양 정상이 합의한 사이버 분야 협력 강화의 후속조치로서 아태 지역체제 내에서 협력과 양국 간 국방 사이버 협력, 사이버 범죄에 대한 공동 대응 등의 다양한 의제에 대해 협의하였다. 또한 아태지역 협력 차원에서도 한국은 2011년 9월 제3차 APEC 사이버보안 세미나를 서울에서 개최하였는데, 이는 2008년 처음 한국에서 제안된 세미나로 APEC 역내 경제협력 국가 간 정보보호 동향 파악 및 정책 공유를 위해 개최되고 있다. 한편 2015년 9월 아태지역 국방 차관급 다자안보협의체인 제4차 서울안보대화(SDD: Seoul Defense Dialogue)에서는 첫 안건으로 사이버 안보를 선정해 논의하기도 했다. 2012년 11월 처음 개최된 서울안보대화는 한반도를 포함한 아태지역 내 안보환경 개선과 다자간 군사적 신뢰 구축을 위해 각국 국방차관이 참여하며 대화를 이어가고 있다.

아태지역 국가들이 역내 안정을 추구하기 위해 1994년 출범한 다자간 정치·안보 협의체인 ARF(ASEAN Regional Forum) 차원에서 진행되는 사이버 협력에도 주목할 필요가 있다. ARF에는 아세안 10개국, 아세안 대화상대국 10개국, 기타 아시아 지역 국가 7개국이 회원국으로 가입했으며 2000년대 중반 이후 중국의 적극적 참여와 2010년 미국의 참여로 영향력이 확대되고 있다. 2007년에는 한국의 주최로 ARF 사이버 테러 세미나를 서울에서 개최하였으며, 2012년 제19차 프놈펜 회의에서는 중국의 주도하에 사이버위협에 공동 대처하기 위한 합동전략개발 협력에 합의했다. 2015년 8월 ARF 외교장관회담에서는 회원국간 신뢰구축을 통해 분쟁을 방지하고, 상호 이해를 제고하기 위해 사이버안보 작업계획(work plan)을 채택했다. 한국도 ARF의 사이버 신뢰구축조치 노력에 적극 부응하여, 2012년 9월 서울에서 관련 세미나를 개최하고, 2013년 9월과 2014년 3월에 개최된 ARF 차원의 사이버 이슈 관련 워크샵 등에 지속적으로 참여하였다.

이상에서 살펴본 아태지역 차원의 사이버 협력이외에 동북아 지역 차원에서 한중일이 중심이 되어 가동하고 있는 사이버 협력도 주목할 필요가 있다. 사실 역사적으로 볼 때 동북아에서 한중일 3국은 IT장관회의를 통해 협력해온 경험이 있다. 한중일 IT장관회의는 2002년에 모로코에서 제1차 회의가 개최된 이후 2003년에 제주에서 제2차 회의와 2004년에 일본 삿포로에서 제3차 회의가 개최되었고, 2006년 3월에 중국 샤먼에서 제4차 회의가 개최된 바 있다. 그러던 것이 2000년대 후반 3국간 IT협력이 다소 소강상태를 거치고 나서 최근 사이버위협에 대한 공동대응의 차원에서 협력의 필요성에 대한 논의가 다시 피어나고 있다. 예를 들어, 2014년 10월 베이징에서 사이버 분야의 3국 간 첫 고위급 회의로서 제1차 한중일 사이버정책협의회가 열렸는데, 각국별 사이버 정책 및 제도, 사이버 공간에 적용 가능한 국제규범, 지역적·국제적 사이버 협력, 3국 간 향후 협력이 가능한 분야 등에 대한 논의를 펼쳤다. 제2차 한중일 사이버정책협의회는 2015년 10월 서울에서 열렸는데, 이 회의에서는 사이버 안보 환경, 각국 사이버 전략·정책, 사이버 공간 국제규범 및 신뢰구축조치, 지역적·국제적 사이버 협력, 사이버 범죄·테러 등과 같은 3국간 협력 의제에 대해서 논의했다. 제3차 한중일 사이버정책협의회는 2016년 하반기 일본에서 개최될 예정이다.

이러한 한중일 사이버 협력이 진행되는 과정에서 아세안은 한중

일 3국이 적극적으로 고려해야 할 중요한 변수이다. 앞서 살펴본 바와 같이, 아세안은 아태지역 사이버 협력이라는 차원에서 ARF라는 아태지역 프레임을 활용하는 동시에 아세안+3의 동남아시아와 동북아시아를 합한 프레임에서 중요한 축을 담당한다. 한중일 3국 중에서 아세안과의 사이버 협력에 가장 적극적으로 나서는 나라는 일본이다. 일본과 아세안의 사이버 보안 정책협력회의는 2009년부터 시작되었는데, 국장급이 참석하는 '고위급정책회의'와 과장급 및 실무담당자를 대상으로 하는 '네트워크보안 워크숍'과 '정보보호 훈련'으로 나누어 개최되고 있다. 특히 2013년 9월에는 사이버 보안에 관한 장관급회의가 개최되어 사이버 공격에 대한 공동대응을 위한 합의문이 발표된 바 있다. 아세안과 일본은 사이버 공격의 위협에 공동으로 대처하기 위해, 공격을 예지하거나 바이러스 감염을 탐지해 경고를 울리는 시스템을 연계 개발한다는 내용을 골자로 한 공동성명도 발표했다.

