최종제출본 | 2020-02-15

사이버 공간의 미중 표준경쟁:

역사적 맥락과 한국에 주는 시사점

U.-S.-China Standard Competition in Cyberspace:

Historical Context and Implications for Korea

김 상 배 | 서울대학교 정치외교학부

<저자소개>

현재 서울대학교 정치외교학부 교수 및 서울대학교 국제문제연구소장이다. 미국 인디애나 대학교(Indiana University)에서 정치학 박사를 취득하였다. 주 연구 분야는 정보혁명과 네트워크의 세계정치, 미중 패권경쟁과 표준경쟁, 중견국 외교전략 등이며, 단독 저서로 『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』 (한울, 2018), 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 (한울, 2014), 『정보혁명과 권력변환: 네트워크 정치학의 시각』 (한울, 2010), 『정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터산업』 (한울, 2007)이 있다.

<국문요약>

이 장은 사이버 공간에서 벌어지는 미국과 중국의 글로벌 패권 경쟁을 사이버 안보 분야의 표준경쟁이라는 시각에서 살펴보았다. 사이버 안보는 기술공학적인 문제일 뿐만 아니라 사이버 공간의 새로운 질서와 국내외 규범 형성을 놓고 벌이는 담론과 법제도 및 정책의 문제로서 국제정치학의 분야에서도 중요한 연구주제로서 주목받고 있다. 이러한 시각에서 볼 때 사이버 안보 분야에서 벌어지는 미중경쟁은 미국이 주도하고 있는 인터넷 분야의 기술패권에 도전하는 중국의 표준전략의 경합, 즉 기술표준경쟁으로 이해해야 한다. 또한 사이버 안보 분야에서 벌어지는 미중경쟁은 이 분야의 정책과 제도 및 글로벌 차원의 규범형성을 놓고 양국이 벌이는 제도표준경쟁으로 볼 수 있다. 가장 포괄적인 의미에서 사이버 안보 분야의 미중경쟁은 사이버 안보와 이를 다루는 국가주권의 개념이 무엇인지에 대한 담론을 둘러싸고 벌어지는 담론표준경쟁이다. 최근 미국과 중국 사이에서 중견국으로서 외교전략의 진로를 고민하고 있는 한국의 입장에서 볼 때, 사이버 안보의 3차원 표준경쟁에 대응하는 문제는 전통적인 외교안보 전략의 분야에 못지않게 중요한 미래전략의 사안이다.

Ⅰ. 머리말

1. 국제정치학의 시각에서 본 표준경쟁

이 장은 사이버 공간에서 벌어지는 미국과 중국의 경쟁을 표준경쟁이라는 시각에서 살펴보았다. 미중 표준경쟁에 주목하는 논의의 이면에는 세계정치에서 벌어지고 있는 '힘의 이동'에 대한 관심이 깔려 있다. 최근 경제적으로 급성장하고 있는 중국이 이에 걸맞은 군사력과 외교력, 그리고 소프트 파워(soft power)까지 갖추고 미국의 글로벌 패권에 도전할 것이냐가 주요 관건이다. 이러한 힘의 이동을 제대로 이해하기 위해서는 어느 한 나라가 물리적 힘이 더 세어져서 상대를 압도하게 되고 이에 따라 국제질서에서 힘의 균형이 변할 것이라는 통상적인 인식의 범위에만 머물러서는 안 된다. 다시 말해 최근 세계 및 동아시아에서 벌어지고 있는 힘의 이동을 제대로 읽어내기 위해서는 미국과 중국이 벌이는 국가 간 패권경쟁이라는 전통적인 시각을 넘어서 좀 더 복합적인 시각을 갖추어야 한다. 이러한 맥락에서 이 장은 표준경쟁을 좀 더 넓은 의미에서 해석하여 미국과 중국이 벌이는 글로벌 패권경쟁을 이해하는 분석틀로 활용하였다.

표준경쟁에 주목한 이유는 최근 미국과 중국이 미래권력의 주도권을 놓고 벌이는 경쟁을 복합적으로 보여주기 위함이다. 사실 표준이라는 말은 기준을 제시하고 평균을 재는 행위에서 우러나오는 권력의 의미를 내포하고 있다. 표준은 아무나 세울 수 있는 것이 아니고 권력을 가진 소수나 공인된 다수에 의해서 설정되는 것이 상례이다. 기준에 부합하는 것을 선택하고 평균에 미달하는 것을 배제하는 메커니즘 자체가 권력을 의미하기 때문이다. 이러한 점에서 표준은 '게임의 규칙'을 부과하는 권력의 대표적인 사례이다. 그렇지만 표준의 권력이 일방적인 방식으로만 작동한다고 생각해서는 결코 안 된다. 표준을 수용하는 사람들도 표준의 권력이 작동하는 데 중요한 역할을 담당한다. 예를 들어 표준은 그 표준을 수용하는 사람의 수가 많을수록, 즉 더 큰 네트워크를 형성할수록 그 가치가 커지는 성격을 지니고 있다. 표준의 권력은 궁극적으로 그 표준을 인정하는 사람들의 행동과 생각을 움직일 수 있을 때 제대로 발휘되는 '네트워크 권력'(network power)의 대표적인 사례이다(김상배. 2010; 2014).

