9장

사이버 안보의 중견국 외교: 가능성과 한계

김상배 (서울대학교 정치외교학부)

1. 서론

최근 한국은 세계정치의 무대에서 새로이 부상하는 중견국으로서 관심을 끌고 있다. 지난 수십 년 동안 증대된 국력이 중견국으로 발돋움하는 물질적 기반이 되었을 뿐만 아니라, 최근 세계정치의 변화는 중견국으로서 외교적 역할을 발휘할 새로운 기회를 제공하였다. 따라서 어렵사리 찾아온 기회를 제대로 살리기 위한 한국의 고민도 깊어만 가고 있다. 강대국들의 틈바구니에서 또는 선진국들과 개도국들 사이에서 한국은 어떠한 역할을 담당해야 하는지, 그리고 한국이 중견국 외교를 펼칠 이슈 영역은 어디인지에 대한 논의가 벌어지고 있다. 세계정치의 구조적 틈새를 비집고 들어가 한국이 중견국 외교를 펼칠 분야로, 원자력 안전, 지구온난화, 보건안보, 사이버 안보 등과 같은 신흥안보 이슈나 국제개발협력이나 글로벌 무역·금융 같은 경제 분야들이 거론된다. 그 중에서도 특히 이 글이 다루고 있는 사이버 안보 이슈는 한국의 중견국 외교를 기대케 하는 대표적인 분야 중의 하나이다.

인터넷의 보급이 매우 미미하여 보안층위를 크게 중시하지 않던 초창기에는 컴퓨터 보안이나 정보보호는 컴퓨터 전문가나 소프트웨어 엔지니어들의 전유물이었다. 그러나 인터넷은 인류가 예상했던 것보다 더 빠른 속도로 더 광범위하게 성장했고 이러한 변화는 사이버 안보와 관련된 기본조건들을 획기적으로 바꾸어 놓았다. 사이버 공간이 비즈니스와 사회적 활동의 장으로서 자리매김을 하는 동안, 악의적 해커나 테러리스트들도 사이버 공간에서의 활동을 강화하였다. 국가 단위를 넘어서 발생하는 이들의 위협에 대처하여 정부기관, 민간기업, 시민단체들은 사이버 공간에서 자신들의 자산과 활동을 보호하기 위한 역량 확보에 경주하고 있다. 외교정책 결정자나 국제정치학자들도 사이버 공간의 안보 문제가 미래의 국가안보 문제로 부상하고 있음을 인정하고 그 실체를 파악하기 위해서 고군분투하고 있다.

사이버 안보는 여러 가지 면에서 국제정치학의 핵심 논제가 되었다. 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 하위 어젠다 중의 하나이다. 최근 사이버 안보 문제는 21세기 세계패권을 놓고 다투고 있는 미국과 중국의 관계에 중요한 현안으로서 거론되기에 이르렀다. 특히 양국은 해킹과 도청 등의 문제를 놓고 갈등의 싹을 점점 키워가고 있다. 사이버 안보는 최근 나타난 신흥이슈임에도 전통적으로 미중관계를 지배해온 전통적인 분야 못지않게 양국의 국가안보를 위협할 수 있는 분야로 간주되고 있다 (Lieberthal and Singer 2012, 1-2).

한국은 이른바 '인터넷 강국'으로 알려져 있다. 첨단 정보통신기기와 세계 최고 수준의 인터넷 인프라를 자랑한다. 그러나 이러한 성과도 북한의 사이버 공격 앞에서는 취약하기 때문에 북한의 사이버 공격을 막기 위한 역량을 키우는 것은 중요한 과제가 아닐 수 없다. 그렇지만 사이버 안보의 게임은 기본적으로 공격이 방어의 우위에 서는 게임이다. 아무리 훌륭

한 방어기술과 전문인력을 갖추고 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 당면한 문제를 풀어나감에 있어서 추구해야 할 국제협력의 방향과 이 분야의 국제규범 형성에 참여하는 과정에서 해결해야 할 과제들에 대해서 살펴보고자 한다.

사이버 안보 분야의 한국외교를 분석하기 위해서 이 글이 원용한 시각은 중견국 외교론이다. 그런데 기존의 중견국 연구는 사이버 안보 분야에서 한국이 취할 외교의 가이드라인을 제공하는 데 불충분하다. 기존 연구는 개별 국가들의 속성이나 능력에 착안해서 세계정치에서 나타나는 중견국의 일반적 역할을 주로 설명한다.[1] 따라서 기존 연구는 세계정치에서 어느 국가가 중견국이라는 점을 확인할 수는 있을지라도, 그 국가가 어떠한 구조적 조건 하에서 어떠한 중견국 외교를 펼치는지에 대해서는 설명하지 못한다. 어느 국가의 행동을 설명함에 있어서 그 국가가 강대국이 아닌 중견국일 경우에는 더욱이 행위자의 속성에 의거해서만 그 국가의 외교적 행동을 설명할 수 없다. 오히려 중견국들의 행동을 설명하는 데 있어는 구조적 조건이라는 변수가 오히려 더 중요한 결정요인일 수도 있다. 이러한 문제의식을 바탕으로 이 글은 네트워크 이론의 시각을 국제정치학에 원용하여,[2] 21세기 한국의 중견국 외교를 모색하기 위해서는 국제체제에서 한국

1) 이러한 행위자의 속성론 또는 행태론에 입각해서 중견국 외교에 대한 이론적 논의를 펼친 연구들로는, Gordon (1966), McLin (1967), Holbraad (1971), Pratt ed. (1990), Cooper, Higgot and Nossal (1993), Cooper ed. (1997), Otte (2000), Gilley and O'Neil eds. (2014) 등을 참조하기 바란다.

2) 네트워크 이론을 국제정치의 이론과 현실에 적용한 사례로는 Hafner-Burton, Kahler and Montgomery (2009), Kahler, ed. (2009), Maoz (2010), Nexon (2009), Goddard (2009) 등을 참조하라. 주로 소셜 네트워크 이론을 원용한 미국 학계의 시각과는 달리 이 글의 시각은 소셜 네트워크 이론이외에도 네트워크 조직 이론, 행위자-네트워크 이론 등을 복합적으

이 차지하고 있는 '구조적 위치'를 파악하는 데부터 논의를 시작해야 한다고 주장한다.[3)]

이러한 구조적 위치론의 시각에서 보면, 중견국의 행위는 어느 나라가 다른 나라와 관계를 맺는 네트워크의 구조적 조건의 영향을 받는다. 다시 말해, 구조가 어떻게 형성되느냐에 따라서 또는 이미 형성된 구조를 어떻게 파악하고 활용하느냐에 따라서, 중견국의 외교적 역할은 일정한 정도의 효과를 볼 수도 있다 (Goddard 2009, 253). 여기서 말하는 구조란 신현실주의 국제정치이론이 말하는 세력분포로서의 '구조'가 아니다 (Waltz 1979). 오히려 여기서 구조는 관련 행위자들의 관계적 구도(relational configuration)이거나 이들 간의 상호작용의 패턴이다 (Tilly 1998; Nexon 2009). 이러한 구조적 위치론의 시각은 네트워크에서 특정한 위치를 차지하고 있는 중견국의 역할을 설명하는 데 유용하다. 중견국 외교의 자율공간을 확보할 수 있게 하는 것은 행위자의 속성이나 이익이 아니라 그 행위자가 차지하고 있는 위치이기 때문이다. 이러한 맥락에서 볼 때, 한국의 중견국 외교도 현재 사이버 안보 분야에서 작동하고 있는 구조적 조건의 내용을 정확하게 파악하고 위치를 잡는 것은 필수적이다.

한국이 추구할 사이버 안보의 중견국 외교와 관련하여 관건이 되는 것은 세 가지 차원에서 형성되는 복합구조이다. 첫째, 사이버 공간의 기술적 구조인데, 이렇게 형성되는 복합 네트워크는 공격에 비해서 방어가 쉽지 않은 구조적 조건을 창출한다. 이러한 기술적 대응의 어려움 때문에 주변 국가들을 활용하는 간접견제나 국제사회에의 호소 등과 같은 중견국 외교의 필요성이 발생한다. 둘째, 사이버 안보 분야의 글로벌 거버넌스 구조인데,

---

로 원용하였다 (김상배 2014).

3) 네트워크의 시각을 취하는 국제정치학의 논의 중에서도 특히 '구조적 위치'를 강조하는 연구로는 Hafner-Burton and Montgomery (2006), Goddard (2009), Nexon and Wright (2007), Nexon (2009) 등을 참조하기 바란다. 국내 국제정치학계에서 구조적 위치론의 문제 제기를 한 중견국 외교 연구로는 김상배 (2011a; 2011b), 김상배 외 (2013), 김상배 (2014), Kim (2014), 김상배 편 (2014; 2015) 등이 있다.

이는 선진국과 개도국이 두 개의 진영으로 나뉘어 경합을 벌이는 양상으로 나타나기 때문에 그 틈바구니에서 입지를 세우기 위해서는 비슷한 처지의 국가들과 연대하는 중견국 외교의 필요성이 발생한다. 끝으로, 21세기의 두 강대국인 미국과 중국의 경쟁이 창출하는 지정학적 구조인데, 이는 이익과 제도 및 관념의 다층적 패권경쟁으로 나타나기 때문에 강대국 중심의 국제규범의 등장을 비판적으로 보완하는 중견국 외교의 필요성이 발생한다. 이러한 사이버 안보 분야의 구조적 조건을 파악하고 이를 활용하는 전략을 세우는 것은, 한국이 중견국 외교를 성공적으로 추진하는 데 있어 필수적인 사안이 아닐 수 없다.

그렇다면 한국의 중견국 외교는 이러한 구조적 조건을 어떻게 활용해야 할까? 이와 관련하여 이 글은 네트워크상의 전략적 요충지를 장악하고 주변의 노드들을 연결해 주는 '중개'의 역할에 특별히 주목한다. 소셜 네트워크 이론가인 로널드 버트(Ronald Burt)에 의하면, 네트워크 게임에서는 중개의 위치를 차지한 자, 즉 중개자들이 그렇지 못한 자들에 대해서 권력을 행사한다고 한다. 특히 '구조적 공백(structural hole)'으로 불리는 네트워크상의 빈틈을 남보다 먼저 찾아서 메움으로써, 중개자는 네트워크 구조에서 중심적 위치를 장악하게 되고 거기에서 비롯되는 독특한 권력을 행사하게 된다는 것이다 (Burt 1992). 이러한 권력은 중개의 이점이 전략적 위치를 점하는 데서 발생한다는 의미에서 '위치권력(positional power)' 또는 행위자의 속성이 아닌 네트워크 자체에서 비롯되는 권력이라는 의미에서 '네트워크 권력(network power)'이라고 개념화되어 왔다.[4] 이 글은 이러한 권력을 추구하는 중견국 외교의 구체적 내용을 중개외교, 연대외교,

4) 이 글에서 중견국 외교에 대한 논의를 펼침에 있어서 네트워크의 특정한 구조적 위치를 장악한 자가 발휘하는 권력에 대한 개념을 이해하는 것은 매우 중요하다. 이러한 권력은 흔히 '위치권력' 또는 '네트워크 권력'으로 개념화되는데, 위치권력에 대해서는 Gould and Fernandez (1989), 장덕진 (2009), 그리고 네트워크 권력에 대해서는 Grewal (2008), Castells (2009), Hafner-Burton, Kahler and Montgomery (2006), 하영선·김상배 편 (2010); 김상배 (2014) 등을 참조하기 바란다.

규범외교 등의 세 가지 측면에서 분석할 것이다.