이상의 논의를 바탕으로 해서 볼 때, 한국의 사이버 외교가 당면한 쟁점과 과제는, 〈그림 3〉에서 보는 바와 같이, 미국이 주도하는 아태지역 협력체제와 미국과는 상이한 프레임을 짤 가능성이 있는 한중일 사이버 협력이나 동아시아 지역협력의 독자적 움직임 사이에서 어느 정도의 비중을 가지고 두 진영에 관여할 것이냐의 문제이다. 물론 다채널 협력의 틀이 형성되면 더할 나위 없이 좋겠지만, 최근의 경향은 동아태의 지역질서 아키텍처를 어떻게 짤 것이냐의 문제를 놓고 미국과 중국의 영향력이 이면에서 충돌하고 있는 점을 볼 때, 경우에 따라서는 불가피한 선택을 해야만 하는 중견국의 딜레마가 한국에게 닥쳐올 가능성도 없지 않다. 이는 앞서 언급한 바와 같이 미국과 중국의 양자관계 사이에서 전략적 선택을 하는 문제보다도 좀 더 복합적이고 입체적인 차원에서 발생하는 문제가 될 터인데, 미국이 짜는 네트워크

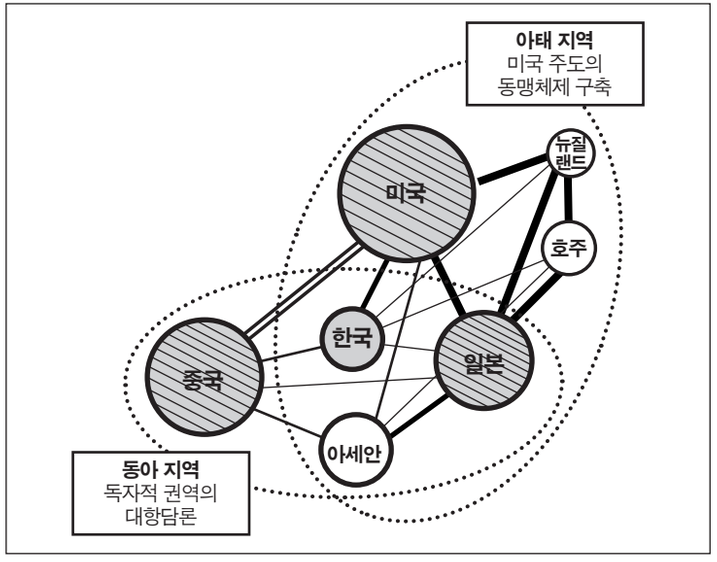

그림 3. 아태 지역동맹과 동아 지역협력 사이의 한국 (가상도)

와 중국이 형성하는 네트워크의 사이에서 한국의 동아태 전략을 설정하는 망제정치(inter-network politics)의 과제가 될 것이다. 이러한 딜레마는 최근 미중 간에 쟁점이 되고 있는 북핵 실험과 사드 미사일의 한반도 배치 문제 등으로 나타난 바 있다.

4. 미러경쟁과 중러협약 사이의 한국

주변4망(網)의 마지막 변수인 러시아는 상대적으로 동아태 지역에서는 존재감이 그리 크지 않다. 이는 러시아가 유럽이나 글로벌 차원에서 미국과 경쟁하면서 세력망의 구조를 형성해가는 주요 행위자라는 사실과 대비된다. 그럼에도 근대 국제정치사에서 러시아가 차지하는 위상과 역할을 고려할 때 동아시아 사이버 세력망에서 빠트릴 수 없는

'약한 고리(weak tie)'임은 분명하다. 동아태 지역에서 러시아가 미미한 변수인 것과는 달리, 다음 장에서 살펴보는 바와 같이, 글로벌 차원에서 진행되는 국제규범 형성과정에서 러시아는 비서방 진영의 리더 역할을 담당하고 있다. 특히 미국과 유럽(특히 나토)에 대해서 각을 세우면서 유럽지역과 유엔(또는 기타 지역기구) 차원의 국제규범 형성의 한 축을 맡고 있다.

이러한 맥락에서 볼 때 주변4망(網)의 한 행위자로서 러시아에 대한 논의는 글로벌 차원에서 벌어지는 미러경쟁의 맥락에서 접근해야 한다. 최근 특히 가시화된 미중 간의 사이버 갈등에 비해서 상대적으로 드러나지는 않지만 미러 간에도 사이버 갈등이 지속적으로 발생하고 있기 때문이다. 예를 들어, 2015년 5월 뉴스위크(*Newsweek*)는 '러시아의 가장 훌륭한 무기는 해커'라는 기사에서 러시아와 중국을 차세대 사이버 전쟁에서 가장 강력한 국가 행위자로 꼽았다. 특히 러시아 해커들은 프로그래밍 분야에서 가장 창의적이고 뛰어난 사이버 전사로 언급됐다. 이 기사에서 보안 컨설팅 업체 '타이아 글로벌(Taia Global)'의 대표는 "중국 위협은 과장됐고 러시아 위협은 과소평가됐다. 러시아인의 기술이 가장 높다"고 말했다(*Russia Focus* 2015.6.26). 물론 미러 간에는 표면적으로는 사이버 협력의 몸짓도 진행 중이다. 예를 들어 2013년 미국과 러시아는 사이버 핫라인을 설치하는 협정을 체결했는데, 이는 냉전 시대의 핵 공포에 대해 사용되었던 것과 유사한 성격이었다. 그러나 2014년 러시아의 우크라이나 침공 이후 양국 간에 체결된 '사이버 공간의 신뢰조치에 관한 협정'과 사이버 공간에서의 신뢰에 관한 양자 간 대통령자문위원회(2009년 선포)는 폐지됐다(Geers, 2015).

미국과 러시아 간에 형성되는 냉기류와는 달리 중국과 러시아는

사이버 협력을 강화하여 2015년 5월 중러 사이버 보안 협약을 체결하는 성과를 거두었다. 이는 중국과 러시아가 사이버 공간에서 서로에 대한 감시를 지양하고 각국의 법집행기관을 통해 기술 전수 및 정보 공유를 하겠다는 내용을 담고 있다. 이 협약은 두 국가가 서로 중대한 인프라만은 건드리지 말자고 암묵적으로 약속한 성격을 갖는다. 이러한 중러협약에 대한 미국의 반응이 다소 냉소적으로 표출된 것은 당연하다. 미국이 인식하기에 이러한 중러 사이버 협력을 통해서 "러시아는 중국이 인터넷 거버넌스에 대해 어떤 입장을 취할 것인지에 대해 설득"하고 있는 것으로 비춰졌다. 더 나아가 "중국은 그냥 모든 일에 미국과 반대의 입장에 서고 싶어서 러시아와 함께 한 것으로 보인다"는 해석도 나왔다(*Russia Focus* 2015.6.26).

