Institute of International Studies at Seoul National University | 국제문제연구소 워킹페이퍼 No.1 (발간일: 2017. 2. 1.)

사이버 안보의 주변4망(網)과 한국:

세력망의 구조와 중견국의 전략

김상배

서울대학교 정치외교학부 교수
인디애나대학교 정치학 박사
전공분야: 정보혁명과 네트워크 세계정치
대표업적: 『아라크네의 국제정치학』(2014), 『정보혁명과 권력변환』(2010), 『정보화 시대의 표준경쟁』(2007) 외 다수

초 록

최근 사이버 안보가 국가안보의 중요한 사안으로 부상하였다. 향후 한국이 사이버 안보 전략을 펼쳐나감에 있어서 주변의 네 나라, 즉 미국, 중국, 일본, 러시아는 중요한 변수가 아닐 수 없다. 이 글은 전통적으로 주변4강(强)이라고 불려온 이들 나라들을 사이버 안보 분야의 특성을 반영하여 네 개의 '네트워크 국가'라는 의미로 '주변4망(網)'으로 개념화하였다. 이는 사이버 안보 분야에서는 각국의 역량과 전략이외에도 이들이 형성하는 관계 구도로서의 네트워크를 정확히 인식하는 것이 중요하다는 문제의식을 기반으로 한다. 사이버 안보의 주변4망(網)론을 체계적으로 제시하기 위해서 이 글은 네트워크 이론, 그 중에서도 특히 소셜 네트워크 이론에서 제시하는 구조적 공백, 위치권력, 중개자 등의 개념들을 원용하였다. 이러한 시각에서 보면, 현재 사이버 안보 분야에서 주변4망(網)이 형성하는 세력망(network of power)의 구조는 동북아 차원에서는 미국과 중국, 지역협력 차원에서는 아시아·태평양과 동아시아, 글로벌 차원에서는 서방 진영과 비(非)서방 진영 간에 벌어지는 망제정치(網際政治, internetwork politics)를 내용으로 한다. 현재 한국은 이러한 사이버 안보 분야 고유의 세력망 구조를 정확히 이해하고 중견국 외교의 전략을 추구할 과제를 안고 있다.

I. 머리말

지난 10여 년 동안 사이버 안보는 해커들의 장난이나 테러리스트들의 공격을 넘어서 국가 행위자들의 공격과 방어, 그리고 경쟁과 협력의 쟁점이 되었다. 글로벌 차원에서는 2007년 에스토니아 사태, 2010년 미국과 이란의 공방, 그리고 최근의 미중 갈등을 거치면서 이제는 국가 행위자들이 전면에 나서는 양상을 보이고 있다. 한반도에서도 주기적으로 발생하는 북한의 사이버 공격이 일단 유사시에 핵과 미사일, 재래식 공격 등과 연계될지도 모른다는 우려를 낳고 있다. 그야말로 사이버 안보는 이제 국가안보의 사안이 되었다. 이렇게 증대된 사이버 안보의 중요성에 비해서 이에 대응하는 대책의 마련은 여전히 빈약하다. 특히 사이버 공격의 기술적 특성은 일국 차원의 방어 역량만으로는 막아내기 어렵게 한다(Deibert, 2013). 사이버 공간의 안보가 단순히 정보보안 전문가들에 의해서만 보장되지 않는 이유이다. 사이버 안보의 확보를 위해서는 주변국들과 정보공유체계를 구축하고, 사법공조를 위한 국제적 노력을 펼치거나, 이 분야의 국제규범 형성에 참여하고, 국제사회에 호소하는 외교적 역량의 발휘가 필요하다. 이런 점에서 사이버 안보는 명실상부하게 국제정치학의 논제로 부상하였다.[1)]

이러한 상황에서 한반도 주변의 네 나라, 즉 미국, 중국, 일본, 러시아는 한국의 사이버 안보 전략에 있어 중요한 변수가 아닐 수 없다. 한국에게 사이버 안보의 문제는 단순한 북한의 공격에서 비롯되는 남북한 문제가 아니라 이들 네 나라와의 관계 속에서 풀어야 하는 숙제이다. 주요 사이버 위협이 북한의 공격에서 비롯되기 때문에 이에 대응하기 위해서 의지하는 가장 유력한 정치군사적 자원이 기존에 한반도 안보의 핵심 변수로 작동해온 한미동맹인 것은 당연하다. 그러나 북한의 사이버 공격이 중국을 경유해서 발생한다는 점에서 중국과의 외교적 협력도 무시할 수 없는 카드이다. 또한 한미일 관계나 한중일 관계의 맥락에서 볼 때 일본은 중요한 연결고리의 역할을 한다. 글로벌 차원으로 눈을 돌리면 러시아도 사이버 안보 분야에서 여전히 무시할 수 없는 변수이다. 요컨대, 지난 백여 년간 한국 외교에서 이들 네 나라와의 관계를 조율하는 것이 핵심적 사안이었다면, 앞으로 사이버 안보 분야에서도 이들과의 관계를 원활하게 풀어가는 것은 중요할 수밖에 없다.

그런데 사이버 안보 분야에서 이들 네 나라를, 일반적으로 부르는 것처럼, 자원권력의 관점에서 본 강대국이라는 의미로 '주변4강(强)'이라고 상정하는 것은 적절치 않다. 기존의 한반도 국제정치 연구는 주로 이들이 형성하는 '세력균형(balance of power, BoP)'의 구

1) 국제정치학의 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. 이밖에 해외연구로 Peritz and Sechrist(2010), Stevens(2012), Junio(2013), Valeriano and Maness(2015) 등도 참조하기 바란다.

조를 분석했다. 그러나 사이버 안보 분야에서 이들 국가들이 생성하는 구조는, 자원권력의 분포로서 '구조' 라기보다는, 오히려 행위자들의 상호작용 과정에서 생성되는 '관계구도(relational configuration)' 로 파악되어야 한다. 물론 사이버 안보 분야에서도 자원권력을 바탕으로 한 지정학적 '구조' 는 여전히 작동한다. 그럼에도 탈(脫)지정학적 공간으로서 사이버 공간을 배경으로 벌어지는 사이버 공격과 방어의 특성을 볼 때, 복합 네트워크 환경에서 형성되는 '세력망(network of power, NoP)' 의 구조를 보려는 노력이 필요하다. 이런 맥락에서 이 글은 사이버 안보 분야의 이들 나라들을 네 개의 네트워크라는 의미로 '주변4망(網)' 이라고 개념화하고자 한다. 사이버 안보 분야에서 주변4망(網)을 논하는 것은 각국의 역량만을 보는 것이 아니라, 이들 나라들의 관계구도, 즉 이들 네트워크가 형성하는 망제정치(網際政治, inter-network politics) 속에서 한국의 전략을 논해야만 한다는 문제의식을 반영한다.

사이버 안보의 주변4망(網)과 한국의 외교전략에 대한 학술적 연구는 별로 진행된 바가 없다. 그나마 미디어를 통해서 제기되고 있는 시각들도 주변4강(强)론으로 대변되는 전통적인 인식 틀에만 의지하고 있다. 예를 들어 사이버 국제협력을 논하는 경우 단순히 군사동맹의 수준에 준하는 한미 사이버 협력 강화만을 견지한다든지, 강대국들의 사이버 경쟁을 논하는 경우에도 이를 '사이버 냉전' 에 비유하는 시각은 지나치게 전통 담론에 의거하고 있다. 또한 군사전략의 시각에서 냉전 시대의 핵전략에 기원을 두는 억지 개념을 사이버 안보 분야에 그대로 원용하거나 유럽의 나토 차원에서 개발된 근대 전쟁법의 적용 시도를 한반도에 들여오려는 시각도 마찬가지로 적절치 못하다. 이러한 시도들은 결국에는 기술과 인력의 역량을 배양한다든지 또는 제도를 강화하고 관련법을 제정하자는 이른바 '사이버 강국' 건설의 과잉 안보화 담론으로 귀결될 가능성마저 안고 있다(Hansen and Nissenbaum, 2009; Rid, 2013). 그러나 사이버 안보의 미래 국가전략은 이러한 단순 발상만으로는 풀 수 없으며, 좀 더 복합적인 접근을 필요로 한다는 것이 이 글의 인식이다.

