사이버 안보의 미중관계: 안보화 이론의 시각*

김 상 배 서울대학교

논 문 요 약

최근 사이버 안보의 문제가 21세기 미중관계의 현안으로 급속히 부상하고 있다. 이 글은 국제안보 분야 코펜하겐 학파의 안보화(securitization) 이론의 시각을 원용하여 현재 사이버 안보 분야에서 미국과 중국이 벌이고 있는 경쟁의 양상을 살펴보았다. 현재 사이버 안보의 미중관계는 세 가지 차원에서 본 안보화 과정의 차이가 단적으로 드러나고 있다. 첫째, 사이버 위협의 성격을 인식함에 있어서 미국이 주로 중국의 해커들에 의한 미국의 지식정보 자원에 대한 공격을 비난한다면, 중국은 미국 IT기업들의 기술패권을 중국의 사이버 안보에 대한 가장 큰 위협으로 간주한다. 둘째, 사이버 안보의 대상과 주체라는 점에서 미국이 주로 물리적 인프라의 안정성 유지와 개인의 인터넷 자유를 보호하는 데 관심이 있다면, 중국의 담론은 인터넷 상에서 유통되는 정보콘텐츠의 정치안전과 인터넷에 대한 검열과 규제를 수행할 수 있는 국가 차원의 정책적 권리에 초점을 둔다. 끝으로, 사이버 세계질서의 구성이라는 점에서 미국의 담론이 다양한 이해당사자가 참여하는 글로벌 거버넌스의 모델을 강조한다면, 중국은 국가 행위자가 주도하는 전통적인 국제기구의 틀을 활용하자는 주장을 펼치고 있다. 이러한 사이버 안보담론의 차이에 내재해 있는 미국과 중국의 이해관계는 앞으로 양국이 사이버 안보의 국내외 질서를 구성하는 경쟁 과정에서 현실화될 것으로 예상된다.

〈주제어〉 사이버 안보, 미국, 중국, 미중관계, 안보화 이론, 국제정치

* 이 논문은 2013년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2013S1A3A2053683)

원고접수일 2014년 10월 09일 | **심사일** 2014년 10월 20일 | **게재확정일** 2015년 03월 27일

한국정치학회보, 49집 1호 2015 봄, 71-97

Ⅰ. 머리말

최근 사이버 안보가 21세기 세계정치의 현안으로 주목을 받고 있다. 특히 2013년 6월 미국과 중국의 두 정상이 만나 양국이 당면한 현안 중의 하나로 거론하면서 사이버 안보는 미중관계의 전면에 부상했다. 그 후 사이버 안보는 양국 간에 진행된 전략경제대화의 의제 중의 하나로서 다루어졌으며, 좀 더 구체적으로는 미 · 중 사이버 보안 실무그룹의 협의가 진행되기도 했다. 그러나 이러한 협력의 몸짓에도 불구하고 물 밑에서는 미 · 중 사이버 갈등은 계속 진행되었다. 이러한 갈등은 2014년 5월 미 법무부가 미국 내 기관들에 대해서 해킹을 감행한 것으로 지목한 중국군 61398부대 장교 5인을 기소하면서 정점에 달한 듯이 보였다. 중국은 이에 즉각 반발하며 미국과의 대화를 중단하는 동시에 중국 시장에 진출한 미국 IT 기업들에 대한 규제의 고삐를 죄기도 했다.

사실 사이버 안보 분야에서 벌어진 미중관계의 이면을 보면, 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. 특히 미 정보당국이 중국을 감청한 데이터를 전송할 때 미국 IT기업인 시스코의 공유기를 사용한 것이 밝혀지면서, 중국 정부가 미국 정부를 상대로 역공을 펼치는 빌미를 제공하기도 했다. 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.

이러한 맥락에서 사이버 안보 분야의 미중관계에 대한 국제정치학의 관심이 늘어나고 있다(Liberthal and Singer, 2012; Manson, 2011; 沈逸, 2010; 蔡翠红, 2012; 김상배, 2012). 그런데 현재 국내외 일부 학계와 미국의 정책그룹에서 사이버 위협에 대처하자며 제기되는 주장들은 대체적으로 전통적인 군사안보론의 시각을 주로 원용하고 있다. 예를 들어, 국내외 학계 일각에서 제기되는 '사이버 억지'의 발상은 사이버 안보의 문제를 이해하고 해법을 모색함에 있어서 핵 안보 연구에서 비롯된 전략론의 시각을 적용하려 한다(Morgan, 2010; Lupovici, 2011; Singer and Shachtman, 2011; 장노순 · 한인택, 2013). 이러한 전략론의 시각과 더불어 사이버 공격의 배후지를 제공한 국가나 업체에 대해서 국제법과 전쟁법을 적용하여 책임을 묻겠다는 접근도 등장하고 있다(Schimit, 2012).

이러한 주장들은 사이버 공격의 범인을 찾아 보복하거나 책임을 묻겠다는 단호함을 표명하는 데에는 효과가 있을지 몰라도, 실제로 발생하는 사이버 위협에 대한 효과적인 처방이 될 수 있을지는 의심스럽다. 무엇보다도 사이버 공간에서 발생하는 위협을 객관적으로 측정하고 이에 보복할 수 있다는 선형적(linear) 사고방식 자체가 논란거리이다. 복잡계 현상에 기반을 두고 있는 사이버 위협에 대한 대책을 단순계 발상에 기반을 둔 전통적인 안보와 억지 개념에서 구하는 잘못을 범할 우려가 있기 때문이다(Beck, 2005; 민병원, 2007). 이러한 상황에서 사이버 안보의 담론을 지나치게 군사전략적 시각에서 접근하는 것은 현실을 엉뚱한 방향으로 재구성할 가능성마저 없지 않다.

사이버 공간의 기술적 속성을 탐구하는 컴퓨터와 정보보안 분야의 연구는 이러한 군사적 시각을 부추기고 있다. 이들 연구가 지니는 문제점은 물리적 환경으로서 인터넷이라는 기술체계 자체에서 발생하는 가능성에만 주목하여 사이버 공격과 테러가 낳을 위험성을 과장하는 경향이 있다는 데 있다. 이러한 기술담론이 앞서의 군사담론과 결합하면서 사이버 공간을 군사적 갈등의 공간으로 보는 이른바 사이버 공간의 군사화(militarization) 현상을 강화할 우려가 있다. 다시 말해, 군사적 위협과 기술적 가능성을 염두에 두고 이에 대비하는 방향으로 막대한 예산과 인력이 투입하여 현실을 재구성하고, 이렇게 구축한 현실이 다시 사이버 공간에서 군사적 경쟁을 촉발하는, '담론과 현실의 상호구성 고리'가 형성될 수 있다(Matusitz, 2006).

이러한 군사 · 기술담론이 먹혀들어가는 것은 사이버 안보 문제의 복잡계적인 특성 때문이다. 실제로 사이버 공격에는 초국적으로 활동하는 비국가 행위자나 이를 지원하는 국가 행위자뿐만 아니라 컴퓨터 바이러스나 악성코드와 같은 소위 '비인간 행위자(non-human actor)'까지도 관여한다(김상배, 2014). 이러한 복잡성으로 인해서 누가 사이버 공격의 주범인지를 밝히기 어려울 뿐만 아니라 만약에 범인을 찾는다고 하더라도 확증보다는 추정하는 경우가 많다. 따라서 실제 범인을 색출하는 문제보다도 누가 범인인지에 대한 담론을 구성하는 것이 더 중요한 경우도 많다(Hansen and Nissenbaum, 2009). 사정이 이렇다 보니까 사이버 위협의 성격이 무엇이고 보호할 대상이 무엇이며 이를 지킬 주체가 누구인지, 그리고 이러한 과정에서 생성되는 질서의 성격을 규명하는 것이 중요할 수밖에 없다. 이러한 상황에서 기술전문성을 갖춘 군사담론이 현실을 규정하고 재구성하는 담론 생성의 힘을 행사하고 있다.

이 글은 국제안보 분야 코펜하겐 학파의 안보화(securitization) 이론의 시각을 원용하여 현재 미국과 중국 사이에서 벌어지고 있는 사이버 안보담론의 경쟁을 살펴보고자 한다. 안보화 이론은 구성주의 시각에서 안보담론이 사회적으로 형성되는 과정을 탐구한다. 물론 실제 사이버 공방이 벌어지겠지만 그 실체를 객관적으로 밝혀내는 것이 용이하지 않은 현재의 상황을 고려할 때, 현 단계 사이버 안보 분야의 갈등은 주로 안보화 경쟁의 양상으로 나타나고 있다는 것이 이 글의 인식이다. 이러한 안보화 이론의 시각에서 볼 때, 사이버 안보를 둘러싸고 전개되고 있는 미중관계는 단순히 해커들의 명시적인 공격과 네트워크 시스템의 물리적 교란, 상업적 · 군사적 정보의 절취와 도용, 그리고 여기서 파생되는 양국 간의 물리적 충돌의 가능성을 논하는 차원을 넘어선다. 현재 벌어지고 있는 미 · 중 경쟁은 안보담론을 구성하고 이를 기반으로 국내 정책과 제도, 그리고 더 나아가 세계질서를 구성하려는 경쟁으로 나타난다.

이 글은 크게 다음과 같은 네 부분으로 구성되었다. 제2장은 안보화 이론의 시각에서 본 사이버 안보 분야의 특성을 살펴보고, 위협의 성격, 안보의 대상과 주체, 세계질서의 구성이라는 세 가지 차원의 분석틀을 제시했다. 제3장은 사이버 위협의 성격을 보는 미국과 중국의 인식의 차이를 각각 '중국해커위협론'과 '미국기술패권경제론'로 개념화하여 살펴보았다. 제4장은 사이버 안보의 대상과 주체에 대한 양국의 차이를 네트워크와 개인의 안보를 강조하는 미국의 담론과 정치안전과 국가주권을 강조하는 중국의 담론으로 나누어 살펴보았다. 제5장은 미국과 중국이 벌이고 있는 사이버 안보화의 경쟁이 이 분야의 세계질서의 구성에 미치는 영향에 대해서 살펴보았다. 맺음말에서는 이 글의 주장을 요약 · 정리하고, 안보화 이

론의 시각을 원용하여 사이버 안보의 세계정치를 보는 작업의 향후 과제에 대해서 간략히 지적하였다.