그런데 이러한 중러협약은 좀 더 넓은 의미에서 벌어지는 지역차원의 협력, 특히 상하이협력기구(SCO)에서 벌어지는 중러협력과 러시아의 적극적 역할과 관련해서 이해해야 한다. 상하이협력기구는 1996년 4월 중국과 러시아, 중앙아시아의 카자흐스탄, 키르기스스탄, 타지키스탄 등이 국경지역의 안정을 위해 '군사 부문 신뢰에 관한 협정'을 체결한 '상하이 5개국 회의'를 모태로 하는 기구이다. 2000년에 우즈베키스탄이 합류한 뒤, 2001년 6월 상하이에서 상하이협력기구로 정식 출범하였다. 상하이협력기구는 사이버 안보 관련 활동을 벌여왔는데, 2011년 '정보안보 영역에서 협력에 관한 합의안'을 도출하며 사이버 안보 관련 역내 국가들 간의 협력을 시작하였다. 이러한 협력에는 사이버 무기개발 및 사용 규제, 정보전쟁에 대한 대비 등의 내용이 포함되었다.

〈그림 4〉에서 보는 바와 같이, 이상에서 살펴본 글로벌 및 동아시아의 세력망 구도 속에서, 즉 미러경쟁과 중러협약의 사이에서 한국

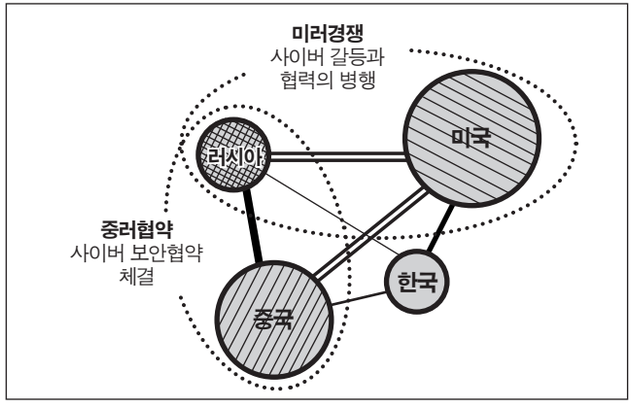

그림 4. 미러경쟁과 중러협약 사이의 한국(가상도)

은 러시아와의 사이버 협력관계를 어떻게 가지고 가야 할 것인가? 앞서 언급한 한일관계와 마찬가지로 한러관계도 사이버 안보의 주변4망(網)에서 일종의 '구조적 공백'이라고 할 수 있을까? 만약에 그렇다면 이러한 공백을 메우기 위해서 한국이 러시아와의 관계에서 할 수 있는 일은 무엇이 있을까? 미국과의 관계를 해치지 않으면서 사이버 안보 분야에서 러시아의 앞선 기술을 이전받고 위협정보도 공유할 방법이 있을까? 또는 중국과 더불어 러시아를 통해서 북한의 사이버 공격 행위를 외교적으로 견제할 방법은 없을까? 더 나아가 한미일 관계의 전통적인 동맹구도를 배후로 하여 한중러의 '약한 고리'를 활용하는 것은 가능할까? 사실 이러한 질문들은 최근 동북아의 주요 행위자로서 러시아의 위상과 역할이 약화되고 있는 이유로 인해서 상대적으로 덜 연구되었지만, 한국이 사이버 주변4망(網) 전략을 성공적으로 추진하기 위해서는 반드시 고려해야 할 문제라고 할 수 있다.

이러한 와중에도 한국과 러시아 간에는 사이버 협력이 진행되고 있다. 2013년 3월 서울에서 외교부 국제안보대사를 수석대표로 하는

제1차 한러 정보보안협의회가 개최된 바 있는데, 이는 2013년 10월로 예정되었던 사이버공간총회 직전에 회의 개최를 홍보하기 위해서 만난 자리에서 다양한 협의를 한 것으로 알려졌다. 예를 들어, 국제 사이버 안보의 현황, 사이버 공간 침해사고 대응 및 핵심기반시설 보호, 사이버 범죄 및 사이버 테러리즘 대응 협력, 사이버 공간에서의 신뢰강화 및 행동규범 개발 공조, 국제·지역기구 및 포럼에서의 협력 등의 의제에 대한 협의가 있었다. 그 후 2014년 5월 모스크바에서 제2차 한러 정보보안 협의회를 개최했다. 2016년 7월에는 모스크바에서 한러 외교부 국제기구국장 협의회(제1차)가 개최되어 유엔평화활동, 난민, 사이버 보안 등 글로벌 현안과 유엔 총회 및 안보리 등 유엔기관의 운영 등에 관한 의견을 교환하였다(연합뉴스 2016.7.8).

IV. 사이버 안보의 국제규범과 중견국 외교

1. 사이버 안보의 국제규범 모색

1990년대 후반부터 진행된 역사를 보면, 사이버 안보 분야의 글로벌 질서 형성은 그 자체가 독립적 이슈로서 다루어졌다기보다는, 넓은 의미에서 본 글로벌 인터넷 거버넌스의 일부로서 취급되어 왔다. 그러다가 2010년대에 들어서면서 사이버 안보 분야에 해당되는 독자적 국제규범을 모색하기 위한 노력들이 진행되기 시작했다. 그러나 아직까지 사이버 테러와 공격에 대해서 기존의 어떠한 규정을 적용하여 규제할지 등에 대한 국제적 합의기반은 마련되고 있지 않은 상태이다(Hurwitz 2014). 마찬가지로 이 분야에서 미국과 러시아, 중국 등의 이해관

계가 충돌하고 있기는 하지만, 아직까지 강대국들 간의 대결이 본격화되었다고 보기에는 이르다. 그럼에도 사이버 안보의 국제규범을 모색하려는 시도는 진행되고 있는데, 현재로서는 다음과 같은 세 가지 층위에 주목할 필요가 있다.