사이버 안보의 주변4망(網)론을 체계적으로 제시하기 위해서 이 글은 네트워크 이론, 그 중에서도 특히 소셜 네트워크 이론에서 제시하는 개념을 원용하였다. 특히 소셜 네트워크 이론이 제시하는 관계구도로서의 구조 개념은 사이버 안보 분야의 구조를 이해하는 데 도움을 준다. 또한 이러한 구조의 특성을 반영하는 개념으로서 구조적 공백(structural hole)이나 사회적 자본(social capital)에 대한 이론적 논의가 유용하다. 더 나아가 이렇게 구조를 보는 시각이 유용한 이유는, 네트워크 구조에 대한 논의를 바탕으로 행위자 차원에서 모색해야 할 구체적인 실천전략을 논하는 실마리를 제공하기 때문이다. 다시 말해 네트워크의 시각은 구조를 새롭게 보게 할 뿐만 아니라 이를 공략하는 행위자의 전략도 새롭게 보게 하는 유용성이 있다. 특히 소셜 네트워크 이론에서 말하는 위치권력(positional power)과 중개자(broker)에 대한 논의는 네트워크상의 빈틈을 공략하는 전략의 의미를 보여준다. 이 글은 네트워크의 구

조와 중개자의 전략에 대한 논의를 국제정치학에 원용한 이른바 '중견국 외교'의 관점에서 한국의 사이버 안보 전략과 외교를 살펴볼 것이다.[2)]

이러한 네트워크의 시각에서 보면, 현재 사이버 안보 분야에서 한반도 주변4망(網)이 형성하는 세력망 구조는 세 층위로 중첩되는 양상으로 나타나는데, 이러한 구도에서 한국이 추구할 중견국 전략의 과제가 발견된다. 첫째, 사이버 안보 주변4망(網)의 주축은 미중관계를 중심으로 형성되는데, 현재 한국의 입장에서는 한미동맹만 강화할 수는 없고 점차 늘어나는 중국과의 상호의존 관계를 고려하는 비대칭 관계조율의 중개외교 전략을 구사할 과제를 안고 있다. 둘째, 동아태 지역 차원에서 사이버 안보의 주변4망(網)은 아태 지역협력과 동아 지역협력의 망제정치 구도로 형성되는데, 현재 한국의 입장에서는 미국이 주도하는 아태 지역동맹과 한중일과 아세안이 모색하는 동아 지역협력의 사이에서 복합적인 역내외 연대외교 전략을 추구할 고민을 안고 있다. 끝으로, 글로벌 차원에서 사이버 안보의 주변4망(網)은 국제규범 형성을 둘러싸고 서방 진영과 비서방 진영이 경쟁하는 구도로 나타나는데, 현재 한국의 입장에서는 이들의 틈바구니에서 강대국들의 제시하는 국제규범을 보완하는 중견국 규범외교의 전략을 추구할 필요가 있다.

이 글은 크게 네 부분으로 구성되었다. 제2장은 소셜 네트워크 이론의 시각을 원용하여 사이버 안보의 세력망 구조와 이에 대응하는 중견국의 네트워크 전략을 이해하는 이론적 논의를 소개하였다. 제3장은 사이버 안보의 주변4망(網) 중에서 미국과 중국이 형성하는 망제정치의 세력망을 그려보고, 이러한 구도 중에서, 특히 한미동맹과 한중협력 사이에서 중견국 한국이 안고 있는 중개외교의 기회와 딜레마에 대해서 살펴보았다. 제4장은 아태 지역동맹과 동아 지역협력의 망제정치라는 구도에서 주변4망(網)의 경쟁 양상을 파악하고 그 안에서 한국이 취할 연대외교 전략의 방향, 특히 일본 변수에 대한 고민을 펼쳐놓았다. 제5장은 글로벌 차원에서 형성되는 사이버 안보의 세력망을 미러경쟁과 중러협약, 그리고 서방 진영과 비서방 진영의 국제규범 형성을 놓고 벌이는 관념과 이익의 경쟁 구도로 파악하고, 그 안에서 중견국 한국이 추구할 규범외교의 필요성을 지적하였으며, 특히 상대적으로 소홀히 취급되고 있는 러시아 변수의 의미를 짚어 보았다. 끝으로 맺음말에서는 이 글의 주장을 종합·요약하고 이 글이 던지는 정책적 함의를 간략히 지적하였다.

2) 자연과학과 사회과학에서 연구되는 네트워크 이론 전반의 맥락에서 본 소셜 네트워크 이론에 대한 논의와 구조적 공백, 사회적 자본 및 위치권력과 중개자 등과 같은 개념들을 국제정치학의 시각에서 소개하고 이를 세력망의 구조와 중견국의 전략에 대한 논의에 접맥한 연구로는 김상배(2014a)를 참조하기 바란다.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

II. 사이버 안보의 네트워크 구조와 전략

1. 네트워크로 보는 세력망의 구조

네트워크 전략을 펼쳐나가는 데 있어서 행위자의 입장에서 일차적으로 필요한 것은 자신을 둘러싸고 형성된 네트워크의 구조를 파악하는 것이다. 여기서 말하는 구조는 현실주의로 대변되는 기존의 주류 국제정치학이 말하는 지정학적 구조, 즉 행위자들 간의 물질적 능력의 분포에 기반을 두는 거시적(macroscopic) 구조가 아니다. 이 글이 원용하는 소셜 네트워크 이론의 구조는 행위자들 간의 관계에서 발견되는 지속적인 패턴으로 파악된 구조를 의미한다. 다시 말해 소셜 네트워크 이론의 구조 개념은 행위자들의 지속적인 상호작용을 통해서 생성되는 관계구도, 즉 네트워크 그 자체라는 맥락에서 이해된다. 지정학적인 거시적 구조에 대비되는 의미에서 일종의 중범위(mesoscopic) 구조라고 할 수 있다. 일반적으로 이러한 중범위 구조는 사회연결망분석(Social Network Analysis, SNA)라는 방법론적 기법을 통해서 가시적으로 그려진다. 최근의 국제정치 연구에서도 이러한 동태적 구조의 개념에 입각한 네트워크 분석이 등장하고 있다. 이렇게 그려지는 구조는 기존의 세력균형의 구조는 아니지만 세력망의 구조를 보여준다는 유용성이 있다.

사이버 안보 분야의 구조를 이해하는 데 있어서 자원권력의 분포로 이해되는 전통적인 의미의 지정학적 구도가 중요하지 않은 것은 절대 아니다. 그러나 사이버 안보 분야의 특성을 제대로 이해하기 위해서는 이상에서 언급한 관계구도로서의 구조, 즉 세력망을 이해하는 것이 필수적이다. 그런데 여기서 발생하는 문제는 사이버 안보 분야에서 형성되는 세력망의 구조를 가시적으로 보여주는 작업이 쉽지 않다는 사실이다.[3] 무엇보다도 복잡한 상호작용을 벌이고 있는 사이버 공간의 흐름을 잡아낼 데이터의 가용성이 문제이다. 이러한 한계를 인정한다는 전제 하에서 이 글은 〈그림-1〉과 같은 글로벌 세력망의 가상도를 그려보는 시도를 했다.

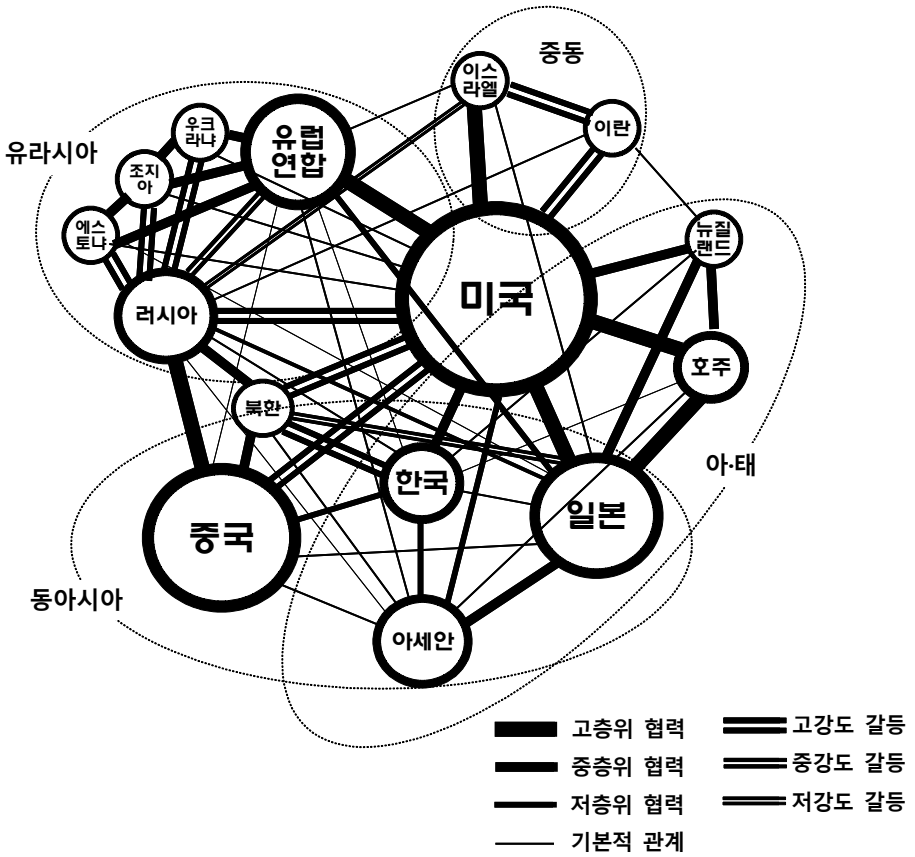
이 그림은 노드와 링크에 대한 엄밀한 데이터를 대입해서 그린 것이라기보다는 대략의 데이터를 염두에 두고 직관적으로 그린 것이다. 다른 크기의 원으로 그려진 노드들은 국가 행위자들을 의미하는데, 군사력이나 경제력, 기술력 등과 같은 대략의 국력의 크기를 염두에 두고 그려 보았다. 〈그림-1〉에서 좀 더 중요한 것은 굵기의 차이로 표현된 링크의 속성인데, 이는 각국 간에 벌어지고 있는 사이버 안보 관련 협력과 갈등의 정도를 표시했다. 사이버 안

3) 이 글에서 탐구하는 사이버 안보의 네트워크 구조에 대한 연구와 맥이 닿는 사회연결망분석(SNA)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(CBM)를 중심으로 세력망 구도를 엿보게 하는 작업을 했다. 그러나 이러한 시도도 역시 사이버 안보 분야 세력망의 특정한 일면만을 보여주는 한계를 넘지는 못했다.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

보 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.

