특집논문

『국가정책연구』
제28권 제3호: 237-263

사이버 안보 분야의 미·중 표준경쟁: 네트워크 세계정치학의 시각*

김상배**

논 문 요 약

이 글은 최근 동아시아 지역뿐만 아니라 글로벌 차원에서 쟁점이 되고 있는 미국과 중국의 패권경쟁을 사이버 안보의 문제에 초점을 맞추어 탐구하였다. 이 글이 사이버 안보의 미·중 패권경쟁을 이해하기 위해서 원용한 분석틀은 표준경쟁을 둘러싼 네트워크 세계정치학의 논의이다. 표준경쟁은, 기술과 산업의 문제일 뿐만 아니라, 관련 정책과 제도 및 해당 분야의 질서와 담론 형성의 문제로서 국제정치학의 시각에서 볼 때도 중요한 연구 어젠다 중의 하나이다. 최근 21세기의 패권국과 도전국인 미국과 중국 사이에서 중견국으로서 외교전략을 모색하고 있는 한국의 입장에서 볼 때, 사이버 안보 분야에서 벌어지는 표준경쟁은 핵안보와 같은 전통안보의 문제에 못지않게 중요한 21세기 국가전략의 사안으로 부상하고 있다. 이 글은 기술, 제도, 담론의 세 가지 차원에서 벌어지는 '3차원 표준경쟁'의 시각에서 사이버 안보 분야의 미·중 표준경쟁을 이론적·경험적으로 조명하고, 그러한 미·중 경쟁의 틈바구니에서 한국이 취할 표준전략의 방향을 가늠해 보았다. 이 글이 밝혀 낸 미국과 중국의 표준경쟁의 양상은 인터넷 보안 기술 분야의 패권을 바탕으로 사이버 공간의 자유로운 활동을 보장하는 네트워크 인프라의 보호를 강조하는 미국의 입장에 대해서, 정권안보와 국가주권의 차원에서 인터넷에 대한 검열과 규제를 정당화하는 중국의 입장이 대립하는 양상으로 나타난다. 이렇게 사이버 안보 분야에서 벌어지는 미국과 중국의 표준경쟁의 양상은 향후 한국의 표준전략과 외교전략이 심각하게 고민해야 하는 구조적 환경의 변화이다.

주제어: 표준경쟁, 사이버 안보, 국제정치, 네트워크, 미국, 중국

* 이 논문은 2014년 한국표준협회의 지원을 받아 수행된 연구임(제2회 표준정책 마일스톤 정책연구: <국가표준 거버넌스 선진화>를 위한 정책연구). 이 논문은 2013년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2013S1A3A2053683)

** 서울대학교 정치외교학부 교수

Ⅰ. 서론

지구화와 정보화 시대를 맞이하여 표준의 중요성에 대한 인식이 높아지고 있다. 표준의 중요성이 커가는 만큼 공식적인 절차와 기관을 통한 표준화의 메커니즘 이외에도 시장에서 벌어지는 사실상의 표준경쟁이 치열해 지고 있다. 여기서 말하는 표준은 좁은 의미에서 보면 전통산업이나 정보기술 분야의 기술표준을 지칭하지만, 넓은 의미에서 보면 그러한 기술표준을 다루는 관리양식, 즉 '표준 거버넌스'의 문제도 포함한다. 다시 말해, 기술표준을 넘어서 정책과 제도, 더 나아가 생각과 가치관의 표준까지도 표준화와 표준경쟁의 대상이 되고 있다. 이러한 양상은 최근 국가 간에 벌어지는 표준경쟁에서도 발견된다. 이 글은 이러한 국가 간 표준경쟁의 시각에서 21세기 세계정치의 주도권을 놓고 경합을 벌이는 두 나라, 즉 미국과 중국의 패권경쟁에 담겨 있는 표준경쟁의 내용을 분석 및 해석하고, 이를 통해서 한국의 표준전략과 좀 더 넓게는 외교전략에 주는 함의를 도출하는 것을 목적으로 한다.

이 글에서 미·중 표준경쟁의 사례로서 주목하는 분야는 사이버 안보이다. 최근 북한의 소행으로 추정되는 사이버 공격이 빈번해지면서 국내에서도 사이버 테러와 공격, 그리고 좀 더 포괄적인 의미에서 본 사이버 안보에 대한 관심이 커지고 있다. 사이버 안보의 문제는 이제는 더 이상 해커들의 장난이나 테러리스트들의 저항수단에 머물지 않고 국가 간의 분쟁으로 확대되고 있다. 최근 미국·이스라엘과 이란 간에 벌어진 사이버 전쟁의 사례나 에스토니아, 그루지야 등에서 발생한 사이버 공격의 배후에서 활약했던 러시아의 역할 등은 사이버 안보의 문제가 매우 중요한 국가안보의 대상이 되었음을 보여준다. 이러한 맥락에서 볼 때, 지난 2013년 6월 미국과 중국의 두 정상인 오바마 대통령과 시진핑 주석이 만나 북한 핵개발 문제와 더불어 사이버 안보 문제를 양국이 당면한 현안으로 거론하면서 사이버 안보는 그야말로 21세기 미중관계의 전면에 부상했다.

그 후 사이버 안보는 미·중 양국 간에 진행된 전략경제대화의 현안 중의 하나로서 다루어졌으며, 좀 더 구체적으로는 미·중 사이버 보안 실무그룹의 협의가 진행되기도 했다. 그러나 이러한 협력의 제스처에도 불구하고 물 밑에서는 사이버 안보 분야의 미·중 갈등은 계속 진행되었다. 미·중 사이버 갈등은 2014년 5월 미 법무부가 미국 내 기관들에 대해서 해킹을 감행한 것으로 지목한 중국군 61398부대 장교 5인을 기소하면서 정점에 달했다. 중국은 이에 즉각 반발하며 미중 대화를 중단하는 동시에 중국 시장에 진출한 미국 IT기업들에 대한 규제의 고삐를 죄기도 했다. 사실 사이버 안보 분야에서 벌어진 미중관계의 이면을 보면, 미국도 중국을 상대로 비밀스러운 정보작전을 벌인 것은 마찬가지여서 2013년 6월 미국 중앙정보국(CIA) 전 직원인 에드워드

스노든(Edward Snowden)은 미국이 장기간에 걸쳐 중국을 포함한 세계 각국의 각종 데이터를 감청해 왔다고 폭로한 바 있었다. 미국과 중국 간에 벌어지는 해킹과 사이버 공격에 대한 정보와 자료가 극히 제한적인 현재의 상황을 염두에 두더라도, 두 강대국 간에는 이미 수년째 치열한 '사이버 전쟁'이 벌어지고 있음을 미루어 짐작할 수 있다.

국제정치학의 분야에서 미국과 중국의 경쟁을 표준경쟁의 시각에서 다룬 연구는 매우 드물다.[1] 그러나 표준경쟁보다는 좀 더 넓은 의미에서 본 미·중 세계패권 경쟁은 최근 국내외 국제정치학의 핵심 주제 중의 하나이다. 이러한 미·중 패권경쟁 전반의 향배를 읽는 데 있어서 사이버 안보나 인터넷, 좀 더 포괄적으로 IT분야에서 벌어질 양국의 경쟁은 중요한 잣대가 될 것이다. 실제로 첨단기술 분야에서 벌어지는 강대국들의 패권경쟁은 국제정치 구조의 변동을 극명하게 보여주는 사례라는 점에서 국제정치학의 오래된 관심사 중의 하나였다. 역사적으로 세계경제의 선도부문, 즉 해당 시기 첨단산업의 향배는 세계패권의 부침과 밀접히 관련된 것으로 알려져 있다(Gilpin, 1987; Modelski and Thompson, 1996). 이러한 맥락에서 볼 때, IT분야, 좀 더 구체적으로는 인터넷과 사이버 안보의 분야는 국제정치학적 함의를 갖는 21세기 선도부문의 대표적인 사례이다. 이 글에서 초점을 두는 '표준'이란 바로 이러한 선도부분의 '게임의 규칙'에 해당된다. 좀 더 넓게 보면 '표준'이란 기술과 산업의 영역을 넘어서 세계패권이 세계정치 분야의 질서를 규정하는 '게임의 규칙'이기도 하다.[2]

사이버 안보의 세계정치는 국가 간의 관계에 주목하는 기존의 전통적인 국제정치학의 안보이론이 제대로 설명하지 못하는 새로운 분야이다. 사이버 안보와 사이버 공간의 독특한 구조와 동학이 기존 이론의 분석의 칼날을 무디게 한다. 공격과 대상이 명확히 구분되는 전통 안보 영역과는 달리 사이버 테러와 공격은 공격의 주체와 보복의 대상을 명확히 판별할 수 없는 복잡계 환경을 배경으로 한다. 게다가 사이버 안보는 국가 행위자뿐만 아니라 비국가 행위자나 악성코드와 같은 소위 '비인간 행위자(non-human actor)'가 복합적으로 관여하는 분야이다. 따라서 만약에 범인을 찾는다고 하더라도 확증보다는 추정하는 경우가 많기 때문에 실제 범인을 색출하는 문제보다도 누가 범인인지에 대한 담론을 구성하는 것이 더 중요한, 일종의 '범죄의 재구성 게임'의 영역이다. 이러한 관점에서 볼 때, 사이버 안보의 세계정치는 전통적인 국제정치의 게임이라기보다는, 새로운 이론적 시각을 필요로 하는, 복합적인 네트워크 세계정치의 게임이다.