첫째, 전통적인 국제법(특히 전쟁법)과 국제기구의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격을 이해하려는 시도이다. 기존 국제법의 틀을 원용하는 사례는, 2013년 3월 나토의 CCDCOE(Cooperative Cyber Defence Centre of Excellence)가 발표한 사이버 전쟁의 교전수칙인, 탈린 매뉴얼을 들 수 있다. 탈린 매뉴얼의 골자는 사이버 공격으로 인해 인명 피해가 발생했을 경우 해당 국가에 대한 군사적 보복이 가능하고, 핵티비스트 등과 같은 비국가 행위자에 대해서도 보복하겠다는 것이다. 더 나아가 사이버 공격의 배후지를 제공한 국가나 업체에 대해서도 국제법과 전쟁법을 적용하여 책임을 묻겠다는 것이다(Schimit 2012). 그러나 2007년 에스토니아 사태 이후 미국과 유럽 국가들이 중심이 되고, 게다가 나토 회원국의 전문가들이 참여하여 러시아에 대응하는 성격을 띰으로써 러시아나 중국 등을 배제한 미국 중심의 시각이 주로 반영되었다는 비판을 받았다(박노형·정명현 2014; Christou 2016).

전통적인 국제기구인 유엔 차원에서 사이버 안보 문제를 다루려는 시도도 최근 빠르게 진행되고 있다. 그 대표적인 사례가 2013년 6월 유엔 GGE에서 합의해서 도출한 최종 권고안이다. 이 권고안은 1998년 러시아가 제안했는데, 미국은 처음부터 러시아의 제안에 대해 동조하지 않았고, 이후로도 소극적인 자세로 사이버 안보 관련 정부 간 협력에 대응해 왔었다. 기존 회의에서는 인터넷의 국가통제를 강조하는 러시아나 중국과 같은 국가들과 이에 반대하는 미국이 극명히 대립했으나, 2013년 6월 개최된 제3차 회의에서는 전체 참여국들이 사이버 공간에서도 기존의 국제법이 적용될 수 있다는 점에 합의하고 이러한 규범이 국가의 역할로 어떻게 연결될 수 있는지에 대해서 지속적으로 연구하기로 합의했다(장규현·임종인 2014; 장노순 2015).

둘째, 사이버 안보의 국제규범을 마련하기 위해서 서방 선진국들이 원용하는 일종의 클럽 모델 형태의 국제협력이다. 전세계 국가를 포괄하는 유엔의 포맷을 빌어 논의하기보다는, 사이버 안보의 직접적인 이해 당사자들이 나서는 방식이라고 할 수 있다. 사이버공간총회가 대표적인 사례인데, 2011년 영국의 런던에서 첫 총회가 열렸다. 2012년 헝가리의 부다페스트에서 총회를 가진 후, 2013년 10월에는 서울에서 제3차 총회가 열렸으며, 2015년에는 네덜란드의 헤이그에서 제4차 총회가 열렸다. 사이버공간총회의 의미는 사이버 공간이라는 포괄적 의제를 명시적으로 내건 본격적인 논의의 장이 출현했다는 데 있으며, 참여국들의 구체적인 이익이 걸린 사이버 안보라는 문제를 가지고 관련 당사국들을 중심으로 구성되었다는 데 있다. 그런데 주로 서방 국가들의 주도하에 이루어져서 러시아나 중국과 같은 국가들의 호응을 얻어내는 것이 큰 과제로 남아 있다.

사실 이렇게 서방 선진국들이 중심이 되어 사이버 공간의 범죄나 위협에 공동으로 대처하려는 사례의 역사는 좀 더 깊다. 초창기 사이버 범죄에 대응해서 국가들이 나서서 상호 간의 법제도를 조율하는 정부 간 네트워크를 구성한 초기 사례로 2001년 조인된, 유럽사이버범죄협약(일명 부다페스트 협약)이 있다. 부다페스트협약은 여러 나라의 사이버 범죄 조목을 일관되게 함으로써 피해를 본 국가가 범죄자가 있는 국가에 고발하면 해당 국가가 처벌할 수 있도록 한 협약이다. 절차적으로 어떠한 사이버 범죄이든 이와 연루된 개인들이 협력하도록 강

제하는 권한을 부여했다. 2016년 8월 현재 유럽 국가들 이외에 미국, 캐나다, 일본 등을 포함한 55개국이 가입되어 있고 이 중 49개국이 비준하였다. 그러나 러시아나 중국 등은 미온적 반응을 보이고 있다. 현재 한국은 부다페스트협약 가입국이 아닌데, 최근에는 협약가입을 주장하는 목소리가 높아지는 가운데, 외교부를 중심으로 법무부, 경찰청 등이 검토 중이다.

끝으로, 글로벌 인터넷 거버넌스의 맥락에서 진행되는 사이버 안보 규범에 대한 논의이다. 인터넷 거버넌스 중에서 사이버 보안 문제는, 최근 국가 간 분쟁의 이슈로 부상하기 전에는 민간 전문가들에 의해서 다루어졌다. 현재 글로벌 인터넷 거버넌스의 골격도 국제기구의 장에서 정부 대표들의 합의에 의해서 이루어진 것이 아니라 주로 미국과 유럽을 배경으로 하는 시민사회, 인터넷 전문가들과 민간사업자, 학계, 국제기구 전문가들이 만들었다(DeNardis 2013). 이러한 면모를 잘 보여주는 사례가, 초창기부터 인터넷을 관리해온 미국 캘리포니아 소재 민간기관인 ICANN이다. 그런데 이러한 모델은 인터넷 전문가들이나 민간 행위자들이 전면에 나서는 모습으로 보이지만, 실상은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판으로부터 자유롭지 못했다(Mueller 2002; 2010). 그러던 중 러시아 등의 문제제기로 인해 2010년대 초반부터 정부 간 포맷인 유엔 GGE에서 사이버 안보 문제를 논하게 되면서 새로운 전기를 맞게 된 것이다.

이밖에도 기존의 국제기구나 새로운 글로벌 거버넌스의 틀을 빌어 사이버 안보에 대한 논의가 진행되었다. 예를 들어 ITU(International Telecommunication Union) 차원에서 최근 들어 정보와 네트워크 및 사이버 안보에 대한 논의가 진행되고 있다. 특히 ITU가 주관하여 2000년대 초반 두 차례에 걸쳐서 열린 정보사회세계정상회의(WSIS: World Summit on the Information Society)에서도, 주로 인터넷 거버넌스와 글로벌 정보격차 해소가 의제였지만, 사이버 안보의 대책을 마련하기 위한 국제적 노력의 단초가 보였다. 주로 네트워크 보안의 신뢰성 강화, 프라이버시 및 고객보호, 범죄와 테러 목적의 사용 예방, 스팸 대응 등을 포함되었다. 이후에는 사이버 안보를 포함한 제반 문제에 대해 국가들을 중심으로 하고 초국적 기업 및 시민사회단체가 참여하는 국제적인 포럼인 인터넷 거버넌스 포럼(IGF: Internet Governance Forum)이 구성되어 진행되고 있다.