그림 1 사이버 안보의 글로벌 세력망(가상도)



〈그림-1〉은 실상도가 아니라는 한계에도 불구하고 사이버 안보 분야의 글로벌 세력망의 전체 구도를 가시적으로 연상하는 효과가 있다는 점에서 일면 유용성이 있다. 또한 〈그림-1〉이 갖는 유용성은 전체 구도의 맥락에서 사이버 안보 분야에서 형성되는 네트워크의 구조적 특성, 특히 사회적 자본이나 구조적 공백 등을 좀 더 가시적으로 살펴볼 수 있다는 데 있다(Burt, 1992; 2005). 구조적 공백을 파악하는 것이 중요한 이유는 이를 메움으로서 새로운 역할과 가치의 창출이 기대되기 때문이다. 틈새를 찾는 것과 더불어 네트워크상에서 상

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

대적으로 밀집되고 중복된 상호작용이 발생하는 부분, 즉 일종의 '배후지'를 파악하는 것도 중요한데, 이는 일찍이 사회적 자본이라는 개념으로 알려져 왔다(Putnam, 1993; Lin, 2001). 이러한 구조적 공백이나 사회적 자본은 실재하는 공간이 아니라 오히려 행위자들에 의해서 적극적으로 구성되는 공간이라는 점에서 전략적 의미가 있다.

2. 네트워크로 보는 중견국의 전략

이상에서 살펴본 구조적 공백과 사회적 자본 개념의 기저에는 노드들 간의 흐름을 중개하는 중개자(broker)의 전략에 대한 관심이 깔려 있다. 그런데 여기서 주목할 것은 네트워크 시각에서 본 중개자의 역할은 행위자의 속성이나 기질에서 나오는 것이 아니라 그 행위자가 네트워크상에서 차지하는 구조적 위치(structural position)에 의해서 비롯된다는 사실이다. 다시 말해, 중개자는 네트워크상의 전략적 요충지를 장악하고 주변의 노드들을 연결해 주는 '중개'의 역할을 담당한다. 특히 구조적 공백을 남보다 먼저 찾아서 메움으로써, 중개자는 네트워크 구조에서 중심적 위치를 장악하게 되고 거기에서 비롯되는 독특한 권력을 행사하게 된다. 이렇게 중개자가 행사하는 권력은 '위치권력(positional power)' 또는 '중개권력(brokerage power)' 등으로 개념화된다(Burt, 1992; 김상배, 2014a).

이러한 중개자와 그 권력에 대한 논의는 노드로서의 국가 행위자인 한국의 중견국 전략에 대한 논의에 적용할 수 있다. 최근 중견국으로서 한국의 외교적 역할을 논하는 것은 국력 크기가 중간이어서 그런 것도 있지만 국제체제에서 한국이 차지하는 구조적 위치가 중개의 역할을 요구하는 데에서 기인하는 바가 크다. 다시 말해, 지난 수십 년 동안 증대된 국력이 한국이 중견국으로 발돋움하는 물질적 기반이 되었을 뿐만 아니라, 최근 세계정치의 변화가 한국으로 하여금 중견국으로서 외교적 역할을 발휘할 새로운 기회를 창출하고 있다는 것이다. 사이버 안보 분야는 중견국으로서 한국의 구조적 위치와 외교적 역할을 논하게 하는 새로운 환경이다. 여기서 한국의 중견국 외교에 제기되는 관건은 사이버 안보의 글로벌 및 동아시아 세력망에서 구조적으로 유리한 위치를 찾아서 이를 활용하는 전략을 펼치는 데 있다. 그렇다면 사이버 안보의 세력망에서 한국이 차지하고 있는 '구조적 위치'는 어디이며, 거기서 구조적 공백이나 사회적 자본을 어떻게 확인할 수 있을까?

〈그림-1〉에서 보는 바와 같이, 그리고 이 글의 본론에서 주장하고 있듯이, 한국이 처해 있는 세력망의 구조와 거기서 기대되는 중견국 전략의 과제는 다음과 같은 세 가지 차원에서 파악된다. 첫째, 일차적으로 양자관계의 차원에서 전통적인 우방인 미국과 최근 급부상하고 있는 중국의 사이에서 한국이 추구할 중견국의 역할을 기대케 한다. 둘째, 다자관계의 차원에서 미국이 주도하는 아태 지역동맹과 동아 지역협력 사이의 '중간지대'에서 한국은 역내외 국가들과의 관계를 새롭게 설정할 과제를 안고 있다. 끝으로 글로벌 차원에서 미국과 서구

국가들을 한편으로 하는 서방 진영과 러시아, 중국 등을 다른 한편으로 하는 비서방 진영의 사이에서 한국은 중견국 규범을 제시하는 외교적 역할을 모색할 과제를 안고 있다. 이렇게 사이버 안보 분야의 다층적 구조를 제대로 파악하고 이를 활용하는 전략을 세우는 것은, 한국이 사이버 안보 외교를 성공적으로 추진하는 데 있어 필수적인 사안이 아닐 수 없다.

이 글은 사이버 안보 분야에서 이상에서 언급한 구조적 조건을 파악해서 활용하는 중견국 외교의 구체적 내용을 중개외교(brokerage diplomacy), 연대외교(coalition diplomacy), 규범외교(normative diplomacy) 등의 세 가지 측면에서 검토할 것이다. 우선 필요한 것은 사이버 안보 분야에서 경쟁하는 행위자들의 관계를 조율하는 중개외교이다. 특히 미국과 중국 사이에서 구조적 공백을 찾아내어 공략함으로써 새로운 관계구도를 창출하는 '비대칭 관계 조율' 의 외교적 역할을 발휘할 필요가 있다. 둘째, 복합적으로 얽혀 있는 아태 지역과 동아 지역의 구도에서 동아태 역내 또는 글로벌 차원의 역외 국가들과의 연대외교를 추구할 필요가 있다. 사실 지금처럼 얽혀있는 동아태 지역의 구도에서 어느 나라도 혼자 나서서 효과적인 결과를 얻어내기는 쉽지 않으며, 생각을 공유하고 행동을 같이하는 동지국가들과 보조를 맞추는 것이 필요하다. 끝으로, 중견국으로서 한국은 나름대로 세계정치의 판세를 읽고 제도와 규범을 설계하는 규범외교의 발상을 가져야 할 것이다. 특히 강대국들이 만들어 놓은 질서를 보완하는 차원에서 규범적 가치와 정당성을 추구하는 중견국 규범의 제시를 생각해 볼 수 있다.

III. 한미동맹과 한중협력 사이의 한국

1. 북한의 사이버 공격과 한미동맹의 과제

사이버 안보 주변4망(網) 중에서도 핵심은 사이버 선진국이자 우방국인 미국과의 기술과 정보공유 및 협력체계를 구축하는 문제이다. 전통안보의 틀 내에서 이미 논의되어 왔지만 최근 북한의 대남 사이버 공격이 문제시되면서 사이버 안보 분야에서도 양국 간 협력이 관심사가 되었다.[4] 미국의 입장에서 보아도 사이버 안보 분야에서 중국과의 갈등이 커지면서 아태 지역에서 동맹을 구축하려는 데 관심을 기울이고 있던 차에, 2014년 말 소니 해킹 사건을 통해서 북미 간에도 갈등이 생기면서 한미 사이버 협력의 조건이 더욱 무르익었다. 실제로

4) 북한의 사이버 공격 역량에 대해서는 객관적인 정보와 분석이 매우 부족하다. 제한적이긴 하지만 흔히 인용되는 자료로는 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.

2014년 11월 북한의 소니 해킹 사건이 발생했을 때 미국이 북한의 소행을 밝혀내는 과정에서 한국의 협조가 있었던 것으로 알려져 있다. 미국은 사이버 공격에 동원된 수단이 2013년 3월 20일 발생했던 한국의 금융기관과 언론사에 대한 공격수법과 유사하다는 사실을 밝혀냈는데, 이를 바탕으로 수사단계에서 한미 간에 정보공유가 이루어졌다고 한다(『보안뉴스』, 2015-07-17).