---

1) 표준경쟁의 시각에서 정보화 시대의 미·중 경쟁을 다룬 연구로는 김상배(2012)가 있다. 유사한 시각에서 1990년대 미국과 일본의 표준경쟁을 다룬 연구로는 김상배(2007)을 참조하기 바란다. IT분야의 미중경쟁을 다룬 연구로 배영자(2011)도 유용하다.

2) 최근의 현상으로서 사이버 안보(또는 넓은 의미의 인터넷) 분야에서 벌어지는 미국과 중국의 경쟁에 대한 연구는 아직 많지 않은데, 몇 가지 사례로 Liberthal and Singer(2012), 沈逸(2010), Manson(2011), 蔡翠红(2012), 김상배(2014, 특히 제11장) 등을 들 수 있다.

이 글은 복합적인 양상으로 전개되고 있는 사이버 안보의 세계정치를 분석 및 해석하기 위해서 최근 국내외 학계의 관심이 높아지고 있는 '네트워크 세계정치학'의 시각을 원용하였다(Hafner-Burton, Kahler, and Montgomery, 2009; Kahler, ed. 2009; Maoz, 2010; 하영선·김상배 편, 2010; 김상배, 2014). 네트워크 세계정치학의 논의 중에서도 사이버 안보 분야에서 다양한 행위자들이 벌이는 새로운 권력게임의 양상을 분석하기 위한 분석틀로서 표준경쟁의 이론적 시각을 원용하였다. 사실 사이버 안보 분야에서 벌어지는 미·중 경쟁은 복합 네트워크의 시각에서 파악해야만 하는 중층적 표준경쟁이다. 이렇게 이해한 표준경쟁의 시각은 통상적으로 원용되는 표준경쟁에 대한 논의를 넘어선다. 기존에 경영학이나 경제학을 중심으로 진행된 표준경쟁에 대한 논의는 좁은 의미에서 기술과 시장 분야에만 초점을 맞추었던 것이 사실이다. 또는 부분적으로 기술표준의 경쟁을 뒷받침하는 표준 관련 제도나 표준 거버넌스로 관심의 범위를 넓히곤 했다. 그러나 네트워크 세계정치학의 시각에서 보면 표준경쟁은 기술표준의 논의를 포함하면서도, 좀 더 넓은 의미에서, 정책도입이나 제도조정, 규범전파의 과정에서 벌어지는 경쟁도 포함한다. 가장 추상적인 수준에서 표준경쟁의 논의는 현실을 관념적으로 구성 및 재구성하는 담론과 가치관의 경쟁에까지도 적용 가능하다.

이렇게 넓은 의미에서 파악한 표준경쟁의 시각에서 볼 때, 사이버 안보 분야의 미·중 경쟁은 단순히 해커들의 명시적인 공격과 네트워크 시스템의 물리적 교란, 상업적·군사적 정보의 절취와 도용, 그리고 여기서 파생되는 양국 간의 물리적 충돌의 가능성을 논하는 차원을 넘어선다. 게다가 사이버 공간의 미중관계는 단순히 갈등이냐 협력이냐, 아니면 누가 승자이고 패자이냐, 그리고 더 나아가 경쟁의 주체가 누구이냐를 묻기가 무색한 복합적인 성격을 지니고 있다. 사이버 안보 분야의 미·중 경쟁은 다차원적인 권력게임을 벌이는 다층적인 행위자들의 네트워크 게임으로 이해해야 한다. 이러한 맥락에서 볼 때 미국과 중국이 벌이는 경쟁은 다양한 행위자들이 벌이는 '네트워크들 간의 정치(inter-network politics),' 즉 망제정치(網際政治)이다. 이 글은 이러한 복합적인 양상으로 전개되는 사이버 안보 분야의 미·중 경쟁을 '3차원 표준경쟁', 즉 기술표준경쟁과 제도표준경쟁, 담론표준경쟁의 시각에서 분석하였다. 이러한 작업을 통해서 이 글이 목적하는 바는 미국과 중국이 벌이는 21세기 패권경쟁을 좀 더 체계적으로 이해하고 이를 바탕으로 향후 한국이 추구할 표준전략, 좀 더 넓은 의미에서는 외교전략의 방향을 가늠해보는 데 있다.

이 글은 크게 다음과 같은 네 부분으로 구성되었다. 제2장은 국제정치학의 시각에서 이익-제도-관념의 차원에서 복합적으로 벌어지는 3차원 표준경쟁, 즉 기술표준경쟁, 제도표준경쟁, 담론표준경쟁에 대한 이론적 분석틀을 제시하였다.[3] 제3장은 사이버 안보 분야에서 벌어지는 미·

중 기술표준경쟁의 성격을 정보산업과 인터넷 보안기술 분야에서 중국이 추구해온, 미국의 기술 패권에 대한 견제와 대항의 연속선상에서 살펴보았다. 제4장은 미국과 중국이 구체적으로는 인터넷 검열 정책, 좀 더 넓은 의미로는 정치경제 모델의 차이에서 드러나는 제도표준경쟁의 양상을 분석하였다. 제5장은 사이버 안보의 정의와 대상, 주체 등과 관련된 안보담론을 둘러싸고 벌어지는 미국과 중국의 담론표준경쟁을 살펴보았다. 맺음말에서는 이 글의 주장을 요약·정리하고, 미국과 중국이 벌이는 3차원 표준경쟁에 대비하는 한국 표준전략에 대한 후속연구의 필요성을 지적하였다.

Ⅱ. 3차원 표준경쟁의 시각

이 글이 사이버 안보 분야에서 벌이는 미국과 중국의 경쟁을 이해하기 위해서 원용한 분석틀은 표준경쟁의 국제정치학적 논의이다(김상배, 2007; 2012). 표준경쟁은 주로 기술과 시장에서 벌어지는 경쟁을 분석하기 위해서 원용된다. 기술의 관점에서 본 표준경쟁이란 시스템을 구성하는 단위들 간의 상호작동성과 호환성을 돕는 규칙이나 기준, 즉 표준을 선점하기 위해서 벌이는 경쟁이다. 역사적으로 표준설정은 공적인(de jure) '표준화'나 사실상(de facto) '표준경쟁'의 두 가지 형태로 진행되었는데, 최근에는 사실상 표준경쟁의 중요성이 더 주목받고 있다. 특히 가전, 컴퓨터, 이동통신, 디지털TV, 인터넷, 스마트폰 등과 같은 IT산업 분야에서 기술표준의 중요성이 커지면서 그 주도권을 놓고 시장에서 벌어지는 표준경쟁의 중요성이 증대되고 있다. 이러한 기술표준경쟁은 주로 민간 기업 차원에서 벌어지지만, 최근 그 중요성이 커지면서 국가 간 경쟁의 양상을 띠기도 한다. 사이버 안보 분야에서 벌어지는 미·중 경쟁도 이러한 IT분야 기술표준경쟁의 성격을 바탕에 깔고 있다.

이러한 표준경쟁을 기술과 산업 분야에서만 논하라는 법은 없다. 실제로 언어나 화폐, 정책과 제도, 규범, 법률과 문화적 관행에 이르기까지 다양한 분야에서 표준경쟁, 통칭해서 제도표준경쟁의 양상이 나타난다. 제도표준경쟁은 기술표준경쟁보다 한 층위 위에서 벌어지는 제도모델의 표준을 놓고 벌이는 경쟁이다. 새로운 기술과 표준의 개발이나 이전 및 확산은 그 자체만의 독립적인 과정이라기보다는 이를 뒷받침하는 제도환경의 변수가 관여하는 사회적 과정이다. 새로운

3) 이 글에서 논지를 전개하는 과정에서 원용한 분석틀은 이익(interests), 제도(institutions), 관념(ideas) 변수의 복합성을 강조하는 사회학적 제도주의 또는 구성적 제도주의의 논의이다(Leander 2000; 김상배 2007). 사회학적 구성주의 분석틀에 의하면, 이익과 제도 및 관념의 변수는 그 선후가 고정적으로 정해져 있는 것은 아니고 연구대상의 성격에 따라서 유연하게 재구성하여 적용할 수 있다. 이 글에서는 사이버 안보 분야의 성격에 맞추어 이익(기술표준경쟁), 제도(제도표준경쟁), 관념(담론표준경쟁)의 순으로 논지를 전개하였다.