II. 안보화 이론으로 보는 사이버 안보

코펜하겐 학파는 기존 안보이론의 국가 중심성과 군사안보 중심성을 비판하고 탈냉전기 안보의 복합성과 안보담론의 규범성을 지적한 것으로 유명하다. 코펜하겐 학파의 안보화 개념은 안보담론이 사회적으로 형성되는 과정을 지칭하는 개념으로서 구성주의 시각에서 안보행위를 이해하는 데 기여한다(Wæver et al. 1993; Wæver 1995; Buzan et al. 1998; Buzan and Hensen. 2009; Balzacq ed., 2011). 안보화 이론에 의하면, 안보란 객관적(또는 주관적)으로 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 과정에서 구성된다. 이러한 과정에서 안보화란 어떤 문제에 여타 비(非)안보 문제가 결여하고 있는 지위와 우선성을 부여하여 그것을 '안보 문제'로서 구성하는 과정이다. 보통의 경우라면 직접적인 위협으로 간주되지 않았을 문제라도 안보 행위자에 의해서 중대한 위협으로 부각되고 비상의 조치를 강구하는 정치적 행위의 계기가 될 수 있다. 이러한 점에서 안보란 특정한 수사적 구조와 정치적 효과를 갖는 담론적 양식이며, 객관적으로 존재하는 현상이라기보다는 간주관적 담론이다.[1)]

국제정치 현실에서 이러한 안보화는 생각과 담론, 더 나아가 이념과 가치관 등의 표준을 놓고 벌이는 경쟁에서 나타난다. 담론은 현실세계의 이익과 제도적 제약을 바탕으로 하여 출현하지만, 역으로 미래세계를 구성 및 재구성하는 방향으로 작동하기도 한다. 다시 말해, 담론은 현실을 바탕으로 하여 구성된 이익이나 제도의 비(非)물질적 반영이기도 하지만, 기존의 이익에 반하거나 제도적 제약을 뛰어 넘어 기성 질서와는 다른 방향으로 현실의 변화를 꾀하는 계기를 제공하기도 한다. 이러한 과정에서 담론은 아직 구체화되지 않은 현실세계의 성격을 정의하며 그러한 과정에서 등장할 미래세계의 의미와 효과를 규정하는 의미를 획득한다. 이러한 담론의 주도권을 둘러싼 경쟁은 단순히 추상적인 관념의 경쟁만을 의미하는 것이 아니고, 보통 새로운 담론의 제시를 통해서 정책과 제도 형성의 방향을 설정하는 경쟁으로 연결된다(김상배, 2012).

이러한 맥락에서 보면 최근에 벌어지고 있는 사이버 안보의 세계정치는 사이버 안보담론의 주도권을 장악하기 위한 경쟁의 성격을 강하게 띠고 있다. 안보화 이론은 사이버 테러와 공격에 의해서 만들어진, 검증 가능한 사실로서의 물리적 공격과는 별도로 진행되고 있는, 사이버 안보담론을 둘러싸고 벌어지는 경

1) 안보화 개념을 소개 또는 적용한 국내 연구로는 민병원(2006), 송영훈(2014)이 있다.

쟁을 보여준다는 점에서 유용하다. 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 위협이다(Rid, 2013). 일각에서 사이버 위협에 대한 회의론이 지속적으로 제기되는 것도 바로 이러한 이유 때문이다.

코펜하겐 학파의 시각에서 사이버 안보를 탐구한 한센과 니쎈바움도 이를 지적하고 있는데, 그들에 의하면 안보화 시각으로 본 사이버 안보담론은 세 가지 특징을 갖는다. 첫째, 사이버 안보담론은 과장스럽게 느껴질 정도로 아직 발생하지 않은, 많은 종류의 다차원적인 사이버 재난과 그 규모 및 파장을 부각시킨다는 점에서 '하이퍼 안보화(hypersecuritization)'의 성격을 갖는다. 둘째, 사이버 안보담론은 하이퍼 안보화의 시나리오를 더욱 실감나고 그럴듯하게 보이게 만들기 위해서 대중들의 '일상적인 안보관행(everyday security practices)', 즉 대중들의 경험, 느낌, 요구, 이익에 호소하는 경향이 강하다. 끝으로, 사이버 안보담론은 일반 대중에게 잘 알려지지 않은 비밀정보와 고도의 전문지식을 독점한 전문가들에 의해서 '기술전문적 담론(technical, expert discourse)'의 독자적 공간을 형성하는 방식으로 생산된다(Hansen and Nissenbaum, 2009).

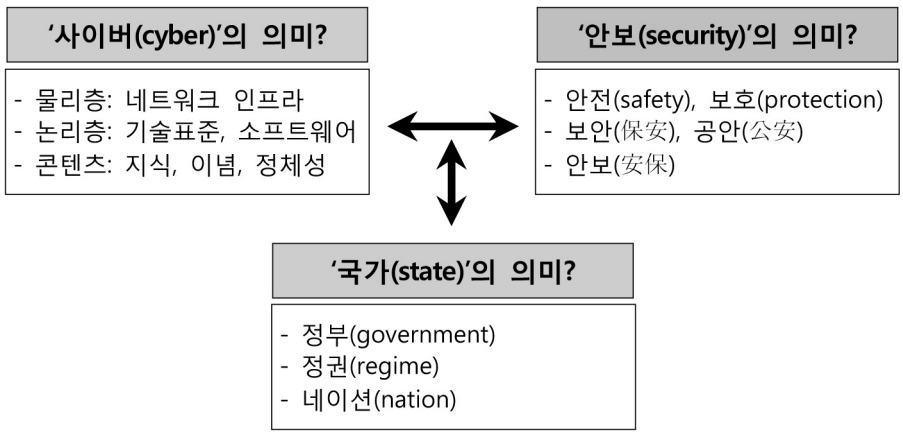
이러한 사이버 안보담론의 특성을 고려할 때, 이 분야에서는 사이버 위협의 '실체'를 논하는 것보다는 사이버 위협의 성격, 안보의 대상 및 주체 및 이러한 과정에서 파생하는 결과에 대해서 '말하는 것'이 더욱 더 중요할 수 있다. 이러한 맥락에서 로널드 디버트(Ronald Deibert)도 사이버 안보에서 중요한 것은 "어떤 의미에서 인터넷이 안보에 대한 위협으로 여겨지느냐, 누가 또는 무엇이 보호해야 할 대상으로 여겨지느냐, 이러한 위협에 대응해서 어떤 구체적인 정치적 조치가 필요하다고 여겨지느냐, 그리고 이상의 과정을 통해서 어떠한 유형의 세계질서가 부상하고 생산 및 재생산되느냐"의 문제라고 지적하고 있다(Deibert, 2002, 118). 요컨대, 사이버 안보 논의에서는 사이버 위협의 성격, 사이버 안보의 대상과 주체, 세계질서의 구성 등의 세 가지 논점을 중심으로 안보담론을 분석하는 것이 중요하다.

이러한 시각에서 보면 사이버 안보담론의 형성과정은 단순히 중립적 시도가 아니라 각기 입장에 따라서 다르게 구성될 수밖에 없는 정치적인 과정이며, 그렇기 때문에 힘 있는 자가 주도하는 권력정치임을 알 수 있다. 이렇게 보면 미국과 중국 사이에서 벌어지고 있는 사이버 갈등의 이면에는 사이버 공간의 안보담론을 선점하려는 경쟁이 자리 잡고 있다. 그렇다면 사이버 안보담론은 어떠한 과정을 거쳐서 구성되는가? 미 · 중 경쟁의 사례를 구체적으로 살펴보기 전에 보기 전에 먼저 사이버 안보라는 용어의 구성과정에 담긴 의미를 좀 더 구별하는 것이 필요하다.

이 글에서 다루는 사이버 안보에 해당하는 내용은 미국과 중국 및 한국에서 각기 다른 용어로 표현되어 왔다. 미국과 한국에서는 사이버 안보(cyber security)와 더불어 정보보안(information security), 정보보호(information protection), 컴퓨터 보안(computer security), 인터넷 보안(internet security), 네트워크 보안(network security) 등의 용어가 혼용된다. 중국에서 인터넷은 '互聯網(互联网)'으로 번역하지만, 인터넷, 네트워크, 사이버 등은 대체로 '網絡(网络)'이라고 번역하고,

'security'는 대체로 '안전(安全)'으로 번역한다. 최근 중국에서 가장 많이 쓰는 용어는 '인터넷 안전(網絡安全)'이다.[2] 그러나 안보화의 시각에서 볼 때 중요한 것은 단순한 용어 선택이 아니라 그 선택 과정의 밑에 깔려 있는 안보담론의 구성이다. 사실 '사이버,' '안보,' '국가'라고 하는 세 용어가 어떠한 방식으로 조합되어 현실을 지시하고 재구성하는 지침이 되느냐가 관건이다(〈그림-1〉 참조).

〈그림-1〉 사이버, 안보, 국가의 개념적 조합?



'사이버(cyber)'라는 접두어는 보통 정보통신기술 관련 행위를 포괄적으로 의미하는데, 대체적으로 네트워크 인프라의 물리적 층위, 소프트웨어나 기술표준 등의 논리적 층위, 지식 · 이념 · 정체성의 콘텐츠 층위 등의 세 층위를 지칭한다. 이러한 시각에서 볼 때, 사이버 안보는 1990년대 초반에는 하드웨어와 소프트웨어의 오작동으로부터 기인하는 컴퓨터 시스템의 장애방지나 인터넷이라는 물리망의 보호에 중점으로 둔 컴퓨터 보안, 정보보호, 네트워크 보안 등의 의미로 이해되었다. 그런데 2000년대 들어서면서 인터넷의 활용이 지구적으로 확산되면서 논리적 층위에 대한 보호가 각국의 주권적 관할권을 넘어서는 안보문제로 인식되기 시작했다. 2000년대 후반 이후 사이버 공간에서 벌어지는 정치 · 사회 · 문화적 활동의 중요성이 강조되면서 사이버 공간의 안전이나 안보로 관심이 넓어졌다. 특히 9.11 테러 이후 외부로부터 악의적이고 의도적인 테러의 공격으로부터 사이버 공간에서의 활동이나 그 기반이 되는 시스템과 지식정보를 보호하려는 정책적 목적이 커졌다.

'안보'라는 용어의 경우 영어에서는 주로 'security'라고 하지만, 이를 번역하는 경우에는 그 용례에 따라서 안전(安全, safety)이나 보호(保護, protection) 등과 같은 중립적인 뉘앙스의 용어로 번역되기도 하고, 경우에 따라서는 국내정치나 치안의 뉘앙스를 갖는 보안(保安)이나 공안(公安)이라는 말로 번역되기도 하며, 대외적인 함의를 가질 때 주로 안보(安保)라고 번역된다. 앞서의 네트워크의 세 층위 중에서

2) 중국에서 사용되는 사이버 안보 관련 용어에 대해서는 王世伟(2012)를 참조하기 바란다.

물리적 층위나 논리적 층위에 해당하는 'security'를 논할 경우는 안전이나 보호, 그리고 경우에 따라서는 안보라고 번역하는 경우가 많고, 콘텐츠 층위의 'security'를 염두에 둘 때는 정치사회적 측면에서 이해된 보안이라고 번역되는 경향이 있다. 그런데 앞서 언급했듯이 최근 들어 사이버 안보의 문제를 단순한 시스템과 정보의 보호나 안전의 의미를 넘어서 좀 더 넓은 의미에서 이해하기 시작하면서 안보라는 말이 더 많이 사용되고 있다.

이러한 '사이버'와 '안보'가 조합되는 과정에 '국가(state)'의 개념을 넣어 보면, 이 글에서 주장하는 사이버 안보담론의 구성을 이해하는 데 도움이 된다. 사실 '국가안보'는 예로부터 (국제)정치학의 주요 관심사였는데, 그 안보담론의 구성방식에 따라서 각기 다르게 이해되어 왔다. 이 글의 주제인 사이버 안보에만 국한시켜서 보더라도, 'security'의 개념은 세 가지 차원의 국가 개념, 즉 '정부(government),' '정권(regime)', '네이션(nation)' 등과 만나서 다르게 구성될 가능성이 크다. '정부'와 만나면 다소 중립적인 안전(safety)이나 보호(protection)의 의미로, 사회(society)와 대립되는 의미에서 파악된 '국가'로서의 '정권'과 만나면 보안(保安)이나 공안(公安)의 의미로, 대외적 차원의 '네이션'과 만나면 안보(安保)의 의미로 구성되곤 한다. 물론 이러한 조합은 절대 고정적인 것은 아니고 다소 도식적일 우려를 무릅쓰고 단순화해 본 것이다. 특히 이러한 세 가지 조합은 객관적으로 존재하는 각기 다른 현실을 지칭하는 것이라기보다는, '국가' 행위자들의 의도에 따라 간주관적으로 구성되는 안보담론의 경쟁을 단면을 보여주는 것으로 이해해야 한다.