이 글은 크게 네 부분으로 구성되었다. 제2절은 사이버 안보 분야에서 발견되는 구조의 성격을 사이버 공간의 복합 네트워크 구조, 사이버 안보 분야의 글로벌 거버넌스 구조, 강대국들의 패권경쟁 과정에서 출현하는 지정학 구조 등의 세 가지 차원에서 살펴보았다. 제3절은 사이버 공간에서 벌어지는 국가 간 갈등, 특히 북한의 대남 사이버 공격이나 미중의 사이버 갈등이라는 맥락에서 외교적 협력의 필요성을 지적하고, 한국이 펼칠 수 있는 중견국 중개외교의 과제를 짚어보았다. 제4절은 사이버 안보 분야의 국제규범 형성과 글로벌 거버넌스의 모색 과정에서 나타나는 관련 당사자들의 이익충돌 구조 속에서 한국이 추구할 중견국 연대외교의 가능성과 한계를 살펴보았다. 제5절은 현재 미국과 중국이 벌이고 있는 사이버 안보경쟁의 이면에 깔린 강대국 담론의 위험성을 지적하고 한국이 대안으로 제시할 수 있는 중견국 규범외교의 내용을 살펴보았다. 끝으로, 결론에서는 이 글의 주장을 종합·요약하였다.

2. 사이버 안보 분야의 구조적 조건

1) 사이버 안보의 복합 네트워크 구조

사이버 공간은 이제 엄연히 우리 삶의 공간이 되었다. 사이버 공간의 기반이 되는, 컴퓨터들의 네트워크는 글로벌 차원에서 설계되고 발전해왔으며, 그러한 과정에서 전통적인 국민국가의 경계를 넘나들며 초국적으로 작동하고 있다. 단순히 영토의 경계만 넘는 것이 아니라 영토귀속성으로부터 어느 정도 자유롭기까지 하다. 사이버 공간의 확장속도가 예상을 뛰어넘고 그 확장범위가 지구 곳곳에 미치는 것만큼, 이에 비례해서 사이버 공간의 범죄와 테러의 위협도 매우 빠른 속도로 늘어나고 있다. 따라서 자신의 컴퓨터와 네트워크에 대해서 적절한 보안조치를 취해 방어하지 않을 경우, 귀중한 자

산과 시설의 피해를 입을 수 있다. 그러나 사이버 안보의 이슈는 전통안보 이슈와는 달리 독특한 기술적 특성을 지니고 있어 방어하는 측에 큰 어려움을 안겨 주고 있다. 특히 네트워크 시스템의 복잡계적 특성은 사이버 위협의 잠재적 위력을 더욱 강화한다. 따라서 사이버 공간의 구조와 동학, 그리고 사이버 안보 게임에 관여하는 행위자들의 성격을 이해하는 것은 이 분야의 중견국 외교를 추진하기 전에 꼭 알아야 할 작업임에 분명하다.

첫째, 사이버 테러와 공격은 복잡계의 특징을 갖는 네트워크 환경에서 발생한다. 사이버 공간은 물리적 인프라와 버추얼 자산들의 복합체이다. 인터넷은 다양한 하드웨어, 소프트웨어, 콘텐츠 등을 바탕으로 한다. 행위자들은 다양하고 때로는 버추얼하고 익명적이다. 사이버 테러와 공격이 발생하더라도 사이버 공간의 이러한 구조와 작동방식의 성격상 누가 주범인지를 밝히기 어렵다. 따라서 '피해자는 있는데 가해자가 없다'는 말을 방불케 하는 현상이 벌어지기도 한다. 경우에 따라서는 네트워크 그 자체가 범인이기도 하다. 게다가 시스템의 사고가 발생해도 이것이 외부로부터의 의도적인 공격 때문인지 아니면 시스템의 오작동으로 인한 사고인지를 밝히는 것도 쉽지 않다. 이란의 나탄즈 원자로에 침입했던 스턱스넷 바이러스의 경우, 2010년 6월까지는 발견되지 않다가 이란 측이 아닌 벨라루스의 보안업체에 의해서 그 감염여부가 밝혀지기도 했다. 이러한 양상들은 모두 복잡계의 특징을 갖는 사이버 공간의 비선형적(non-leaner) 성격에서 기인한다.

둘째, 이러한 사이버 공간의 복잡성은 코펜하겐 학파로 알려진 국제안보 연구자들이 제시한 안보화(securitization) 이론이 적용될 여지를 낳는다 (Buzan et al 1998; Wæver et al. 1993; Wæver 1995; Hansen and Nissenbaum 2009). 안보화 이론에 의하면, 안보는 객관적으로 실재하는 어떤 조건이라기보다는 현존하는 위협이 무엇인가에 대한 사회적 합의를 간주관적으로 구성하는 정치적 담론이다. 다시 말해, 안보는 객관적으로 존재하기보다는 안보 행위자에 의해서 현존하는 위협의 대상, 즉 안전이 보장되어야 할 안보의 대상이 무엇인지를 정치적으로 쟁점화하는 과정

에서 구성된다. 이러한 시각에서 보면 사이버 안보는 전형적인 안보화의 사례이다. 사실 사이버 안보라는 현상은 아직까지도 그 위협의 실체와 효과가 명시적으로 입증되지 않았다. 사이버 안보의 문제는 실제로 큰 재앙의 형태로 발생한 실재(real)하는 위협이거나 또는 검증 가능한 형태의 사건이라기보다는 아직까지는 전문가들이나 정치가들이 구성한 현실 속에서 버추얼(virtual)하게 존재하는 위협이기 때문이다 (Rid 2013).

셋째, 사실 사이버 테러나 공격과 관련된 문제의 많은 부분들이 인터넷이라는 독특한 시스템 아키텍처를 배경으로 해서 발생한다. 아무리 잘 설계된 정보시스템이라도 기술적으로 복잡하기 때문에 버그를 완전히 없앨 수는 없다. 이는 외부의 침투와 변경으로부터 시스템을 취약하게 만드는, 일종의 기술적 복잡성의 부산물이다. 이러한 빈틈, 즉 '착취혈(exploit)'은 해커들이 외부에서 침투하여 시스템의 변경이나 훼손을 시도하는 목표가 되기 때문이다 (Galloway and Thacker 2007). 컴퓨터 바이러스와 악성코드도 바로 이러한 빈틈을 착취한다. 이러한 빈틈이 완전히 메워지지 않는 한, 사이버 안보의 게임은 공격자가 방어자에 비해서 유리한 위치에 있는 게임일 수밖에 없다. 게다가 컴퓨터 시스템에 대한 사이버 테러와 공격이 미치는 피해는 기술 시스템 내에만 국한되는 것이 아니라, 사회시스템 전체에도 미칠 수 있다는 점에서 그 위력이 과장되기도 한다.

넷째, 컴퓨터 바이러스, 악성코드, 경우에 따라서는 네트워크 그 자체가 사이버 테러와 공격에 독특한 성격을 부여하는 일종의 비인간 행위자(non-human actor)로서 작동한다. 시스템의 빈틈을 공격하고 시스템의 기능을 저하시키는 컴퓨터 바이러스와 악성코드에는 다양한 것들이 있다. 스턱스넷, 플레임, 샤문 등이 그것들이다. 전쟁에서 사용되는 무기가 재래식 무기냐 핵무기냐에 따라서 전략전술이 달라지듯이, 사이버 공격에서도 컴퓨터 바이러스와 악성코드의 존재는 사이버 안보의 게임 자체에 큰 영향을 미치는 독립변수이다. 디도스(DDoS: Distributed Denial of Service) 공격은 비인간 행위자의 능력을 보여주는 대표적인 사례이다. 디도스 공격

에서 많은 호스트 서버들이 목표시스템에 과부하가 걸리게 하는 과정에서 좀비 컴퓨터들은 봇넷의 일부가 되어 일종의 비인간 행위자로서 활동한다. 최근 APT(advanced persistent threats) 공격과 같이, 좀 더 정교한 방법들이 급속히 늘어나고 있다.

다섯째, 사이버 테러와 공격의 문제는 단순히 컴퓨터나 인터넷의 물리적 속성과 관련된 기술적인 문제로만 보기는 어렵다. 사이버 테러와 공격은 다양한 비국가 행위자들이 복합 네트워크 환경을 배경으로 하여 참여하는 '비대칭 전쟁(asymmetric war)'의 대표적 사례이다. 비대칭 전쟁이란 힘과 규모의 면에서 비대칭적인 행위자들이 비대칭적인 수단을 동원하여 서로 다른 비대칭적 목적을 수행하기 위해서 이루어지는 전쟁을 의미한다. 기본적으로 사이버 테러와 공격은 국가 행위자들이 아니라 위계조직의 모습을 따르지 않고 체계적으로 조직되지 않은 네트워크 형태의 다양한 비국가 행위자들이 벌이는 게임이다. 최근 인터넷의 확산으로 인해서 네트워킹에 드는 비용이 급속히 하락함에 따라 이러한 비국가 행위자들이 역사의 전면에 그 모습을 드러내면서 예전에는 상상할 수도 없었던 독특한 종류의 '힘'을 발휘하고 있다. 잘 알려진 비국가 행위자는 '어노니머스'나 '정의의 검'과 같은 해커 집단이 있다.

끝으로, 사이버 안보는 비국가 행위자들의 관심사만은 아니다. 2000년대 말엽 이후로 종전에는 비국가 행위자들의 배후에서 조연 배우의 역할을 담당하던 국가 행위자들이 사건의 전면에 나서고 있다. 국가안보에 대한 사이버 공격의 잠재적 충격에 대한 관심이 늘어나면서 많은 나라들이 사이버 군사력을 확대하기 시작했다. 2007년의 에스토니아에 대한 사이버 공격이나 2008년 그루지야에 대한 디도스 공격의 사례처럼, 실제로 물리적 전쟁의 개시를 전후하여 이와 병행하는 방법으로 국가 간의 사이버 공격이 감행될 가능성은 매우 크다 (Evron 2008; T.L. Thomas 2009; Hansen and Nissenbaum 2009). 2010년 미국과 이스라엘이 감행한 이란에 대한 사이버 공격은, 국가가 직접 나서서 사이버 공격을 주도한 것이 언론을

통해서 알려진 첫 사례이다. 미국-이스라엘과 이란 사이에서 오고간 사이버 공격은 사이버 안보를 국가안보라는 지정학적 지평에 올려놓았다 (*New York Times*, 2012-10-13).

요컨대, 사이버 테러와 공격은 오프라인에서 발생하는 전통 안보 이슈와는 달리 복합 네트워크를 특징으로 하는 사이버 공간의 구조와 동학을 바탕으로 해서 벌어진다. 사이버 안보의 문제는 전통적인 안보의 경계로 간주되었던 국민국가 단위의 영토적 경계의 의미도 점차로 허물어 가고 있다. 안보 게임에 관여하는 행위자의 성격 변화도 급속히 벌어지고 있다. 대부분의 사이버 공격주체는 해커집단이나 테러리스트와 같은 비국가 행위자들이었다. 그러나 최근 정부의 비호를 받는 사이버 부대원들이 암약하고 있다. 이런 점에서 보면 사이버 안보 분야는 안보게임에 임하는 주체로서 국가 행위자와 비국가 행위자 간의 경계가 희미해지고 있는 대표적인 사례이다. 그야말로 사이버 안보의 세계정치는 다양한 행위자들이 온라인과 오프라인을 오고가며 복합적인 경합의 양상을 보이는 이른바 '비대칭 망제정치(asymmetric inter-network politics)'의 사례이다 (김상배 2014).

2) 사이버 안보의 글로벌 거버넌스 구조

1990년대 후반부터 진행된 역사를 보면, 사이버 안보 분야의 질서형성은 그 자체가 독립적 이슈로서 다루어졌다기보다는, 넓은 의미에서 본 인터넷 거버넌스의 일부로서 취급되어 왔다 (Mueller 2002; 2010; DeNardis 2013). 그러다가 2010년대에 들어서면서 사이버 안보 분야의 국제규범을 모색하기 위한 노력들이 진행되기 시작했다. 그러나 아직까지 사이버 안보 분야에서 사이버 테러와 공격에 대해서 기존의 어떠한 규정을 적용하여 규제할지 등에 대한 국제적 합의기반은 마련되어 있지 않다. 마찬가지로 이 분야에서 미국과 러시아, 중국 등의 이해관계가 충돌하고 있기는 하지만, 아직까지 강대국들 간의 대결이 본격화되었다고 보기도 이르다. 그럼에도 사이버 안보의 글로벌 거버넌스에 대한 입장의 차이는 엄연히 존재하는데, 현재로서는 다

음과 같이 세 가지 차원에서 벌어지는 경합에 주목할 필요가 있다.