북한의 사이버 능력과 위협에 대한 정보가 필요한 상황에서 한국의 정보제공은 미국의 관심을 끄는 좋은 카드인 것이 사실이다. 그러나 한국이 미국에 줄 수 있는 것이 북한에 대한 정보뿐인 상황에서 미국으로부터 최신 사이버 보안기술 이전과 같은 실질적인 협력을 얻어내는 것은 쉽지 않다는 비판도 제기되었다(Lim, 2016). 예를 들어, 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』 2015-07-24). 한미 간에 사이버 기술력의 비대칭성이 엄연히 존재하는 상황에서 실질적 협력의 어려움을 엿보게 하는 대목이 아닐 수 없다.

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 '사이버 안보 협력채널' 을 신설하고 국제사회에서 사이버 안보 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 2013년 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. 2016년 3월에는 미래부 차관의 방미를 계기로 한미 ICT 정책포럼의 후속조치로서 양국이 사이버 보안 기술 공동개발과 사이버 보안 분야 국장급 회의의 정례화에 합의했다.

이러한 과정에서 제기되었던 한미 사이버 협력의 쟁점 중의 하나는, 북한에 대한 사이버 억지력을 보강하는 차원에서 한미 상호방위조약의 틀 내에 사이버 안보의 문제를 포함시킬 것이냐의 문제였다. 다시 말해, 핵공격과 재래식 공격과 관련하여 작동하고 있는 한미동맹을 가동하여 미국의 이른바 '사이버 우산'을 빌려 쓸 것이냐의 문제였다.[5] 국내 일각에서는 오프라인 동맹의 경우처럼 온라인에서도 한미 사이버 동맹을 구축하는 차원에까지 협력을 강화하자는 주장이 제기되기도 하였다. 그러나 탈냉전 이후 세계정치의 시대적 상황변화와 사이버 안보 문제가 지니는 쟁점의 고유한 성격, 그리고 사이버 안보 문제뿐만 아니라 지정학적 문제가 복합적으로 작용하는 한반도 주변4망(網)과의 관계 등을 고려할 때, 한국이 한미 사이버 협력을 무조건 동맹 수준으로 격상시키는 것만이 능사가 아님을 명심할 필요가 있다.

기존의 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 없기 때문이다. 그야말로 협력영역, 협력주체, 협력정도 등이 다양하게 나타나는 비대칭 복합동맹이라는 맥락에서 한미 사이버 협력의 문제에 접근할 필요가 있다(유지용·이강규, 2013).

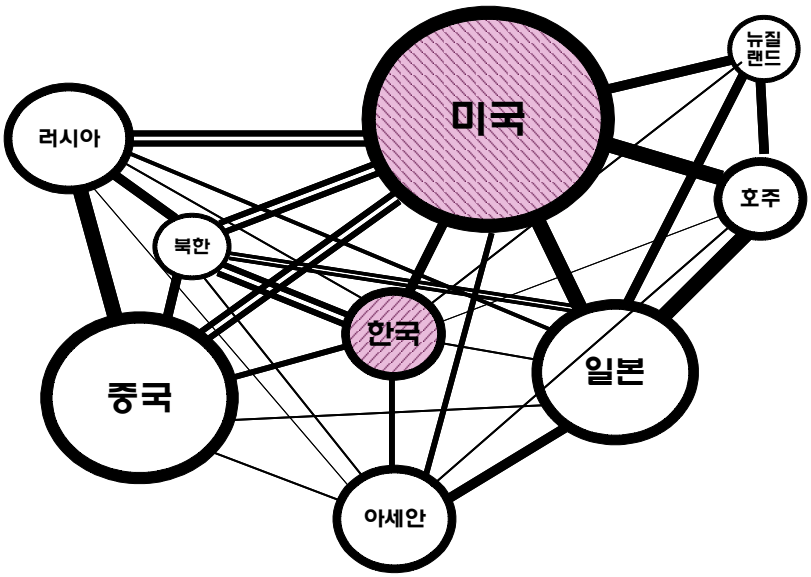
예를 들어, 한미 사이버 협력을 가장 높은 수위까지 상승시켜, 다음 장에서 살펴보는 바와 같이, 미일 방위협력지침이나 나토 차원에서 거론되는 사이버 집단자위의 고층위 협력의 차원에까지 격상시키는 것이 맞을까? 한미 사이버 협력의 내용으로 공동 사이버 전쟁게임이나 공동 사이버 군사훈련, 분석도구의 공동개발 등과 같은 공동 연구개발 등의 중층위 협력

5) 이러한 논의는 최근 국내외 학계에서 거론되고 있는 사이버 억지(cyber deterrence) 개념의 적용 가능성에 대한 논의와 맥을 같이 한다. 사이버 억지의 개념을 검토한 연구로는 Morgan(2010), Lupovici(2011), Singer and Shachtman(2011), Nye(2011; 2013), 장노순·한인택(2013), 민병원(2015) 등을 참조하기 바란다.

의 수준에서 머무는 것이 맞을까? 아니면 한미 사이버 협력은 낮은 수위의 협력으로만 유지하는 것이 맞을까? 이러한 저층위 협력으로는 사이버 공격과 관련된 위협정보, 군사정보 등의 공유, 국가차원의 정책이나 예산, 군사독트린에 대한 내용 공유, 실무차원의 핫라인 개설, 의견교환 및 컨설팅 진행, 사이버 안보 및 사이버 규범 관련 워크숍 개최, 사이버 군사 부문 인적교류 등과 같은 신뢰구축조치 등이 포함된다(Lim, 2016)

이렇게 여러 층위의 사이버 협력 방안을 고민하는 것은, 국내 일각에서 제기하는 바와 같이, 한미 사이버 협력을 저층위 협력에서 시작해서 고층위 협력으로 발전시키자는, 이른바 기능주의적 접근과는 그 성격이 다르다. 사실 이러한 기능주의적 접근은 이른바 '아시아 패러독스' 를 해소하기 위한 방안으로 연성안보 분야의 협력에서 시작해서 경성안보 분야의 협력으로 발전시켜 나가자는 '동북아평화협력구상' 의 고민과 맞닿는다. 그렇지만 사이버 안보 분야의 협력은 저층위에서 고층위로 나아가는 일방향 모델을 설정할 성질의 것이 아닐 뿐만 아니라, 만약에 가능하더라도 무작정 정치군사동맹 수준의 고층위 협력모델을 지향할 문제도 아니다. 오히려 다층위에서 복합적인 협력의 틀을 만들어내는 것이 더 유용할 수도 있다.

그림 2 동아태 사이버 안보 세력망 속의 한미동맹(가상도)



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 근접 중심성을 강화하는 시도이외에도 연결 중심성과 매개 중심성의 강화를 복합적으로 고려하는 발상이 필요하다. 특히 다음 절에서 살펴보는 바와 같이, 중국과의 사이버 협력의 문제 또는 사이버 안보 분야 이외에서 진행되고 있는 중국 및 기타 주변 국가

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

들과의 협력을 염두에 둘 때, 한미 간의 링크만을 강화하겠다는 발상으로 사이버 협력의 문제를 진행할 것은 아니다. 이러한 맥락에서 보면, 한미 사이버 협력은 〈그림-2〉에서 가상도를 그려본 바와 같이, 동아시아 사이버 안보 세력망의 복합적인 맥락 속에서 그 미래를 설정해야 하는 문제라고 할 수 있다.

2. 북중 변수와 미중 사이 한국의 딜레마

이렇게 복합적 시각을 견지하더라도 한미 사이버 협력의 문제를 풀어나가는 데 있어서 제일 큰 고민거리는 중국이다.[6] 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』, 2015-07-24). 게다가 북한이 사이버 거점으로 활용하는 국가라는 점에서 중국 변수는 사이버 안보 분야에서 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 이끌어 낼만한 사이버 외교력도 부족했다. 그러니 공격의 배후를 북한이라고 '추정'만 할 뿐 증거도 찾지 못하고 더 이상의 후속조치도 취하지 못했다"고 한다(『디지털타임즈』, 2015-05-13).

미국의 입장에서도 북한의 사이버 공격에 대처하는 데 있어 중국과의 협력은 중요한 변수였다. 미국은 소니 해킹 사건 이후 그 배후로 지목한 북한의 사이버 공격을 차단하기 위해 중국 정부에 협조를 요청한 것으로 알려져 있다(*New York Times*, 2014-12-20). 그러나 미중 두 강대국이 사이버 안보협력을 펼치는 것은 쉽지만은 않아 보인다. 정작 양국 간에 사이버 안보 분야에서 갈등이 진행 중이기 때문이다. 2000년대 후반부터 미국 정부와 언론은 중국의 해커들이 중국 정부와 군의 지원받아서 미국 정부와 기업들의 컴퓨터 네트워크를 공격한다는 주장을 펼쳐왔다. 2014년 3월 미 법무부가 미국의 정보인프라에 대한 해킹 혐의로 중국군 장교를 기소한 사건은 양국 간 갈등의 현주소를 극명하게 보여준다. 이에 대해 중국 정부도 미국의 주장이 근거가 없을 뿐만 아니라 미국이 중국 해커의 공격설을 유포하는 이면에는 중국의 성장을 견제하고 사이버 안보를 빌미로 하여 자국 이익의 보호에 나선 미국의 속내가 있다고 받아치고 있다. 이러한 와중에 2013년 6월 터진 이른바 '스노든 사건'은

6) 중국의 사이버 안보 능력과 전략에 대한 포괄적인 연구로는 Lindsay et al, eds.(2015)가 유용하다. 이외에도 정책보고서 차원에서 집필된 것으로, Lieberthal and Singer(2012), Chang(2014) 등도 중국의 사이버 안보 전략에 대한 유용한 내용을 담고 있다.