기술과 산업에서 효과적인 경쟁을 벌이기 위해서는 민간 행위자들의 혁신뿐만 아니라 국가의 규제나 육성정책의 역할, 과학기술과 교육의 인프라 등과 같은 제도환경의 조성, 즉 일종의 제도표준의 우위를 겨루는 보이지 않는 경쟁이 동시에 진행된다. 보통 국제정치학에서 제도표준에 대한 논의는 기업모델, 산업모델, 정책모델 등의 형태로 알려져 있다. 역사적으로 국가 차원에서는 영국 모델, 후발 자본국 모델, 포디즘(Fordism), 냉전모델, 일본모델, 윈텔리즘(Wintelism) 등과 같은 정치경제 모델로 나타났다(김상배, 2007). 최근 워싱턴 컨센서스와 베이징 컨센서스로 불리는 미국과 중국의 정치경제 모델의 경쟁에 주목하는 것도 바로 이러한 맥락이다.

사실 이렇게 넓은 의미에서 보면 국제정치 자체가 표준경쟁이다. 특히 네트워크 세계정치학의 시각에서 볼 때, 기술표준의 개발과 수용, 정책과 제도의 도입, 규범의 전파 등은 중립적으로 이루어지는 것이 아니고 권력현상을 수반한다. 표준설정의 권력은 어느 행위자가 물질적 자원을 많이 보유하고 있다고 해서 생겨나는 종류의 것이 아니다. 오히려 물질적 권력은 빈약하더라도 행위자 차원을 넘어서 작동하는 네트워크의 속성을 잘 이해하고 자신이 제시한 표준을 지지하는 세(勢)를 많이 모으는 것이 중요하다. 이렇게 많은 지지자를 끌어 모을 수 있는 자가 여타 표준과의 관계에서 유리한 위치를 차지하여 호환성을 제공하는 역할을 담당할 가능성이 높다. 또한 이러한 능력을 가지고 있으면 자신의 이해관계를 반영하여 네트워크상에서 게임의 규칙을 장악할 가능성도 높다. 일단 이렇게 설계된 네트워크는 지배표준으로 작동하면서 더 많은 세력을 결집하게 되는 구조적 강화의 고리를 형성한다. 국제정치학의 시각에서 볼 때 이러한 표준경쟁의 양상은 지구화와 정보화, 그리고 네트워크 시대로 대변되는 21세기 세계정치에서 더욱 두드러지게 나타나고 있다(김상배, 2014).

가장 추상적인 의미에서 표준경쟁은, 기술과 제도의 차원을 넘어서, 생각과 담론, 더 나아가 이념과 가치관 등의 표준을 놓고 벌이는 경쟁, 통칭해서 담론표준경쟁으로 이해할 수 있다. 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 기성질서와는 다른 방향으로 현실의 변화를 꾀하는 계기를 제공하기도 한다. 이러한 과정에서 담론표준경쟁은 아직 구체화되지 않은 현실세계의 성격을 정의하며 그러한 과정에서 등장할 미래세계의 의미와 효과를 규정하는 경쟁을 뜻한다. 구체적으로 이러한 경쟁은 대상의 종류와 성격, 그리고 그 대상이 안고 있는 문제점과 이를 해결할 주체에 대한 담론을 누가 그리고 어떻게 규정하느냐의 양상으로 전개된다. 이러한 시각에서 볼 때, 담론표준경쟁은 단순히 추상적인 관념의 경쟁을 의미하는 것이 아니고, 앞서 언급한 기술표준경쟁이나 제도표준경쟁과 구체적으로

연계해서 이해할 수 있는데, 보통 새로운 담론의 제시를 통해서 기술혁신이나 제도조정의 방향이 설정되기 때문이다.

이상의 시각을 원용할 때, 미국과 중국이 사이버 안보 분야에서 벌이는 경쟁은 인터넷 기술의 혁신과 이를 뒷받침하는 인터넷 관련 정책과 제도의 성격, 그리고 21세기 패권을 노리는 두 나라의 비전 제시라는 세 가지 차원에서 파악된 표준경쟁이다. 기술과 제도, 담론이 복합적으로 작용하는 표준경쟁이라는 의미에서 '3차원 표준경쟁'이라고 명명할 수 있겠다. 물론 표준경쟁의 양상을 이렇게 세 가지 차원으로 구분한 것은 분석상의 편의에 의한 것이지 실제 현실이 이렇게 따로따로 움직이는 것은 아니다. 기술은 정치적인 것이고 기존의 제도적 조건에 영향을 받을 뿐만 아니라, 미래를 구성하는 담론의 구속을 받는다. 이 글이 인터넷 보안기술과 서비스 산업 분야에서 벌이는 기술표준경쟁의 양상을 넘어서 다층적으로 벌어지는 기술-제도-담론 표준경쟁의 시각을 취한 것은 이러한 이유 때문이다. 이하에서는 사이버 안보 분야의 미·중 표준경쟁에 담긴 3차원 표준경쟁의 복합적 동학을 살펴보겠다.

Ⅲ. 사이버 안보의 미·중 기술표준경쟁

2013-14년 스노든 사건과 미 법무부의 중국군 기소 사건 등을 거치면서 미·중 사이버 갈등이 심해지고 있다. 사실 이 과정에서 거론된 문제들의 사실 여부를 객관적으로 규명하는 작업은 좀 더 시간이 걸릴 것 같다. 그럼에도 표준경쟁의 시각에서 볼 때 주목해야 할 점은 이러한 갈등의 이면에 사이버 공간에서의 미국의 기술패권과 이를 경계하는 중국의 의구심어린 움직임이 치열하게 경합하고 있다는 사실이다. 특히 중국 정부는 미국 IT기업들이 제공하는 컴퓨터와 네트워크 장비의 보안문제를 우려한다. 인터넷 보안기술과 관련하여 중국이 미국 IT기업들에게 너무 많이 의존하고 있으며, 혹시라도 양국 간에 문제가 발생할 경우, 이들 기업들이 미국 편을 들 것이라는 걱정이다. 사실 미국의 IT기업들은 사이버 공간의 중요한 기술과 산업을 거의 독점했다. 예를 들어, 시스코는 네트워크 장비 분야에서, 퀄컴은 칩 제조 분야에서, 마이크로소프트는 운영체계 분야에서, 구글은 검색엔진 분야에서, 페이스북은 SNS 분야에서 모두 독점적인 위치에 차지하고 있다. 중국은 일단 양국 간에 사이버 전쟁이 발발한다면 이들 기업들이 모두 미국 정부에 동원될 것이라고 보고 있다(鲁传颖, 2013).

이러한 문제의식을 바탕으로 중국 정부와 기업들은 1990년대 이래 미국의 IT기업에 대한 기술의존을 줄이고 중국의 독자표준을 모색하려는 노력을 펼쳐온 바 있다. 이러한 점에서 사이버 안보 분야의 미·중 경쟁은 기술표준경쟁의 성격을 띤다. 그런데 여기서 한 가지 유의할 점은 이

분야에서 벌어지는 미국과 중국의 경쟁이 새로운 대안표준을 제시해서 맞불작전을 하는 적극적인 형태의 전형적인 기술표준경쟁의 모습이라기보다는 지배표준을 회피하거나 또는 지배표준으로부터 자유로운 독자적 표준공간을 확보하려는 소극적인 형태로 진행됐다는 사실이다. 이러한 특징은 컴퓨터 및 인터넷 기술과 관련된 안보담론의 관점에서도 양국의 경쟁을 파악하려는 이 글의 시각과도 맥이 닿는다. 구체적으로 사이버 안보 분야 미·중 기술표준경쟁은 컴퓨터 운영체계, 대규모 서버, 네트워크 장비, 모바일 운영체계 등에 구축된 미국 IT기업들의 지배에 대한 중국의 우려에서 시작되었다.

역사를 거슬러 올라가 보면, 1990년대 말과 2000년대 초 컴퓨터 운영체계의 보안 문제를 우려한 중국 정부는 마이크로소프트의 지배표준에 대한 대항의 차원에서 오픈소스 소프트웨어인 리눅스 운영체계와 애플리케이션 개발을 지원하였다. 이러한 과정에서 중국의 리눅스 업체들은 정부의 강력한 지원에 힘입어 리눅스 보급의 선봉장 역할을 담당하였는데, 1999년 8월 중국과학원이 후원하여 설립된 '홍치(紅旗)리눅스'가 가장 대표적인 사례이다. 중국 정부가 리눅스 운영체계를 지원한 정책의 배경에는 경제적 동기 이외에도 마이크로소프트의 플랫폼 독점으로 인해 발생할 가능성이 있는 보안 문제에 대한 민족주의적 우려가 자리 잡고 있었다. 그러나 궁극적으로 중국의 리눅스 실험은 기대했던 것만큼의 큰 소득을 거두지는 못했다(김상배, 2012).