이렇게 세 가지 층위에서 복합적으로 전개되고 있는 사이버 안보의 제도화 과정에는 크게 두 진영의 관념과 이익이 대립하고 있다. 우선 다중이해당사자주의(multistakeholderism)와 정부간주의(intergovernmentalism)로 대별되는 두 가지 관념이 각을 세우고 있다. 앞서 언급한 ICANN 모델은 개인, 전문가 그룹, 민간 기업, 시민사회, 국가 행위자 등이 다양하게 참여하는 다중이해당사자주의의 실험대였다. 그런데 이러한 모델은 인터넷 전문가들이나 민간 행위자들이 전면에 나서는 모습으로 보이지만, 실상은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판으로부터 자유롭지 못했다. 이러한 미국과 ICANN 주도의 인터넷 거버넌스 모델에 대해서 인터넷 초창기에는 상대적으로 뒤로 물러서 있던 국가 행위자들이 좀 더 적극적으로 나서 유엔이나 ITU같은 전통 국제기구의 틀을 활용해야 한다는 정부간주의가 대두하였다. 인터넷 발전의 초기에는 선발주자로서 미국의 사실상 영향력을 인정할 수밖에 없었지만 인터넷이 지구적으로 확산되고 다양한 이해관계의 대립이 첨예해지면서 여태까지 용인되었던 관리방식의 정당성을 문제 삼을 수밖에 없다는 것이었다.

이러한 관념의 대립 이면에는 미국과 유럽 국가들이 주도하는 서

방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 비서방 진영을 다른 한편으로 하는 두 진영이 대립하는 지정학적 구도가 겹쳐진다. 넓은 의미의 글로벌 인터넷 거버넌스에서도 이러한 입장 차이가 드러나는데, 좀 더 구체적으로 사이버 안보의 질서형성 과정에서 이들 두 진영은 좀 더 극명한 입장 차이를 보인다. 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 필요시 정보통제도 가능한 공간이므로 기존의 인터넷 거버넌스를 주도해 온 서방 진영의 주장처럼 민간 중심의 다중이해당사자주의에 의해서 사이버 공간을 관리할 수는 없다고 주장한다. 요컨대, 현재 사이버 안보(넓게는 인터넷 거버넌스)의 국제규범 형성과정은, 〈그림 5〉에서 보는 바와 같이, 두 개의 네트워크가 다층적으로 경쟁하는 이른바 망제정치(網際政治, inter-network politics)의 양상을 보이고 있다.

2. 사이버 안보 분야의 중견국 외교

한국이 추구할 사이버 안보 외교의 관건은 동아시아 세력망과 복합적인 글로벌 거버넌스의 구도 안에서 구조적으로 유리한 위치를 찾아서 이를 활용하는 전략을 펼치는 데 있다. 이상에서 설명한 바를 반복컨대, 현재 미국과 서구 국가들을 한편으로 하는 서방진영과 러시아, 중국 등을 다른 한편으로 하는 비서방 진영의 지정학적 경합이 벌어지고 있다. 또한 이러한 구도는 선진국 클럽과 개도국 그룹이 두 개의 진

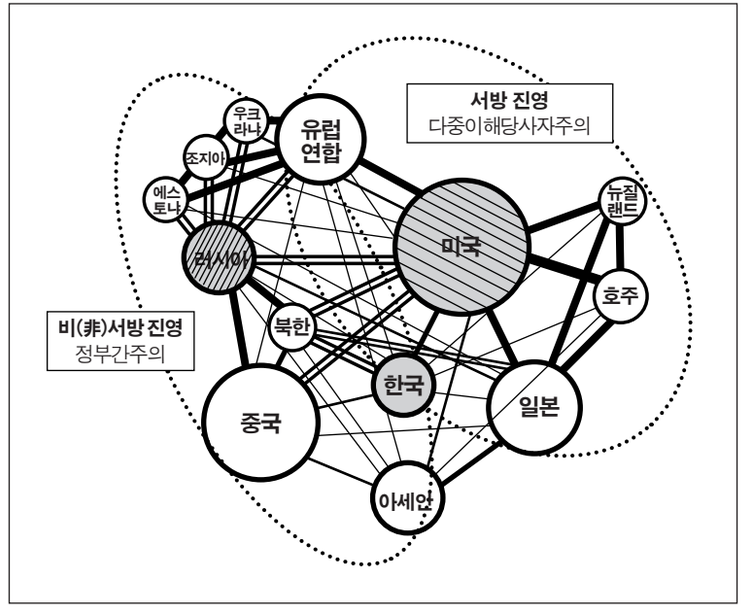

그림 5. 서방 진영과 비(非)서방 진영 사이의 한국 (가상도)

영으로 나뉘어 경합을 벌이는 양상과 겹쳐진다. 이러한 경합은 이익과 제도 및 관념의 다층적 경쟁으로 나타난다. 이러한 사이버 안보 분야의 구조적 조건을 파악하고 이를 활용하는 전략을 세우는 것은, 한국이 사이버 안보 외교를 성공적으로 추진하는 데 있어 필수적인 사안이 아닐 수 없다. 그렇다면 한국 외교는 이러한 구조적 조건을 어떻게 활용해야 할까? 이 글은 그 구체적 내용을 중견국 외교론의 시각, 특히 중개외교(brokerage diplomacy), 연대외교(coalition diplomacy), 규범외교(normative diplomacy)의 세 가지 시각에서 검토해 보고자 한다.