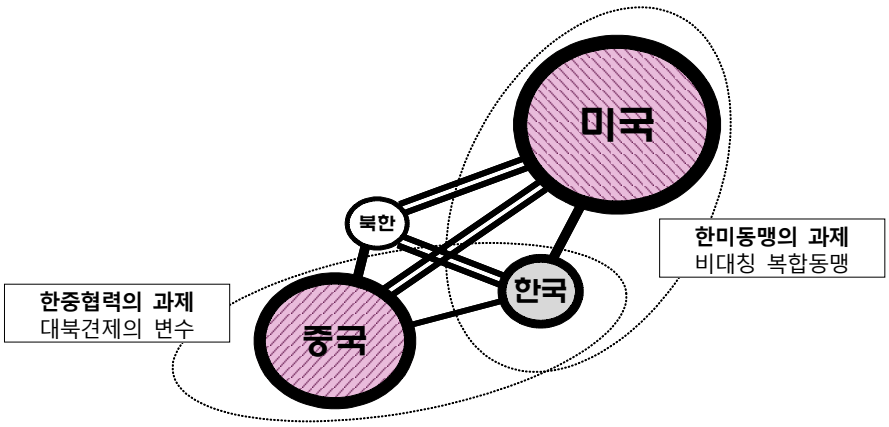
중국이 미국의 주장을 맞받아치는 유리한 환경을 제공하기도 했다.

사실 최근 미국과 중국이 사이버 안보 분야에서 벌이는 갈등은 단순한 컴퓨터 해킹의 문제가 아니라 21세기 패권경쟁을 놓고 벌이는 다층적인 경쟁의 성격을 띤다(김상배, 2015a). 이러한 과정에서 미국이 주로 글로벌 패권의 관점에서 정보인프라와 지적재산의 안정성을 강조한다면, 중국은 국가주권론의 입장에서 인터넷 상에서 유통되는 콘텐츠의 '정치적 안전'을 확보하는 데 주안점을 둔다. 한국의 입장에서 볼 때 미국과 중국 두 강대국이 이렇게 사이버 안보에 대해서 상이한 입장을 취하고 있다는 사실은 한국에게는 풀어가기 어려운 외교적 딜레마를 안겨 줄 가능성이 있다. 미중 양측으로부터 협력을 요청받고 있는 상황에서 한국이 그 틈바구니에서 무언가 선택을 강요받는 상황이 창출될 가능성이 있다는 것이다. 현재 한국은 미중 양국 사이에서 어느 한쪽으로 치우치지 않으면서도, 의미 있는 역할을 담당해야 하는 외교적 과제를 안고 있다.

이상에서 언급한 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 사이버 보안 국장급 협력회의를 개최했는데, 이는 2014년 10월 미래부와 공신부가 체결한 '사이버 보안 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(『연합뉴스』 2015-10-28). 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(『전자신문』 2015-12-17).

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

그림 3 한미동맹과 한중협력 사이의 한국(가상도)



현재 미국과 중국이 사이버 안보 분야에서 갈등하고 경쟁하는 상황에서 한국은, 〈그림-3〉에서 보는 바와 같이, 한미동맹과 한중협력의 사이에서 형성되는 이 분야의 구조적 조건을 파악하고 그 안에서 전략적으로 적절한 위치를 설정해야 하는 과제를 안고 있다. 이는 중견국으로서 한국외교가 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. 그러나 사이버 안보 분야의 상황은 한국이 추구하려는 중개외교에 기회를 제공하는 동시에 위협 요인으로 작동하기도 한다. 다시 말해 이러한 과제가 쉽지 않은 것은 두 강대국 사이에서 공략해야 할 구조적 공백이 역으로 중견국 외교를 제약하는 '구조적 딜레마'가 될 가능성이 있다.

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 만류했던 상황에서 발생한 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.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

IV. 아태협력과 동아협력 사이의 한국

1. 미국의 아태전략과 한일 사이버 협력

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(Lewis, 2015). 이러한 미일동맹의 변화는 미국이 사이버 안보를 포함하여 새로이 강화하고 있는 아태 지역동맹 전략의 연속선상에서 이해해야 한다. 2015년 5월말 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』, 2015-06-04). 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 언급했다(『문화일보』 2015-07-02).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.

이러한 맥락에서 미일관계를 보면, 최근 양국 간에는 사이버 안보 분야의 협력 체제를 강화 시켜가는 이유를 잘 이해할 수 있다. 2013년 설립된 미일 사이버 안보정책 실무그룹이 공개한 성명은 "악의적인 사이버 활동가들의 수준이 점차 정교화하고 있다"고 밝히면서 공동대응의 방향을 제시했다. 그 후 미국의 협력 요구에 대해서 일본은 2014년 사이버방위대를 만들어 화답했다. 2015년 4월엔 미일동맹을 사이버와 우주까지 확대하는 방위협력지침 개정안을 발표하면서 사이버 안보 분야의 공조를 포함시켰다. 미국과 일본은 2015년 4월 양자동맹을 사이버 공간과 우주까지 확대하는 방위협력지침 개정안을 발표하였다. 또한 2015년 5월 공개된 미일 양국의 공동성명에 따르면, 미국은 군사 기지와 사회 기반시설에 대한 사이버 공격에 대처할 수 있도록 일본을 지원하기로 했다. 미국이 이른바 '사이버 우산'을 일본까지 연장해 제공하기로 합의한 것이다. 이밖에도 미일 간에 사이버위협안보그룹의 설치, 사이버 합동훈련 실시, 사이버 훈련 기술협력과 인적교류 등에 이르기까지 다양한 협력과 공조가 진행되고 있다(『뉴스1』, 2015-06-01; 『조선닷컴』, 2015-07-24). 이러한 미국과의 협

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

력을 배후로 삼아서 일본은 다각적 파트너십 강화를 목적으로 영국, 인도, 유럽연합, 아세안 등과 사이버 보안 정책협력회의를 정기적으로 개최하고 있다(Matshbara, 2014).

이렇게 강화되고 있는 미국 주도의 아태 사이버 지역동맹의 틀 중에서 상대적으로 가장 '약한 고리' 는 한일 사이버 협력이다. 다시 말해, 현재 동아시아 주변4망(網)의 구도에서 한일관계는 일종의 '구조적 공백' 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』 2016-04-04). 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 나타난 나토의 실험은 기본적으로는 오프라인 냉전동맹 모델의 온라인으로의 확장으로 이해된다. 따라서 만약에 미국이 이러한 나토 모델을 원형으로 하여 아태지역에서 사이버 협력 체제를 구축하려 시도한다면, 북한과 대치하고 있는 특수한 상황에 처한 한국의 입장에서는 조심스러운 일이 아닐 수 없다. 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.

이러한 변수들을 고려해야 함에도 불구하고, 한국이 사이버 안보 전략을 모색함에 있어서 아태지역에서의 협력은 여전히 중요하다. 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 차원에

서도 한국은 2011년 9월 제3차 APEC 사이버 보안 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(Seoul Defense Dialogue, SDD)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.

2. 한중일 사이버 협력과 동아시아 지역협력

이상에서 살펴본 아태지역 차원의 사이버 협력이외에 동북아 지역 차원에서 한중일이 중심이 되어 가동하고 있는 사이버 협력에도 주목할 필요가 있다(Thomas, 2009). 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 사이버 위협에 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 한중일 3국이 적극적으로 고려해야 할 중요한 변수이다. 한중일 3국 중에서 아세안과의 사이버 협력에 가장 적극적으로 나서는 나라는 일본이다. 이것은 2005년 이후 대외전략에서 동아시아 지역을 주요 협력대상으로 분류하기 시작한 것과 맥락을 같이한다. 아세안을 대표로 하는 동아시아 지역은 일본에 있어 경제적 협력관계가 깊고, 한국, 중국과의 경쟁관계에 있어서도 전략적으로 관계 강화가 필요한 지역으로 분류되고 있다. 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

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

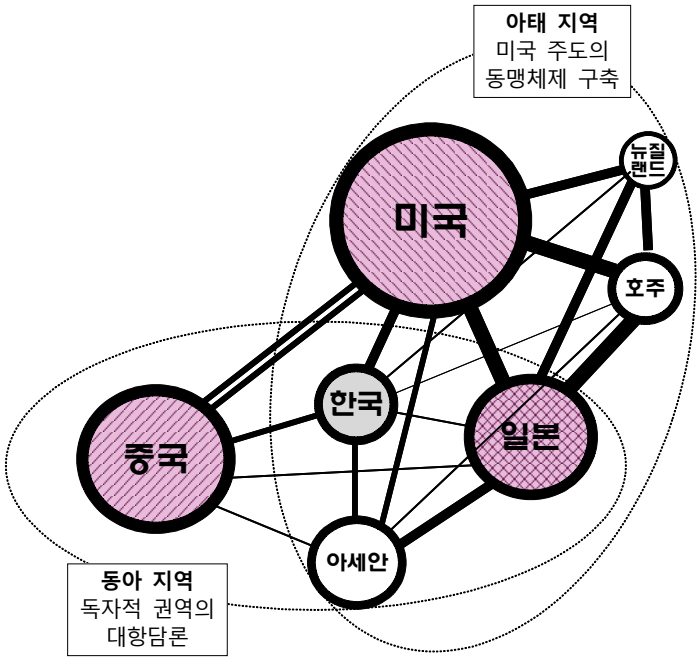
합의문이 발표된 바 있다. 아세안과 일본은 사이버 공격의 위협에 공동으로 대처하기 위해, 공격을 예지하거나 바이러스 감염을 탐지해 경고를 울리는 시스템을 연계 개발한다는 내용을 골자로 한 공동성명도 발표했다.