중국 정부는 홍치리눅스의 설립과 더불어 민용 및 군용의 운영체계 개발에도 나섰는데, 2001년에 개발되어 2007년부터 사용된 '갤럭시기린'과 2003년 개발을 시작한 '차이나스탠다드리눅스' 운영체계가 그 사례들이다. 그러다가 2006년에 중국 정부의 체계적인 지원이 이루어지면서 2010년에는 '네오기린'이라는 이름으로 두 운영체계가 통합되었는데, 이는 '제2의 홍치리눅스'라고 불리면서 중국산 운영체계의 대표 브랜드로 발돋움했다(「中国电子报」, 2010-12-21). 이에 대해서는 미국 정부도 특별한 관심을 보였는데, 2009년 국회청문회에서는 중국의 운영체계와 관련된 보안 문제가 제기되었다. 중국이 독자적인 운영체계를 개발하여 중국의 주요 기관에 보급한다면 이는 미국의 사이버 공격을 무력화시킬 수도 있다는 것이었다(「网易科技」, 2009-05-13). 한편 2014년 마이크로소프트의 윈도XP 서비스 종료를 계기로 중국 정부는 리눅스 배포판인 우분투 계열의 '기린'을 국가 운영체계로 발표하면서 공공기관을 중심으로 오픈소스 운영체계로의 전환을 추진하고 있다(「지디넷코리아」, 2014-2-17).

사이버 안보 표준과 관련된 중국의 독자표준 시도를 보여주는 다른 하나의 사례는 중국이 2003년 11월 발표한 무선랜 보안 프로토콜인 WAPI(Wireless Authentication and Privacy Infrastructure)이다. 당시에는 IEEE에 의해 개발된 802.11 Wi-Fi가 세계적으로 널리 사용되는 무선 LAN 보안 표준이었다. 그러나 Wi-Fi가 보안상 취약점을 가지고 있다는 사실이 알려지면서

중국은 Wi-Fi의 보안상 문제를 빌미로 WAPI를 국내표준으로 제정하려는 시도를 펼쳤다. WAPI는 Wi-Fi에 기반을 둔 칩과 호환되지 않는다는 점에서 독자적 기술표준의 성격을 지녔다, 중국 정부는 노트북과 PDA와 같은 무선장비에 대하여 중국산 장비뿐만 아니라 모든 수입 장비에 대해서도 WAPI 표준을 수용할 것을 요구했다. 만약에 WAPI 보안 표준이 채택됐더라면 미국 업체들은 중국과 기타 시장을 위해 각각 두 가지 종류의 칩을 생산해야만 했을 것이다(Lee and Oh, 2006).

인텔을 비롯한 미국 IT기업들이 반대가 심했던 것은 당연했다. 인텔이 WAPI를 지원하지 않기로 발표하자 중국 정부는 WAPI 표준을 충족시키지 못할 경우 중국 내에서 영업을 할 수 없을 것이라고 경고하기도 했다. WAPI와 관련하여 더 문제가 된 것은 세계무역기구(WTO) 기술무역장벽(TBT: Technical Barriers to Trade) 조항의 위반 가능성이었다. 이러한 상황에서 미국의 칩 제조업체들은 미국 정부의 개입을 요구했고, 결국 미국 정부가 중재에 나섰다(이희진·오상조, 2008). 한편 2004년부터 중국은 WAPI의 국제표준 채택을 위해서 나섰는데, 8년이 지난 2014년 1월에 이르러서야 WAPI의 핵심기술특허가 겨우 통과되었다. WAPI가 공식적인 국제표준으로서 인정받기는 했으나 소기의 성과를 거두었다고 보기는 어려운 상황이었다.

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 안전 검사'를 의무화하는 조치로 나타났다. 중국 정부의 보안검사는 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」, 2014-05-29). 2014년 7월에는 중국 당국이 반독점법 위반 혐의로 마이크로소프트에 대한 조사에 돌입했는데, 이러한 행보는 중국산 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 서

버로 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. 미국 국가안보국(NSA)이 중국에서 도·감청 프로그램을 운용하며 시스코의 설비를 활용했다는 사실이 폭로된 것이 화근이었다. 중국내 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」 2014-05-29). 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 중국인민공안대의 마딩(馬丁) 인터넷보안

연구소장에 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, 월스트리트저널(WSJ)은 “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」, 2014-08-07).

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 기술표준경쟁이 아니라 이 분야의 정책과 제도의 표준으로 연결된다는 중국 정부의 인식을 보여준다.

Ⅳ. 사이버 안보의 미·중 제도표준경쟁

기술과 시장에서 나타난 미국 IT기업들과 중국 정부의 갈등은 중국의 인터넷 검열 정책과 법제도를 둘러싼 갈등으로도 나타났다. 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 맥락에서 중국 정부는 중국 내의 인터넷 서비스 제공자들이 자체 검열을 수행하도록 요구했다. 예를 들어, 마이크로소프트의 경우도 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).

이러한 중국의 인터넷 검열과 정치적 억압에 대한 반발이 없을 수 없었다. 2010년 1월 12일에 이르러 구글은 중국 시장에서 철수할 수도 있다고 발표하였다. 그 이유는 크게 두 가지였다. 그 하나는 2009년 12월 중국 해커들에 의해 구글 기반의 이메일 서비스를 사용하는 인권 운동가들의 계정이 해킹 당했다는 것이었고, 다른 하나는 구글의 지적재산권에 대한 심각한 침해가 있었다는 것이었다. 이러한 이유로 구글은 중국어판 검색의 결과를 내부검열하지 않기로 결정했다고 밝혔다. 마침내 2010년 4월에는 중국 본토의 사이트를 폐쇄하고 홍콩에 사이트를 개설하여 이를 통해 검색서비스를 우회적으로 제공하게 되었다. 중국 정부가 구글의 홍콩 우회 서비스를 완전 차단하지는 않았지만, 구글의 철수 결정은 중국과 미국뿐만 아니라 국제사회에서 많은 논란을 불러 일으켰다(Hughes, 2010).

이러한 일련의 사태에 대해 중국 정부도 신속하게 대응했다. 구글의 철수 결정 발표 직후인 1월 13일 해킹과는 전혀 관련이 없다는 공식 입장을 밝히면서, 정부가 해커를 동원한다는 논리 자체가 성립되지 않는다고 주장했다. 중국은 다른 국가와 마찬가지로 법에 의거하여 인터넷을 관리하고 있으며 국제적인 인터넷 기업이 중국 내에서 기업 활동을 하려면 중국의 국내법을 따라야 하고, 정부는 당연히 중국 내에 만연하는 외설적 표현과 인터넷 사기의 폐해로부터 중국 인민을 보호해야 한다는 논리를 폈다. 중국 현실로 볼 때 중국에 악영향을 주는 인터넷 위협에 대한 정부의 대응은 오히려 부족하며 중국도 해커 공격의 피해자라는 논리로 구글의 주장에 정면으로 맞섰다. 중국 정부는 구글의 결정은 개별기업의 행위라고 의미를 축소하면서 이를 미중 관계와 중국의 이미지 훼손 등과 결부시키는 것을 경계하였다.

양국의 정부까지 가세한 6개월여 간의 논란 끝에 결국 2010년 6월말 구글은 중국 시장에서의 인터넷영업면허(ICP)의 만료를 앞두고 홍콩을 통해서 제공하던 우회서비스를 중단하고 중국 본토로 복귀하는 결정을 내리게 되었다. 이러한 구글의 결정은 중국 내 검색 사업의 발판을 유지하기 위한 결정으로 중국 당국을 의식한 유화 제스처로 해석되었다. 구글이 결정을 번복한 이유는 아마도 커져만 가는 거대한 중국 시장의 매력을 떨쳐버릴 수 없었을 것이기 때문일 것이다. 이에 대해 중국 정부는 7월 20일 구글이 제출한 인터넷영업면허의 갱신을 허용했다고 발표했다. 지메일 해킹 사건으로 촉발된 구글과 중국 정부 사이의 갈등에서 결국 구글이 자존심을 접고 중국 정부에 '준법서약'을 하는 모양새가 되었다(김상배, 2012).

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.

사실 당시 미국 정부가 가세하면서, 사태는 구글이라는 개별기업 차원을 넘어 미국이라는 국가의 외교 차원의 갈등으로 비화될 조짐을 보였다. 2010년 1월 15일 미국 정부는 구글의 입장에 대한 지지를 표명하였는데 중국 정부가 사이버 공격의 원인에 대한 구체적 정보를 밝혀야 한다는 것이었다. 1월 21일에는 힐러리 클린턴(Hillary Clinton) 미 국무장관은 구글의 결정을 언급하면서 인터넷과 정보 자유의 문제를 제기한 구글의 결정을 치켜세웠다(Clinton, 2010). 여기에 더해 미 상원은 구글 해킹 사건을 비난하고 중국 정부에 진상조사를 촉구하는 결의안을 채택하고 표현과 언론의 자유를 제한하는 중국의 정책을 비판했다. 또한 오바마 행정부는 미국의 대만 무기 수출 계획안을 발표한데 이어 달라이 라마를 접견하겠다고 발표하기도 했다. 중국 위안화의 환율 문제나 반덤핑 관세와 같은 무역장벽의 문제가 제기되기도 하였다. 구글 사건은 미중관계 전반으로 확대되는 듯이 보였다.