이렇게 상이한 안보담론이 가능하다는 것은 각기 다른 별개의 지시대상을 놓고 이에 대한 상이한 담론이 있다는 것이 아니라, 동일한 지시대상을 놓고 각기 다른 안보담론이 경쟁적으로 구성된다는 것을 의미한다. 게다가 이들 담론들은 서로 관련이 없는 별개의 현상으로서 따로따로 진행되는 것이 아니라, 상호성찰적으로 여타 담론을 의식하면서 구성된다(Hansen and Nissenbaum, 2009: 1163). 이렇게 사이버 안보의 개념은 개별적 지시대상, 위협, 정책대안, 세계질서에 대한 각기 다른 담론을 놓고 이익과 가치가 교차하는 지점에서 생산된다(Deibert, 2002). 다시 말해 국가안보, 정권안보, 사회안보, 개인안보, 네트워크 안보 중에서 무엇을 우선시하느냐에 따라서 사이버 안보의 성격이 달라지고, 위협의 대상이 물리적 인프라냐, 정보지식 자산이냐, 이념과 사상의 콘텐츠냐에 따라 사이버 안보를 보는 시각과 해법이 달라진다. 특히 이러한 사이버 안보의 성격은 국가, 정권, 사회, 기업, 개인 등과 같은 담론 형성의 주체와 관련해서 구체적인 정치적 함의를 획득한다. 사이버 안보화의 과정은 단지 '말싸움'으로 끝나는 것이 아니라 그 '말'을 통해서 구성될 미래의 방향을 놓고 벌이는 이익과 권력의 게임이기 때문이다.

이러한 양상은 사이버 안보 분야에서 벌어지는 미 · 중 경쟁에서의 안보담론의 차이로 나타난다. 다시 말해 사이버 안보의 미 · 중 경쟁은 새롭게 창발하는 사이버 안보의 현실에 대한 안보담론의 표준을 놓고 벌이는 안보화의 세계정치이다. 현재 미국과 중국 간에 벌어지는 논쟁점은 기본적으로 사이버 위협의 성격과 안보의 대상이 무엇이며 그 문제를 해결하는 주체가 누구인가를 보는 담론의 차이에서 비롯된다. 더 나아가 이러한 담론의 차이는 사이버 안보 분야에서 세계질서의 형성 과정에 대한 입장 차이로 표출되었다. 이러한 미 · 중 경쟁은 단순한 관념 차원의 경쟁이 아니라 이를 통해서 구성될 미래의 방향을 놓고 벌

이는 이익의 갈등이기도 하다. 다시 말해, 사이버 안보담론의 형성은 단순히 중립적 시도가 아니라 각기 입장에 따라서 자신의 이익에 맞추어 현실을 재구성하는 권력정치의 과정이라고 할 수 있다.

Ⅲ. 사이버 위협의 성격에 대한 인식

1. 미국의 '중국해커위협론'을 둘러싼 공방

2000년대 후반부터 미국 정부와 언론은 중국 해커들의 공격이 미국의 근간을 뒤흔드는 위협이라는, 소위 '중국해커위협론'을 펼쳤다.[3] 중국의 해커들이 중국 정부와 군의 지원받아서 미국의 물리적 인프라와 지식정보 자산을 심각하게 침해하고 있다는 것이었다. 예를 들어 미국 정부가 소위 '오로라 공격(Aurora attack)'이라고 명명한 2009년의 해킹 사건은 구글뿐만 아니라 아도비나 시스코 등과 같은 미국의 IT기업들을 목표로 하여 중국 해커들이 벌인 일이라는 것이다(Clark, 2011). 2010년 구글 사건 당시에도 중국의 해커들이 적극적인 역할을 한 것으로 알려졌다(Barboza, 2010). 이러한 안보담론은 미국의 인권 단체, 정부관리, 각계 전문가 등에 의해서 확산되었는데, 중국의 영토 내에 서버를 설치하거나 또는 이메일 서비스를 제공하고 검열기술을 판매하는 행위를 제한하자는 주장으로 나타났다(USAID, 2010).

2010년대에 들어서도 중국의 해커 공격에 대한 미국 측의 비난의 목소리가 높아지면서 미국과 중국 간의 사이버 갈등이 증폭되었다. 2013년 2월 미국의 컴퓨터 보안회사인 맨디언트는 76쪽에 걸친 보고서를 통해 그동안 간헐적으로 탐지된 중국군의 사이버 테러와 공격의 실태를 종합적이고 자세하게 파헤쳤다. 이들 공격은 정보통신 · 항공우주 · 행정 · 위성 · 통신 · 과학연구 · 컨설팅 분야에 집중되었으며, 주로 지적재산권과 연구개발의 내용을 훔치는 데 주안점을 두었다는 것이었다. 해킹 문제가 커지자 백악관 국가안보보좌관 토머스 도닐런(Thomas Donilon)은 중국에 해킹을 중단하라고 촉구하기도 했다. 맨디언트는 2014년에도 비슷한 내용의 보고서를 냈는데, 미국 정부의 요구에도 불구하고 중국이 지속적으로 해킹을 벌이고 있다는 내용을 담았다. 특히 이들 사이버 공격이 노린 것이 미국 기업들이 지적재산권을 가지고 있는 기술과 정보라는 사실을 심각하게 여겼다. 2014년 5월 미 법무부의 중국군 장교 기소에서도 중국의 해킹 공격이 미국의 정보통신 인프라에 집중해 있다고 지적했다. 2014년 7월 잭 루(Jack Lew) 미 재무장관도 중국의 해킹으로부터 헤지펀드와 투자자산회사의 사이버 보안 대책 마련에 적극 나서야 할 것

3) 중국 해커에 의한 공격에 대한 미국의 '피해자 담론'은 2000년대 후반 본격적으로 제기되었다. 이러한 미국의 안보 담론에 대해서는 Dahong(2005), US-China Economic and Security Review Commission(2009), Barboza(2010), Hvistendahl(2010), Clark(2011) 등을 참조하기 바란다.

이라고 강조했다(『조선일보』 2014/7/30).

이러한 미국의 비난에 대해서 중국 정부는 외교부 대변인 성명을 통해 미국이 주장하는 해커들의 공격은 국경을 넘어서 익명으로 발생하는 것으로 미국 측이 주장하는 해킹의 증거라는 것을 어떻게 확증할 수 있는지 모르겠다는 논조의 비판을 가했다. 중국군이 해커 공격의 배후라는 결론은 근거가 없다는 것이었다. 중국 외교부 부장인 양제츠(杨洁篪)도 "최근 해커공격 보도가 많이 나오고 있는데 그 중 다수가 중국을 지목하고 있다. 이러한 보도가 시선을 끌 수 있을지는 모르지만 논리가 맞지 않는 말이다. 사실 중국은 사이버 안보에 있어서는 약소단체에 속한다. 중국은 해커공격을 가장 많이 받는 나라 중 하나다. 중국 정부는 해커공격 행위를 반대하고 이미 유관 법률규정을 제정하여 명확히 금지하고 있다"는 주장을 펼쳤다(『环球网』, 2013/3/9).

이러한 와중에 터진 소위 '스노든 사건(또는 프리즘 사건)'은 중국의 주장에 명분을 실어 주었다. 2013년 6월 미국의 전직 CIA직원인 에드워드 스노든은, 미국 정부가 '프리즘'이라는 감시 프로그램을 이용해서 2009년부터 중국에 대해 수백 건의 해킹을 벌여왔다고 폭로했다. 중국 정부는 이러한 미국의 시도를 표리부동한 행위로 보고 비난의 목소리를 높였다. 예를 들어, 중국 국방부 대변인 경얜성(耿雁生)은 "미국이 중국 정부, 상업회사, 개인 등에 대해서 실행한 감시, 도청, 해킹은 충분히 미국의 허위성과 패도를 드러내고 있다. 우리는 앞으로 효과적인 조치를 취하여 사이버 안보 방어를 강화해 나갈 것"라고 말했다(『人民网』 2014/4/1).

중국의 주장에 의하면, 오히려 "미국이 스스로 해커의 공격으로부터 제일 피해를 보는 나라라는 인식을 조장하고 있다"는 것이었다(蔡翠红, 2012). 또한 "미국이 중국해커위협론을 조장하여 여론의 우위를 점해 중국의 사이버 군사기술의 발전을 압제하려 한다"고 했다. 또한 미국이 '중국해커위협론'을 유포하는 이면에는 경제무역 측면에서 중국 기업의 부상을 도전으로 인식하고 사이버 안보를 빌미로 하여 자기보호에 나선 미국 기업들과 미국 정부의 속내가 있다고 평가했다(周琪 · 汪晓风, 2013, 46). 미국은 "국제사회에서 인터넷을 둘러싸고 진행되는 일련의 문제들에 대하여 냉전진영의 논리를 조장하고 있는데, 이를 통하여 중국 해커의 위협을 제기하고 인터넷 심사 등을 이용하여 중국의 이미지에 손상을 주어 인위적으로 중국과 러시아를 세계 대다수 국가들과 대조되게 하고 있다"는 것이었다(『参考消息网』, 2014/1/03).

이러한 와중에 2014년 5월 20일에 미국은 중국에 대해서 맞불을 놓았다. 미 법무부는 펜실베니아 주 연방지방법원에 왕둥 등 중국 군부대 소속 장교 5명을 산업스파이와 기업비밀절취 등 6개 혐의로 기소했다. 미 법무부에 따르면 이들 5명은 웨스팅하우스와 US스틸 등 5개 기업과 미 철강노조의 컴퓨터를 해킹해서 피해 기업의 제품이나 재무구조에 대한 기밀 정보를 빼냈으며, 이로 인해 해당 기업과 경쟁 관계였던 중국 기업들이 큰 이익을 봤다고 주장했다. 에릭 홀더(Eric Holder) 미 법무장관은 "중국 군인에게 경제 스파이 혐의가 적용된 이번 사건은 해킹 혐의로 (외국)정부 관계자를 기소한 첫 사례"라며 "절취된 기업 비밀의 범위로 볼 때 이번 일은 중대하며 공세적으로 대응할 필요가 있다"고 강조했다(『전자신문』, 2014/6/15).

이에 대해 중국 정부는 이러한 조치가 "미국이 위선적이고 이중적인 기준을 적용하고 있다"는 사실을

보여주는 것이라고 주장하며 즉각적으로 반박했다(『동아일보』, 2014/5/27). 친강(秦剛) 중국 외교부 대변인은 "중국 장교들에 내려진 혐의는 미국이 의도적으로 조작한 것으로 국제관계를 지배하는 기본 규범을 심각하게 위반했다고 비판한 뒤 미국 당국은 즉시 실수를 수정하고 이런 주장을 철회"하라고 강조했다. 또한 친 대변인은 "사이버 안보 확립을 위해 양국이 [2013년] 4월 체결한 사이버 워킹그룹의 활동을 중단시키기로 결정했다"며 "미국은 즉각 기소를 철회하라"고 요구했다"(『동아일보』, 2014/5/27). 이러한 사태의 전개에 대해서 중국의 모 일간지는 '망기정인(枉己正人, 자기 자신은 바르지 않으면서 남을 바르게 하려 하다)는 표현까지 써가며, "미국의 패권주의가 작동하고 있다"고 비난하기도 했다(『环球网』, 2014/5/23).