이와 유사한 맥락에서 아태지역 국가들이 역내 안정을 추구하기 위해 ARF(ASEAN Regional Forum) 차원에서 진행되는 사이버 협력에도 주목할 필요가 있다. 1994년 출범한 다자간 정치 · 안보 협의체인 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 합동전략 개발 협력에 합의했다. 2015년 8월 ARF 외교장관 회담에서는 회원국 간 신뢰구축을 통해 분쟁을 방지하고, 상호 이해를 제고하기 위해 사이버 안보 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.

이상의 논의를 바탕으로 해서 볼 때, 한국의 사이버 외교가 당면한 쟁점과 과제는, 〈그림-4〉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 네트워크와 중국이 형성하는 네트워크의 사이에서 한국의 동아태 전략을 설정하는 망제정치의 과제가 될 것이다. 이러한 딜레마는 최근 미중 간에 쟁점이 되고 있는 북핵 실험과 사드 미사일의 한반도 배치 문제 등으로 나타난 바 있다.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

그림 4 아태 지역동맹과 동아 지역협력 사이의 한국(가상도)



중견국 외교의 이론적 관점에서 볼 때 이러한 지역협력 구도에서 발생하는 구조적 딜레마 상황을 풀어가는 해법은 뜻을 같이하는 동지국가들(like-minded countries)과 공동보조를 취하는 연대외교의 전략에 있다. 한미일 관계와 한중일 관계를 배후로, 또는 아태 지역동맹과 동아 지역협력을 배후로 미국과 중국이 대립하는 경우, 한국은 그 사이에서 외로이 입장을 설정하려 시도하기보다는 비슷한 처지에 있는 국가들과 공동보조를 맞추는 지혜가 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 경우에 한국이 적극적으로 고려해야 하는 변수는 아세안이 아닐 수 없다. 또한 최근 한국(K)이 강조하고 있는 중견국 정부간 협의체인 믹타(MIKTA)의 나머지 네 국가들, 즉 멕시코(M), 인도네시아(I), 터키(T), 호주(A) 등과의 연대도 동아시아를 넘어서는 글로벌 차원에서 고려할 중견국 연대외교의 변수이다.

V. 서방 진영과 비서방 진영 사이의 한국

1. 미러경쟁과 중러협약 사이의 한국

주변4망(網)의 마지막 변수인 러시아는 상대적으로 동아태 지역에서는 존재감이 그리 크지

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

않다. 그러나 글로벌 차원에서 벌어지는 미러경쟁이 동아태 지역에 미칠 영향을 과소평가할 수는 없다. 최근 가시화된 미중 갈등에 비해서 상대적으로 드러나지는 않지만, 미러 간에도 사이버 갈등이 지속적으로 발생하고 있기 때문이다. 특히 서방 전문가들은 다른 어느 나라보다도 러시아를 주요 위협으로 보고 있다. 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*, 2015-06-26).

물론 미러 간에는 표면적으로는 사이버 협력의 몸짓도 진행 중이다. 예를 들어 미국과 러시아는 2013년에 사이버 긴장 완화를 한 걸음 발전시키고 미래의 컴퓨터 관련 위기를 해소하기 위해, 냉전 시대의 핵 공포에 대해 사용되었던 것과 유사한 사이버 핫라인을 설치하는 협정을 체결했다. 이는 냉전 시대의 핵 공포에 대해 사용되었던 것과 유사한 성격이었다. 그러나 스노든 사태에도 불구하고 유지되는 듯 보이던, 미러 사이버 우호관계는 2014년 들어 러시아가 우크라이나를 침공하면서 분위기가 반전되었다(Geers, 2015). 러시아의 우크라이나 침공 이후 양국 간에 체결된 '사이버 공간의 신뢰조치에 관한 협정' 과 사이버 공간에서의 신뢰에 관한 양자 간 대통령자문위원회는 폐지된 것이다(*Russia Focus*, 2015-06-26)

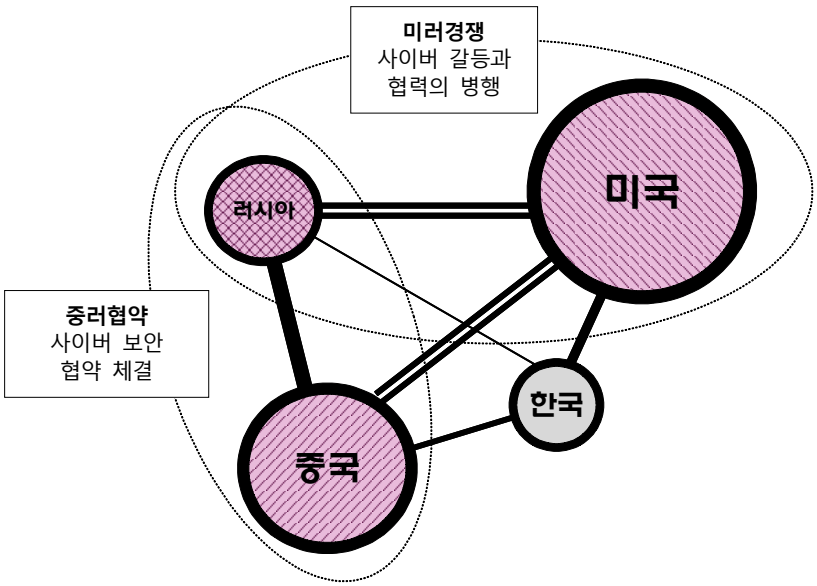
미국과 러시아 간에 형성되는 냉기류와는 달리 중국과 러시아는 사이버 협력을 강화하여 2015년 5월 중러 사이버 보안 협약을 체결하는 성과를 거두었다. 이는 중국과 러시아가 사이버 공간에서 서로에 대한 감시를 지양하고 각국의 법집행기관을 통해 기술 전수 및 정보 공유를 하겠다는 내용을 담고 있다. 이 협약은 두 국가가 서로 중대한 정보 인프라만은 건드리지 말자고 암묵적으로 약속한 성격을 갖는다. 이러한 중러협약에 대한 미국의 반응이 다소 냉소적으로 표출된 것은 당연하다. 미국이 인식하기에 중국과 러시아는 글로벌 인터넷 거버넌스 분야에서 민간, 시민사회, 정부가 함께 국경과 같은 경계선 없이 개방하자는 서방측의 주장에 반하여 주권은 여기서도 유효하다는 주장을 강조하는 것으로 이해되었다. 더 나아가 "중국은 그냥 모든 일에 미국과 반대의 입장에 서고 싶어서 러시아와 함께 한 것으로 보인다" 는 해석까지도 나왔다(*Russia Focus*, 2015-06-26).

이러한 중러협약은 좀 더 넓은 의미에서 러시아가 벌이는 국제협력이라는 맥락에서 이해할 필요가 있다. 러시아는 지역협력과 국제기구 차원에서 사이버 안보 관련 국제규범을 구축해 나갈 것을 천명하였다. 그 중에서도 상하이협력기구(SCO)에서 벌어지는 협력에 주목할 필요가 있다. 2001년 6월 출범한 상하이협력기구에서는 인터넷과 사이버 안보 및 인터넷 테러 같은 문제들을 논의하면서 인터넷 거버넌스에서 정부의 역할을 증대시키려는 노력을 모으고 있다. 사이버 안보와 관련하여 상하이협력기구는 2011년 '정보안보 영역에서 협력에 관한

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

합의안' 을 도출하며 역내 국가들 간의 협력을 시작하였다. 이러한 협력에는 사이버 무기개발 및 사용 규제, 정보전쟁에 대한 대비 등의 내용이 포함되었다. 이외에도 러시아는 브릭스(BRICS) 국가들과의 국제적인 사이버 안보의 증진을 위한 공동의 노력을 경주하기 위한 협의를 진행하여 왔으며, 사이버 안보와 인터넷 관리에서의 국가주권을 강화하려는 협력이 이루어지고 있다. 이밖에도 러시아는 지역적 수준에서 유럽안보협력기구(OSCE)나 아시아안보포럼(ARF)의 사이버 안보 관련 협의에도 적극적으로 참여하고 있다.