이렇듯 2010년의 구글 사건은 단순한 인터넷 비즈니스 분야의 소동이나 이를 대하는 해당 국가의 정부정책이라는 차원을 넘어서는 국가 간 제도표준경쟁의 면모를 지니고 있었다. 이 사건의 결말은 구글이 고개를 숙이고 다시 중국 시장으로 돌아감으로써 일단락된 것처럼 보이지만, '이미지의 세계정치'라는 시각에서 보면 권위주의적 인터넷 통제정책을 펴는 중국 정부에 대해서 일종의 '도덕적 십자군'으로서 구글의 이미지를 부각시킨 사례일 수 있다. 이렇게 보면 중국 정부가 거대한 국내시장을 무기로 구글을 굴복시켰다고 할지라도 실제로 누구의 승리였는지를 묻는 것이 간단하지 않게 된다. 왜냐하면 구글 사건은 양국의 정부와 기업(그리고 네티즌)들이 추구하는 정책과 제도의 표준을 놓고 벌인 경쟁이었기 때문이다(김상배, 2012).

2010년 구글 사건에 표명된 중국 정부의 태도는 2013-14년 스노든 사건과 중국군 기소 사건을 거치면서 더욱 완강해졌다. 예를 들어, 시진핑 주석은 2014년 7월 16일 브라질 국회에서 행한 연설에서, 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 "이는 곧 모두가 아

는 상식을 의미 한다"며 "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 미국과 중국의 인식과 제도의 차이는 사이버 안보 분야에서 국제규범의 형성 과정에 대한 양국의 입장 차이로 표출되었다.

역사적으로 사이버 안보 분야의 국제규범 형성은 그 자체가 독립적 이슈로서 다루어졌다기보다는, 넓은 의미에서 본 인터넷 거버넌스의 일부로서 논의되어 왔다(Mueller, 2010; DeNardis, 2013). 이러한 인터넷 거버넌스를 지배한 것은 미국을 기반으로 하여 활동하는 인터넷 전문가들과 민간사업자들이 자율적으로 거버넌스의 체계였는데, 이는 소위 이해당사자주의(multistakeholderism)로 불린다. 이해당사자주의의 구상을 잘 보여주는 사례는 초창기부터 인터넷을 관리해온 미국 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 모델의 실험대였다. 그런데 이러한 모델은 인터넷 전문가들이나 민간 행위자들이 전면에 나서는 모습으로 보이지만, 실상은 미국 정부가 뒤에서 사실상 패권을 발휘하고 있다는 비판으로부터 자유롭지 못했다(김상배, 2010).

이러한 기존의 인터넷 거버넌스 모델에 대해서 최근 개도국들이 반론을 제기하고 있다. 개도국들은 인터넷 분야에서 이해당사자주의를 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)을 찾아가는 과정과 맞물렸다. 특히 인터넷 거버넌스의 운영 과정에 국가 행위자들의 영토주권이 좀 더 적극적으로 인정되어야 한다는 것이다(김의영·이영음, 2008; Cowhey and Mueller, 2009).

이상의 인터넷 거버넌스의 구도를 염두에 두고 사이버 안보의 국제규범 형성을 둘러싸고 벌어지는 미국과 중국의 표준경쟁을 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. 서방 진영은 사이버 공간에서

표현의 자유, 개방, 신뢰 등의 기본 원칙을 존중하면서 개인, 업계, 시민사회 및 정부기관 등과 같은 다양한 이해당사자들의 의견이 수렴되는 방향으로 국제규범을 모색해야 한다고 주장한다. 이에 대해 러시아와 중국으로 대변되는 진영은 사이버 공간은 국가주권의 공간이며 필요시 정보 통제도 가능한 공간이므로 기존의 인터넷 거버넌스를 주도해 온 서방 진영의 주장처럼 민간 중심의 이해당사자주의에 의해서 사이버 공간을 관리할 수는 없다고 주장한다(강하연, 2013; 장규현·임종인, 2014).

이러한 대립의 구도에서 볼 때, 사이버 안보 분야에서 벌어지는 미·중 경쟁은 국제규범의 미래를 놓고 벌이는 세 가지의 경합이 복합적으로 나타나는 국제적 차원의 제도표준경쟁으로 볼 수 있다. 먼저 눈에 띄는 것은 사이버 공간에서는 여전히 전통적인 국가 행위자들끼리의 경합이 발견되는데, 미국과 서방 선진국들이 주도하는 '패권의 표준'과 중국과 여타 개도국들이 제기하는 '대항의 표준'이 맞선다. 여기에 이해당사자들이 형성해온 '민간 표준'과 국가 행위자들이 주도하는 '국가 표준'의 경합이 중첩된다. 이러한 표준경쟁의 가장 상위에 겹쳐서 자리 잡은 것은 초국적으로 다양한 행위자가 참여하는 '거버넌스의 표준'과 정부 간 관계를 바탕으로 한 '국제기구의 표준'이 경합하는 양상이다. 이러한 세 층위의 제도표준경쟁의 구도에서서 대체로 미국이 전자의 논리를 취한다면 중국은 후자의 논리에 기반을 두고 있다.

Ⅴ. 사이버 안보의 미·중 담론표준경쟁

가장 추상적인 차원에서 볼 때 사이버 안보의 미·중 표준경쟁은 사이버 안보담론의 표준을 놓고 벌이는 경쟁이다. 사실 사이버 안보라는 현상은 아직까지도 그 위협의 실체와 효과가 명시적으로 입증되지 않았다(Rid, 2013). 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). 이렇게 보면 미국과 중국 사이에서 인터넷과 관련된 보안기술(또는 기술표준)이나 인터넷 정책과 규범 등과 관련하여 벌어지고 있는 경쟁은 모두 사이버 공간의 안보담론을 선점하려는 경쟁과 밀접히 관련된다. 이는 단순히 관념의 차이가 아니라 이를 통해서 구성될 미래의 방향을 놓고 벌이는 이익규정의 차이에 기반을 두고 있기 때문이다. 특히 '사이버'와 '안보'라는 말이 '국가'에 의해서 조합되는 과정에서 그러한 담론의 차이가 극명하게 드러난다. 미국과 중국의 사례만 보더라도, '사이버'와 '안보'는 세 가지 차원의 국가 개념, 즉 '정부(government),' '국가(state)', '네이션(nation)' 등과 만나서 다르게 구성된다.

'사이버'라는 말이 인프라나 네트워크와 같은 물리적 층위나 논리적 층위를 지칭하면 컴퓨터 보안, 정보보호, 네트워크 보안 등에서 보이는 것처럼, 안전(安全, safety)이나 보호(保護, protection) 등과 같은 중립적인 뉘앙스를 갖는다. 지식, 이념, 정체성 등과 같은 콘텐츠 층위를 지칭하면, 경우에 따라서는 국내정치나 치안의 뉘앙스를 갖는 보안(保安)이라는 말로 번역되기도 하며, 대외적인 함의를 가질 때는 주로 안보(安保)라고 번역된다. 또한 '안보'가 '정부'와 만나면 다소 중립적인 '안전'이나 '보호'의 의미로, '사회(society)'와 대립되는 의미의 '국가'와 만나면 '보안'의 의미로, 대외적 차원의 '네이션'과 만나면 '안보'의 의미로 구성되곤 한다. 이러한 세 가지 조합은 객관적으로 존재하는 각기 다른 현실을 지칭하는 것이라기보다는, '국가' 행위자들의 의도에 따라 간주관적으로 구성되는 안보담론에 담긴 현실이다. 사이버 안보 분야에서 벌어지는 미·중 경쟁에는, 다음과 같은 세 가지 차원에서 구성되는 안보담론의 차이가 발견된다.

첫째, '정부' 차원에서 본 미국의 사이버 안보담론은 중국의 해커들이 미국의 물리적 인프라와 지식정보 자산을 심각하게 침해하고 있다는 주장으로 나타난다. 2000년대 후반부터 미국 정부와 언론은 중국 해커들의 공격이 미국의 근간을 뒤흔드는 위협이라는, 소위 '중국해커위협론'을 펼쳤다.[4] 중국의 해커들이 중국 정부와 군의 지원받아서 미국 정부와 기업들의 컴퓨터 네트워크를 공격한다는 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).