우선 주목할 필요가 있는 것은 전통적인 국제법(특히 전쟁법)의 틀을 원용하여 사이버 공간에서 발생하는 해킹과 공격을 이해하려는 움직임이다. 2013년 3월 NATO의 CCDCOE(Cooperative Cyber Defence Centre of Excellence)가 발표한 사이버 전쟁의 교전수칙인, 탈린 매뉴얼(Tallinn Manual)이 일례이다 (Schimit 2012). 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, NATO 회원국의 전문가들이 참여하여 러시아에 대응하는 성격을 띰으로써 러시아나 중국 등을 배제한 미국 중심의 시각이 주로 반영되었다는 비판을 받았다.

최근 전통적인 국제기구인 유엔 차원에서 사이버 안보 문제를 다루려는 시도도 빠르게 진행되고 있다. 그 대표적인 사례가 2013년 6월 유엔 군축 및 국제안보 위원회 산하 정보보안 관련 정부전문가그룹(Group of Governmental Experts, 이하 GGE)이 합의해서 도출한 최종 권고안이다. 이 권고안은 1998년 러시아가 제안했는데, 미국은 처음부터 러시아의 제안에 대해 동조하지 않았고, 이후로도 사이버 안보 관련 국제협력에 소극적인 자세로 대응해 왔었다. 이후 2004년부터는 GGE의 포맷을 빌어 국제안보 차원에서 사이버 안보 문제에 대한 논의가 진행되어 왔는데, 2013년 6월 개최된 회의에서는 전체 참여국들이 사이버 공간에서도 기존의 국제법이 적용될 수 있다는 점에 합의하였다 (장규현·임종인 2014; 장노순 2015).

두 번째는 사이버 안보의 국제규범을 마련하려는 서방 선진국들의 국제협력 움직임이다. 사이버공간총회가 대표적인 사례인데, 사이버 공간의 안보 문제와 기타 관련 의제들을 논의하기 위해서 2011년 영국의 런던에

서 첫 총회가 열렸다. 2012년의 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 이루어졌기 때문에 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)에도 주목할 필요가 있다. 유럽사이버범죄협약은 여러 나라의 사이버 범죄 조목을 일관되게 함으로써 사이버 범죄와 관련하여 공격당한 국가가 범죄자가 있는 국가에 이를 고발하면 해당 국가가 처벌할 수 있도록 한 협약이다. 또한 절차적으로 어떠한 사이버 범죄이든 이와 연루된 개인들로부터 협력을 강제할 수 있는 권한을 부여했다. 그러나 이에 대해서 러시아나 중국 등은 미온적 반응을 보이고 있다 (Brenner 2007).

끝으로 세 번째는 인터넷 거버넌스의 일환으로 보는 사이버 안보의 질서모색 움직임이다. 현재 우리가 사용하는 인터넷의 기본골격은 미국에 활동기반을 두는 민간전문가들이 자율적으로 구축한 이른바 '다중이해당사자주의(multistakeholderism)' 메커니즘을 통해 형성되었다. 이러한 면모를 잘 보여주는 사례가, 초창기부터 인터넷을 관리해온 미국 캘리포니아 소재 민간기관인 ICANN(Internet Corporation for Assigned Names and Numbers)이다. 여러모로 보아 ICANN 모델은 개인, 전문가 그룹, 민간 기업, 시민사회, 국가 행위자 등이 다양하게 참여하는 '다중이해당사자주의'의 실험대였다. 그런데 이러한 모델은 인터넷 전문가들이나 민간 행위자들

이 전면에 나서는 모습을 보이지만, 실상은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판으로부터 자유롭지 못했다 (Mueller 2002).

이러한 미국과 ICANN 주도의 인터넷 거버넌스 모델에 대해서 최근 구사회주의권 국가들과 개도국들이 반론을 제기하고 있다. 이들 국가들은 미국의 인터넷 패권을 견제하기 위해서는 '정부간주의(inter-governmentalism)에 기반을 두고, 현재 모든 국가들이 참여하고 있는 전통적인 국제기구의 틀을 활용해야 한다고 주장한다. 인터넷 발전의 초기에는 선발주자로서 미국의 영향력을 사실상 인정할 수밖에 없었지만 인터넷이 지구적으로 확산되고 다양한 이해관계의 대립이 첨예해지면서 여태까지 용인되었던 관리방식의 정당성을 문제 삼을 수밖에 없다는 것이었다 (Mueller 2010). 특히 이러한 움직임은 인터넷 초창기에 상대적으로 뒤로 물러서 있던 국가 행위자들이 인터넷 거버넌스에서 고유한 활동영역, 예를 들어 글로벌 정보격차나 사이버 안보 등을 찾아가는 과정과 맞물렸다.

이상의 세 가지 차원은 미국과 유럽 국가들이 주도하는 서방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 개도국 진영을 다른 한편으로 하는 두 개의 진영이 대립하는 지정학적 구도와 겹쳐진다. 서방 진영은 사이버 공간에서 표현의 자유, 개방, 신뢰 등의 기본 원칙을 존중하면서 개인, 업계, 시민사회 및 정부기관 등과 같은 다양한 이해당사자들의 의견이 수렴되는 방향으로 세계질서를 모색해야 한다고 주장한다. 이에 대해 러시아와 중국으로 대변되는 진영은 사이버 공간은 국가주권의 공간이며 필요시 정보통제도 가능한 공간이므로 기존의 인터넷 거버넌스를 주도해 온 서방 진영의 주장처럼 민간 중심의 이해당사자주의에 의해서 사이버 공간을 관리할 수는 없다고 주장한다.

3) 사이버 안보 분야 미중 패권경쟁의 구조

최근 사이버 안보는 21세기 세계패권을 놓고 벌이는 미중관계의 현안으로 부상했다 (Shen 2010; Manson 2011; Liberthal and Singer 2012; 김상

배 2012). 2013년 6월 미국과 중국의 두 정상은 양국이 당면한 현안 중의 하나로 사이버 안보를 거론했다. 그 후 사이버 안보는 양국 간에 진행된 전략경제대화의 의제 중의 하나로서 다루어졌으며, 미·중 사이버 보안 실무그룹의 협의가 진행되기도 했다. 이러한 사이버 안보 분야의 경쟁 이면에는 21세기 세계패권을 놓고 벌이는 두 나라의 경쟁이 있다. 이러한 미중 간의 패권경쟁의 양상은 사이버 공격과 해킹을 둘러싼 공방, 인터넷 정책과 제도의 차이, 사이버 안보담론의 차이 등과 같은 세 가지 차원에서 나타난다.

첫째, 미중 간에는 실제로 사이버 공격과 해킹이 벌어지고 있다. 특히 미국의 시각에는 중국 해커들이 중국 정부의 지원을 받아서 미국 정부와 기업들의 컴퓨터 네트워크를 공격하는 것으로 비친다. 이러한 중국의 해킹은 미국 고위 관리의 계정까지도 목표로 하고 있어 미국 국가안보의 근간을 뒤흔드는 위협이라고 인식되고 있다 (US-China Economic and Security Review Commission 2009). 예를 들어 미국 정부가 이른바 '오로라 공격(Aurora attack)'이라고 명명한 2009년의 해킹 사건은 구글뿐만 아니라 아도비나 시스코 등과 같은 미국의 IT기업들을 목표로 하여 중국 해커들이 벌인 일이라는 것이다. 2010년 구글 사건 당시에도 중국의 해커들이 적극적인 역할을 한 것으로 알려져 있다.

이러한 갈등은 2014년 5월 미 법무부가 미국 내 기관들에 대해서 해킹을 감행한 것으로 지목한 중국군 61398부대 장교 5인을 기소하면서 정점에 달한 듯이 보였다. 미국도 중국을 상대로 비밀스러운 정보작전을 벌이기는 마찬가지였다. 2013년 6월 미국 중앙정보국(CIA) 전 직원인 에드워드 스노든(Edward Snowden)이 폭로한 내용에 따르면, 미국 정부는 '프리즘'이라는 프로그램을 통해서 장기간에 걸쳐 개인 이메일을 비롯한 각종 데이터를 감청해 온 것으로 드러났다. 미국과 중국 간에 벌어지는 해킹과 사이버 공격에 대한 정보가 극히 제한적인 현재의 상황을 염두에 두더라도, 두 강대국 간에는 이미 수년째 치열한 '사이버 전쟁'이 벌어지고 있음을 미루어 짐작할 수 있다 (*Guardian,* 2014-5-20).

둘째, 사이버 안보 분야에서 벌어지는 미국과 중국의 경쟁은 사이버 안보와 관련된 인터넷 정책과 규제제도를 놓고 벌어지는 양상을 보이고 있다. 이러한 갈등은 중국 정부와 미국의 민간기업 사이에서 벌어지고 있다. 미국 기업들과의 갈등이 불거지는 와중에 중국 정부는 국가보안에 위해가 될 외래 기술들을 차단하고 인터넷상의 불건전하고 유해한 정보를 검열하는 것은 주권국가의 정부가 취할 수 있는 법적 권리라는 태도를 취했다. 이러한 중국의 인터넷 검열과 정치적 억압에 대한 반발이 있을 수밖에 없었다. 2010년 1월 12일에 이르러 구글은 중국 시장에서 철수할 수도 있다고 발표하였다.

2010년 구글 사건이 주는 의미는, 단순히 미국의 IT기업과 중국 정부의 갈등이라는 차원을 넘어서, 양국의 정치경제 모델의 차이를 보여주었다. 이 사건에서 나타난 구글의 행보가 미국 실리콘밸리에 기원을 두는 기업-정부 관계를 바탕에 깔고 있다면, 이를 견제한 중국 정부의 태도는 중국의 국가정책 모델에 기반을 둔다. 미국 내에서 IT기업들이 상대적으로 정부의 간섭을 받지 않고 사실상 표준을 장악하기 위한 경쟁을 벌인다면, 중국에서는 아무리 잘나가는 기업이라도 정부가 정하는 법률상 표준을 따르지 않을 수 없는 상황이었다. 이러한 점에서 구글 사건은 워싱턴 컨센서스와 베이징 컨센서스로 알려져 있는 미국과 중국의 정치경제 모델의 경쟁 또는 제도표준의 경쟁을 성격을 바탕에 깔고 있었다.

끝으로, 가장 추상적인 차원에서 볼 때 사이버 안보의 미·중 경쟁은 사이버 안보담론의 차이를 반영하는 경쟁이다. 앞서 언급했듯이, 사이버 안보라는 현상은 아직까지도 그 위협의 실체와 효과가 명시적으로 입증되지 않았다. 따라서 이 분야의 담론을 형성하는 과정이 중요할 수밖에 없다. 현재 미국과 중국 간에 벌어지는 논쟁점은 기본적으로 사이버 안보의 대상이 무엇이며 그 문제를 해결하는 주체가 누구인가를 규정하는 담론의 차이에서 비롯된다 (Hansen and Nissenbaum 2009).

사이버 위협의 성격에 대한 인식이라는 점에서 미국은 중국 정부의 비호를 받는 중국 해커들의 공격을 가장 큰 위협으로서 보는 데 비해, 중국은

인터넷과 정보통신기술 분야에서 미국 IT기업들이 장악하고 있는 기술패권을 가장 큰 위협으로 보고 있다. 사이버 안보의 대상과 주체라는 점에서 미국의 담론은 주로 물리적 네트워크 인프라의 안정성 확보와 개인의 프라이버시 및 인터넷 자유의 보호에 주력한다면, 중국의 담론은 인터넷 상에서 유통되는 정보콘텐츠의 정치안전 확보에 주안점을 두어 인터넷에 대한 검열과 규제를 수행할 수 있는 개별 국가 차원의 정책적 권리를 강조하는 국가 주권의 관점에서 접근한다. 사이버 세계질서의 구성에 대한 입장이라는 점에서 미국은 시민사회, 인터넷 전문가들과 민간사업자, 학계, 국제기구 전문가 등과 같은 다양한 이해당사자들이 참여하는 글로벌 패권의 자유주의적 시각을 반영한다면, 중국은, 러시아나 여타 개도국들과 보조를 같이하여, 인터넷 분야에서 '다중이해당사자주의'의 명분을 내건 미국의 패권을 견제하기 위해서는 국가 행위자들이 주도하는 전통적인 국제기구의 틀을 활용해야 한다고 주장한다.