이렇게 표준을 세우는 권력은 오늘날의 일만은 아니다. 널리 알려진 몇 가지 사례를 들어 보자. 중국 천하를 통일한 진시황이 벌인 일련의 표준화 작업(문자, 도량형, 화폐 등)은 현실 권력의 위세를 바탕으로 이루어졌다. 미국의 남북전쟁 당시 북군이 행한 선구적인 소총 표준화 작업은 전쟁의 승패를 가르는 요인 중의 하나로 작용했다. 이밖에도 근대 산업화 과정에서 철도 궤간(軌間)을 둘러싼 표준화나 자동차 산업의 부품 표준화 등을 둘러싼 논란은 정치적·경제적 경쟁의 단면을 보여주었다. ICT분야에서 타자기의 자판배열이나 VCR시장을 놓고 벌어진 표준경쟁도 유명한 사례이다. 컴퓨터와 이동통신 및 디지털TV 분야의 표준경쟁은 좀 더 최근에 벌어진, 우리에게 익숙한 사례들이다.

이들 사례에서 보는 바와 같이, 기술자원의 우위를 바탕으로 우수한 제품을 생산한 측보다는 자신이 제시한 기술표준을 지지하는 세(勢)를 모아서 사실상(*de facto*) 표준을 세우는 측이 승자된다. 그야말로 내편을 많이 모아서 성공적으로 네트워크를 형성하는 것이 승리의 비결인 셈이다. 기술표준의 힘은 적절한 메커니즘을 통해 가능한 한 많은 사람들에 의해서 그 표준이 채택되어 공유될 때 발생한다. 이러한 이유로 인해서 표준은 국가나 공식협회 및 국제기구들이 나서는 '표준화'의 형태를 통해서 제정되는 경우가 많았다. 그런데 최근 IT산업 분야에서 기술표준 자체의 가치가 높아지면서 그 주도권을 놓고 시장에서 경쟁을 벌이는 '표준경쟁'의 중요성이 증대되었다. 이러한 표준경쟁을 통해서 기술표준을 장악하는 측은 해당 시장을 구조적으로 지배하는 승자로 군림하면서 모든 것을 독식할 가능성이 높다(김상배, 2007).

이렇게 표준을 세우는 권력의 개념은 기술과 정보 분야의 사례에만 국한된 것이 아니다. 넓은 의미에서 보면 표준의 권력은 세계정치 전반에도 적용할 수 있다. 사실 글로벌 스탠더드(global standard)라는 말은 지난 20여 년 동안 우리 사회에서 가장 많이 회자되던 용어 중의 하나이다. 일상생활에서 사용하는 제품의 규격에서부터 기업의 구조조정이나 정부정책의 개혁, 그리고 문화적 삶이나 생각하는 방식의 변화에 이르기까지 우리 사회 어디에도 파고들지 않은 곳이 없었다. 최근 정보통신혁명은 표준의 세계정치, 즉 네트워크 권력정치의 부상에 생동감을 부여하고 있다. 특히 인터넷이 만들어 놓은 네트워크 환경을 배경으로 정보와 지식을 전파하고 소통하는 과정에서 표준의 권력을 장악하려는 현상이 그 범위나 강도 면에서 점점 강화되고 있다. 그야말로 지구화 시대의 표준, 즉 '글로벌 스탠더드'를 장악하기 위한 경쟁이, 단순한 제품과 기술의 표준을 넘어서, 세계정치의 제도와 규범, 더 나아가 생각과 정체성을 설계하는 영역에까지 퍼져 나가고 있다.