게다가 이들 사이버 공격이 노린 것이 미국 기업들의 지적재산권이라는 것을 심각하게 여겼다. 앞서 언급한 2013년 멘디언트의 보고서나 2014년 3월 미 법무부의 중국군 장교 기소도 중국의 해킹 공격이 정보통신, 항공우주, 행정, 위성, 통신, 과학연구, 컨설팅 분야에 집중해 있다고 지적했다. 2014년 7월 잭 루(Jack Lew) 미 재무장관도 중국의 해킹으로부터 헤지펀드와 투자자산회사의 사이버보안 대책 마련에 적극 나서야 할 것이라고 강조했다(「조선일보」 2014-7-30). 이러한 안보담론은 자연스럽게 미국의 인권 단체, 정부관리, 각계 전문가 등을 중심으로 중국에 대해서 인터넷 검열기술을 제공하는 것을 금지하는 것이 필요하다는 문제제기를 하게 했다. 이러한 취지에서 중국의 영토 내에 서버를 설치하거나 또는 이메일 서비스를 제공하고 검열기술을 판매하는 것을 제한해야 한다는 주장도 제기되었다(USAID, 2010).

이러한 '중국해커위협론'에 대해서 중국은, "미국이 스스로 해커의 공격으로부터 제일 피해를

4) 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.

보는 나라라는 인식을 조장하고 있다"는 논리로 맞섰다(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: p.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).

이에 비해 중국이 사이버 안보담론의 구성에서 중시하는 것은 소위 '정치안전'에 대한 위협이었다. 중국 인터넷정보판공실 부주임 왕슈쥔(王秀军)에 따르면, 현재 중국이 "관심을 가지고 있는 인터넷안전은 의식형태의 안전, 데이터안전, 기술안전, 응용안전, 자본안전, 루트안전 등이 포함되는데... 총괄적으로 보면 정치안전이 근본이 된다"고 하였다. 그에 의하면, "현재, 외부세력들이 인터넷을 [중국에] 대한 침입과 파괴의 주요 루트로 삼는데 인터넷자유라는 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 의식형태영역에 대한 침투와 반(反)침투의 투쟁에서 승리를 취득하느냐의 여부"는 많은 부분에서 중국의 미래에 중요하다는 것이다(「大公网」, 2014-5-18).

둘째, 국내적인 의미의 '국가' 차원에서 본 미국의 사이버 안보담론은 개방된 공간으로서 인터넷 상에서의 개인의 권리와 표현의 자유 등의 가치를 표방하고 이에 대한 침해를 경계하는 내용을 담고 있다. 앞서 언급한 구글 사건이 터질 무렵인 2010년 1월 21일 행한 힐러리 클린턴 미국무장관의 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).

이러한 주장의 연속선상에서 볼 때, 앞서 살펴본 2010년 구글 사건은 미국과 중국의 인터넷 정책의 차이를 넘어서 인터넷에 담긴 정치담론의 차이, 즉 자유롭고 개방된 인터넷의 담론과 통제되고 폐쇄된 인터넷의 담론을 놓고 벌어진 표준경쟁의 성격을 갖고 있었다. 당시 구글로 대변되는 미국의 IT기업들(그리고 미국 정부)이 중국 정부(또는 중국의 네티즌)를 상대로 해서 반론을 제기한 핵심 문제는 인터넷 자유라는 보편적 이념의 전파를 거스르는 중국 정치사회체제의 특성이었다. 이러한 점에서 구글 사건은 '정치이념의 표준경쟁'이기도 했다. 양국 간에 이러한

차이가 발생하는 것은, 일차적으로는 양국 국내체제의 제도와 정책, 그리고 역사문화적 전통과 연관되겠지만, 미국과 중국이 세계체제에서 각각 패권국과 개도국으로서 차지하고 있는 국가적 위상과도 관련이 있다(김상배, 2012).

이러한 미국의 사이버 담론에 대해서 중국은 인터넷을 검열하고 규제하는 정책적 자율성을 정당화하는 논리를 폈다. 중국이 중시하는 것은 '개인 차원의 인터넷 자유'라기보다는 '국가 차원의 인터넷 자유'이다. 왕정핑(王正平)과 쉬테광(徐铁光)의 설명에 의하면, "일개 국가의 사이버에 대한 기본요구에는 인터넷자유와 사이버안보가 포함되어 있다. 국가인터넷자유에는 자국 인터넷에 대한 자유적인 관리가 포함됨으로 타국의 간섭을 받으면 안 된다. 한 나라의 사이버안보를 수호하기 위해서는 그 나라는 인터넷심사를 진행할 필요가 있는 것이다. 중국과 일부 개도국의 인터넷심사정책을 서방국가들에서 지적하는 것은 그들 국가와 국민들의 기본수요를 침해하는 것"이라고 한다(王正平·徐铁光, 2011: p. 107). 이러한 논리의 연속선상에서 보면, 2010년 구글 사건에 대한 중국 정부의 대처방식도 국가의 권리라는 차원에서 정당화된다.

이러한 중국의 눈으로 볼 때, 미국의 인터넷 자유에 대한 담론은 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 중국세력과 중국의 민족분열세력들에 자금을 지원해주어 백도어프로그램을 개발하고 사용하게 하여 중국의 사회모순과 민족관계의 부정적 측면을 주객관적으로 확대 해석한 것은 중국의 국가안보에 위협으로 되고 있다. 미국과 중국이 '인터넷 자유'를 두고 벌이는 게임은 양국의 의식형태와 가치관의 분쟁이 사이버 공간으로 연장된 것이고 양국이 주권과 인권, 주권과 안보를 두고 벌이는 분쟁이 정보화 시대에 반영된 것"이라고 했다(奕文莉, 2012. pp. 30-31). 이러한 시각에서 볼 때, 미국은 "개도국 국가들의 인터넷규제에 대하여 비평을 할 뿐, 자신이나 동맹국들의 인터넷규제에 대해서는 보고도 못 본체"하고 있는데, 이는 인터넷 자유와 사이버 안보에서 이중표준을 구사함으로써 "자신과 동맹국들에게 하나의 표준, 개도국 국가들에게 또 다른 표준을 제시하고 있는 것"으로 인식되었다(王正平·徐铁光, 2011: p. 106).

끝으로, 대외적인 의미의 '네이션'의 차원에서 본 미국의 사이버 안보담론은 글로벌 패권담론을 바탕에 깔고 있다. 인터넷이 발달하여 전세계적으로 확장되면서 미국은 사이버 공간을 정보의 흐름이 초국경적으로 이루어지는 글로벌 공간으로 상정하고 이러한 사이버 공간의 자유주의적 질서 구축에 방해가 되는 요인을 제거한다는 차원에서 사이버 안보의 담론을 제시하였다. 미국의 사이버 전략의 목표는 바로 이러한 글로벌 공간에서 패권질서를 수립하는 것이었는데, 선발자의 이득을 바탕으로 민간 이해당사자들이 주도하는 글로벌 거버넌스의 메커니즘의 이면에서

사실상의 패권을 행사하는 것이다. 이러한 미국의 글로벌 패권담론은 앞서 언급한 국제규범의 형성과정에서 나타나는 미국의 입장과 일맥상통하는 바가 크다.

이에 대해 중국은 반(反)패권주의적이고 민족주의적인 국가주권의 안보담론을 펼치고 있다. 특히 중국 정부는 국내 차원의 권위주의적 통치를 정당화하고 대외적 압력에 대항하는 과정에서 급속한 경제적 성장과 함께 형성된 중국 국민들의 자부심과 사이버 민족주의 담론을 결합시켰다(Chao, 2005; Zakaria, 2010). 이와 관련하여 앞서 언급한 2014년 7월 16일 브라질 국회에서 행한 시진핑 주석이 행한 연설이 주는 시사점이 큰데, 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 "각국은 모두 자국의 정보 안보를 지켜야 하며 어떤 국가는 안전하고 어떤 국가는 불안전하거나 심지어 타국 안보를 희생해 자국이 말하는 절대 안보를 지켜서는 안 된다"며 상호신뢰 원칙을 존중해야 한다고 말했다(「아주경제」, 2014-7-17).

이렇듯 중국에서 사이버 공간은 국가 차원의 네트워크 인프라 위에 구축된 것으로 국가주권의 관할권 하에 있는 것으로 간주된다. 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: p. 49).

요컨대, 미국과 중국은 사이버 안보담론의 구성과정에서도 세 가지 차원에서 표준경쟁을 벌이고 있는 것으로 파악된. 미국의 담론이 주로 물리적 정보 인프라로서 컴퓨터 시스템과 네트워크 인프라, 지식정보 자산, 지적재산권의 안보를 유지하는 데 관심이 있다면, 중국의 담론은 인터넷 상에서 유통되는 콘텐츠, 즉 정치적 담론이나 이념의 내용에 주안점을 둔다. 미국의 담론이 민간의 프라이버시 보호, 보편적 인권과 표현의 자유에 관심이 있다면, 중국의 담론은 정권안보의 차원에서 인터넷에 대한 검열과 규제를 강조한다. 미국의 담론이 글로벌 패권의 자유주의적 담론을 강조하는 입장이라면, 중국의 담론은 반(反)패권주의적이고 민족주의적인 국가주권의 안보담론이다.