요컨대, 미중 두 강대국은 다층적 수준에서 사이버 안보의 경쟁을 벌이고 있다. 게다가 이 두 강대국이 앞서 말한 바와 같이 인터넷 거버넌스와 관련된 두 가지의 다른 입장을 가진 국가군을 이끌고 있다. 미국과 중국이 향후 가까운 미래에 협력과 갈등 중에 어떠한 관계를 설정하느냐의 문제는, 사이버 안보 분야에서 중견국 외교를 추구하는 한국의 입장에서는 매우 중요한 국가전략적 관심사가 아닐 수 없다. 그렇다면 이상에서 살펴본 바와 같은 구조적 조건을 가지고 있는 사이버 안보 분야에서 한국이 취할 중견국 외교의 구체적인 내용은 무엇인가? 이 글은 중견국 외교의 3대 축이라고 할 수 있는 중개외교, 연대외교, 규범외교의 측면에서 사이버 안보 분야 한국이 취할 수 있는 전략의 가능성과 한계에 대해서 검토하고자 한다.

3. 사이버 안보와 중견국 중개외교

중견국 외교의 핵심 중의 하나는 네트워크상에서 벌어지는 행위자들 간의

관계를 조율하는 중개외교(brokerage diplomacy)에 있다. 네트워크상에서 전략적 위치를 차지하고 구조적 공백을 보완함으로써 중견국은 강대국들 사이에서 또는 선진국들과 개도국들 사이에서 중개의 역할을 발휘할 가능성이 있다. 이러한 중개외교의 어려움은 보통 비대칭적인 관계조율의 필요성이 동시에 발생하기 때문에 나타난다. 이러한 과정이 쉽지 않은 이유는, 새로운 관계의 수립은 대부분의 경우 기존의 관계를 파괴해야 하는 비용을 수반하는 경우가 많기 때문이다. 게다가 맺고 끊기의 중개를 어떻게 하느냐에 따라서 행위자들은 완전히 다른 네트워크의 환경에 놓이게 되고, 더 나아가 네트워크 게임의 기본 어젠다를 바꿈으로써 네트워크 구조 자체를 변경할 실마리가 마련되기도 한다. 이러한 맺고 끊기의 과정은 기회비용을 감수하는 전략적인 선택의 과정이다.

1) 사이버 안보 분야의 국가 간 협력

최근 북한의 대남 사이버 공격이 늘어나고 있다. 그러나 사이버 안보 분야의 특성상 방어와 억지 역량의 구축만으로 대응방안을 충분하게 마련하기는 쉽지 않다. 사이버 안보 분야의 기술 구조적 특성상 방어를 위해서 구축된 방패는 빈틈이 있을 수밖에 없기 때문이다. 사이버 공격은 국제적인 차원에서 관련 국가 행위자들(또는 비국가 행위자들)이 협력하고 공조하여 막아내야 할 문제이기도 하다. 이러한 관점에서 볼 때, 한국도 좀 더 적극적으로 주변국들과의 국제협력을 추구할 필요가 있다. 북한의 사이버 공격과 관련하여 일차적으로 관건이 되는 것은 주변국들과 정보공유체계를 만들고, 기술협력과 사법공조를 위한 외교적 노력을 펼치는 데 있다.

우선 사이버 공격으로 인해 피해를 본 국가나 기관들끼리 서로 정보를 공유하고 정책적으로 공조하는 협력관계의 구축이 필요하다. 특히 사이버 선진국이자 한국의 우방국인 미국과의 정보공유 및 협력체계를 구축하는 문제가 핵심이다. 예를 들어 2014년 11월 북한의 소니 해킹 사건이 발생했을 때 미국이 북한의 소행을 밝혀내는 과정에서 한국의 기술적인 협조가

있었던 것으로 알려져 있다. 미국은 사이버 공격에 동원된 수단이 2013년 3월 20일 발생했던 한국의 금융기관과 언론사에 대한 공격수법과 유사하다는 사실을 밝혀냈는데, 이는 수사단계에서 한미 간에 정보공유가 이루어졌음을 보여주는 것이다 (『보안뉴스』, 2015.07.17). 이러한 협력관계의 구축 및 확대를 염두에 두고 한미 양국 간에 사이버정책협의회나 사이버 안보 공동대응 워킹그룹 또는 민간 사이버 포럼 등을 설치하여 운영하는 방안 등이 검토되고 있다.

사이버 공간에서의 억지력을 보강하는 차원에서 한미 방위협력을 강화하는 방안도 검토되고 있다. 미국은 소니 해킹 사건 때 자국의 사이버 수사력을 총 동원하여 공격의 배후를 북한이라고 규정하고 복합적인 대응방안을 펼친 바 있다 (『보안뉴스』, 2015.07.17). 예를 들어 미국은 북한 통신망을 일시적으로 마비시킨 것으로 알려졌으며, 경제적인 차원에서 금융제재를 가하는 조치를 취할 것을 고려하기도 했다. 미국이 실제로 북한의 사이버 공격에 대한 정보를 수집하고 이에 대한 비례적 대응을 펼칠 수 있는 사이버 공격력과 더 나아가 이를 밑받침하는 물리력과 경제력을 보유하고 있다는 점에서 미국의 이러한 조치들은 실질적인 억지력으로 작동할 가능성이 없지 않다. 이러한 맥락에서 최근 국내에서는 사이버 안보의 문제를 한미 상호방위조약의 틀 내에 포함시킴으로써 미국의 '사이버 우산'을 빌어 북한을 억지하는 방안이 거론되고 있다 (『디지털타임즈』, 2015.05.13).

사실 일본의 경우에는 이미 우방국인 미국과 사이버 안보 분야의 협력체계를 갖추었다. 2015년 5월 30일 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 (『조선닷컴』, 2015.07.24). 그러나 한국이 미일 사이버 안보협력에 준하는 공조를 한미 간에 그대로 원용하기에는 다소 고민스러운 부분이 있다. 무엇보다도 한미 사이버 안보협력을 풀어나가는 데 있어서 제일 큰 고민거리는 중국이다. 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 제기되고 있다 (『조선닷컴』, 2015.07.24.). 2014~2015년 미국의 고고도 미사일 방어체계인 사드(THAAD)의 배치 문제가 한국과 중국 간의 외교적 문제로 불거졌을 때 한국이 처했던 딜레마와 비슷한 상황이 당시 한미 사이버 안보협력과 관련해서도 발생했던 것이다.

군사적 측면이외에 사이버 외교라는 차원에서도 중국은 중요한 변수이다. 중국은 북한이 사이버 거점으로 활용하는 국가이기 때문이다. 현재 한국이 스스로 북한의 사이버 공격을 탐지하고 수사할 기술력이 모자란 상황에서 중국의 협조를 얻어낼 수 있는 외교력은 중요한 변수가 아닐 수 없다. 실제로 정보보안 전문가인 임종인 대통령 안보특보에 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). 이러한 맥락에서 볼 때, 한중 양국 간 사이버 수사공조와 사이버 안보 협력을 성사시켜 중국을 북한으로부터 분리시키는 외교적 노력은 중국을 우회해서 북한을 억지하는 효과를 노릴 수 있다.

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 문제와 관련된 갈등이 진행 중이기 때문이다. 2000년대 후반부터 미

국 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 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, 2015). 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.

2) 사이버 안보 분야 중개외교의 과제

미국과 중국 사이에서 형성되는 사이버 안보 분야의 구조적 조건을 파악하고 그 안에서 전략적으로 중요한 위치를 잡는 것은 한국의 중개외교가 추구할 목표임에 분명하다. 왜냐하면 이러한 사이버 안보 분야의 구조적 공백을 메우는 과정에서 중개를 위한 구조적 기회가 제공될 뿐만 아니라 이

를 통해서 한국은 중견국에게 허용되는 네트워크 권력, 즉 중개권력과 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 이하에서 살펴보는 사이버 안보 분야의 현황은 한국이 추구하려는 중개외교에 기회를 제공하는 동시에 위협 요인으로 작동하기도 한다.

첫째, 한국은 사이버 안보 분야에서 경합하는 미국과 중국의 상이한 기술표준 사이에서 기회와 도전을 동시에 경험할 가능성이 있다. 사실 사이버 안보 분야의 중개 이슈는 미국과 중국 사이에서 기술표준을 선택하는 문제와 관련된다. 한국은 미국의 지배표준과 호환성을 유지해야 하는지, 아니면 지배표준의 문턱을 넘어서 중국이 구축하려는 대안표준의 진영으로 이동해야 하는지가 관건일 수밖에 없다. 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 종류의 선택이 어려울 수밖에 없는 이유는, 이 사안이 외교적 문제와 관련되기 때문이다. 예를 들어, 사이버 안보 분야에서 한국은 한미동맹을 고수할 것이냐 아니면 한중협력을 강화할 것이냐의 선택에 놓일 수도 있다. 이러한 선택은 한편으로는 새로운 관계를 수립하고 다른 한편으로는 기존의 관계를 끊는 '맺고 끊기'의 과정을 의미한다. 이는 보통 기회비용을 감수하고 전략적으로 선택을 하는 '비대칭적 관계조율'의 과정을 수반한다. 이러한 관계의 연결과 단절의 과정은 중개외교의 핵심인데, 간혹 중개의 과정은 네트워크의 구조를 바꾸고 완전히 새로운 네트워크 환경을 만들어 네트워크 게임의 어젠다 자체를 바꾸기도 한다. 그러나 이렇게 한국

이 미국과 중국 사이에서 비대칭적 관계조율을 추구하는 중개외교를 모색함에 있어서 두 나라를 허브로 하는 강대국의 네트워크 사이에서 호환성을 잃지 말아야 함을 명심해야 할 것이다.

둘째, 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. 한국은 일견 호환되지 않는 양국의 인터넷 거버넌스 모델 사이에서 중개의 역할을 할 가능성이 있는가? 여기서 우리는 중개자로서의 중견국의 역할이 완전히 새로운 모델을 창출하는 것보다는, 기본 모델들의 결합 및 복합의 전략과 친화성이 있다는 사실에 주목할 필요가 있다. 이 글은, 이를 실질적으로 새로운 콘텐츠를 생산하는 모델과 대비되는 의미에서, '메타모델'이라고 부르고자 한다. 중개자로서 중견국은, 비록 완전히 새로운 것을 발명할 수는 없더라도, 이미 존재하는 것들을 창의적으로 엮는 '메타능력'을 보유할 수 있다. 중개자의 역할이 매력적이나 아니냐의 문제는 그 나라가 채택한 전략의 콘텐츠 문제가 아니라, 기존의 다양한 콘텐츠들을 어떻게 통합하고 엮어서 주위의 국가들에게 무난하게 수용될 수 있느냐에 달려 있다.

이른바 서울 컨센서스로 대변되는 한국의 정치경제 모델은 이와 관련된 좋은 사례를 제공한다. 정치경제 발전 분야에서 이른바 '한국모델'은 개도국들의 관심사뿐만 아니라 선진국들의 관심사를 모두 품으면서 결합한다는 의미에서 성공적인 '메타모델'의 사례이다. 실제로 한국모델은 최근 '베이징 컨센서스'로 개념화되는, 경제성장을 추구하는 권위주의 모델에서 시작했지만, 괄목할만한 경제발전을 달성한 이후에는 정치적 민주주의의 목표도 달성하는, 이른바 '워싱턴 컨센서스'로 이르는 동태적인 모델이다 (손열 편 2007). 이러한 맥락에서 보면, 사이버 안보에서도 이른바 서울 컨센서스의 모델을 개발하여 대외적으로 알리는 방안은 미국과 중국을 동시에

만족시키고, 더 나아가 선진국과 개도국 진영을 모두 끌어안는 그럴듯한 시나리오가 될 수 있다. 그러나 최근 한국의 상황을 돌아보면, 민간부문이 주도하는 인터넷 경제의 번영을 달성하였음에도 불구하고, 아직도 사이버 공간의 시민사회의 활동에 대해서 국가가 개입하는 나라로 간주된다는 사실은 이러한 시나리오의 실효성을 떨어뜨리는 큰 한계로 작용한다.