2. 중국의 '미국기술패권경계론'과 그 여파

사이버 공방에 임하는 중국의 담론에는 정보통신기술 분야 미국의 기술패권과 이를 경계하는 의구심이 강하게 담겨 있었다. 특히 중국 정부는 미국 기업들이 제공하는 컴퓨터와 네트워크 장비의 보안문제를 우려했다. 인터넷 보안기술과 관련하여 중국이 미국 IT기업들에게 너무 많이 의존하고 있으며, 혹시라도 양국 간에 문제가 발생할 경우, 이들 기업들이 미국 편을 들 것이라는 걱정이었다. 사실 미국의 IT기업들은 사이버 공간으로 통하는 중요한 기술과 산업을 거의 독점했다. 예를 들어, 시스코는 네트워크 장비 분야에서, 퀄컴은 칩 제조 분야에서, 마이크로소프트는 운영체계 분야에서, 구글은 검색엔진 분야에서, 페이스북은 SNS(social networking service) 분야에서 모두 독점적인 위치에 차지하고 있었다. 중국은 일단 양국 간에 사이버 전쟁이 발발한다면 이들 기업들이 모두 미국 정부에 동원될 것이라고 보았다(鲁传颖, 2013).

2014년 5월 미 법무부가 해킹 혐의로 중국군 장교 5인을 기소한 사건은 미국의 기술패권에 대한 중국의 우려에 불을 붙였다. 구체적으로 중국 정부의 반발은 시중에 판매되는 미국 기업들의 IT제품과 서비스에 대해 '인터넷 안전검사'를 의무화하는 조치로 나타났다. 중국 정부의 보안 검사는 마이크로소프트와 IBM, 시스코, 애플 등에 집중되었다(『매일경제』 2014/5/23). 실제로 중국 정부는 보안강화 등을 이유로 공공기관용 PC에 마이크로소프트의 최신 윈도8 운영체계 사용을 금지시켰다. 당시 중국 언론은 외국산 운영체계를 사용하면 보안 문제가 발생할 수 있다는 우려 때문에 이런 결정이 내려졌다고 일제히 보도했다. 반면 당시 미국과 주요 외신들은 미국 정부가 중국군 현역 장교 5명을 사이버 스파이 혐의로 정식 기소한 것에 대한 보복이라는 해석을 내놓았다(『아시아경제』, 2014/7/29).

비슷한 맥락에서 중국 정부는 중국내 은행의 IBM서버를 중국산 서버로 대체할 것을 추진하기로 했다. 이러한 중국의 조치는 IBM이외에도 매킨지나 보스턴컨설팅 같은 미국 기업들에게도 영향을 미쳤는데, 무역기밀의 유출을 방지하기 위한 거래 단절 명령이 내려졌다(『环球网科技』, 2014/5/29). 2014년 7월에는 중국 당국이 반독점법 위반 혐의로 마이크로소프트에 대한 조사에 돌입했는데, 이러한 행보는 중

국산 소프트웨어 업체에 반사이득을 주는 효과를 낳았다. 특히 이 중 가장 주목받는 업체는 중국 최대의 서버 기업인 랑차오(浪潮)였다. 미국과의 사이버 갈등이 거세어지면서 중국 정부는 정부기관의 IBM서버 의존도를 낮추기 위해 자국 브랜드인 랑차오 서버로 교체해서 사용하도록 지시하기도 했다(『아주경제』, 2014/7/30).

이러한 문제와 관련해서는 미국의 반응도 별반 다르지 않았다. 2014년 6월 미국 정부도 자국 기술이 중국으로 유출될 수 있다는 국가안보의 문제를 우려해서 중국 기업인 레노버가 IBM의 x86서버 사업을 인수하는 것을 지연시켰다. 레노버가 IBM서버 사업부를 인수할 경우 펜타곤이 중국 해커의 공격으로부터 취약해 질 수 있다는 이유였다. 사실 미국 정부가 IBM-레노버 간 거래에 대해 우려를 표명한 것은 이것이 처음이 아니었다. IBM은 2005년에 자사 PC 사업부를 레노버에 매각했는데, 당시 익명의 미국 군 사이버 책임자는 공군에 공급된 레노버 노트북이 중국의 해킹에 노출돼 있다는 의혹을 제기했다. 결국 해당 노트북들은 반품됐고, 미국 제품으로 교체됐다(『지디넷코리아』, 2014/6/27).

가장 큰 쟁점은 역시 중국 내에서 60-80%의 점유율을 보이고 있는, 미국의 통신장비 업체 시스코였다. 2012년 말 현재 시스코는 금융업계에서 70% 이상의 점유율을 보이고 있으며, 해관, 공안, 무장경찰, 공상, 교육 등 정부기관들에서 50%의 점유율을 넘어섰고, 철도시스템에서 약 60%의 점유율을 차지했다. 민간항공, 공중 관제 백본 네트워크에서는 전부 시스코의 설비를 사용하고 있고, 공항, 부두, 항공에서 60% 이상을, 석유, 제조, 경공업, 담배 등 업계에서 60% 이상의 점유율을 차지하고 있다. 심지어 인터넷 업계에서도 중국 내 상위 20개 인터넷 기업들에서 시스코 제품이 차지하는 비율이 약 60%에 해당되고 방송국과 대중 매체 업계에서는 80% 이상이다. 인터넷랩의 창시자인 팡싱둥(方兴东)은, "시스코가 중국경제의 중추신경을 장악하고 있어 미국과 중국 간에 충돌이 발생하면 중국은 저항할 능력이 없을 것"이라고 지적했다(『新浪网』, 2012/11/27).

이러한 상황에서 '스노든 사건' 이후 시스코가 중국 정부의 견제를 더욱 많이 받게 되었다. 미국이 중국에서 도 · 감청 프로그램을 운용하며 시스코의 설비를 활용했다는 사실이 폭로된 것이 화근이었다. 중국 내 유관기관의 검증결과 시스코의 라우터 제품에 히든백도어를 삽입한 문제가 밝혀졌다. 그 무렵 미국 정부가 ZTE와 화웨이의 설비 구매를 금지한다고 발표한 사건도 중국 정부와 기업들이 노골적으로 시스코 장비를 기피하는 경향을 부추겼다(『环球网科技』 2014/5/29). 시스코 내부 사정에 정통한 인사에 의하면, "최근 상하이유니콤, 광둥모바일, 그리고 시스코와 오랫동안 거래한 차이나텔레콤이 잇달아 시스코의 설비를 다른 제품으로 교체하기 시작했다"고 한다(Economy Insight, 2014/1/1).

한편 중국 관영 CCTV는 2014년 7월 11일 애플의 모바일 운영체계 iOS-7의 '자주 가는 위치(frequent location)' 기능이 중국의 경제상황이나 국가기밀정보에까지 접근할 수 있다며 "국가안보에 위협적 존재"라고 주장했다. 중국 공안부 직속 중국인민공안대 인터넷보안연구소장 마딩(馬丁)에 의하면, "이 기능이 매우 민감한 정보를 모으는 데 쓰일 수 있으며 애플이 마음만 먹으면 주요 정치인이나 언론인 등의 위치와 소재를 파악할 수 있다"고 주장했다. 이러한 주장들은 중국이 미국 기업들의 중국시장 잠식을 견제하려 한다는 미국 측의 해석을 낳았다. 예를 들어, 월스트리트저널은 "사이버 해킹과 관련된

미국 정부의 문제 제기에 대한 중국 정부의 보복 신호"라고 보도했다(『서울경제』, 2014/7/13).

미 경제 주간지 블룸버그에 의하면, 중국 정부는 2014년 8월 해킹과 사이버 범죄를 둘러싼 중국과 미국 간 긴장이 고조되는 가운데 정부 조달 품목 목록에서 애플의 아이패드, 아이패드 미니, 맥북 에어, 맥북 프로 등 총 10개 모델을 제외했다. 중국 조달 당국은 최근 백신 소프트웨어 업체인 시만텍, 카스퍼스키 제품 구매도 중지했고, 마이크로소프트도 에너지 효율성이 있는 컴퓨터 제품군 정부 조달 목록에서 제외됐다. 블룸버그는 이와 같은 중국 정부의 해외 기업에 대한 견제가 스노든 사건과 미 법무부의 중국군 장교 5명 기소 사건 이후 가열된 중국과 미국의 사이버 갈등과 밀접히 연관된 것으로 해석했다(『뉴시스』, 2014/8/07).

이러한 일련의 사태에 대한 논평을 요청받은 중국 외교부 대변인 친강(秦剛)은 주장하길, "인터넷 정보화 시대에서 인터넷 안전, 정보안전은 국가안전의 중요한 구성부분이다. 최근 중국 정부의 유관 부처에서 관련된 정책은 연구 중에 있는 것인데 인터넷 정보안전을 보다 강화해 나갈 것이다. 우리는 대외개방정책을 고수하고 있고 계속하여 해외기업들의 중국투자와 경영을 환영하며 앞으로도 적극적으로 해외와의 협력을 강화해 나갈 것이다. 그러나 그것이 외국기업 혹은 중외합자기업이라 할지라도 중국의 법률과 규정을 존중하는 것이 중요한 전제가 되어야 하고 중국의 국가이익과 국가안전에 부합되어야 한다"고 말했다(『新华网』, 2014/5/28). 친 대변인의 이러한 언급은 컴퓨터와 사이버 보안기술을 둘러싼 미 · 중 논란이 단순한 기술과 산업의 문제가 아니라 이 분야의 정책과 제도의 표준으로 연결된다는 중국 정부의 인식을 보여준다.

Ⅳ. 사이버 안보의 대상과 주체에 대한 담론

1. 네트워크 안보와 사이버 전쟁의 담론

사이버 안보의 대상과 주체와 관련하여 미국의 담론은 무엇보다도 미국 내 뿐만 아니라 글로벌 차원의 물리적 네트워크 인프라의 안정성을 확보하는 데 주 관심을 둔다. 사실 미국은 사이버 공격을 감행할 수 있는 자원과 기술을 가장 많이 보유하고 있는 나라이지만, 사이버 공격을 받을 경우 가장 많은 피해를 볼 수밖에 없는 나라이기도 하다. 다시 말해, 미국은 세계 어느 나라보다도 발달된 정보 인프라를 구비하고 있고, 국가 발전과 운영에 있어 이러한 인프라에 대한 의존도가 높기 때문에 사이버 공격에 대한 취약성이 지극히 높은 국가이다. 따라서 전통적 군사력에서 열세인 국가들이 미국을 상대로 하여 사이버 공간에서 비대칭적 공격을 감행할 유인이 높은 것이 사실이다. 이러한 맥락에서 물리적 네트워크 자체를 보호하는 것이 미국의 큰 관심사일 수밖에 없다.