Ⅵ. 결론

이 글은 사이버 안보의 세계정치를 표준경쟁의 국제정치학이라는 시각에서 살펴보았다. 사이버 안보는 컴퓨터와 인터넷 분야 보안기술의 개발과 확산이 주요 관건이 되는 분야이다. 따라서 이 분야에서 기술표준을 장악한다는 것은 사이버 공간에서 벌어지는 활동의 안보 문제를 보장하는 것으로 직결된다. 이런 점에서 사이버 안보 분야에서 벌어지는 세계정치는 기본적으로 기업 간, 그리고 국가 간에 벌어지는 기술표준경쟁을 기본으로 한다. 그러나 사이버 안보는 사이버 공간의 국내외 규범과 질서 형성을 놓고 벌이는 담론과 법제도의 문제와도 밀접히 연결된다. 최근 미국과 중국 사이에서 중견국으로서 외교전략의 진로를 고민하고 있는 한국의 입장에서 볼 때도 이러한 중층적인 의미를 지니고 있는 사이버 안보의 문제는 북한의 핵무기 개발 문제를 둘러싼 전통안보의 문제에 못지않게 중요한 안보문제이다. 이러한 문제의식을 바탕으로 이 글은 기술, 제도, 담론의 세 가지 차원에서 벌어지는 3차원 표준경쟁의 시각에서 사이버 안보 분야에서 두 강대국인 미국과 중국이 벌이고 있는 패권경쟁을 이론적·경험적으로 조명하였다.

첫째, 사이버 안보 분야에서 벌어지는 미국과 중국의 기술표준경쟁은 미국이 주도하고 있는 인터넷과 사이버 안보 분야의 기술패권에 대항하는 중국의 독자적인 표준전략의 경합으로 이해된다. 사실 PC시대부터 정보산업 분야에서 미국의 IT기업들과 중국 정부(또는 중국 기업)와 벌인 기술표준에 대한 논란은 잘 알려져 있는 사실이다. 인터넷 시대의 사이버 안보 분야에서도 이러한 기술표준을 둘러싼 경쟁은 미국과 중국이 사이버 갈등을 치루는 수면 아래에서 치열하게 벌어지고 있다. 주로 미국의 IT기업들이 제공하는 컴퓨터 운영체계나 인터넷 시스템 장비에 대한 보안문제가 중국 정부의 큰 우려사항이다.

둘째, 사이버 안보 분야에서 벌어지는 미국과 중국의 표준경쟁은 사이버 안보와 관련된 인터넷 정책과 제도 및 글로벌 차원의 규범형성을 놓고 벌어지는 제도표준경쟁의 양상으로 나타나고 있다. 기술표준 분야의 도전에서는 중국이 미국 IT기업들의 벽을 쉽게 넘을 수 없었던 반면, 제도표준의 분야에서는 나름대로 효과적으로 미국의 공세를 견제하고 있다. 중국 시장에 진출하려는 기업은 누구라도 중국 정부의 규제지침을 따라야만 중국 시장에 진출할 수 있기 때문이다. 게다가 중국의 인구와 시장 규모의 힘은 일차적으로는 무역장벽으로 작동할 수 있으며 장기적으로는 독자표준을 추구할 배후지가 된다. 중국이 아직까지는 역부족이었지만 지속적으로 독자적인 기술표준을 모색하는 것은 바로 이러한 맥락에서 보아야 한다.

끝으로, 사이버 안보 분야의 미·중 표준경쟁은 사이버 안보의 개념이 무엇이고 그 내용이 무엇인지에 대한 담론을 둘러싸고 벌어지는 표준경쟁이다. 현재 미국과 중국 간에 벌어지는 사이

버 안보와 관련된 논점의 차이는 문제 자체를 보는 시각의 차이에서 비롯된다. 미국이 주요 정보 인프라로서 컴퓨터 시스템의 네트워크 안보를 유지하는 데 관심이 있다면, 중국은 인프라 자체 보다는 인터넷에 반영되는 정치안전에 주안점을 둔다, 이러한 차이는 민간을 중심으로 추구되는 인터넷 자유와 좀 더 넓게는 글로벌 안보를 강조하는 미국 정부의 입장과 정권안보 또는 국가주권의 차원에서 인터넷에 대한 검열과 규제를 정당화하는 중국 정부의 입장 간에 존재하는 차이로 드러난다.

요컨대, 이러한 3차원 표준경쟁의 시각에서 볼 때, 사이버 안보 분야에서 벌어지는 미국과 중국의 경쟁은, 예전에 국제정치에서 출현했던 패권경쟁과는 달리 복합적인 권력게임을 벌이는 다층적인 행위자들의 네트워크 게임으로 이해해야 한다. 이 글에서 '미국'과 '중국'이라고 통칭해서 지칭하기는 했지만, 엄밀히 따져보면 경쟁에 참여하는 행위자들의 성격 자체가 전형적인 국가 행위자라기보다는 정부와 다국적 기업뿐만 아니라 해커들의 네트워크까지도 관여하는 복합적인 모습이다. 게다가 이들이 사이버 안보 분야에서 벌이는 경쟁의 양상도, 적어도 현재까지는, 물리적이거나 물질적인 갈등과 경쟁을 보이기보다는 시장에서의 기술표준과 정책·제도의 우수성, 그리고 대상의 성격과 해결 주체에 대한 담론 형성을 놓고 벌이는 모습으로 나타나고 있다. 이런 점에서 사이버 안보의 세계정치는 물질적 권력의 행사를 통해서 나타나는 국가들 간의 정치, 즉 '국제정치(國際政治, inter-national politics)'의 게임이라기보다는 국가 및 비국가의 복합 행위자들이 벌이는 표준경쟁의 네트워크 세계정치 게임이다. 서론에서 사이버 안보 분야의 미·중 표준경쟁을 '망제정치(網際政治, inter-network politics)'라고 명명한 것은 바로 이러한 이유 때문이다.

이렇게 사이버 안보 분야에서 복합적으로 벌어지는 미국과 중국의 표준경쟁은 단순히 두 나라의 관계에만 그치는 것이 아니라, 동아시아와 세계정치 전반에 광범위한 영향을 미친다. 21세기 세계패권을 놓고 자웅을 겨루는 두 나라의 경쟁이 야기하는 변화의 소용돌이로부터 한국도 자유로울 수는 없다. 특히 최근처럼 중견국으로서 한국이 새로운 외교의 방향을 모색하고 있는 시점에서 사이버 안보의 미·중 경쟁은 미래전략의 차원에서 고민해야 하는 중요한 구조적 환경의 변화이다. 이 글의 논의를 바탕으로 볼 때, 사이버 안보 분야에서 벌어지고 있는 미·중 3차원 표준경쟁은 한국의 표준전략, 또는 표준경쟁의 관점에서 본 외교전략에 적어도 다음과 같은 세 가지 묶음의 질문을 던지게 한다.

첫째, 만약에 사이버 안보 분야의 기술표준과 관련하여 미국과 중국의 사이에서 한국이 선택을 해야 한다면 어떻게 해야 할 것인가? 미국의 글로벌 지배표준을 계속 고수할 것인가, 중국이 독자적으로 추진하는 표준 진영에 편입할 것인가, 아니면 중견국으로서 한국의 독자표준을 개발

할 것인가? 그리고 이러한 표준선택의 상황이 단순한 기술과 산업 분야가 아닌 한미동맹과 한중협력의 재조정 문제라는 외교문제로서 다가올 경우는 어떻게 할 것인가? 둘째, 인터넷과 사이버 안보 분야의 국내정책과 제도모델(좀 더 구체적으로는 표준 거버넌스 모델)을 모색함에 있어서 한국이 추구할 방향은 어디인가? 미국이 주창하는 민간 주도의 이해당사자주의 모델인가, 아니면 중국이 고수하려고 하는 국가 주도의 인터넷 통제 모델인가? 그리고 만약에 사이버 안보 분야에서 워싱턴 컨센서스나 베이징 컨센서스와 같은 정치경제 모델을 설정할 수 있다면, 그 사이에서 중견국으로서 한국이 추구할 사이버 안보 분야의 '서울 컨센서스'는 가능할까? 끝으로, 미국과 중국이 서로 상이한 사이버 공간의 안보담론을 모색하는 경쟁을 벌이는 와중에 한국이 제시하는 담론의 내용은 무엇인가? 미국이 전파하고 있는 인터넷 자유의 보편주의적 안보담론인가. 아니면 중국이 지키려고 하는 사이버 주권의 민족주의적 안보담론인가? 그 사이에서 중견국으로서 한국이 새로운 안보담론의 생성할 여지는 없는가? 예를 들어, 강대국들이 추구하는 힘의 논리에 기반을 둔 안보담론이 아닌, 규범과 윤리를 강조하는 사이버 공간의 담론을 구성할 수는 없을까?