끝으로, 사이버 안보 분야 한국의 중견국 중개외교는 글로벌 인터넷 거버넌스와 관련하여 발견되는 두 가지 상이한 입장 사이에서 기회와 도전을 동시에 맞고 있다. 최근 한국은 글로벌 인터넷 거버넌스의 미래를 그리는 두 가지 상이한 비전 사이에서 자국의 위치를 잡는 데 큰 어려움을 겪고 있다. 미국이나 서방 국가들에 의해서 제시되는 비전은 인터넷이 좀 더 개방적이고 자유로워야 한다는 믿음에 기반을 두고 있는 데 비해, 러시아, 중국 또는 개도국들에 의해서 제기되는 또 다른 비전은 사이버 공간에 대한 국가의 주권과 개입의 필요성을 지지한다. 이 문제에 대한 한국의 공식적인 입장은 UN, ITU, OECD, ICANN 등이 주도하는 글로벌 인터넷 거버넌스에 대해 개방적이고 유연한 자세를 취하여 모두 참여하고 모두 지지하는 '망라형 모델'로 알려져 있다. 이러한 입장은 현재 경합하고 있는 두 가지 비전을 복합하는 전략으로 이해될 수 있다. 그러나 이렇게 모든 것을 망라하는 스타일의 혼합전략은 일종의 딜레마 상황에 처했을 때 한국의 구조적 위치잡기에 큰 도움을 주지 못한다.

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 있다. 결과적으로 한국은 89개국의 개도국 그룹에 합류해서 ITR개정에 찬성표를 던졌다(도표 9.1의 검은색). ITR개정에 공식적으로 반대한 국가들은 55개국 이었으며(도표 9.1의 진한 회색), 나머지 국가들은 비회원국들이었다(도표 9.1의 연한 회색). 한국의 투표 직후 한국의 어느 언론보도는 한국

도표 9.1 2012년 WCIT의 ITR 개정 투표에 참가한 나라들의 분포

출처: 『동아일보』 (2012.12.17)

정부가 인터넷을 통제하려는 속내를 드러낸 행태였다고 비난했다(『동아일보』, 2012.12.17). 정부가 개정된 ITR가 국내 규정이나 국가이익에 모순되지 않는다고 발표했지만, 언론은 OECD 회원국이자 2010년에는 G20의 주최국이었던 한국이 민주주의 정치체제와 자유무역체제를 신봉하는 서방 국가들과 다른 입장을 취했다는 사실을 우려했다. 이러한 연속선상에서 볼 때, 향후 사이버 안보의 국제규범과 글로벌 거버넌스 형성 과정에서 한국은 유사한 종류의 딜레마를 다시 겪을 가능성이 크다.

4. 사이버 안보와 중견국 연대외교

중견국 외교의 궁극적인 성패는 얼마나 많은 국가들의 지지를 모을 수 있느냐에 달려 있다. 다시 말해 중견국 외교는 혼자서 발휘할 수 있는 힘보다는 여럿이 모여서 발휘하는 힘, 즉 집합권력(collective power)을 바탕으로 하는 경우가 많다. 전통 국제정치의 경우에는 주로 군사력이나 경제력과 같은 하드 파워 자원에 의거해서 집합권력이 작동했다면, 최근에는 지식, 문화, 이념 등을 통해서 상대방을 끌어들이고 설득하는 소프트 파워를 바탕으로 한 집합권력이 중요해졌다. 이렇게 세를 모으는 중견국 외교는 주

로 비슷한 생각을 가지고 있는 동지국가들(like-minded countries)과 공동보조를 취하는 연대외교(coalition diplomacy)의 형태로 나타난다. 강대국들 사이의 틈새를 공략하는 중개외교를 펼치는 경우에도 혼자 나서기보다는 비슷한 처지의 국가들과 함께 나서는 것이 성공할 가능성이 높다. 이러한 종류의 중견국 외교는 주로 글로벌 거버넌스의 장이나 국제규범의 형성과정에서 나타난다.

1) 사이버 안보 분야의 국제규범 형성

초국적으로 발생하는 사이버 공격에 대한 국제적 대책은 양자협력을 통해서 이루어지기도 하지만 국제사회에의 호소, 국제기구와의 긴밀한 협력, 그리고 새로운 국제규범 형성에의 참여 등을 통해서도 우회적인 효과를 볼 수 있다. 그러나 아직까지 사이버 안보 분야에는 사이버 공격에 대하여 어떠한 규범을 적용하여 제재할지에 대한 합의된 국제규범이나 국제법 등이 마련되지 못하고 있다. 또한 현재로서는 사이버 테러와 공격이 발생하고 그 공격주체를 색출하더라도 국제적으로 호소하거나 공격행위에 대한 처벌이나 제재에 대해 논의할 수 있는 외교의 공간이 마땅히 없다. 예를 들어 천안함 사건이나 연평도 포격 사건이 발생했을 때에는 유엔 안보리에 호소할 통로가 있었으나, 북한의 소행으로 추정되는 사이버 공격이 발생해도 마땅히 호소할 통로(예컨대, 사이버 안보리)는 없는 실정이다. 현재 국제사회에서 다양한 방식으로 모색되고 있는 사이버 안보의 국제규범 형성과정에 적극적으로 참여하는 것 자체가 중요한 대응방안이 될 수 있다.

앞서 언급한 바와 같이 전통적인 국제법의 틀을 사이버 공격에 원용하려는 움직임에 주목할 필요가 있다. 기존 국제법의 틀을 적용하여 북한의 사이버 공격을 불법행위로 규정하고 이에 대해 국제사회가 규제할 수 있는 원칙을 마련하여 이를 북한에 강제할 수 있다면 그 의미는 클 것이다. 이러한 국제법적 접근은 중국을 북한으로부터 분리하는 효과도 얻을 수 있을 것이다. 이와 관련하여 사이버 공격에 대한 '국가책임의 원칙'을 적용하는

문제가 관건이다. 사이버 공격의 명백한 증거가 제시될 경우 지리적으로 사이버 공격의 근원지 혹은 경유지가 된 국가는 사이버 공격에 대해서 적절한 조치를 취하는 원칙을 적용하려는 것이다 (임종인 외, 2013). 그러나 이러한 국제법 원칙의 적용문제는 아직까지는 희망사항일 뿐 실제로 실현될 때까지는 갈 길이 멀다. 그럼에도 앞서 언급한 탈린 매뉴얼은 사이버 교전규칙을 만들려는 시도로서 주목을 받고 있는데, 소니 해킹 사건 이후 미국은 북한에 대한 '비례적 대응'을 모색하는 과정에서 탈린 매뉴얼에서 다루어진 조항들을 원용하려 했던 것으로 알려졌다.

전쟁법의 원칙을 사이버 안보에 적용하려는 탈린 매뉴얼에 대한 국제적 합의가 쉽게 이뤄지지 않는데 비해, 전통적인 국제기구인 유엔에서 사이버 안보 문제를 다루려는 시도는 최근 진척을 보고 있다. 앞서 언급한 GGE에서는 최근 최종 권고안을 합의 도출했다. 이 권고안은 1998년 러시아가 제안한 이후 미국의 소극적 반응으로 미루어져 오다가 2004년부터는 GGE의 포맷을 빌어 국제안보 차원에서 논의가 진행되어 왔다. 기존 회의에서는 인터넷의 국가통제를 강조하는 러시아나 중국과 같은 국가들과 이에 반대하는 미국이 극명히 대립했으나 2013년 6월 개최된 회의에서는 전체 참여국들이 사이버 공간에서도 기존의 국제법이 적용될 수 있다는 점에 합의하고 이러한 규범이 국가의 역할로 어떻게 연결될 수 있는지에 대해서 지속적으로 연구하기로 합의하였다.

한편 OECD 국가들을 중심으로 하는 선진국 정부들 간 협의체의 틀을 기반으로 하여 열린 사이버공간총회에서의 참여도 주목할 필요가 있다. 사이버공간총회는 사이버 공간의 안보 문제와 기타 관련 의제들을 논의하기 위해서 2011년 영국의 런던에서 첫 총회가 열린 이후 부다페스트(2012년 제2차), 서울(2013년 제3차)를 거쳐서 헤이그(2015년 제4차)에서 네 차례에 걸쳐서 총회가 열린 바 있다. 한국의 입장에서 볼 때, 서울이 런던과 부다페스트 등의 유럽 국가들의 수도에 이어 세 번째로 사이버공간총회를 유치하여 성공적으로 개최했다는 사실은 사이버 외교의 의미 있는 성과가 아

닐 수 없다.

이러한 맥락에서 유럽사이버범죄협약(즉 부다페스트 협약)에의 가입도 적극적으로 검토할 필요가 있다. 그러나 부다페스트 협약의 노력은 국가가 중심이 되다보니 민간 행위자들을 네트워크로 끌어들이는 데 있어 한계가 있다는 지적이 있어 왔다. 또한 유럽 중심의 사이버 안보 분야 규범 설정이라는 지역적 한계를 드러냄으로써 보편적인 국제규범으로 발전하지 못하고 있다. 2012년 4월 현재 유럽의 국가들 이외에 미국, 캐나다, 일본 등을 포함한 47개국이 가입되어 있고 33개국이 비준하였는데, 한국은 아직 가입하지 않고 있다. 그런데 최근 국내에서도 부다페스트 협약에의 가입을 주장하는 목소리가 높아지는 가운데, 몇 년 전부터 외교부를 중심으로 법무부, 경찰청 등이 가입 여부를 검토 중이다 (『전자신문』, 2015.08.04).

사이버 안보의 특성을 고려할 때, 이상에서 소개한 국제협력의 움직임에는 다소 조심스럽게 접근해야 하는 부분도 없지 않다. 사이버 공간의 복합 네트워크적 성격이나 사이버 공격에 참여하는 행위자들의 다양한 성격을 고려할 때 사이버 안보의 문제를 국가 행위자들을 중심으로 보고 민간 행위자들의 역할을 미미한 것으로 취급할 우려가 있기 때문이다. 사실 사이버 안보 문제는 최근 수 년 동안 국가 간 분쟁의 이슈로 부상하기 전에는 시민사회, 인터넷 전문가들과 민간사업자, 학계, 국제기구 전문가들이 자율적으로 구축한 메커니즘을 통해서 이루어졌다. 이런 맥락에서 볼 때 다양한 통로를 통해서 진행되고 있는 사이버 안보 분야의 글로벌 거버넌스의 모색 과정을 면밀히 살펴보는 것이 필요하다.

앞서 살펴본 바와 같이, 현재 사이버 안보(좀 더 포괄적으로 말하면 인터넷)의 글로벌 거버넌스에 대한 논의에는 이른바 다중이해당사자주의와 정부간주의로 대별되는 두 가지 입장이 각을 세우고 있다. 그런데 한국의 경우 이들 두 가지 입장 사이에서 아직도 인터넷 거버넌스나 사이버 안보 문제를 어떤 입장에서 다루어야 할지에 대해 명확히 입장을 설정하지 못하고 있다. 이러한 혼란은 앞서 언급한 WCIT의 ITR의 개정 과정에 참여할

당시에 드러났다 (강하연, 2013, 102-105). ITR의 규제조항이 급변하는 기술 환경에 부합하지 않으므로 폐기해야 한다는 선진국들의 입장과 ITR의 개정과 강화를 통해 개별 국가 차원의 규제정책의 기조를 유지하려는 개도국들의 입장 사이에서 한국은 후자의 편에 섰는데, 이러한 선택은 이후 국내 언론의 신랄한 비판의 대상이 된 바 있다.