이러한 미국의 담론은 어느 기관이 대내적으로 보유한 데이터나 정보의 안전을 보장하는 것뿐만 아니라 상업적 목적에서 이루어지는 인터넷 상거래의 안전성 확보를 문제시한다. 네트워크 안보의 담론은 정보흐름의 장애를 줄이고 속도를 향상시키는 데 초점을 두며, 컴퓨터 시스템에 대한 불법침입, 컴퓨터 바이러스의 악의적 사용의 방지를 목적으로 한다. 생산과 자본이 지구화되는 상황에서 안전한 전자상거래 환경의 확보는 세계 패권국으로서 미국의 관심사가 아닐 수 없다. 미국은 사이버 공간을 초국경적으로 정보가 유통되는 글로벌 공간으로 상정하고 이러한 사이버 공간의 자유주의적 질서 구축에 방해가 되는 요인을 제거하기 위해서 노력해왔다. 이러한 미국의 안보담론은 후술할 세계질서의 형성과정에서 나타나는 미국의 입장과도 맥이 닿는다(Deibert, 2002, 130-131).

이러한 네트워크 안보 담론의 이면에는 인터넷 자유와 프라이버시의 보호를 주 내용으로 하는 개인안보에 대한 관심이 존재한다. 정치적 관점에서 본 미국의 사이버 안보담론은 개방된 공간으로서 인터넷 상에서의 개인의 권리와 표현의 자유, 프라이버시 등의 가치를 표방하고 이에 대한 침해를 경계하는 내용을 담고 있다. 특히 국가와 기업에 의한 프라이버시의 침해 가능성과 이러한 과정에서 개인의 권리와 인권의 보호를 중요시했으며 이러한 담론은 실제로 미국 내에서 엄격한 프라이버시를 보호하는 정책적 · 법적 대응으로 나타난 바 있다. 후술할 구글 사건이 터질 무렵인 2010년 1월 21일 행한 힐러리 클린턴 미 국무장관의 연설은 미국이 추구하는 인터넷 자유의 가치를 잘 설명했다. 클린턴 장관에 의하면, 미국은 정치적 동기에서 이루어지는 규제에 반대하고 인터넷을 통해서 시민들의 표현의 자유를 지원할 것이라고 밝혔다(Clinton, 2010).

그러나 이러한 네트워크 안보와 개인안보 담론의 기저에서 '네이션' 차원에서 보는 군사담론이 형성되어 왔음도 간과해서는 안 된다. 이는 국토안보와 군사전략의 차원에서 파악된 네트워크 안보에 대한 논의로 통한다. 1990년대 중후반 이래 군사전략의 공간으로서 사이버 공간의 사용가능성이 거론되면서 비국가 행위자들이나 테러리스트에 의한 사이버 테러와 전쟁이 심각한 위협으로 인식되어 왔다. 이는 정보화 시대의 새로운 전쟁의 양식에 대한 논의와 맞물리면서 군사전략론의 주요 논제로서 다루어졌다(Arquilla and Ronfeldt, 1996; 2001; Libicki, 2009). 이러한 과정에서 인터넷은 미국에 도전하는 국가 행위자들이 동원할 수 있는 공격의 매개체로 평가되었는데, 특히 러시아, 중국 등이 이러한 사이버 공간에서의 전쟁을 준비하는데 경주하고 있다고 파악되었다. 앞서 언급한 바와 같이 '중국해커위협론'을 강조하는 미국의 담론은 바로 이러한 사이버 전쟁 담론과 연결된다.

이러한 사이버 전쟁 담론은 미국 내에서 컴퓨터와 정보 안보를 보장하는 정책적 대응과 기구 설치 및 예산배분 등으로 이어졌다. 그 중에서 미국의 사이버 전쟁 담론이 반영된 대표적 사례 중의 하나는 오바마 정부 출범 이후 2009년에 이루어진 '사이버 사령부'의 창설이다. 2010년 미국 국방성 QDR(Quadrennial Defense Review)에도 이러한 사이버 안보전략이 구체화되면서 반영되었다. 2011년 7월에는 미 국방부의 '사이버 공간 작전수행을 위한 전략(Strategy for Operating in Cyberspace)'이 발표되었다. 2012년 5월에는 미 국방부가 'Plan X' 프로젝트를 발표했는데, 이 프로젝트는 미 국방부의 사이버 전략 증강계획을 위한 일환으로 2017년까지 1조 8,000억 원의 예산을 투입

하여 사이버전 실전에 활용할 수 있는 사이버 무기 개발을 추진하고, 전세계 컴퓨터 도메인과 서버를 표시할 수 있는 디지털 전장지도를 개발한다는 것이었다. 2012년 10월에는 미 국보안보부가 사이버 예비군 창설을 발표했으며, 2013년의 국방수권법(National Defense Authorization Act)에서는 사이버 공간에서 군의 위상과 역할, 권한을 강화하였다. 2014년에는 사이버 안보 강화를 위하여 국방부와 국토안보부를 비롯하여 전 기관의 사이버 안보 관련 예산이 크게 증액되었다.

이러한 일련의 전개과정에서 한 가지 주목할 것은 2010년대에 들어서면서 사이버 안보에 대한 미국의 태도가 점차로 '방어의 개념'으로부터 '공격의 개념'으로 변화했다는 사실이다. 방어를 위해서라면 선제공격의 개념을 도입할 수 있다는 미국 정부의 결연한 의지를 보여주는 사례는, 사이버 공격에 대해서는 미사일을 발사해서라도 강력히 대응하겠다는 2012년 5월 미 국방부의 발표이다. 그러나 앞서 지적한 것처럼 도대체 '누구'를 향해서 미사일 공격을 가하겠다는 것인지 의문으로 남을 수밖에 없었다. 사이버 안보의 속성상 공격을 가할 위험이 있는 특정 대상을 선정하여 미리 억지하거나 대비한다는 것이 쉬운 일은 아니기 때문이다. 한편, 2012년 6월 당시 미 국방장관 지명자였던 리언 패네타는 상원군사위원회 청문회에서도 미국에 대한 '제2의 진주만 공격'이라는 비유를 사용해가며 미국의 정부, 전력, 금융 등 기간 시설에 대한 사이버 공격이 될 수 있다고 경종을 울리는 증언을 한 바 있다.

2. 정치적 정권안보와 정책적 권리의 담론

이에 비해 중국이 사이버 안보담론의 구성에서 중시하는 대상은 '정치안전' 즉 정권안보의 확보이다. 중국 인터넷정보판공실 부주임 왕슈쥔(王秀军)에 따르면, 현재 중국이 "관심을 가지고 있는 인터넷 안전은 의식형태의 안전, 데이터 안전, 기술안전, 응용안전, 자본안전, 루트 안전 등이 포함되는데... 총괄적으로 보면 정치안전이 근본이 된다"고 하였다. 그에 의하면, "현재, 외부세력들이 인터넷을 [중국에] 대한 침입과 파괴의 주요 루트로 삼는데 인터넷 자유라는 미명으로 계속하여 [중국에] 대한 공격을 가하면서 [중국의] 사회안정과 국가안전을 파괴하려 시도하고 있다"는 것이다. 특히 "인터넷 신기술은 일부 인사들의 새로운 전파도구로 사용되어 불법정보와 유해정보"를 퍼뜨리게 하고 있으며, "인터넷상의 의식형태 영역에 대한 침투와 반(反)침투의 투쟁에서 승리를 취득하느냐의 여부"는 많은 부분에서 중국의 미래에 중요하다는 것이다(『大公网』, 2014/5/18).

이러한 시각에서 보면, 중국에게 있어서 미국이 주장하는 인터넷 자유란 보편적 가치라기보다는 미국이 자국의 패권을 투영하는 수단에 불과하다. 중국의 유엔주재 특명전권군축대사 왕췬(王群)은 말하길, "인터넷은 이미 미국이 의식형태와 가치관 전파 및 정권교체를 실행하는 중요한 도구가 되었다. 특히 미국이 일부분의 반(反) 중국세력과 중국의 민족분열세력들에 자금을 지원해주어 백도어 프로그램을 개발하고 사용하게 하여 중국의 사회모순과 민족관계의 부정적 측면을 주객관적으로 확대 해석한 것은 중국의 국가안보에 위협으로 되고 있다. 미 · 중이 '인터넷 자유'를 두고 벌이는 게임은 양국의 의식형태와 가치관

의 분쟁이 사이버 공간으로 연장된 것이고 양국이 주권과 인권, 주권과 안보를 두고 벌이는 분쟁이 정보화 시대에 반영된 것"이라고 했다(奕文莉, 2012, 30-31).

이러한 의식과 관련하여 2014년 7월 16일 브라질 국회에서 시진핑 주석이 행한 연설이 주는 시사점이 크다. 시 주석은, "비록 인터넷이 고도의 글로벌화라는 특징을 가지고 있지만 각 국가의 정보영역의 주권이익은 침범 당해서는 안 되며, 인터넷 기술이 발달하더라도 타국의 정보 주권을 침범해서는 안 된다"고 주장했다. 시 주석은 과거 러시아 방문 당시 제기했던 '신발론'도 재차 언급하며 말하길, "신발이 발에 맞는지 안 맞는지는 신발을 신은 사람만이 알 수 있는 것"이라고 말했다. 그는 "세계에 그 어떤 만병통치약이 없고 어느 곳에서도 다 옳은 진리는 없으며, 각국은 자신의 국정 상황에 맞는 발전의 길을 걸어야 한다"고 강조했다. 이는 중국의 인권 문제나 주변국과의 영토분쟁 등과 관련한 미국이나 서방의 간섭에 대해 경고하고, 2013-14년에 걸쳐서 미국과 사이버 갈등을 겪고 있는 상황을 지적한 것으로 해석됐다(『아주경제』, 2014/7/17).

이러한 중국의 사이버 안보에 대한 인식은 인터넷을 검열하고 규제하는 정책적 자율성을 정당화하는 데 담론적 자원으로서 활용된다. 여기서 중국이 중시하는 것은 개인 차원의 인터넷 자유라기보다는 국가 차원의 인터넷 자유로서 이는 인터넷에 대한 규제와 검열을 정당화하는데 원용된다. 왕정핑(王正平)과 쉬테광(徐铁光)의 설명에 의하면, "일개 국가의 사이버에 대한 기본요구에는 인터넷 자유와 사이버 안보가 포함되어 있다. 국가 인터넷 자유에는 자국 인터넷에 대한 자유적인 관리가 포함됨으로 타국의 간섭을 받으면 안 된다. 한 나라의 사이버 안보를 수호하기 위해서는 그 나라는 인터넷심사를 진행할 필요가 있다. 중국과 일부 개도국의 인터넷 심사정책을 서방 국가들에서 지적하는 것은 그들 국가와 국민들의 기본수요를 침해하는 것"이라고 한다(王正平 · 徐铁光, 2011, 107).

이러한 인식은 중국 시장에 진출한 미국 IT기업들에 대한 규제라는 형태로 나타났다. 중국 정부는 인터넷상의 불건전하고 유해한 정보를 차단하고 검열하는 것은 주권국가의 정부가 취할 수 있는 법적 권리이며, 인터넷 자유의 논리를 내세워 중국의 정책과 제도를 비판하는 것은 주권국가에 대한 내정간섭이라는 것이었다. 이러한 맥락에서 중국 정부는 중국 내의 인터넷 서비스 제공자들이 자체 검열을 수행하도록 요구했다. 예를 들어, 마이크로소프트는 중국이 제시하는 인터넷과 관련된 정책이나 기타 제도의 표준을 수용해야만 했다. 시스코, 야후 등과 같은 미국의 IT기업들은 중국 정부가 시장접근을 위한 조건으로서 제시한 자체검열의 정책을 수용하고 나서야 중국 시장에 진출할 수 있었다. 구글도 2006년에 중국 시장에 진출할 당시 여타 미국의 IT기업들과 마찬가지로 정치적으로 민감한 용어들을 자체 검열하라는 중국 정부의 요구를 수용하였다(Hughes, 2010, 20).