첫째, 중견국 외교의 핵심은 네트워크상의 관계를 조율하는 중개외교에 있다. 네트워크상에서 전략적 위치를 차지하고 구조적 공백을 보완함으로써 중견국은 강대국들 사이에서 또는 선진국들과 개도국들

사이에서 중개의 역할을 발휘할 가능성이 있다. 예를 들어 최근 사이버 안보 분야에서 갈등을 겪고 있는, 미국과 중국 사이에서 형성되는 사이버 안보 분야의 구조적 조건을 파악하고 그 안에서 전략적으로 중요한 위치를 잡는 것은 한국의 중개외교가 추구할 목표임에 분명하다. 왜냐하면 사이버 안보 분야의 구조적 공백을 메우는 과정에서 중개를 위한 구조적 기회가 제공될 뿐만 아니라 이를 통해서 한국은 중견국에게 허용되는 이른바 위치권력을 행사할 수 있기 때문이다. 따라서 한국의 입장에서 볼 때, 사이버 안보 분야의 구조적 조건에 부합하는 방향으로 외교전략의 방향을 설정하는 것은 필수적이라고 할 수 있다. 그러나 사이버 안보 분야의 현황은 한국이 추구하려는 중개외교에 기회를 제공하는 동시에 위협 요인으로 작동하기도 한다.

앞서 언급한 바와 같이, 한국은 사이버 안보 분야에서 경합하는 미국과 중국의 상이한 기술표준 사이에서 기회와 도전을 동시에 경험할 가능성이 있다. 중견국 한국에게는 미국의 지배표준과 호환성을 유지해야 하는지, 아니면 지배표준의 문턱을 넘어서 중국이 구축하려는 대안표준의 진영으로 이동해야 하는지가 관건일 수밖에 없다. 기술표준 문제가 한국의 중견국 중개외교에 부과하는 기회와 도전은 양국의 인터넷 관련 정책과 규제제도, 즉 인터넷 거버넌스 상의 차이에서도 발견된다. 인터넷 거버넌스 모델을 세움에 있어서 한국의 선택은 미국이 추구하는 민간 주도 모델과 중국이 지지하는 국가 개입 모델 사이에 놓여 있다. 사이버 안보 분야 한국의 중견국 중개외교는 글로벌 인터넷 거버넌스와 관련하여 발견되는 두 가지 상이한 입장 사이에서도 기회와 도전을 동시에 맞고 있다. 예를 들어, 2012년 12월 두바이에서 열린 WCIT(World Conference on International Telecommunication)에서 시도된 ITR(International Telecommunications Regulation)의 개정을 위한 투표를 벌일 당시 한국은 선진국과 개도국 사이에 끼어서 난감한 상황이 연출되었던 바 있었다.

둘째, 중견국 외교 추진과정에서 발생하는 딜레마 상황을 풀어가기 위해서는 뜻을 같이하는 동지국가들(like-minded countries)과 공동보조를 취하는 연대외교의 전략이 필요하다. 예를 들어 글로벌 거버넌스의 장에서 다중이해당사자주의와 정부간주의가 대립하는 경우, 그 사이에서 외로이 입장을 설정하려 시도하기보다는 비슷한 처지에 있는 국가들과 공동보조를 맞추는 것이 필요하다. 다시 말해 사이버 안보 분야의 어젠다 설정과 관련하여 중간지대에 있는 동지국가 그룹들의 역할을 새로이 규정하고 가능한 한 많은 지지 국가군을 모으려는 노력이 필요하다. 이러한 연대외교의 노력은 사이버 안보 분야에서 서로 상이한 해법을 가진 강대국 그룹들 사이에서 발생할 수도 있는 중개자로서의 딜레마를 완화시키는 데도 도움이 될 것이다. 강대국들 사이의 틈새를 공략하는 중개외교를 펼치는 경우에도 혼자 나서기보다는 비슷한 처지의 국가들과 함께 나서는 것이 성공할 가능성이 높다.

동지국가는 원래부터 관념과 이익을 같이 하는 국가들일 수도 있고 아니면 해당 이슈구조에서 유사한 위치를 차지하는 국가들일 수도 있다. 따라서 인터넷 거버넌스와 사이버 안보 분야에서도 고정된 대상이 있다기보다는 사안에 따라서 유연하게 내 편을 모아야 할 것이다. 이런 맥락에서 볼 때, 사이버 안보 분야에서 동지국가들의 연대외교를 추진하는 것과 관련하여, 최근 한국이 강조하고 있는 중견국 정부간 협의체인 믹타(MIKTA) 외교에 주목할 필요가 있다. 믹타는 2013년 6월 출범한 멕시코(M), 인도네시아(I), 한국(K), 터키(T), 호주(A)의 5개국 정부간 협의체이다. 2014년부터 G7/8, 브릭스(BRICS) 또는 IBSA 등과 같은 정부 간 네트워크와 유사한 맥락에서 시작했다. 현

재 믹타는 가능성이 높은 분야를 중심으로 협력사업을 발굴하려는 노력을 펼치고 있는데, 에너지 거버넌스, 테러리즘 대응, 경제통상 협력, 거버넌스 및 민주주의, 지속가능 개발, 양성평등, 유엔평화유지활동(PKO) 등을 다루기로 합의하였으며, 사이버 안보는 이러한 이슈들에 포함되는 대표적인 하위 분야이다.

끝으로, 사이버 안보 분야의 중견국 외교는 국제규범의 설계에 참여하는 규범외교도 필요로 한다. 사실 역사적으로 국제규범을 설계하는 외교는 강대국의 몫이었다. 그러나 중견국도 강대국이 만든 세계질서의 규범적 타당성에 문제를 제기하고 좀 더 보편적인 규범의 필요성을 강조하는 이른바 규범외교를 모색할 수 있을 것이다. 상대적으로 군사력이나 경제력에서 약세인 중견국의 입장에서 볼 때 이러한 규범외교의 추구는 일정한 효과를 얻을 수 있는 것이 사실이다. 특히 규범외교의 전략은 기성 세계질서의 운영방식에 대한 보완적 비전을 제시함으로써 강대국 위주의 논리에 대한 어느 정도의 반론을 제기하는 효과가 있다. 강대국들이 주도하고 있는 사이버 안보 국제규범의 정당성을 문제시하는 중견국 규범외교는 가능할까?