2) 사이버 안보 연대외교의 가능성

사이버 안보 분야의 국제규범 형성에 참여하는 과정에서 발생하는 딜레마적인 상황을 풀어나가는 중견국 외교 중의 하나가 연대외교이다. 예를 들어 글로벌 거버넌스의 장에서 다중이해당사자주의와 정부간주의가 대립하는 경우, 그 사이에서 외로이 입장을 설정하려하기보다는 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 안보분야에서 서로 상이한 해법을 가진 강대국 그룹들 사이에서 발생할 수도 있는 중개자로서의 딜레마를 완화시키는 데도 도움이 될 것이다.

사이버 안보보다는 좀 더 넓은 의미이기는 하지만, 인터넷 거버넌스 분야에서 동지국가들의 연대외교를 추진하는 것과 관련하여, CIGI(Centre for International Governance Innovation)에서 수행된 한 연구는 매우 흥미로운 시사점을 주는 연구결과를 내놓았다. CIGI연구는 2012년 WCIT ITR개정에 찬반 투표한 국가들을 여러 가지 지표에 의거해서 분석했는데, 이를 토대로 미래의 글로벌 인터넷 거버넌스 논쟁에서 부동(浮動)국가로서 행동할 가능성이 있는 30개의 국가그룹을 분류했다. 또한 이들 30개 국가들을 표 9.1에서 보는 바와 같은 네 개의 그룹으로 분류했다 (Maurer and Morgus 2012).

〈그룹-I〉은 ITR에 반대투표를 한 13개 부동국가들인데, 알바니아, 아르

표 9.1 미래의 잠재적 부동국가 30개국

ITR개정 반대국	ITR개정 찬성국		
I.	II. OECD 회원국	III. FOC 회원국	IV. 잠재적 부동국가
알바니아	멕시코	가나	아르헨티나
아르메니아	한국	튀니지	보츠와나
벨라루스*	터키		브라질
콜롬비아			도미니카공화국
코스타리카			인도네시아
그루지야			자메이카
인도			말레이시아
케냐			나미비아
몰도바			파나마
몽골			싱가포르
페루			남아프리카공화국
필리핀			우루과이
세르비아			

출처: Maurer and Morgus (2014), p.10; 이영음 (2014)에서 재인용.

메니아, 벨라루스, 콜롬비아, 코스타리카, 그루지야, 인도, 케냐, 몰도바, 몽골, 페루, 필리핀, 세르비아 등이 여기에 속한다. 이들 13개 국가들은 어떠한 국가그룹에도 속하지 않지만 WCIT에서 ITR개정에 반대한 그들의 입장은 장래에도 유사한 형태로 반복될 가능성이 있다는 점에서 부동국가로 분류했다고 한다. 게다가 이들 국가들은 향후 글로벌 인터넷 거버넌스의 과정에서 다른 국가들에게 입장을 바꾸라고 설득하고 영향을 미칠 자원을 지니고 있다는 점에서 주목할 필요가 있다는 것이다.

〈그룹-II〉는 OECD 회원국인 멕시코, 한국, 터키 등이 해당되고, 〈그룹-III〉는 FOC(Freedom Online Coalition)[5] 회원국인 가나와 튀니지가 속한다. 이들 다섯 나라는 OECD와 FOC 회원국이라는 사실로부터 영향

5) FOC(Freedom Online Coalition) 회원국은 현재 22개국이다. 이들 연합은 자신들을 전세계적인 차원에서 인터넷 자유(표현, 결사, 집회의 자유와 온라인 프라이버시)를 증진하기 위해서 활동하는 정부 간 연대라고 규정한다 (Maurer and Morgus, 2014: pp.7-8).

을 받을 가능성이 있는 나라들이다. 다시 말해, 이들의 OECD와 FOC에서의 활동은 이들이 ITR개정 투표에서 보인 찬성 투표와 상충하는 면이 없지 않다. 게다가 이들은 앞으로 OCED와 FOC 내의 동료국가들로부터 이들의 멤버십과 활동에 적절한 방향으로 투표에서의 선택을 바꾸도록 압력을 받을 가능성이 있다.

〈그룹-IV〉는 ITR 개정에 찬성한 12개 나라들이 속하는데, 아르헨티나, 보츠와나, 브라질, 도미니카공화국, 인도네시아, 자메이카, 말레이시아, 나미비아, 파나마, 싱가포르, 남아프리카공화국, 우루과이 등이 해당된다. CIGI의 연구는 기타 몇 가지 지표들에 의거하여 이들 국가들을 잠재적 부동국가로 분류했는데, 이들 국가에서 인터넷이 중요하다는 점, 이들 국가들의 다양한 특성이 미래의 투표행태를 바꿀 가능성이 있다는 점 등을 근거로 들고 있다.

30개 부동국가에 대한 CIGI 연구의 분류는 사이버 안보 분야, 좀 더 넓게는 글로벌 인터넷 거버넌스 분야에서 한국이 추구할 중견국 외교의 아이템으로서 동지국가들과의 연대외교의 방향을 가늠케 한다는 점에서 시사하는 바가 크다. 우선, 중견국의 연대외교라는 시각에서 〈그룹-II〉에 속한 ITR 찬성 국가들과 공동보조를 맞추는 것은 실현가능성이 매우 높아 보인다. 흥미롭게도 〈그룹-II〉의 세 나라, 즉 멕시코, 터키, 한국 등은 최근 주목받고 있는 중견국 정부협의체인 믹타(MIKTA)[6] 의 참여국이기도 하다. 믹타의 동지국가 연대외교를 확장하는 차원에서 〈그룹-III〉에 속하는 가나, 튀니지 등과 같은 FOC 국가들은 매우 유력한 파트너가 될 수 있을 것으로 예상된다.

〈그룹-IV〉에 속하는 잠재적인 부동국가들과 연대하는 것은 좀 더 복합적인 접근을 필요로 한다. 이들 12개 국가 중에서 믹타의 멤버인 인도네시아

6) 믹타(MIKTA)는 멕시코, 인도네시아, 한국, 터키, 호주의 머리글자를 따서 이름 붙여진 5개국 외교장관들의 비공식 협의체이다. 2012년 2월 시작된 믹타는 여러 차례 회의를 개최하고 개발협력, 기후변화, 사이버 안보, 보건 안보, 재난관리, 인도적 지원 등과 같은 글로벌 거버넌스 분야의 현안에 대한 협력방안을 논의하고 있다. 2014년 9월부터 한국이 1년 동안 믹타의 간사국을 맡은 바 있다.

는 연대외교를 펼칠 수 있는 첫 번째 후보이다. 또한 IBSA[7] 로 분류되는 두 나라인 브라질과 남아공도 글로벌 인터넷 거버넌스 분야에서 한국과 보조를 같이할 수 있는 파트너이다. 흥미롭게도 이들 나라 중에서 브라질은 현재 미국이 주도하고 있는 ICANN 중심의 글로벌 인터넷 거버넌스 체제를 개혁하는 데 있어서 중견국 리더십을 발휘하고 있다. ITR개정에는 반대한 국가로서 〈그룹-I〉에 속하는 또 다른 IBSA 국가인 인도와도 연대외교를 펼치는 것으로 고려해 볼 수 있을 것이다. 한편 CIGI연구에서 언급한 30개 부동국가군에는 속하지는 않지만, 믹타의 멤버로서 최근 활발히 중견국의 연대외교에 참여하고 있는 호주도 중요한 연대의 대상이 될 수 있을 것이다.

이러한 연대외교를 추진함에 있어서 연대 파트너를 선정하는 것만큼이나 중요한 것은 적절한 연대외교의 이슈를 개발하고 상호 연계하는 문제이다. 사이버 안보의 중견국 연대외교를 추진함에 있어 일차적으로는 글로벌 인터넷 거버넌스의 다양한 이슈들이 이슈연계의 후보가 될 수 있을 것이다. 더 나아가 인터넷 거버넌스의 경계를 넘어서 연대외교의 효과성을 증진시키기 위해서 여타 경제와 안보 이슈들을 사이버 안보의 이슈들과 연계하는 방안도 실현 가능성이 높은 선택지이다. 예를 들어, 공적개발원조(ODA)는 사이버 안보 분야의 중견국 외교와 연계시켜서 의미 있는 효과를 볼 수 있는 분야로 거론되고 있다. 또한 원자력 안전, 환경안보, 보건안보 등과 같은 여타 신흥안보 분야의 이슈들도 중견국 외교의 차원에서 사이버 안보와 결합될 수 있는 아이템들이다.

5. 사이버 안보와 중견국 규범외교

중견국 외교는 세계정치의 판세를 읽고 제도와 규범을 설계하는 외교와도 관련된다. 사실 역사적으로 이렇게 제도와 규범을 설계하는 외교는 강대국

7) IBSA는, 브릭스(BRICS) 중에서 중국과 러시아를 뺀 나머지 세 나라, 즉 인도, 브라질, 남아공 등의 느슨한 정부협의체를 부르는 말이다.

의 몫이었다. 그러나 중견국도 세계질서 전체를 설계할 수는 없더라도 주어진 분야의 하위 설계자 정도의 역할은 할 수 있을 것이다. 예를 들어, 강대국이 만든 세계질서의 규범적 타당성에 문제를 제기하고 좀 더 보편적인 규범의 필요성을 강조하는 이른바 규범외교(normative diplomacy)의 모색은 가능할 수 있을 것이다. 이러한 과정에서 강대국 중심의 제로섬 게임 담론의 구조적 공백을 공략하는 중개외교와 이러한 행보에 힘을 싣기 위한 연대외교의 전략이 복합적으로 동원될 수 있다. 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.

1) 사이버 안보 분야의 강대국 담론

현재 강대국들이 주도하고 있는 사이버 안보 분야의 세계질서는 지나치게 근대 국제정치의 지배담론에 기반을 두고 있다. 이는 현실주의 국제정치이론에서 상정하고 있는 국제정치의 이미지를 과도하게 강조하는 담론이라는 의미에서 '과잉 현실주의(hyper-realism)' 담론이라고 부를 수 있겠다. 근대 국제정치이론의 주류를 이루는 현실주의 담론은 국제정치의 주요 행위자로서 국민국가를 설정하고 이들이 벌이는 하드 파워 게임의 과정에서 생성되는 국제정치의 제로섬 게임적 양상에 주목한다. 지구화, 정보화, 민주화로 대변되는 변화를 겪고 있는 오늘날에도 이렇게 현실주의 담론이 상정하고 있는 현실은 엄연히 존재한다. 그러나 오늘날 세계정치의 변화는 단지 그러한 제로섬 게임의 양상으로만 파악할 수 없는 복합적인 모습으로 전개되고 있다. 따라서 현실주의 국제정치이론의 담론에 지나치게 집착해서 세상을 볼 경우, 자칫 담론이 현실을 왜곡하는 과잉 담론 현상이 출현할 가능성이 있다.

최근 사이버 공간에서 벌어지는 경쟁과 갈등, 그리고 그러한 연속선상에서 출현하는 주요 국가들의 사이버 안보 전략의 양상을 보면, 이러한 과

잉 현실주의 담론에 의해서 현실이 재구성되고 있는 것 같은 느낌을 지울 수 없다. 특히 미국이나 중국, 러시아 등과 같은 강대국들이 벌이는 안보화 게임이나 사이버 공간의 군사화 게임은 단순히 관련 행위자들의 이해관계가 조정되고 갈등하는 차원을 넘어서 강대국들이 나서서 벌이는 21세기 패권경쟁의 한 단면을 보는 듯하다. 게다가 아직 사이버 안보 문제를 다룰 국제규범이 마련되지 않은 상황에서 사이버 안보 분야는, 현실주의 국제정치이론이 상정하는 것과 유사한, 전형적인 무정부상태(anarchy)로 개념화되고, 그러한 환경 아래에서 전통적인 국제정치 행위자로서 국가 행위자들이 전면에 나서 제로섬 게임의 경쟁을 벌이는 세상으로 그려진다.