이렇듯 국제정치학의 시각에서 볼 때 표준경쟁은 통상적인 기술표준경쟁의 의미를 넘어서 좀 더 넓은 의미에서 이해되어야 한다. 경영학이나 경제학을 중심으로 진행된 표준경쟁에 대한 기존의 논의는 기술과 시장 분야에만 초점을 맞추었던 것이 사실이다. 따라서 표준경쟁의 정치사회적 그리고 사회문화적 동학을 분석하려는 노력이 부족하였다. 한편 (국제)정치학의 시각에서 표준경쟁을 분석한 기존 논의들은, 경제학·경영학의 논의에 비해서, 표준의 작동방식에 대한 구체적 탐구가 상대적으로 미흡했다. 따라서 표준경쟁의 논의를 분석적으로 펼치기보다는 다소 은유적으로 원용하는 아쉬움이 없지 않았다. 이러한 맥락에서 이 장은 국가 및 비국가 행위자들이 벌이는 다층적 표준경쟁의 동학을 네트워크 권력의 시각에서 업그레이드시키는 노력을 펼쳐보고자 한다. 이 장에서 살펴본 미중 패권경쟁의 사례들은 바로 이러한 표준경쟁의 세계정치라는 시각에서 이해할 수 있는 현상들이다(김상배, 2012).

2. 3차원 표준경쟁의 시각

이 장이 사이버 안보 분야에서 벌이는 미국과 중국의 경쟁을 이해하기 위해서 원

용한 분석틀은 표준경쟁의 국제정치학적 논의이다. 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 ICT산업 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 미중 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 기술과 산업에서 효과적인 경쟁을 벌이기 위해서는 새로운 제도환경의 조성, 즉 일종의 제도표준의 우위를 겨루는 보이지 않는 경쟁이 동시에 진행된다. 보통 국제정치학에서 제도표준에 대한 논의는 기업모델, 산업모델, 정책모델 등의 형태로 알려져 이다. 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. 국제정치학의 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. 이러한 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 공간에서 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 장이 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.

Ⅱ. 미중 표준경쟁의 역사적 맥락

역사적으로 국제정치의 분야에서 발생한 패권경쟁은 이른바 선도부문(leading sector), 특히 첨단기술 분야에서 벌어지는 주도권 경쟁의 형태로 나타났다. 선도부문에서 벌어지는 강대국들의 패권경쟁은 국제정치 구조의 변동을 반영하는 사례라는 점에서 국제정치이론의 오래된 관심사 중의 하나이다. 실제로 역사적으로 해당 시기 선도부문에서 나타났던 경쟁력의 향배는 글로벌 패권의 부침과 밀접히 관련된 것으로 알려져 있다. 가장 비근한 사례로는 20세기 전반 전기공학이나 내구소비재 산업, 또는 자동차 산업 등을 둘러싸고 벌어진 영국과 미국의 패권경쟁을 들 수 있다. 좀 더 가까이는 20세기 후반 가전산업과 컴퓨터 하드웨어 및 소프트웨어 산업에서 벌어진 미국과 일본의 패권경쟁을 들 수 있다. 이러한 연속선상에서 21세기 선도부문인 컴퓨터 산업과 인터넷 서비스 분야에서의 미국과 중국의 패권경쟁도 이해할 수 있다

(Gilpin, 1987; Modelski and Thompson, 1996; 김상배, 2007; 2012; 2014).

1. 컴퓨터 소프트웨어 기술의 표준경쟁

1990년대 말과 2000년대 전반 마이크로소프트와 중국 정부가 컴퓨터 운영체계를 놓고 표준경쟁의 형태를 띠는 경합을 한 차례 벌인 바 있었다. 당시의 경쟁은 마이크로소프트의 지배표준에 중국이 도전장을 던지면서 발생했다. 중국은 1990년대 후반부터 대항담론의 차원에서 독자표준을 모색하였는데, 리눅스가 그 사례이다. 오픈소스 소프트웨어인 리눅스는 1991년에 출현하였는데, 소소코드를 소유하고 공개하지 않는 윈도 운영체계에 대한 대안을 모색하려는 의도에서 등장했다. 리눅스는 지난 20여 년 동안 서버나 워크스테이션 등과 같은 대용량 컴퓨터를 중심으로 성장하여 최근 모바일 컴퓨팅 분야로 확장되었다. 이러한 리눅스는 시장에서의 성공여부를 떠나서 운영체계 소프트웨어의 대항표준이라는 관점에서 주목을 받아 왔다.

중국 정부도 일찌감치 리눅스의 이러한 대항표준으로의 성격에 착안하여 다양한 지원을 아끼지 않았다. 1990년대 말과 2000년대 초에 중국 정부는 리눅스 운영체계와 애플리케이션 개발 사업에 막대한 예산을 지원하였다. 이러한 과정에서 중국의 리눅스 전문기업들은 정부의 강력한 지원에 힘입어 리눅스 보급의 선봉장 역할을 담당하였는데, 1999년 8월 중국과학원이 후원하여 설립된 '홍기리눅스'라는 기업이 가장 대표적인 사례이다. 중국 정부가 리눅스 운영체계를 지원한 정책의 배경에는 경제적 동기 이외에도 마이크로소프트의 플랫폼 독점에 대한 민족주의적 관점에서 본 우려도 자리 잡고 있었다. 궁극적으로 중국의 리눅스 실험은 마이크로소프트와의 관계에서 기대했던 것만큼의 큰 소득을 거두지는 못했다. 중국의 리눅스가 잘못했다기보다는 오히려 중국 시장에서 마이크로소프트가 선전을 벌였기 때문이었다.