그림 5 미러경쟁과 중러협약 사이의 한국(가상도)



〈그림-5〉에서 보는 바와 같이, 이상에서 살펴본 글로벌 및 동아시아의 세력망 구도 속에서, 즉 미러경쟁과 중러협약의 사이에서 한국은 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

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

할 수 있다.

이러한 와중에도 한국과 러시아 간에는 사이버 협력이 진행되고 있음을 잊지 말아야 할 것이다. 2013년 3월 서울에서 외교부 국제안보대사를 수석대표로 하는 제1차 한러 정보보안 협의회가 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』, 2016-07-08).

2. 다중이해당사자주의와 정부간주의 사이의 한국

동아태 지역에서 러시아가 미미한 변수인 것과는 달리, 글로벌 차원에서 진행되는 국제규범 형성과정에서 러시아는 비서방 진영의 리더 역할을 담당하고 있다. 특히 미국과 유럽(특히 나토)에 대해서 각을 세우면서 유럽지역과 유엔 차원의 국제규범 형성의 한 축을 맡고 있다. 이러한 맥락에서 볼 때 다양한 통로를 통해서 복합적으로 진행되고 있는 사이버 안보 분야(좀 더 넓은 의미에서 인터넷 분야)의 글로벌 거버넌스의 모색 과정에서 형성되는 세력망 구조를 면밀히 살펴보는 것이 필요하다. 사실 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(Hurwitz, 2014). 이와 관련하여 다음과 같은 세 가지 층위에 주목할 필요가 있다.

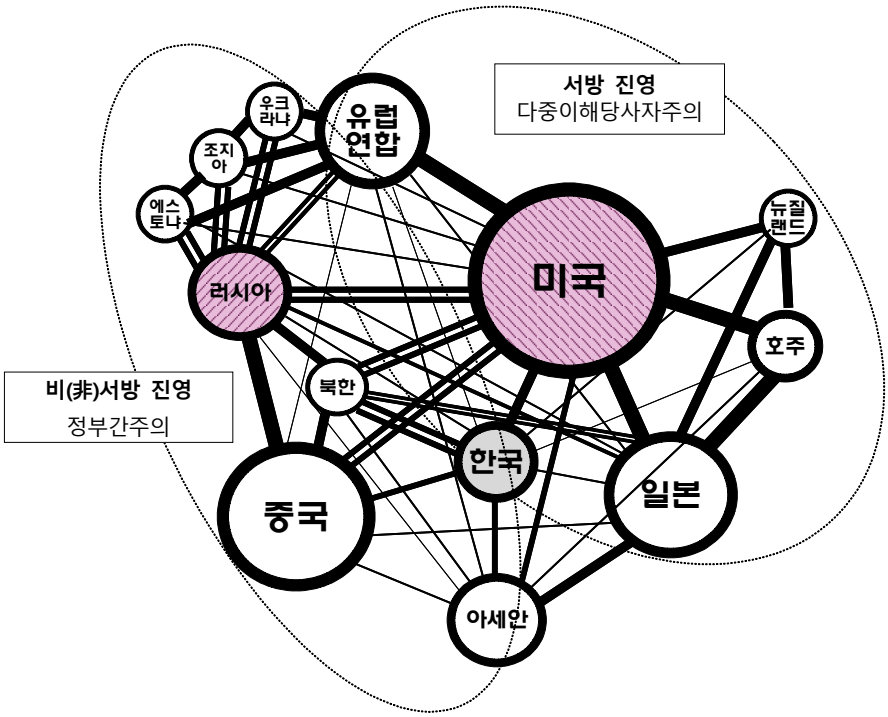
첫째, 글로벌 인터넷 거버넌스의 차원에서 진행되는 사이버 안보 관련 국제규범에 대한 논의이다. 현재 글로벌 인터넷 거버넌스의 골격은 국제기구의 장에서 정부 대표들의 합의에 의해서 이루어진 것이 아니라 주로 미국과 유럽을 배경으로 하는 시민사회, 인터넷 전문가들과 민간사업자, 학계, 국제기구 전문가들이 만들었다(DeNardis, 2013). 이러한 면모를 잘 보여주는 사례가, 초창기부터 인터넷을 관리해온 미국 캘리포니아 소재 민간기관인 ICANN이다. 그런데 이러한 모델은 인터넷 전문가들이나 민간 행위자들이 전면에 나서는 모습으로 보이지만, 실상은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판으로부터 자유롭지 못했다(Mueller, 2002; 2010). 이러한 미국의 패권에 대해 국제기구 차원에서 반론이 제기되었는데, 그 대표적인 사례가 ITU가 주관하여 2000년대 초반 두 차례에 걸쳐서 열린

WSIS(World Summit on the Information Society)와 그 후속 포맷으로 진행되고 있는 IGF(Internet Governance Forum)이다.

둘째, 전통적인 국제법(특히 전쟁법)과 국제기구의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격에 대응하려는 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(Schimit, 2012; Schmitt and Vihul, 2014; 박노형 · 정명현. 2014). 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. 한편 전통 국제기구 차원에서 사이버 안보 문제를 다루려는 시도로서 2013년 6월 유엔 GGE에서 합의해서 도출한 최종 권고안이 있다. 이 권고안은 1998년 러시아가 제안했는데, 미국은 처음부터 러시아의 제안에 대해 동조하지 않았고, 이후로도 소극적인 자세로 사이버 안보 관련 정부 간 협력에 대응해 왔었으나, 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).

끝으로, 사이버 안보의 국제규범을 마련하기 위해서 서방 선진국들이 원용하는 일종의 클럽 모델이다. 전세계 국가를 포괄하는 유엔의 포맷을 빌어 논의하기보다는, 사이버 안보의 직접적인 이해 당사자들이 나서는 방식이라고 할 수 있다. 2011년에 시작된 사이버공간총회가 대표적인 사례인데, 사이버 공간이라는 포괄적 의제를 명시적으로 내건 본격적인 논의의 장이 출현했다는 데 그 의미가 있다. 사실 이렇게 서방 선진국들이 중심이 되어 사이버 공간의 범죄나 위협에 공동으로 대처하려는 사례의 역사는 좀 더 깊다(Christou, 2016). 초창기 사이버 범죄에 대응해서 국가들이 나서서 상호 간의 법제도를 조율하는 정부 간 네트워크를 구성한 초기 사례로 2001년 조인된, 유럽사이버범죄협약(일명 부다페스트 협약)이 있다. 부다페스트협약에는 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.

그림 6 서방 진영와 비(非)서방 진영 사이의 한국(가상도)



이렇게 세 가지 층위에서 복합적으로 전개되고 있는 사이버 안보의 제도화 과정에는 크게 두 진영의 관념과 이익이 대립하고 있음에 주목해야 한다. 우선 다중이해당사자주의(multistakeholderism)와 정부간주의(inter-governmentalism)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 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판을 받아왔다. 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 서방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 비서방 진영을 다른 한편으로 하는 두 진영이 대립하는 지

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

정학적 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-6〉에서 보는 바와 같이, 두 개의 네트워크가 다층적으로 경쟁하는 이른바 망제정치의 양상을 보이고 있다.

이러한 국제규범 형성의 구도에서 한국은 어떤 입장을 취해야 할까? 한국의 중견국 외교의 시각에서 강대국들이 주도하는 국제규범 형성에 단순히 참여하는 전략의 차원을 넘어서 사이버 안보 분야의 특성에 부합하는 규범을 제시하는 적극성을 보일 필요가 있다. 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. 특히 규범외교의 전략은 기성 세계질서의 운영방식에 대한 보완적 비전을 제시함으로써 강대국 위주의 논리에 대한 어느 정도의 반론을 제기하는 효과가 있다. 여기서 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 규범외교의 매우 중요한 내용이 될 수 있다는 것이다.

VI. 맺음말

오늘날 사이버 안보는 국가안보와 외교전략의 어젠다로 명실상부하게 부상했다. 공격이 우위에 서는 이 분야의 특성상 방어와 억지 역량의 구축이나 추진체계 정비와 법제정의 노력만으로 효과적인 대응방안을 마련할 수 없다는 것이 중론이다. 이런 점에서 초국적으로 발생하는 사이버 공격에 적절히 대응하기 위해서는 주변 국가들과의 국제협력과 이러한 과정에서 발생하는 문제들을 풀어가는 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 외교 추진에 대한 인식의 제고와 적극적인 실천은 매우 중요한 일이 아닐 수 없다. 특히 북한의 사이버 공격과 관련하여 관건이 되는 것은 이들 국

가들과의 정보공유 네트워크를 구축하고, 사법공조를 위한 외교적 노력을 펼치거나, 국제규범의 형성과정에 참여하여 호소할 수 있느냐의 여부이다.