실제로 미국은 중국 해커들의 소행으로 추정되는 사이버 공격을 국가안보의 위협으로 인식하고, 미사일을 발사해서라도 '사이버 진주만'의 재난을 막겠다고 공언하고 있다. 이에 대해서 중국도 사이버 공간의 질서 형성과정에서 나타나는 미국의 패권을 비난하면서 자국의 기술 시스템과 정치체제에 대한 주권적 통제의 필요성을 주장한다. 이러한 와중에 21세기 패권을 겨루는 두 강대국 간에 진행되고 있는 것으로 보이는 사이버 공격과 방어의 게임은 계속 상승작용을 벌이고 있다. 이러한 양상은 정치와 군사 영역을 넘어서 경제와 무역 분야에도 확대되어, 미국은 2012년 국방수권법을 제정해 외국 장비가 국가시설에 도입되는 것을 사실상 원천 봉쇄했다. 마찬가지로 중국도 외산(특히 미국산) 장비를 국가시설에 들이려면 소스코드를 공개하라는 원칙을 주장하고 있다 (『디지털타임즈』, 2015.05.13). 자칫 잘못하다가는 양국 간의 무역 분쟁이 발생할 가능성까지도 우려되고 있는 실정이다.

이렇게 강대국들이 벌이는 패권경쟁 담론이 사이버 공간에까지 침투하는 구도는 한국의 입장에서 볼 때 결코 좋을 게 없다. 게다가 남북한이 대치하고 있고 한반도를 두고 미국과 중국이 주도권 경쟁을 하는 상황에서 한국이 미국과 중국의 사이에 벌어질 사이버 전쟁이나 무역 분쟁에서 어느 한 편을 들기는 어려운 실정이다. 미국에 대한 안보 의존도나 중국에 대한

무역 의존도가 매우 높은 상황에서 자칫 큰 문제가 불거질 우려가 있기 때문이다. 또한 미국과 중국 사이에서, 그리고 북한과의 관계에서 과잉 현실주의 담론에 기반을 둔 군사전략의 시각으로 현실을 이해하는 접근도 조심스럽게 살펴보아야 한다. 이러한 군사전략 담론에 의거하여 한미 간의 사이버 안보협력을 이해하고 중국이나 북한과의 관계를 설정하는 것은 자칫 큰 부담으로 다가올 우려가 있다. 예를 들어, 중국이나 북한의 소행으로 추정되는 사이버 공격에 대해서 한미 간의 집단자위권을 근거로 물리적 반격을 가해야만 하는 상황이 창출될 경우 자칫 한반도가 사이버 전쟁터, 더 나아가 물리적 전쟁터가 될 우려도 있다.

이러한 연속선상에서 보면, 전통적인 국제법과 국제기구의 틀을 활용하여 사이버 안보의 국제규범을 만들려는 시도 자체도 성찰적으로 보아야 할지 모른다. 최근 미국과 NATO, 유엔 등을 중심으로 사이버 공격에 대해 전쟁법을 적용하려는 시도를 벌이고 있는데, 이러한 접근이 한국에 주는 의미가 무엇일지에 대해서 냉철하게 생각해 볼 필요가 있다. 사이버 안보의 국제규범을 국민국가(nation-state)들의 관계, 즉 국제(國際, inter-national)의 틀에서 접근하는 것이 맞는가에 대한 성찰이 필요하다. 다시 말해 탈(脫)지정학적이고 초국적으로 작동하는 사이버 안보의 문제를 국민국가들 간의 관계라는 틀로 보는 근대 국제정치 담론 자체에 대해서 성찰적인 입장이 필요하다. 사이버 안보의 이슈는 탈린 매뉴얼이나 유엔 GGE 같이 전통적인 국제법과 국제기구의 형식에만 의존해서는 해결될 문제가 아니라는 것을 알아야 할 것이다. 그도 그럴 것이 사이버 안보의 문제는 기본적으로 근대 국제정치의 틀을 넘어서는 탈근대 신흥안보의 이슈이기 때문이다.

2) 사이버 안보 분야 규범외교의 방향

사이버 안보 분야의 중견국 규범외교는 탈지정학적이고 탈근대적인 신흥안보 이슈로서 이 분야가 지니는 구조적 조건에 대한 철저한 이해를 바탕으로 추진되어야 한다. 사이버 공격과 방어는 그 주체와 보복의 대상을 확

인하는 것이 쉽지 않은 복합 네트워크 환경에서 발생한다. 사이버 공간에서의 국가나 기업 행위자들에 대한 공격도 전통적인 국가 행위자가 아니라 비국가 행위자들이나 이들을 전면에 내세운 국가-비국가 복합체들에 의해서 감행되고 있다. 게다가 사이버 공격은 점점 더 진화하여 인간 행위자와 (컴퓨터 바이러스나 악성코드 등과 같은) 비인간 행위자의 경계도 허물고 있다. 이러한 의미에서 전통적인 권력정치와 국가안보의 개념에 기반을 두고 있는 단순계적인 접근은 복잡성을 본질로 하는 사이버 안보의 구조적 조건을 파악하는 데 한계가 있을 수밖에 없다. 따라서 현재 강대국들이 생성하고 있는 담론보다 좀 더 복합적인 발상으로 사이버 안보의 세계정치를 풀어나가려는 새로운 접근법이 필요하다.

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 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 전략을 넘어서 사이버 안보 분야의 특성에 부합하는 좀 더 보편적인 규범을 주장하거나 더 나아가 새로운 규범을 제시하는 적극성을 보일 필요가 있다. 이와 관련하여 이 글은 한국이 추구할 사이버 안보 분야 규범외교의 방향을 아래와 같은 세 가지 측면에서 제시하고자 한다.

첫째, 냉전에 비유하거나 제로섬 게임적 군비경쟁에서 유추하는 강대국들의 안보담론을 비판하고 보완하는 규범외교를 펼칠 수 있을 것이다. 최근 '사이버 공간의 군사화'라는 시각에서 사이버 공간에서의 안보 문제를 보려는 경향이 늘어나고 있다 (Lawson 2012). 사이버 분쟁은 현대 전쟁의 첨단 양식 중의 하나로 묘사되며 사이버 무기는 대량 파괴 무기와 같은 맥락에서 파악된다. 실제로 미국과 중국 두 강대국은 상호 간의 사이버 공격과

방어를 위한 역량을 강화하기 위해서 경주하고 있으며, 사이버 군비경쟁이 벌어지는 것이 아니냐는 전망도 나오고 있다. 이러한 상황에서 사이버 공간의 군사화와 사이버 위협의 안보화는 정당화되고 강화된다. 그런데 강대국들이 이렇게 제로섬 게임에 입각한 군비경쟁의 유추에 집착하는 한 사이버 안보 문제는 해결되기는커녕 오히려 사이버 공간에서도 '안보 딜레마'가 발생할 수 있다. 이러한 맥락에서 한국이 강대국들 사이에서 사이버 공간의 탈군사화된 평화담론을 제시하는 중견국 규범외교를 추구해 봄직하다.

둘째, 사이버 안보 분야에 전통적인 '국제' 담론을 적용하는 시도의 한계를 지적하고 이를 극복하는 차원에서 '탈(脫)국제(post-international)' 담론을 강조하는 규범외교를 필칠 수 있을 것이다. 특히 국가 단위의 사고를 바탕으로 사이버 안보 문제를 보는 기존의 국제법적 접근을 보완하는 담론을 개발할 필요가 있다. 최근 글로벌 학계에서는 사이버 공간에서의 무력사용과 사이버 위협에 기존의 국제법(특히 전쟁법)의 틀을 적용하기 위한 연구를 벌이고 있다 (Liaropoulos 2011). 앞서 언급한 탈린 매뉴얼은 기존의 국제법 규범을 초국적 사이버 위협의 사례에 적용하려는 대표적인 시도이다. 그렇지만 사이버 안보의 세계정치에서 발생하는 공격과 방어의 비대칭적 구도를 고려하면, 근대 국제정치의 경우처럼 공격과 방어의 행위자들을 이분법적으로 보고 이들 사이의 공방을 법규범으로 풀어보려는 해법은 실효성이 떨어진다. 지금 필요한 것은 사이버 안보 이슈의 탈국제적이고 복합 네트워크적인 동학을 다룰 수 있는 좀 더 복합적인 규범이다. 이러한 맥락에서 중견국으로 한국은 현재의 '국제' 담론을 보완하는 새로운 '네트워크' 담론을 개발하는 데 기여할 필요가 있다.

끝으로, 강대국들의 권력담론을 보완하는 차원에서 그 동안은 국내적 구도에서 주로 논의되어 온 사이버 윤리의 문제를 국제적 장에 확장하는 규범외교를 펼칠 수 있을 것이다. 기존의 사이버 윤리는 컴퓨터가 어떻게 프로그램되어야 하느냐, 누가 디지털 데이터를 소유하느냐, 온라인상의 음란물에 대한 접근은 얼마나 허용되어야 하느냐 등과 같은 문제들을 중심으로 논의

되어 왔다. 이제 이러한 사이버 윤리의 논쟁은 국제 또는 초국적 사이버 안보 이슈들로 확장될 필요가 있다. 인터넷 사용이 지속적으로 증가함에 따라 나타나는, 개인정보의 국제적 도용이나 국제 사이버 범죄 및 국가 간의 컴퓨터 해킹과 사이버 테러 등의 문제를 국가 간의 윤리적 문제로 다룰 수는 없을까? 역사적으로 안보 문제가 윤리적 논쟁을 야기했던 전례에 비추어 볼 때, 사이버 안보 분야에서도 그러한 윤리적 논쟁이 벌어질 가능성이 크다. 이러한 맥락에서 볼 때, 사이버 윤리 분야에서 새로운 담론을 개발하여 힘의 논리에 기반을 둔 강대국들의 안보담론을 제어하는 효과를 노려볼 수 있다.

최근 초보적이지만 사이버 안보 분야에서 이러한 중견국 규범외교 담론의 가능성을 엿보게 하는 사례들이 등장하고 있다. 예를 들어, 사이버 안보 분야에서 미국과 중국의 신경전이 벌이고 있는 가운데 한국의 전자정부 사이버 보안시스템이 중동 국가들로부터 러브콜을 받고 있다고 한다. 한국형 보안 패키지에 러브콜이 쏟아지는 데에는 미국과 중국이 사이버 안보 분야에서 대립하고 있는 분위기도 영향을 미친다. 미국과 중국이 서로 싸움을 하느라 시스템 수출 등에 신경을 쓰지 못하는 상황에서 대안으로 한국 제품에 관심을 두는 곳이 많다는 것이다. 이들 나라에 비해 한국 제품의 가격 경쟁력이나 기술이 우수하다는 점도 변수이다 (『머니투데이』, 2015.06.29). 최근 한국은 발달된 정보인프라로 인해 세계의 주목을 받고 있고, 사이버 위협 상황에서 대응력을 키워왔을 뿐만 아니라, 미국이나 중국, 러시아, 이스라엘 등에 비해 어느 한쪽으로 치우치지 않은, 역량 있는 '사이버 중립국'의 이미지를 키워가고 있는 것으로 판단된다 (『디지털타임즈』, 2015.05.13).

6. 결론

사이버 안보 이슈가 21세기 세계정치의 전면으로 부상하면서 주요 국가들 간의 갈등이 깊어가는 가운데 이 분야의 국제규범 형성을 놓고 이해관계가

얽히고 있다. 이제 사이버 안보는 단순한 컴퓨터 보안전문가들의 영역이 아니라 외교정책 결정자들이나 군사 전략가들이 관심을 가질 수밖에 없는 국가안보와 외교 전략의 문제로 부상했다. 이러한 사이버 안보의 국제정치학적 중요성을 염두에 두고, 이 글은 사이버 안보 분야에서 한국이 담당할 수 있는 중견국 외교의 역할을 네트워크 이론의 시각에서 살펴보았다. 네트워크 이론의 시각을 원용하여 중견국 외교의 가능성과 한계를 검토하는 과정에서 이 글이 강조한 것은 행위자들의 속성이 아니라, 다음과 같이 세 가지 측면에서 파악되는, 사이버 안보 분야의 고유한 구조적 조건을 이해하는 것이 중견국 외교의 성패를 가늠하는 관건이라는 점이었다.