국제정치학의 시각에서 볼 때, 표준경쟁과 표준전략에 대한 논의는 중견국 외교전략 연구에 매우 유용한 이론적 자원을 제공하는 것이 사실이다. 그러나 현재 이용 가능한 자료의 성격이나 국내외 학계의 연구 실정을 고려할 때, 사이버 안보의 세계정치에 대한 실증적 연구가 그리 용이하지만은 않은 실정이다. 따라서 미국과 중국의 사이에서 헤쳐 나갈 한국의 표준전략의 내용을 탐구하는 작업도 쉽지 않다. 그럼에도 지금 이 시점에서 사이버 안보 분야, 그리고 좀 더 넓게는 21세기 세계정치 전반에서 미국과 중국이 벌이는 표준경쟁의 전개양상을 올바로 이해하고 이에 대응하는 표준전략 또는 외교전략의 방향을 수립하는 작업은 시급히 필요하다. 이 글에서 살펴본 사이버 안보 분야의 미·중 표준경쟁에 대한 논의가 이에 대응하는 한국의 표준전략에 대한 후속 정책연구를 유발하기를 기대해 본다.

참 고 문 헌

강하연(2013). ICT교역의 글로벌 거버넌스, 서울대학교 국제문제연구소 편. 「커뮤니케이션 세계정치」 기획특집 <세계정치> 33(2). 서울: 사회평론: 73-109.

김상배(2007). 「정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터산업」 파주: 한울.

김상배(2010). 「정보혁명과 권력변환: 네트워크 정치학의 시각」 파주: 한울.

김상배(2012). 정보화시대의 미·중 표준경쟁: 네트워크 세계정치이론의 시각, 「한국정치학회보」 46(1): 383-410.

김상배(2014). 「아라크네의 국제정치학: 네트워크 세계정치이론의 도전」 파주: 한울.

김의영·이영음(2008). 인터넷과 거버넌스: ICANN의 ccNSO 형성과정에서 ccTLDs 세력의 역할을 중심으로, 「국제정치논총」 48(2): 173-196.

「뉴시스」(2014). 중국 정부, 애플제품 정부 조달 품목서 제외, 8월 7일. <http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140807_0013095370&cID=10808&p ID=10800> (검색일: 2014년 8월 8일).

「매일경제」(2014) 인민군 해킹혐의로 기소되자 중, 미 기업에 보복, 5월 23일. <http://news.mk.co.kr/newsRead.php?year=2014&no=800319> (검색일: 2014년 5월 25일).

배영자(2011). 미국과 중국의 IT 협력과 갈등: 반도체 산업과 인터넷 규제 사례, 「사이버커뮤니케이션학보」 28(1): 53-88.

「서울경제」(2014). '아이폰 마찰'까지... 골 깊어지는 미-중, 7월 13일. <http://economy.hankooki.com/lpage/worldecono/201407/e2014071318142069760.htm> (검색일: 2014년 7월 14일).

「아시아경제」(2014). 미 IT공룡들, 중국정부의 파상공세에 움찔, 7월 29일. <http://www.asiae.co.kr/news/view.htm?idxno=2014072908235745851> (검색일: 2014년 7월 30일).

「아주경제」(2014). 중국 시진핑 '미국 앞마당' 브라질 국회 연설 '무슨 말 했나', 7월 17일. <http://www.ajunews.com/view/20140717151605782> (검색일: 2014년 7월 18일).

「아주경제」(2014). MS 반독점법 조사설에 중국 국산 소프트웨어 '반사이득', 7월 30일. <http://www.ajunews.com/view/20140730133939299> (검색일: 2014년 7월 31일).

이희진·오상조(2008). 중국의 정보통신기술 표준 전략: 한국의 정보통신산업에 주는 함의, 「정보화정책」 15(4): 55-68.

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

「조선일보」(2014). 중국 상하이 소재 61486부대 12국이 하는 일은..., 7월 30일. <http://news.chosun.com/site/data/html_dir/2014/07/30/2014073001530.html> (검색일: 2014년 7월 31일).

「지디넷코리아」(2014). 중국 정부판 리눅스, 130만 다운로드 돌파, 2월 17일. <http://www.zdnet.co.kr/news/news_view.asp?artice_id=20140217095449&type=det> (검색일: 2014년 8월 11일).

하영선·김상배(편)(2010). 「네트워크 세계정치: 은유에서 분석으로」 서울: 서울대학교출판문화원.

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.

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.

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 사이버 안보문제에서 중국을 겨누는가), 「时事报告(시사보고)」 第7期.

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.

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.

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.

「大公网(대공망)」(2014). 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, 5月 18日. <http://news.takungpao.com/mainland/focus/2014-05/2481785.htm> (검색일: 2014년 7월 18일).

「网易科技(망역과기)」(2009). 美称中国军用电脑装国产操作系统'麒麟'(미국에 의하면 중국군용 컴퓨터들은 국산 운영체제인 '기린'을 설치하였다고 한다), 5月 13日. <http://tech.163.com/09/0513/15/5971ICO9000915BD.html> (검색일: 2014년 5월 15일)

「环球网科技(환구망과기)」(2014). 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), 5月 29日. <http://tech.huanqiu.com/it/2014-05/5007875.html> (검색일: 2014년 7월 18일).

「新浪网(시나넷)」(2012). 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), 11月 27日<http://finance.sina.com.cn/china/20121127/064513805924.shtml> (검색일: 2014년 7월 25일).

「新华网(신화망)」(2014). 外交部: 中方正研究政策加强网络信息安全(외교부: 중국은 현재 인터넷정보 안전의 강화를 위한 정책을 연구 중이다), 5月 28日. <http://news.xinhuanet.com/world/2014-05/28/c_1110904778.htm> (검색일: 2014년 7월 16일).

「中国电子报(중국전자보)」(2010). 中标软件与国防科大联手做强国产操作系统(차이나스탠더드소프트웨어사는 국방과학기술대와 손을 잡고 국산 운영체계를 강화시켜 나간다, 12月 21日. <http://cyyw.cena.com.cn/a/2010-12-21/129291519751092.shtml> (검색일: 2014년 5월 15일)

「参考消息网(참고소식망)」(2014). 三大措施打造'网络国门'(3대 조치로 '국가사이버게이트'를 만들어야 한다), 1月 3日. <http://ihl.cankaoxiaoxi.com/2014/0103/326499.shtml> (검색일: 2014년 7월 16일).

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

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: 2014년 8월 12일).

Cowhey, Peter and Milton Mueller(2009). Delegation, Networks, and Internet Governance, in Miles Kahler. ed. *Networked Politics: Agency, Power, and Governance.* Ithaca and London: Cornell University Press.

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

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

Economy Insight(2014). 스노든 사태로 날벼락 맞은 시스코, 1월 1일<http://www.economyinsight.co.kr/news/articleView.html?idxno=2123> (검색일: 2014년 5월 21일)

Gilpin, Robert(1987). *The Political Economy of International Relations.* Princeton, NJ: Princeton University Press.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander 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.

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

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

Kahler, Miles(ed.)(2009). *Networked Politics: Agency, Power, and Governance.* Ithaca and London: Cornell University Press.

Lee, Heejin and Sangjo Oh(2006). A Standards War Waged by a Developing Country: Understanding International Standard Setting from the Actor-Network Perspective, *Journal of Strategic Information Systems.* 15: 177-195.

Leander, Anna(2000). A Nebbish Presence: Undervalued Contributions of Sociological Institutionalism to IPE, in Ronen Palan(ed). Global Political Economy: Contemporary Theories. New York: Routledge: 184-196.

Lieberthal, Kenneth and Peter W. Singer(2012). *Cybersecurity 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

Modelski, George and William R. Thompson(1996). *Leading Sectors and World Powers: The Coevolution of Global Politics and Economics.* Columbia: University of South Carolina 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.

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.

Zakaria, Fareed(2010). Clash of the Titans, *Newsweek.* January 25: 34-36

김상배(金湘培): 미국 Indiana University, Bloomington 대학교에서 정치학 박사학위(논문: Wintelism vs. Japan: Standards Competition and Institutional Adjustment in the Global Computer Industry, 2000)를 취득하고, 현재 서울대학교 정치외교학부 교수로 재직 중이다. 주요 연구관심 분야는 정보혁명과 네트워크의 세계정치이며, 주요 저서로는『정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터 산업』(한울, 2007),「정보혁명과 권력변환: 네트워크 정치학의 시각」(한울, 2010),「아라크네의 국제정치학: 네트워크 세계정치이론의 도전」(한울, 2014) 등이 있다(ssangkim@snu.ac.kr).

<논문접수일:2014년 8월 14일/논문수정일:2014년 9월 10일/게재확정일:2014년 9월 23일>