사이버 안보 분야의 중견국 규범외교는 탈지정학적이고 탈근대적인 신흥안보 이슈로서 이 분야가 지니는 구조적 조건에 대한 철저한 이해를 바탕으로 추진되어야 한다. 이 대목에서 강대국들이 주도하고 있는 사이버 안보 국제규범의 정당성을 문제시하는 중견국 규범외교의 설 자리가 생긴다. 군사적 능력이나 경제적 자원이 부족한 중견국에게 있어, 권력지향적 외교와 대비되는 의미에서 보는, 규범지향적인 외교는 효과적인 방책이 될 수 있다. 보편적 규범에 친화적인 외교는 글로벌 청중에게 매력적으로 비칠 뿐만 아니라, 중견국이 추구할 연대외교의 매우 중요한 내용이 될 수 있다. 따라서 중견국의 입장에서는 강대국들이 주도하는 국제규범 형성에 단순히 참여하는 전략의 차원을 넘어서 사이버 안보 분야의 특성에 부합하는 좀 더 보편적인 규범을 주장하거나 더 나아가 새로운 규범을 제시하는 적극성을 보일 필요가 있다.

V. 맺음말

최근 북한의 사이버 공격이 지속적으로 늘어나고 있다. 밖으로 알려진 큰 규모의 공격이외에도 알려지지 않은 작은 규모의 공격까지 포함하면 지금도 사이버 공간에서는 보이지 않는 '버추얼 창'과 이를 막으려는 '그물망 방패'의 경합이 계속되고 있는지도 모른다. 가장 최근에 알려진 사이버 공격 중에서 큰 파장을 일으킨 사건은 아마도 2014년의 소니 해킹 사건과 한수원 사태일 것이다. 북미 간에도 긴장감이 감돌았으며 국내에서도 사이버 공격에 대한 경각심이 고조되어 사이버 안보의 추진체계를 정비하는 조치들이 잇달아 이루어진 바 있다. 이제 사이버 안보는 단순한 컴퓨터 보안전문가들의 영역이 아니라 군사 전략가들이나 외교정책 결정자들이 관심을 가져야만 하는 국가안보와 외교전략의 어젠다로 명실상부하게 부상했다. 이러한 문제의식을 바탕으로 이 글은 사이버 안보 분야에서 한국이 추구할 전략과 외교의 내용을 세 가지 측면에서 살펴보았다.

첫째, 기술개발이나 인력양성을 통한 사이버 방어의 역량을 증대하고 사이버 안보 분야의 특성에 맞는 억지의 역량을 키우는 것이 필요하다. 또한 사이버 안보 분야의 국내 추진체계를 정비하고 좀 더 효과적인 대응 전략의 추진을 뒷받침하는 법적 근거의 마련에도 힘써야

한다. 사이버 안보 추진체계의 정비를 바탕으로 사이버 안보와 관련된 중장기 국가전략을 수립하여 좀 더 체계적인 대응책을 마련할 필요가 있다. 또한 단순히 사이버 안보 추진체계를 정비하는 차원을 넘어서 사이버 안보 관련 법제정을 위한 다각적인 노력도 필요하다. 이러한 법제정의 필요성에 동조하여 여태까지 국회에는 관련 법안들이 다수 제출된 바 있는데, 실무기관들의 정책집행의 효율성뿐만 아니라 국민적 동의를 얻을 수 있는 방향으로 관련법 제정을 추진해야 하는 과제를 안고 있다.

둘째, 초국적으로 발생하는 사이버 공격에 적절히 대응하기 위해서는 동아시아 주변 국가들과의 협력이 필수적이다. 공격이 우위에 서는 이 분야의 특성상 방어와 억지 역량의 구축이나 추진체계 정비와 법제정의 노력만으로 효과적인 대응방안을 마련할 수 없다는 것이 중론이다. 이런 점에서 기술과 정보를 공유하고 법적으로 공동보조를 취할 수 있는 외교적 노력이 병행되어야 한다. 한국의 입장에서 볼 때, 전통적인 우방국인 미국과 일본, 그리고 최근 그 중요성이 커지고 있는 중국 및 글로벌 변수로서 의미를 갖는 러시아 등과의 사이버 외교관계에 대한 인식의 제고가 필요하다. 특히 북한의 사이버 공격과 관련하여 관건이 되는 것은 이들 국가들과의 정보공유 네트워크를 구축하고, 사법공조를 위한 외교적 노력을 펼치거나, 국제사회에 호소하고 도움을 요청하는 외교적 역량의 발휘이다.

끝으로, 국제적인 차원에서 사이버 안보의 대응방안을 모색하는데 있어서 양자 간의 국제협력이라는 구도보다 좀 더 넓은 의미의 다자 구도에서 접근하는 시도도 필요하다. 아직까지 사이버 안보 분야에는 사이버 공격에 대해서 어떠한 규범을 적용하여 제재할지에 대한 합의기반이 마련되지 않고 있다. 최근 전통적인 국제법과 국제기구의 틀을 원용하여 규범을 마련하려는 움직임이 선진국들을 중심으로 진행되고 있다. 이러한 사이버 안보의 국제규범 형성과정에 적극적으로 참여하는 것 자체가 중요한 대응방안이 될 수 있다. 그러나 이러한 국가 간 관계의 틀 이외에도 다양한 통로를 통해서 민간 행위자들이 주도하고 있는 글로벌 거버넌스의 모색 과정을 예의 주시하는 것도 필요하다.

사이버 안보의 세계정치는 역사에서 전례를 찾을 수 없는 궤적을 따라서 끊임없이 진화해 갈 가능성이 크다. 중견국으로서 한국이 사이버 안보 분야의 고유한 구조와 동학을 이해하고 이에 대해서 적절한 대응책을 마련하는 것은 매우 중요하다. 예를 들어 사이버 안보와 전통안보는 어떠한 질적인 차이를 갖는지, 사이버 안보의 기술과 전략의 역량 면에서는 어느 나라가 앞서는지, 이 분야의 국제규범 형성에서 누가 어느 진영에 속해서 경쟁하고 있는지, 두 강대국인 미국과 중국이 형성해갈 관계는 어떠한 성격일 것인지 등을 파악하는 것은 매우 중요하다. 다시 말해, 진화하는 사이버 안보 분야의 맥락을 파악하고 그 안에서 적절한 위치를 설정하는 것은 핵심적인 미래 국가전략의 사안이 아닐 수 없다. 이를 바탕으로 어떠한 종류의 외교적 역할을 추구할지에 대한 방향을 모색할 수 있을 것이기 때문이다. 이런 맥락에서 이 글은 중견국 외교의 이론적 자원들을 적용하여 한국이 추구해야 할 사이버 안보 분야 외교전략의 방향을 제시하였다.