첫째, 사이버 안보는 전통 안보 문제와는 다른 고유한 기술 구조적 특징을 지니고 있다. 그 중에서도 사이버 위협의 잠재적인 위력을 이해하는 핵심은 인터넷의 복합 네트워크적인 특성이다. 사이버 위협은 지속적으로 진화할 뿐만 아니라 점차로 민간과 군사 영역, 비국가와 국가 행위자, 그리고 인간과 비인간 행위자의 구분을 흐려놓고 있다. 둘째, 사이버 안보, 좀 더 넓게는 인터넷 거버넌스 분야에서 두 국가군이 경쟁을 벌이는 구도가 펼쳐지고 있다. 인터넷이 좀 더 개방되고 자유로워야 한다고 믿는 서방국가들이 주도적인 가운데, 러시아, 중국 및 개도국 진영이 인터넷의 국가 통제 모델을 주장하면서 도전하고 있다. 끝으로, 미국과 중국의 패권경쟁 구도가 사이버 안보 분야에서도 나타나고 있다. 사이버 안보 분야의 보안기술, 규제정책, 안보담론 등을 둘러싸고 두 강대국의 상이한 입장이 충돌하는 모습을 보이고 있다.

이러한 구조적 특징을 지닌 사이버 안보의 세계정치가 작동하는 양상을 보면 전통안보의 영역에서 국민국가들이 벌였던 '국제정치'의 영역을 넘어서는 모습을 보인다. 사이버 안보의 세계정치는 다양하고 복합적인 행위자들이 벌이는 이른바 '비대칭 망제정치'의 영역에 속한다. 전통안보 이슈와 그 성격이 구별되는 사이버 안보 이슈의 가장 큰 차이점은 그 위협의 발생이 사이버 공간이라고 하는 복합 네트워크 환경을 바탕으로 하여 이루어지

고 있다는 점이다. 그러한 사이버 위협에 대응하는 국제정치적 해법도 국가 행위자뿐만 아니라 다양한 비국가 행위자들이 참여하는 글로벌 거버넌스의 틀을 따르고 있다. 이러한 복합적인 행위자들이 그들의 정치적 필요와 이익을 만족시키기 위해서 경쟁하면서 다방면에서 충돌할 것이 예상된다.

이렇듯 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 중요하지 않을 수 없다. 다시 말해, 진화하는 사이버 안보 분야의 맥락을 파악하고 그 안에서 적절한 위치를 설정하는 것은 핵심적인 국가전략적 사안이 아닐 수 없다. 이를 바탕으로 어떠한 종류의 외교적 역할을 추구할지에 대한 방향을 모색할 수 있을 것이기 때문이다.

이 글은 중견국 외교의 이론적 자원들을 적용하여 한국이 추구해야 할 사이버 안보 분야 외교전략의 방향을 세 가지 차원에서 제시하였다. 우선 필요한 것은 사이버 안보 분야에서 경쟁하는 행위자들의 관계를 조율하는 중개외교이다. 특히 이 분야의 구조적 공백을 찾아내고 공략함으로써 새로운 관계구도를 창출하는 '맺고 끊기'의 외교적 발상이 필요하다. 둘째, 복합적으로 얽혀 있는 구조 하에서 어느 중견국이라도 혼자 나서서 효과적인 결과를 얻어내기는 쉽지 않다. 이러한 점에서 중견국 외교에서 가장 중요한 것은 생각을 공유하고 행동을 같이하는 동지국가들을 가능한 한 많이 모으는 연대외교이다. 끝으로, 중견국 외교가 염두에 두어야 할 또 하나의 과제는 중견국으로서 나름대로의 세계질서를 구상하는 설계외교를 추구해야 한다는 점이다. 특히 강대국들이 만들어 놓은 질서를 보완하는 차원에

서 규범적 가치와 정당성을 추구하는 규범외교를 생각해 볼 수 있다.

요컨대, 한국은 진화하는 사이버 안보 분야의 구조적 조건 하에서 다층적으로 형성되는 비대칭적인 관계를 조율하는 외교적 능력을 갖추어야 한다. 한국은 단순한 연결자가 아니라 상이한 행위자들 간의 관계에 상호작동성과 호환성을 제공하는 적극적 중개자로서 행동할 수 있다. 이러한 중개의 역할을 완수하기 위해서는 생각을 같이 하는 동지국가들을 규합하는 것이 필수적이며 널리 글로벌 차원에서도 지지자들을 끌어 모을 수 있어야 할 것이다. 가장 추상적인 차원에서도 중견국으로서 한국은 전체 시스템의 설계자는 아니더라도 강대국이 운영하는 시스템의 프로그램을 보완하는 하위 설계자의 역할을 담당할 수 있을 것이다. 사이버 안보 분야는 이러한 중견국 외교의 복합적 역량을 가늠하는 실험대라고 할 수 있다.

참고문헌

강하연. 2013. "ICT교역의 글로벌 거버넌스." 서울대학교 국제문제연구소 편. 『커뮤니케이션 세계정치』 기획특집 〈세계정치〉 33(2). 사회평론, 73-109.

김상배. 2011a. "네트워크로 보는 중견국 외교전략: 구조적 공백과 위치권력 이론의 원용." 『국제정치논총』 제 51집 3호, 51-77.

_____. 2011b. "한국의 네트워크 외교전략: 행위자-네트워크 이론의 원용." 『국가전략』 제 17권 3호 5-40.

_____. 2012. "정보화시대의 미·중 표준경쟁: 네트워크 세계정치이론의 시각." 『한국정치학회보』 제 46집 1호, 383-410.

_____. 2014. 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 한울.

_____ 편. 2014. 『네트워크 시대의 외교안보: 중견국의 시각』 사회평론.

_____ 편. 2015. 『제3세대 중견국 외교론: 네트워크 이론의 시각』 사회평론.

김상배·이승주·배영자 편. 2013. 『중견국의 공공외교』 사회평론.

손열 편. 2007. 『매력으로 엮는 동아시아: 지역성의 창조와 서울 컨센서스』 지식마당.

이영음. 2014. "글로벌 인터넷 거버넌스 논의에서의 멀티스테이크홀더개념 정립 및 적용 방법." 비전통 안보와 중견국 외교 집담회 발표문. 5월 8일.

임종인·권유중·장규현·백승조. 2013. "북한의 사이버전력 현황과 한국의 국가적 대응전략." 『국방정책연구』 제 29권 4호 9-45.

장규현·임종인. 2014. "국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로." 『정보통신방송정책』 26집 5호, 21-52.
장노순. 2015. "사이버 안보와 국제규범 구축의 외교전략: 정부전문가그룹(GGE)의 활동을 중심으로." 2015년 하계 여수 한국국제정치학회 발표논문.
장덕진. 2009. "정치권력의 사회학적 분해: 자원 권력과 네트워크 권력." 김상배. 편. 『소프트 파워와 21세기 권력: 네트워크 권력론의 모색』 197-241. 한울.
하영선·김상배 편. 2010. 『네트워크 세계정치: 은유에서 분석으로』 서울대학교출판문화원.
Brenner, Susan W. 2007. "Council of Europe's Convention on Cybercrime." J.M. Balkin and Information Society Project, Yale Law School. *Cybercrime: Digital Cops in a Networked Environment.* New York: New York University Press, pp. 207-220.
Burt, Ronald S. 1992. *Structural Holes: The Social Structure of Competition. Cambridge.* MA: Harvard University Press.
Buzan, Barry, and Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis.* Boulder: Lynne Rienner.
Castells, Manuel. 2009. *Communication Power.* Oxford and New York: Oxford University Press.
Cooper, Andrew F. ed. 1997. *Niche Diplomacy: Middle Powers After the Cold War.* London: Macmillan.
Cooper, Andrew F., and Richard A. Higgott, and Kim Richard Nossal. 1993. *Relocating Middle Powers: Australia and Canada in a Changing World Order.* Vancouver: UBC Press.
DeNardis, Laura. 2013. *The Global War for Internet Governance.* Yale University Press.
Evron, Gadi. 2008. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs* 9(1): 121-126.
Galloway, Alexander R. and Eugene Thacker. 2007. *The Exploit: A Theory of Networks.* Minneapolis and London: University of Minnesota Press.
Gilley, Bruce, and Andrew O'Neil. eds. 2014. *Middle Powers and the Rise of China.* Washing DC: Georgetown University Press.
Goddard, Stacie E. 2009. "Brokering Change: Networks and Entrepreneurs in International Politics." *International Theory* 1(2): 249-281.
Gordon, J. King. 1966. "Canada's Role as a Middle Power." Contemporary Affairs. 35. *The Canadian Institute of International Affairs*, Toronto.
Gould, Roger V. and Roberto M. Fernandez. 1989. "Structures of Mediation: A Formal Approach to Brokerage in Transaction Networks." *Sociological Methodology* 19: 89-126.

Grewal, David Singh. 2008. *Network Power: The Social Dynamics of Globalization.* New Haven and London: Yale University Press.
Hafner-Burton, Emilie M., and Alexander H. Montgomery. 2006. "Power Positions: International Organizations, Social Networks, and Conflict." *Journal of Conflict Resolution* 50(1): 3–27.
Hafner-Burton, Emilie M., and Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organization* 63(3): 559–592.
Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53(4): 1155–1175.
Holbraad, Carsten. 1971. "The Role of Middle Powers." *Cooperation and Conflict* 6(1): 77–90.
Kahler, Miles. ed. 2009. *Networked Politics: Agency, Power, and Governance.* Ithaca and London: Cornell University Press.
Kim, Sangbae. 2014. "Roles of Middle Power in East Asia: A Korean Perspective." *EAI Middle Power Diplomacy Initiative Working Paper*–02, East Asia Institute.
Lawson, Sean. 2012. "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States." *First Monday.* 17(2). http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.
Levy, Pierre. 1999. *Collective Intelligence: Mankind's Emerging World in Cyberspace,* Basic Books.
Liaropoulos, Andrew. 2011. "Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict." *Greek Politics Specialist Group Working Paper,* no.7.
Lieberthal, Kenneth, and Peter W. *Singer. 2012. Cyber security and U.S.–China Relations.* China Center at Brookings.
Manson, George Patterson, 2011. "Cyberwar: The United States and China Prepare For the Next Generation of Conflict." *Comparative Strategy* 30(2): 121–133.
Maoz, Zeev. 2010. *Networks of Nations: The Evolution, Structure and Impact of International Networks, 1816–2001.* Cambridge and New York: Cambridge University Press.
Maurer, Tim, and Robert Morgus. 2014. "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate," *CIGI Internet Governance Papers No. 7 Series: Internet Governance.* http://www.cigionline.org/sites/ default/files/no7_2.pdf.
McLin. Jon B. 1967. *Canada's Changing Defense Policy, 1957–1963: The Problems of a Middle Power in Alliance.* Baltimore: Johns Hopkins Press.
Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace.* Cambridge, MA: The MIT Press.

_____. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge and London: MIT Press.
Nexon, Daniel, and Thomas Wright. 2007. "What's at Stake in the American Empire Debate?" *American Political Science Review* 101(2): 253-271.
Nexon, Daniel. 2009. *The Struggle for Power in Early Modern Europe: Religious Conflict, Dynamic Empires, and International Change.* Princeton, NJ: Princeton University Press.
Otte, Max. 2000. *A Rising Middle Power?: German Foreign Policy in Transformation, 1989-2000.* New York: St. Martin's Press.
Pratt, Cranford. ed., 1990. *Middle Power Internationalism: The North-South Dimension.* Kingston and Montreal: McGill-Queen's 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: 13-37.
Thomas, Timothy L. 2009. "Nation-state Cyber Strategies: Examples from China and Russia." In Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. eds. *Cyberpower and National Security.* 465-488. Washington DC: Center for Technology and National Security Policy, National Defense University.
Tilly, Charles. 1998. "Contentious Conversation," *Social Research* 653(3): 491-510.
US-China Economic and Security Review Commission. 2009. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* McLean, VA: Northrop Grumann Corporation Information Systems Sector.
Wæver, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. 1993. *Identity, Migration and the New Security Agenda in Europe.* London: Pinter.
_____. 1995. "Securitization and Desecuritization." in Ronnie Lipschutz. ed. *On Security.* New York: Columbia University Press.
Waltz, Kenneth N. 1979. *Theory of International Politics.* New York: Random House.