이러한 중국의 인터넷 검열 정책에 대한 미국 IT기업들의 반발이 없을 수 없었다. 2010년 1월 12일 구글은 자사 이메일 서비스에 대한 해킹과 지적재산권 침해를 이유로 중국 시장에서 철수하겠다고 발표하면서, 중국과 미국뿐만 아니라 국제사회에서 많은 논란을 일으켰다(Hughes, 2010). 이러한 일련의 사태에 대해 중국 정부는 국제적인 인터넷 기업이 중국 내에서 기업 활동을 하려면 중국의 국내법을 따라야 한다는 주장을 폈다. 구글 사건이 주는 의미는, 단순히 미국의 IT기업과 중국 정부의 갈등이라는 차원을

넘어서, 양국의 정치경제 모델의 차이를 보여주었다는 데 있다. 이 사건에서 나타난 구글의 행보가 미국 실리콘밸리에 기원을 두는 인터넷 자유 담론을 바탕에 깔고 있다면, 이를 견제한 중국 정부의 태도는 중국의 정치체제에 친화적인 정책적 주권담론에 기반을 둔다(김상배, 2012).

이렇듯 중국에서 사이버 공간은 국가 차원의 네트워크 인프라 위에 구축된 것으로 국가주권의 관할권 하에 있는 것으로 간주되었다. 다시 말해, 국가주권은 국가 고유의 권리로서 그 관할권의 범위는 인류활동 공간의 확장과 함께 육지에서 해양으로, 그리고 하늘로 연장되었으며, 사이버 공간에까지 확장되어 사이버 주권을 논할 수 있게 되었다는 것이다. 중국의 담론체계 내에서 "주권국가는 사이버 공간의 발전을 추진하고 사이버 공간의 안정을 수호하며 사이버 공간의 안보를 보호할 책임이 있음은 물론 법에 근거하여 사이버 공간에 대한 관리를 행사하고 사이버 범죄를 단속하고 정보 프라이버시를 보호할 권력을 가진다. 따라서 사이버 공간은 '글로벌 공공영역'이 아닌 국가주권의 중요한 부분"이라는 것이다(鲁传颖, 2013, 49). 이러한 연속선상에서 중국은 국내 통치를 정당화하고 대외적 압력에 대항하는 과정에서 급속한 경제적 성장과 함께 형성된 중국 국민들의 자부심과 사이버 민족주의 담론을 결합시키려는 노력을 벌였다(Chao, 2005; Zakaria, 2010).

Ⅴ. 사이버 세계질서의 구성에 대한 입장

사이버 위협에 대한 인식과 이에 대응하는 정책적 대응양식의 선택은 이 분야의 세계질서를 구성하는 담론으로 연결된다. 1990년대 후반부터 펼쳐진 역사를 보면, 사이버 안보 분야의 세계질서 형성은 그 자체가 독립적 이슈로서 다루어졌다기보다는, 넓은 의미에서 본 인터넷 거버넌스 분야 질서형성의 일부로서 논의되어 왔다(Mueller, 2010; DeNardis, 2013). 아직까지 사이버 안보 거버넌스 분야에서 규범, 법, 사이버 교전의 규칙을 어떻게 정할지, 사이버 행위에 대해서 어떠한 기존규정을 적용할지에 대한 합의기반은 마련되지 않고 있다. 마찬가지로 이 분야에서 미국과 중국의 대결구도도 명시적인 차이로 드러났다고 평가하기에는 다소 이르다. 그럼에도 양국의 안보담론의 차이가 이 분야의 세계질서를 구성하는 과정에서 투영되는 양상은 발견할 수 있다. 이러한 구도는 대략 '다중이해당사자주의(multistakeholderism)'와 '정부간주의(inter-governmentalism)'로 대별해서 볼 수 있다.

현재 우리가 사용하는 인터넷의 기본골격은 국제기구의 장에서 정부 대표들의 합의에 의해서 이루어진 것이 아니라 시민사회, 인터넷 전문가들과 민간사업자, 학계, 국제기구 전문가들이 자율적으로 구축한 거버넌스 메커니즘을 통해서 이루어졌다. 특히 미국에 활동적 기반을 두는 다양한 이해당사자들의 주도로 구축되어 왔다. 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 참

여하는 '다중이해당사자주의'의 실험대였다. 그런데 이러한 모델은 인터넷 전문가들이나 민간 행위자들이 전면에 나서는 모습으로 보이지만, 실상은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판으로부터 자유롭지 못했다(Mueller, 2002).

이러한 기존의 인터넷 거버넌스 모델에 대해서 최근 개도국들이 반론을 제기하고 있다. 개도국들은 인터넷 분야에서 '다중이해당사자주의'를 바탕으로 한 미국의 패권을 견제하기 위해서는 모든 국가들이 참여하는 전통적인 국제기구의 틀을 활용해야 한다고 주장한다. 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(Mueller, 2010). 특히 이러한 움직임은 인터넷 초창기에는 상대적으로 뒤로 물러서 있던 국가 행위자들이 인터넷 거버넌스에서 고유한 활동영역, 예를 들어 글로벌 정보격차나 사이버 안보 등을 찾아가는 과정과 맞물렸다. 특히 인터넷 거버넌스의 운영 과정에 국가 행위자들의 영토주권이 좀 더 적극적으로 인정되어야 한다는 것이다(김의영 · 이영음, 2008; Cowhey and Mueller, 2009).

최근 유엔과 같은 전통적인 국제기구들이 인터넷 거버넌스 분야에 진출하는 현상은 이러한 맥락에서 이해할 수 있다. 예를 들어, 전통적으로 전기통신 분야의 국제기구로 활동해온 유엔 산하의 ITU(International Telecommunication Union)가 민첩하게 움직이고 있다. ITU가 주도하여 2003년에 제네바와 2005년에 튀니스에서 두 차례에 걸쳐서 열린 바 있는 정보사회세계정상회의(World Summit on the Information Society, WSIS)가 그 대표적인 사례이다. 기존의 인터넷 거버넌스 이슈에 더불어 글로벌 정보격차 해소와 기타 문화적, 규범적 차원의 문제가 새로운 국제적 이슈로서 제기되었으며, 사이버 안보는 여러 가지 이슈 트랙 중의 하나로서 계속 논의되었다.

선진국 정부들 간 협의체의 틀을 기반으로 하여 열린 사이버공간총회에도 주목할 필요가 있다. 사이버공간총회는 사이버 공간의 안보 문제와 기타 관련 의제들을 논의하기 위해서 2011년 영국의 런던에서 첫 총회가 열렸다. 2012년의 헝가리의 부다페스트에서 총회를 가진 후, 2013년 10월에는 서울에서 제3차 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.

앞서의 국제기구와는 성격을 달리하지만, 지역 다자안보기구 차원에서 사이버 안보에 대한 대책을 강구하는 움직임도 주목할 필요가 있는데, 북대서양조약기구(NATO) CCDCOE(Cooperative Cyber Defence Centre of Excellence)가 2013년 3월 발표한 사이버 전쟁의 교전수칙인, 소위 '탈린 매뉴얼(Tallinn Manual)'이 대표적인 사례이다. 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 되어 NATO 회원국의 전문가들이 참여하여 러시아에 대응하는 성격을 띰으로

써 균형 잡힌 시각보다는 러시아나 중국 등이 배제된 채 미국 중심의 시각에 반영된 결과라는 비판이 제기된다.

이상의 복합적 구도를 염두에 두고 사이버 안보의 세계질서 형성을 둘러싸고 벌어지는 미국과 중국의 담론경쟁을 이해할 수 있다. 이러한 미 · 중 경쟁의 구도는, 좀 더 넓게 보면, 미국과 영국이 주도하는 서방 진영을 한편으로 하고, 러시아와 중국을 중심으로 한 개도국 진영을 다른 한편으로 하는 두 개의 진영 구도로 이해할 수 있다. 사이버 안보의 세계질서 형성과 관련하여 두 진영은 극명한 입장 차이를 보이고 있다. 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. 이러한 입장 차이는 최근 러시아와 중국 등이 제기한 다음과 같은 세 가지 사례에서 드러난 바 있다.

첫 번째 사례는 2011년 9월 22일 52개 국가의 정보기관 지도부가 러시아 예카테린부르크에서 모여서 개최한 '제2차 고위급 안보회의'에서 러시아가 제안한 ICIS(International Convention on Information Security)이다. 이에 앞서 9월 12일에는 러시아, 중국, 타지키스탄, 우즈베키스탄 4개국의 유엔대표들은 66차 유엔총회에서 ICIS의 초안을 제출한 바 있다. ICIS는 가입국의 정보보안을 확보하고 평화와 협력, 조화가 실현되는 정보공간을 조성하기 위해 가입국 간 협력의 법적 · 조직적 근거를 확보하는 것을 목적으로 하였다. 또한 인터넷에 대한 회원국의 주권을 보장하고 안정된 글로벌 사이버 안보 문화를 형성해야 한다고 강조했다. 아울러 기존의 정치, 역사, 문화적 특수성에 대한 존중의 입장을 표명하였는데, 이는 사이버 안보의 문제에 대한 러시아와 중국 등의 입장을 반영하는 것이었다(국가정보보호백서, 2012). 당시 러시아 외교부는 "우리가 먼저 선제적으로 대응하여 서방의 수중에서 주도권을 뺏어왔다. 전 세계는 우리가 제정한 규칙에 대하여 논의하게 될 것이고 영국은 대회의[4] 의제를 바꿀 수밖에 없을 것"이라고 논평했다(『参考消息网』 2011/11/02).

두 번째 사례는 2012년 12월 두바이에서 열린 WCIT(World Conference on International Telecommunication)에서 시도된 ITR(International Telecommunications Regulation)의 개정 과정에서 드러난 서방 진영과 개도국 진영의 대립이다. ITR은 전기통신 업무의 일반 원칙과 규정을 담고 있었는데, 그 내용이 너무 포괄적이고 모호해서 오랫동안 유명무실한 문서로만 남아 있었다. 게다가 ITR은 회원국들로 하여금 자신들의 사정에 맞추어 규제정책을 추진할 재량권을 너무 많이 부여하고 있었기 때문에 급변하는 기술환경을 따라잡기에는 미흡하다는 지적이 선진국들을 중심으로 제기되었다. 이러한 맥락에서 2012년 WCIT에서 ITR의 폐기를 주장하는 선진국들의 입장과 ITR의 개정과 강화를 주장하는 개도국들의 입장이 대립하는 양상이 나타났다. 이러한 과정에서 개도국들은 ITR을 통해 개별 국

4) 2011년 영국 런던에서 벌인 사이버공간총회를 의미한다.

가 차원의 규제정책의 기조를 유지하려 했는데, 특히 인터넷에 대한 규제권한을 확보하려 했다(강하연, 2013, 102-105).