사이버 안보 분야에서 작동하는 세력망의 구조와 이에 대응하는 중견국으로서 한국의 전략을 살펴보기 위해서 이 글은 네트워크 이론을 원용하였다. 사이버 안보 분야에서도 여전히 물질적 권력의 관점에서 본 주변4강(强)의 구조가 작동하고 있음은 물론이다. 그러나 사이버 안보 분야의 기술적 특성은, 이러한 전통안보의 지정학적 구조에 대한 이해와 더불어 탈(脫)지정학적 차원에서 형성되는 사이버 네트워크의 관계구조를 복합적으로 고려할 필요성을 제기한다. 네트워크 이론의 시각을 원용하여 복합적으로 파악하는 사이버 안보의 세력망은 주변4망(網)으로 개념화된다. 이러한 구도에서 동아시아 사이버 안보의 세력망 구조는 한국에게 세 가지 차원의 구조적 공백과 여기서 파생되는 중견국 전략의 가능성과 딜레마를 논하게 한다. 이러한 세 가지 차원의 과제는 일국 차원에서 사이버 안보에 대처하는 차원을 넘어서 양자관계와 다자관계, 그리고 글로벌 공간의 규범형성에 참여하는 과정에서 발견된다.

첫째, 한국을 둘러싸고 형성되는 사이버 안보의 구조는 전통적인 우방인 미국과 최근 급부상하고 있는 중국의 사이에서 형성되는 패권경쟁의 구조로 이해된다. 이러한 양자의 패권구조는 동아시아 지역차원에서만 형성되는 것이 아니라 글로벌 차원에서도 21세기 세계질서의 구조변동을 엿보게 한다는 점에서 중요한 주제이다. 이러한 구도에서 오프라인 동맹뿐만 아니라 사이버 안보 분야에서도 한국은 미국과 밀접한 관계를 유지하고 있다. 그러나 최근 벌어지는 문제들은 한국의 입장에서 미국과의 사이버 협력만을 일방적으로 강화시켜나갈 수 없는 애로점을 낳는다. 중국을 경유하여 사이버 공격을 벌이는 북한을 추적하고 견제하는 차원에서 중국의 협조가 필요하기 때문이다. 이러한 맥락에서 미중 사이에서 비대칭적인 관계조율을 통해 입지를 세워가야 하는 중견국으로서 한국의 고민이 있다. 이는 최근 한국 외교가 전반적으로 미국과 중국 사이에서 안고 있는 어려움이기도 하다.

둘째, 한국을 둘러싼 사이버 안보의 세력망은 미중의 양자 구도를 넘어서, 한편으로는 한미일 삼각관계(또는 더 넓게는 아태 지역동맹)의 지원을 바탕으로 하고, 다른 한편으로는 한중일 삼각관계(동북아 또는 아세안까지 포함하여 동아 지역협력)가 대치하는 양상으로도 이해된다. 실제로 미국은 사이버 안보 분야에서 최근 아태 지역 국가들과의 연대전략을 통해서 유럽지역에 버금가는 사이버 지역동맹을 구축하려는 행보를 보이고 있다. 다른 한편으로는 미국의 기술패권에 대한 대항담론의 차원에서 한중일, 그리고 좀 더 넓게는 아세안까지도 포함하는 동아시아 지역협력의 구도가 2000년대 초반부터 펼쳐져 왔다. 이러한 아태지역 구도와 동아지역 구도의 '중간지대'에 놓인 한국은 중개자로서의 기회와 딜레마를 동시에 겪을 가능성이 크다. 이러한 구도에서 한국은 연대외교의 맥락에서 일본이나 아세안 등과의 관계를 새롭게 정립할 필요가 있다.

끝으로, 글로벌 차원에서 한국에 영향을 미치는 세력망은 사이버 안보 분야의 국제규범

형성 과정에서도 작동하고 있다. 현재의 양상은 미국과 서구 국가들을 한편으로 하는 서방 진영과 러시아, 중국 등을 다른 한편으로 하는 비서방 진영의 지정학적 경합으로 나타나고 있다. 또한 이러한 구도는 사이버 공간의 관리에 대한 담론과 이익을 둘러싸고 선진국 클럽과 개도국 그룹이 경합을 벌이는 모습과 겹쳐진다. 이러한 구도 형성에서 주변4망(網) 국가 중에서 러시아는, 동아시아에서는 미미한 변수이지만, 글로벌 차원에서는 중요한 변수임을 명심해야 할 것이다. 특히 미러경쟁과 중러협약의 구도 사이에서, 그리고 서방 진영과 비서방 진영의 입장 차이 사이에서 러시아가 미국을 상대로 제기하고 있는 대항담론이 한국의 사이버 외교전략에 던지는 의미를 진지하게 고려해야 할 것이다.

이상에서 세 층위로 파악한 사이버 안보 분야의 복합구조를 파악하고 이를 활용하는 전략을 마련하는 것은, 한국이 사이버 안보 외교전략를 성공적으로 추진하는 데 있어 필수적인 사안이 아닐 수 없다. 특히 한국이 추구할 외교전략의 관건은 미중 양자 구조와 동아시아 세력망 및 글로벌 거버넌스의 구도 안에서 가능한 한 구조적으로 유리한 위치를 찾아서 이를 활용하는 중견국의 전략을 펼치는 데 있다. 이러한 시각에서 볼 때, 중견국으로서 한국이 사이버 안보 분야의 고유한 구조와 동학을 이해하고 이에 대해서 적절한 대응책을 마련하는 이른바 '지식외교'를 추진할 필요가 있다. 특히 전통안보와는 질적으로 상이한 특성을 지니고 있는 사이버 안보 분야에 대한 연구를 바탕으로 한국 국가이익의 현주소가 어디인지를 면밀히 검토하는 '공부하는 외교'가 시급히 필요하다. 지난날의 개도국 외교 시절에는 공부하지 않고도 강대국들을 따라가도 무방했다면, 오늘날 한국의 중견국 외교는 스스로 공부하지 않으면 아무도 길을 알려주지 않기 때문이다.

요컨대, 진화하는 사이버 안보 분야의 구조를 파악하고 그 안에서 적절한 위치를 설정하는 것은 미래 국가전략의 핵심적 사안이 아닐 수 없다. 무엇보다도 사이버 안보의 세계정치를 기존의 세력균형 시각을 넘어서 세력망의 입체적 시각으로 보는 발상의 전환이 필요하다. 물론 사이버 안보의 이슈가 장차 동아시아의 고질적인 지정학적 이슈와 복합될 가능성도 놓쳐서는 안 된다. 그러나 동시에 냉전 시대에 잉태된 단순동맹 전략의 시각에서 주변4망(網)과의 관계를 풀어가는 오류도 경계해야 한다. 그도 그럴 것이 사이버 안보를 위한 바람직한 대응방안은 어느 일면만을 강조하는 접근이 아니라 기술과 전략, 국가와 사회, 일국적 대응과 외교적 대응, 양자적 해법과 다자적 해법, 지역적 협력과 글로벌 협력 등을 다방면으로 아우르는 복합전략에서 찾아야하기 때문이다. 사이버 안보 문제가 급속히 21세기 국가안보의 문제로 부상하는 속도만큼 우리 모두의 중지(中智)를 모아서 이 분야에서 제기되는 위협에 대한 대응방안을 시급히 궁리하는 국제정치학적 연구가 시급히 필요한 때이다.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

참고문헌

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

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

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

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

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

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

김흥광. 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

유지용·이강규. 2013. "사이버 안보 국제협력과 한국의 정책방향." 『주간국방논단』. 제1471호. 한국국방연구원.

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 대응전략." 『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.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

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

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

Burt, Ronald S. 2005. *Brokerage and Closure: An Introduction to Social Capital.* New York: Oxford University Press.

Chang, Amy. 2014. *Warring State China's Cybersecurity Strategy.* Center for a New American Security.

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)

Junio, Timothy J. 2013. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies.* 36(1). pp.125-133.

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*

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

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.

Lieberthal, Kenneth and Peter W. Singer. 2012. *Cybersecurity and U.S.-China Relations*. China Center at Brookings.

Lim, Jong In. 2016. "Measures to Strengthen ROK-U.S. Cyber Cooperation." The 18th ROK-US Defense Analysis Seminar.

Lin, Nan. 2001. *Social Capital: A Theory of Social Structure and Action*. Cambridge: Cambridge University Press.

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.

Matshbara, Mihoko. 2014. "Countering Cyber-Espionage and Sabotage: The Next Steps for Japanese-UK Cyber-security Co-operation." *The RUSI Journal*, 159(1), pp.86-93.

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

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr

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

Peritz, Aki J. and Michael Sechrist. 2010. *Protecting Cyberspace and the US National Interest.* Belfer Center for Science and International Affairs. Harvard Kennedy School.

Putnam, Robert D. 1993. *Making Democracy Work: Civic Traditions in Modern Italy.* Princeton: Princeton University Press.

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.

Schmitt, Michael N. and Liis Vihul. 2014. "The Nature of International Law Cyber Norms." *Tallinn Paper*. No.5.

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.

Stevens, Tim. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy,* 33(1), pp.148-170.

Thomas, Nicholas. 2009. "Cyber Security in East Asia: Governing Anarchy." *Asian Security*. 5(1), pp.3-23.

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford and New York: Oxford University Press.

Institute of International Studies, Seoul National University
220-506, Seoul National University, 1 Gwanak-ro, Gwanak-gu, Seoul, 08826 South Korea
Tel. +82-2-880-6311 Fax. +82-2-871-4115 E-mail. iis@snuiis.re.kr Web. www.snuiis.re.kr