요컨대 향후 한국이 북한의 사이버 공격을 포함한 초국적 사이버 공격에 능동적으로 대응하고 좀 더 평화롭고 안전한 사이버 공간을 확보하기 위해서는 이 글에서 제시한 대응방안들에 진지한 검토가 필요하다. 그러나 이와 동시에 각 대응방안들이 그 기저에 깔고 있는 과잉담론화의 가능성과 각 담론들이 상호 충돌하는 딜레마의 상황을 풀어나갈 지혜도 필요하다. 그도 그럴 것이 바람직한 대응방안은 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 찾아야하기 때문이다. 사이버 안보 문제가 급속히 21세기 국가안보의 문제로 부상하는 속도만큼 우리 모두의 중지를 모아서 이 분야에서 제기되는 위협에 대한 대응방안을 시급히 궁리하는 국제정치학적 연구가 시급히 필요한 때이다.

참고문헌

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

_____. 2014b. "사이버 안보 분야의 미·중 표준경쟁: 네트워크 세계정치학의 시각." 『국가정책연구』28(3), pp. 237-263.

_____. 2015a. "사이버 안보의 미중관계: 안보화 이론의 시각."『한국정치학회보』49(1), pp. 71-97.

_____. 2015b. "버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 북한." 윤영관·전재성·김상배 편.『네트워크로 보는 세계 속의 북한』늘품플러스, pp. 155-200.

_____. 2015c. "사이버 안보의 복합 지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계."『국제·지역연구』24(3), pp. 1-40.

_____. 2016. "사이버 안보의 중견국 외교: 가능성과 한계." 손열·김상배·이승주 편. 『한국의 중견국 외교』명인문화사, pp. 269-311.

김홍광. 2011. "북한의 사이버 테러능력." 북한민주화네트워크 편,『2011 북한의 사이버 테러 관련 긴급 세미나 자료집』.

민병원. 2015. "사이버공격과 사이버억지의 국제정치: 규제와 새로운 패러다임을 중심으로." 『국가전략』21(3), pp. 37-61

박노형·정명현. 2014. "사이버전의 국제법적 분석을 위한 기본개념의 연구: Tallinn Manual의 논의를 중심으로."『국제법학회논총』59(2), pp. 65-93

이상현. 2008. "정보보안 분야의 지식질서와 동아시아." 김상배 외.『지식질서와 동아시아: 정보화시대 세계정치의 변환』한울, pp. 295-330.

임종인·권유중·장규현·백승조. 2013. "북한의 사이버전력 현황과 한국의 국가적 대응 전략." 『국방정책연구』29(4), pp. 9-45.

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

장노순. 2016. "사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로." 『정치정보연구』19(1), pp. 1-28.

장노순·한인택. 2013. "사이버안보의 쟁점과 연구 경향."『국제정치논총』53(3), pp. 579-618.

조현석. 2012. "사이버 안보의 복합세계정치." 하영선·김상배 편.『복합세계정치론: 전략과 원리, 그리고 새로운 질서』한울, pp. 147-189.

최인호. 2011. "사이버 안보의 망제정치: 사이버 창이냐? 디지털 방패냐?" 김상배 편. 『거미줄 치기와 벌집 짓기: 네트워크 이론으로 보는 세계정치의 변환』한울, pp. 285-325.

허영호. 2014. "국가 사이버테러 방지에 관한 법률안(서상기의원 대표발의), 국가 사이버안전 관리에 관한 법률안(하태경의원 대표발의)." 국회 정보위원회 검토보고서.

Christou, George. 2016. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Palgrave Macmillan UK.

Deibert, Ronald J. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: Signal.

DeNardis, Laura. 2013. *The Global War for Internet Governance*. Yale University Press

Geers, Kenneth. 2015. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence(CCDCOE)

Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53(4), pp. 1155–1175.

Hurwitz, Roger. 2014. "The Play of States: Norms and Security in Cyberspace." *American Foreign Policy Interests*, 36(5), pp. 322–331

Jun, Jenny, Scott LaFoy, and Ethan Sohn. 2015. *North Korea's Cyber Operations: Strategy and Responses*, Center for Strategic and International Studies (CSIS)

Kim, Geun-hye, Kyung-bok Lee and Jong-in Lim. 2015. "CBMs for Cyberspace beyond the Traditional Security Environment: Focusing on Features for CBMs for Cyberspace in Northeast Asia." *The Korean Journal o f Defense Analysis*. 27(1), pp. 87–106.

Kim, Sangbae. 2014. "Cyber Security and Middle Power Diplomacy: A Network Perspective." *Korean Journal of International Studies*, 54(4), pp. 323–352.

Lewis, James Andrew. 2015. *U.S.-Japan Cooperation in Cybersecurity*. A Report of the CSIS Strategic Technologies Program. CSIS.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford and New York: Oxford University Press.

Lupovici, Amir. 2011. "Cyber Warfare and Deterrence: Trends and Challenges in Research." *Military and Strategic Affairs*. 3(3), pp. 49–62.

Mansourov, Alexandre. 2014. "North Korea's Cyber Warfare and Challenges for the U.S.–ROK Alliance." Academic Paper Series. Korea Economic Institute of America. December 2.

Morgan, Patrick M. 2010. "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm." Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy. National Research Council.

Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: The MIT Press.

Mueller, Milton L. 2010. *Networks and States; The Global Politics of Internet Governance*. Cambridge and London: MIT Press.

Nye Jr. Joseph S. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter, pp. 18–38.

Nye, Joseph S. 2013. "From bombs to bytes: Can our nuclear history inform our cyber future?" *Bulletin of the Atomic Scientists*. 69(5), pp. 8–14

Rid, Thomas. 2013. *Cyber War will not take place*. Oxford and New York: Oxford University Press.

Schmitt, Michael N. 2012. "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed." *Harvard International Law Journal*. 54, pp. 13–37.

Singer, Peter W. and Noah Shachtman. 2011. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive." August, 15, The Brookings Institution.