세 번째 사례는 2013년 6월 유엔 군축 및 국제안보 위원회 산하 정보보안 관련 정부전문가그룹(GGE, Group of Governmental Experts)에서 합의해서 도출한 최종 권고안이다. 이 권고안은 1998년 러시아가 제안했는데, 미국은 처음부터 러시아의 제안에 대해 동조하지 않았고, 이후로도 소극적으로 자세로 사이버 안보 관련 국제협력에 대응해 왔었다. 이후 2004년부터는 정부전문가그룹(GGE)의 포맷을 빌어 국제안보 차원에서 사이버 안보 문제에 대한 논의가 진행되어 왔다. 기존 회의에서는 인터넷의 국가통제를 강조하는 중국과 이에 반대하는 미국이 극명히 대립했었으나 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(장규현 · 임종인, 2014).

이상의 내용에서 엿볼 수 있는 사이버 안보 분야에서 벌어지는 미 · 중 경쟁은 세계질서의 미래를 놓고 벌이는 세 가지 차원의 경합이 복합적으로 나타나는 일종의 담론표준경쟁이다. 먼저 눈에 띄는 것은 사이버 공간에서는 여전히 전통적인 국가 행위자들끼리의 경합이 발견되는데, 미국과 서방 선진국들이 주도하는 패권의 표준과 러시아 및 중국과 여타 개도국들이 제기하는 대항의 표준이 맞선다. 여기에 이해당사자들이 형성해온 민간 표준과 국가 행위자들이 주도하는 국가 표준의 경합이 중첩된다. 이러한 표준경쟁의 가장 상위에 겹쳐서 자리 잡은 것은 초국적으로 형성되는 글로벌 거버넌스의 표준과 전통적인 국제기구의 표준이 경합하는 양상이다. 이러한 세 층위의 담론표준경쟁의 구도에서 대체로 미국이 전자의 논리를 취한다면 중국은 후자의 논리에 기반을 두고 있다(김상배, 2012).

Ⅵ. 맺음말

이 글은 최근 동아시아 지역뿐만 아니라 글로벌 차원에서도 관심이 집중되고 있는 사이버 안보 분야의 미중관계를 다루었다. 최근 쟁점이 되고 있는 사이버 안보의 문제는 사이버 테러와 공격 및 방어의 문제일 뿐만 아니라 사이버 공간의 새로운 질서와 국내외 정책 및 규범 형성을 놓고 벌이는 제도화와 담론형성의 문제로서 국제정치학의 분야에서도 중요한 연구주제로서 주목받고 있다. 특히 현재 양국이 수행하고 있는 사이버 공격과 방어의 양상에 대한 객관적 실체가 아직 드러나지 않은 상황에서도 사이버 안보의 문제는 21세기 세계패권을 놓고 벌이는 양국 관계의 핵심 현안으로 이해되고 있다.

이러한 문제의식을 바탕으로 이 글은 안보화 이론의 시각에서 사이버 안보의 미중관계를 이론적 · 경험적으로 조명하였다. 이러한 시각에서 볼 때 현재 사이버 안보 분야에서 벌이는 미국과 중국의 경쟁은 사이버 위협의 성격이 무엇이고, 안보의 대상과 주체가 무엇인지에 대한 담론형성을 둘러싸고 벌어지고 있다. 이러한 담론경쟁은 양국의 국내제도뿐만 아니라 세계질서의 구성과정에도 투영된다. 사이버 안보의

세계정치를 보는 미국과 중국의 입장 차이는 바로 이러한 사이버 안보화의 차이에서 비롯된다. 현재 사이버 안보 분야에서 드러나는 미 · 중 양국의 차이는 다음과 같은 세 가지 차원에서 대비된다.

첫째, 사이버 위협의 성격에 대한 인식이라는 점에서 미국은 중국 정부의 비호를 받는 중국 해커들의 공격을 가장 큰 위협으로서 본다. 이들 공격은 정보통신 · 항공우주 · 행정 · 위성 · 통신 · 과학연구 · 컨설팅 분야에 집중되고 있으며, 주로 미국이 보유한 지적재산권과 연구개발의 내용을 훔치는 데 주안점을 두는 것으로 인식한다. 이에 비해, 중국은 인터넷과 정보통신기술 분야에서 미국 IT기업들이 장악하고 있는 기술패권을 가장 큰 위협으로 보고 있다. 특히 컴퓨터 운영체계와 네트워크 장비 보안기술과 관련하여 중국이 미국 기업들에게 너무 많이 의존하고 있어, 혹시라도 양국 간에 문제가 발생할 경우 이들 IT기업들이 미국 편을 들 것을 우려한다.

둘째, 사이버 안보의 대상과 주체라는 점에서 미국의 담론은 주로 물리적 네트워크 인프라의 안정성 확보와 개인의 프라이버시 및 인터넷 자유의 보호에 주력한다. 2010년대에 들어서는 테러 집단이나 비국가 행위자들이 도발하는 사이버 테러와 공격에 대비하는 국토안보 보장 차원의 국가적 대응책 마련에 열중하고 있다. 이에 비해, 중국의 담론은 인터넷 상에서 유통되는 정보콘텐츠의 정치안전 확보에 주안점을 둔다. 중국은, 개인의 권리 차원에서 인터넷 자유를 이해하기보다는, 인터넷에 대한 검열과 규제를 수행할 수 있는 개별 국가 차원의 정책적 권리를 강조하는 국가 주권의 관점에서 접근한다.

끝으로, 사이버 세계질서의 구성에 대한 입장이라는 점에서 미국은 시민사회, 인터넷 전문가들과 민간 사업자, 학계, 국제기구 전문가 등과 같은 다양한 이해당사자들이 참여하는 글로벌 거버넌스 모델을 지지한다. 이러한 미국의 담론은 글로벌 패권의 자유주의적 시각을 반영하는데, 미국이 사실상 패권을 발휘하는 ICANN의 인터넷 거버넌스 모델로 나타난 바 있다. 이에 비해 중국은, 러시아나 여타 개도국들과 보조를 같이하여. 인터넷 분야에서 '다중이해당사자주의'의 면분을 내건 미국의 패권을 견제하기 위해서는 국가 행위자들이 주도하는 전통적인 국제기구의 틀을 활용해야 한다고 주장한다.

이렇게 안보담론 생성에서 나타나는 양국의 차이와 그 이면에 존재하는 양국 이해관계의 차이는 앞으로 미 · 중 양국이 벌일 국내제도와 세계질서 구성 경쟁에 반영될 것으로 예상된다. 최근 드러나는 사이버 테러와 공격의 양상은 이러한 안보화의 담론경쟁이 점점 더 실질적으로 현실화될 가능성이 있음을 보여준다. 이러한 점에서 코펜하겐 학파의 안보화 이론은, 아직 객관적인 정보가 제한적으로만 알려져 있는 현재의 상황에서, 앞으로 벌어질 사이버 안보의 미중관계를 미리 읽어내는 유용성을 갖는다. 그러나 향후 사이버 안보의 미중관계와 세계정치의 연구에서 안보화 이론이 안고 있는 한계도 지적하지 않을 수 없다.

특히 안보화 이론은 담론이 현실을 만들어가는 구성주의적 차원을 강조하는 효과가 있는 반면, 막상 현실 자체에서 작동하는 관련 행위자들의 이익의 구조나 동학에 대해서는 둔감하다. 로널드 디버트도 지적하길, 안보화 이론의 비판적 시각은 "인터넷 환경에서의 안보 문제를 이해하는 결정적인 분석틀을 제공하지만, 여전히 궁극적으로는 불완전하다"고 한다. 안보화 이론은 경쟁하는 안보담론의 규범적 성격을 잘 드러내 주지만, 그 담론들 중에서 어느 것이 결국 지배적이 될 것인지에 대한 예측을 하지 못한다. 따라서 그러한 담론들이 자리를 잡고 유통되고 경쟁하는 물질적 맥락을 보아야 한다고 주장한다(Deibert,

2002, 116).

이러한 관점에서 볼 때, 향후 사이버 안보의 미중관계와 세계정치의 연구가 관심을 두어야 할 부분은 안보담론이 생성되고 현실화되는 사이버 공간의 기술구조와 정치사회적 동학이다. 실제로 사이버 안보는 전통안보와 구별되는 물질적 특성을 갖는다. 해커들이 개별적으로는 미미한 존재이면서도 인터넷 세상에 큰 위협을 가할 수 있는 계기가 사이버 공간의 구조적 속성에서 비롯된다. 사이버 테러와 공격에서는 인간 행위자 이외에도 컴퓨터 바이러스나 악성코드, 또는 컴퓨터 시스템 자체와 같은 일종의 '비인간 행위자'가 관여한다. 또한 사이버 안보는 전통적인 안보 행위자로서 국가뿐만 아니라 초국적으로 활동하는 비국가 행위자들의 존재감이 두드러진 분야이다. 사이버 안보의 세계정치가 지니는 복합성을 분석하기 위해서는 안보화 이론의 담론 변수이외에도 이들 변수를 모두 고려하여야 할 것이다.

사이버 안보 분야에서 복합적으로 벌어지는 미국과 중국이라는 두 강대국이 벌이는 경쟁은 단순히 두 나라의 관계에만 그치는 것이 아니라, 세계정치와 동아시아 정치의 구조 전반을 엿보게 하는 중요한 주제이다. 그도 그럴 것이 21세기 세계정치에서 자웅을 겨룰 강대국인 두 나라의 관계는 단순한 양자관계의 의미를 넘어서 한국을 포함한 세계 모든 나라에 영향을 미치는 세계정치 구조의 양대 축을 의미하기 때문이다. 이런 점에서 두 강대국의 경쟁이 야기하는 변화의 소용돌이로부터 한국도 자유로울 수는 없다. 특히 최근 양국 사이에서 중견국으로서 외교전략을 고민하고 한국의 입장에서 볼 때 사이버 안보의 문제는 전통안보의 문제에 못지않게 중요한 국가적 사안임이 분명하다.

참고문헌

강하연. 2013. “ICT교역의 글로벌 거버넌스.” 서울대학교 국제문제연구소 편. 『커뮤니케이션 세계정치』 기획특집 〈세계정치〉 33집 2호. 사회평론, 73-109.

김상배. 2012. “정보화시대의 미 · 중 표준경쟁: 네트워크 세계정치이론의 시각.” 『한국정치학회보』 46집 1호, 383-410.

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

김의영 · 이영음. 2008. “인터넷과 거버넌스: ICANN의 ccNSO 형성과정에서 ccTLDs 세력의 역할을 중심으로.” 『국제정치논총』 48집 2호, 173-196.

민병원. 2006. “탈냉전시대의 안보개념 확대: 코펜하겐 학파, 안보문제화, 그리고 국제정치이론.” 서울대학교 국제문제연구소 편. 『세계정치와 동아시아 안보』. 서울:인간사랑, 13-61.

민병원. 2007. “탈냉전기 안보개념의 확대와 네트워크 패러다임.” 『국방연구』 50집 2호, 23-55.

송영훈. 2014. “테러리즘과 난민문제의 안보화: 케냐의 난민정책을 중심으로.” 『국제정치논총』 54집 1호, 195-230.

장규현 · 임종인, 2014. “국제 사이버보안 협력 현황과 함의: 국제안보와 UN GGE 권고안을 중심으로.” 『정보통신방송정책』 26집 5호, 21-52.

장노순 · 한인택. 2013. “사이버 안보의 쟁점과 연구 경향.” 『국제정치논총』 53집 3호, 579-618.

『뉴시스』. 2014/8/7. “중국 정부, 애플제품 정부 조달 품목서 제외.” http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140807_0013095370&cID=10808&p ID=10800 (검색일: 2014. 8. 8).

『동아일보』. 2014-5-27. “미국-중국 이번엔 ‘사이버 스파이’ 갈등.” http://news.donga.com/3/02/20140527/63787658/1 (검색일: 2014. 5. 28).

『매일경제』. 2014/5/23. “인민군 해킹혐의로 기소되자 중, 미 기업에 보복.” http://news.mk.co.kr/newsRead.php?year=2014&no=800319 (검색일: 2014. 5. 25).

『서울경제』. 2014/7/13. “‘아이폰 마찰’까지... 골 깊어지는 미-중.” http://economy.hankooki.com/lpage/worldecono/201407/e2014071318142069760.htm (검색일: 2014. 7. 14).

『아시아경제』. 2014/7/29. “미 IT공룡들, 중국정부의 파상공세에 움찔.” http://www.asiae.co.kr/news/view.htm?idxno=2014072908235745851 (검색일: 2014. 7. 30).

『아주경제』. 2014/7/17. “중국 시진핑 ‘미국 앞마당’ 브라질 국회 연설 ‘무슨 말 했나’.” http://www.ajunews.com/view/20140717151605782 (검색일: 2014. 7. 18).

『아주경제』. 2014/7/30. “MS 반독점법 조사설에 중국 국산 소프트웨어 ‘반사이득’.” http://www.ajunews.com/view/20140730133939299 (검색일: 2014. 7. 31).

『전자신문』. 2014-6-15. “미 · 중, 신사이버 냉전...태평양에 사이버 전운.” http://www.etnews.com/20140613000100 (검색일: 2014. 6. 19).

『조선일보』. 2014/7/30. "중국 상하이 소재 61486부대 12국이 하는 일은..." http://news.chosun.com/site/data/html_dir/2014/07/30/2014073001530.html (검색일: 2014. 7. 31).

『지디넷코리아』 2014/2/17. "중국 정부판 리눅스, 130만 다운로드 돌파." http://www.zdnet.co.kr/news/news_view.asp?artice_id=20140217095449&type=det (검색일: 2014. 8. 11).

Arquilla, John and David Ronfeldt. 1996. *The Advent of Netwar.* Santa Monica, CA: RAND Corporation.

Arquilla, John and David Ronfeldt. 2001. "The Advent of Netwar (Revisited)." in John Arquilla and David Ronfeldt, eds. 2001. *Networks and Netwars: The Future of Terror, Crime and the Militancy.* Santa Monica, CA: RAND Corporation, 1-27.

Balzacq, Thierry, ed. 2011. *Securitization Theory: How Security Problems Emerge and Dissolve.* London and New York: Routledge.

Barboza, David. 2010. "Hacking for Fun and Profit in China's Underworld." *New York Times*. February 2.

Beck, Ulrich. 2005. "World Risk Society and the Changing Foundations of Transnational Politics." in Edgar Grande and Louis W. Pauly, eds. 2005. *Complex Sovereignty: Reconstituting Political Authority in the Twenty-first Century*. Toronto: University of Toronto Press, 22-47.

Buzan, Barry and Lene Hensen. 2009. *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis.* Boulder: Lynne Rienner.

Chao, Leon. 2005. "The Red Hackers: Chinese Youth Infused with Nationalism." *Chinascope.* May, 8-13.

Clark, Richard. 2011. "China's Cyberassault on America." *Wall Street Journal*, June 15.

Clinton, Hillary. 2010. "Remarks on Internet Freedom." A Speech delivered at The Newseum, Washington, DC. January 21, 2010 http://www.state.gov/ secretary/20092013clinton/rm/2010/01/135519.htm (검색일: 2014. 8. 12).

Cowhey, Peter and Milton Mueller. 2009. "Delegation, Networks, and Internet Governance." Miles Kahler. ed. *Networked Politics: Agency, Power, and Governance*. Ithaca and London: Cornell University Press, 173-193.

Dahong, Min. 2005. "The Passionate Time of Chinese Hackers." *Chinascope.* May, 14-25.

Deibert, Ronald J. 2002. "Circuits of Power: Security in the Internet Environment," in James

N. Rosenau and J.P. Singh. eds. *Information Technologies and Global Politics: The Changing Scope of Power and Governance.* Albany, NY: SUNY Press, 115-142.

DeNardis, Laura. 2013. *The Global War for Internet Governance.* New Heaven, CN: Yale University Press.

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

Hughes, Rex. 2010. "A Treaty for Cyberspace." *International Affairs* 86(2): 523-541.

Hvistendahl, Mara. 2010. "China's Hacker Army." *Foreign Policy*. March 3, 2010.

Libicki, Martin C. 2009. *Cyber Deterrence and Cyber War*. Santa Monica, CA: RAND Corporation.

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

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

Manson, George Patterson, 2011. "Cyberwar: The United States and China Prepare For the Next Generation of Conflict." *Comparative Strategy* 30(2): 121-133.

Matusitz, Jonathan A. 2006. Cyberterrorism: A Postmodern View of Networks of Terror and How Computer Security Experts and Law Enforcement Officials Fight Them. Ph.D. Dissertation, University of Oklahoma.

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.

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.

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.

US Department of State and US Agency of International Development(USAID). 2010. Leading Through Civilian Power The First Quadrennial Diplomacy and Development Review.

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.

Wæver, Ole. 1995. "Securitization and Desecuritization." in Ronny Lipschutz. ed. *On Security*. New York: Columbia University Press, 46-86.

Zakaria, Fareed. 2010. "Clash of the Titans." Newsweek. January 25, 36.

鲁传颖(루촨잉). 2013. "试析当前网络空间全球治理困境(사이버 공간의 글로벌 거버넌스가 당면한 딜레마에 대한 분석),『现代国际关系(현대국제관계)』 2013年 第11期. 48-54.

沈逸(썬이). 2010. "数字空间的认知，竞争与合作-中美战略关系框架下的网络安全关系(디지털 공간에 대한 인지, 경쟁과 협력: 미중 전략관계 프레임 속에서의 사이버 안보 관계)." 『外交评论(외교평론)』 第2期, 38-47.

王世伟(왕쓰웨이). 2012. "中国国家信息安全的新特点与文化发展战略(중국 국가정보안전의 신특점과 문화발전 전략." 『图书情报工作』 第6期, 8-13.

王正平(왕정핑) 徐铁光(쉬테광). 2011. "西方网络霸权主义与发展中国家的网络权利(서방의 사이버패권주의와 개발도상국의 사이버권리)." 『思想战线(사상전선)』, 第2期 第37卷. 105-111.

奕文莉(이원리). 2012. "中美在网络空间的分歧与合作路径(중국과 미국의 사이버공간에서의 분열와 협력의 경로)." 『现代国际关系(현대국제관계)』 第7期, 28-33.

周琪(저우치) · 汪晓风(왕샤우펑). 2013. "美国缘何在网络安全上针对中国(미국은 무엇 때문에 사이버안보문제에서 중국을 겨누는가)." 『时事报告(시사보고)』 第7期, 46.

蔡翠红(차이추이홍). 2012. "网络空间的中美关系竞争，冲突与合作(사이버공간에서의 미중관계: 경쟁, 충돌과 협력)." 『美国研究(미국연구)』 第3期, 107-121.

『大公网(대공망)』, 2014/5/18. "国信办副主任谈网络安全: 管理不好或致'国将不国'(국가인터넷정보판공실 부주임 인터넷안전을 논하다: 제대로 된 관리를 못하면 '국장불국'이 될 수 있다." http://news.takungpao.com/mainland/focus/2014-05/2481785.htm (검색일: 2014. 7. 18).

『新浪网(시나넷)』 2012/11/27. "数据称中国信息安全在思科等美企面前形同虚设(데이터에 근거하면 중국의 정보안전은 시스코와 같은 미국기업 앞에서는 유명무실하다)". http://finance.sina.com.cn/china/20121127/064513805924.shtml (검색일: 2014. 7. 25).

『新华网(신화망)』, 2014/5/28. "外交部: 中方正研究政策加强网络信息安全(외교부: 중국은 현재 인터넷정보안

전의 강화를 위한 정책을 연구 중이다)” http://news.xinhuanet. com/world/2014-05/28/c_1110904778.htm (검색일: 2014. 7. 16).

『人民网(인민망)』, 2014/4/1. “国防部: 美网络监控行为暴露其虚伪霸道(국방부: 미국의 사이버감시 행위는 자신의 허위와 패도를 드러나게 했다).” http://yuqing.people. com.cn/n/2014/0401/c210115-24792166.html (검색일: 2014. 7. 23).

『参考消息网(참고소식망)』, 2011/11/02. “中俄与欧美争夺网络空间主导权(중 · 러는 구미와 사이버공간의 주도권을 두고 다툰다)” http://world.cankaoxiaoxi.com/2011/ 1102/4962.shtml (검색일: 2014. 7. 18).

『参考消息网(참고소식망)』, 2014/1/03. “三大措施打造‘网络国门’(3대 조치로 ‘국가사이버게이트’를 만들어야 한다). http://ihl.cankaoxiaoxi.com/2014/0103/326499.shtml (검색일: 2014. 7. 16).

『环球网(환구망)』, 2013/3/09. “杨洁篪: 中国在网络安全方面是弱势群体(양제츠: 중국은 사이버안보 면에서 약소단체이다).” http://china.huanqiu.com/roll/2013-03/ 3716669.html (검색일: 2014. 7. 17).

『环球网(환구망)』, 2014/5/23. “专家: 中国维护网络安全 美枉己正人曝强盗逻辑(전문가: 중국은 사이버안보를 수호, 미국의 망기정인은 강도논리를 드러내다).” http://world. huanqiu.com/article/2014-05/5003716.html (검색일: 2014. 7. 16).

『环球网科技(환구망과기)』. 2014-/5/29. “中美网络安全战升级 中国科技企业或迎春天(중 · 미 사이버안보전의 가열로 중국과학기술기업은 봄날을 맞이할 것이다)” http:// tech.huanqiu.com/it/2014-05/5007875.html (검색일: 2014. 7. 18).

U.S.-China Relations in Cyber Security: A Perspective of Securitization Theory

KIM Sangbae Seoul National University

Abstract

Cyber security has rapidly emerged as one of the major concerns in the U.S.-China relations of the 21st century. This paper relies on the perspective of securitization theory presented by the Copenhagen School in international security studies, and examines the dynamics of the competition between the United States and China in the cyber security domain. U.S.-China relations in cyber security are currently reflected in the different securitization processes at the three levels. First, while the United States points to cyber threats by Chinese hackers' attacks to its computer infrastructure and information resources, China securitizes technological hegemony of the U.S. multinational corporations as threats to its market and regime. Second, while the United States highlights cyber security at the individual level such as protection of privacy, human rights, and freedom of expression, China has been more concerned about Internet freedom at the national level through means to secure domestic political stability such as censorship and regulations. Finally, while the United States security discourses have been based on the neo-liberal visions for the world order in cyberspace, the Chinese discourses are composed of nationalist visions of state sovereignty in the world order. It is expected that the two world powers' interests are possibly conflicting in building the future world order in the cyber security domain.

Key words : Cyber Security, United States, China, U.S.-China Relations, Securitization Theory, International Relations