실제로 마이크로소프트는 2000년대 중후반에 걸쳐서 다양한 사업 전략을 구사하여 중국의 소프트웨어 시장에 대한 구조적 지배의 촉수를 서서히 뻗쳐 갔다. 특히 소스코드의 개방과 대폭적인 가격 인하 전략이 먹혀들었다. 2003년에는 마이크로소프트는 중국을 포함한 60개국에 윈도의 소스코드를 개방했을 뿐만 아니라 필요에 따라서 개작할 수 있도록 허용하는 전략을 택하였다. 또한 당시 중국 내에 횡행하던 마이크로소프트 제품에 대한 불법복제와 관련해서도 마이크로소프트는 기존의 발상을 전환하는 전략을 선택했다. 결국 중국에서 불법복제를 멈출 길이 요원하다면 아예 공개적으로 불법복제를 인내하는 것이 최선의 전략이라는 결론에 도달했다.

이와 병행하여 마이크로소프트는 미국과 유럽 및 다른 나라들에서는 수백 달러를 받던 윈도와 오피스군의 가격을 중국 시장에서는 단 7-10달러(학생판은 3달러)만 받고 제공하는 전략을 택했다. 이러한 결정의 이면에는 가격을 대폭 인하해서 똑같은 가격으로 정품을 얻을 수 있다면 왜 불법복제를 하겠느냐는 생각이 자리 잡고 있었다. 실제로 중국의 뒷골목 시장에서 판매되는 복제품은 디스크 값만 쳐도 인하된 가격의 윈도보다 비쌌다. 이렇게 가격의 문턱을 낮춰서 중국의 사용자들이 정품 소프트

웨어를 구입하도록 유도함으로써, 불법복제 제품이나 리눅스로부터 분리시키는 효과를 보았다.

이러한 마이크로소프트의 전략들은 역설적으로 중국 내에서 정품 소프트웨어의 사용률이 늘어나는 결과를 낳았다. 중국 정부는 점차로 공공기관에서 정품 소프트웨어를 사용하도록 요구했다. 마이크로소프트에게 더욱 고무적인 것은 2006년에 중국 정부가 자국 내 민간 PC제조업자들에게도 정품 소프트웨어를 탑재하도록 요구한 일이었다. 마이크로소프트가 자체적으로 평가하기를, 2006년과 2007년에 걸쳐서 정품 소프트웨어를 탑재한 컴퓨터들의 숫자가 1년 6개월 만에 20퍼센트에서 40퍼센트로 늘어났다. 그 결과 윈도·오피스 제품의 대폭적 할인에도 불구하고 2007년 현재 마이크로소프트는 약 7억 달러의 수익을 거두었다. 이는 마이크로소프트가 세계시장에서 거둔 수익의 1.5퍼센트에 불과하지만, 윈도가 중국 내에서 약 90퍼센트의 시장점유율을 차지하는 성공이었다.

컴퓨터 소프트웨어 분야에서 벌인 미국과 중국의 경쟁은 언뜻 보기에는 마이크로소프트가 소소코드를 개방했을 뿐만 아니라 불법복제를 허용하고 제품가격을 대폭 인하하면서 중국의 정부와 사용자에게 고개를 숙이고 들어간 것처럼 보였다. 그러나 표준경쟁의 시각에서 보면 실상은 반대로 해석될 여지가 더 많다. 결과적으로 마이크로소프트의 문턱 낮추기에 이은 개방표준의 전략으로 인해서 중국은 독자표준을 수립하려는 전략을 포기하고 마이크로소프트의 표준으로 편입되었기 때문이다. 실제로 2000년대 중반 이후 펼쳐진 마이크로소프트의 공세적인 가격정책과 친화적 사업 전략으로 인해서 중국은 리눅스를 개발하기보다는 마이크로소프트의 제품을 저렴한 비용으로 수용하는 방향으로 선회하였다. 결국 표준이라는 관점에서 보면 중국 표준은 없고 마이크로소프트의 표준만이 남는 상황이 발생한 것이다.

2. 인터넷 정책과 제도의 표준경쟁

마이크로소프트는 기술표준경쟁에서는 승리했을지 몰라도 중국이 제시하는 인터넷과 관련된 정책이나 기타 제도와 관련된, 비(非)기술적인 차원의 표준을 수용해야만 했다. 중국 정부는 정책과 제도의 국가별 차이나 정치사회 체제의 발전 정도라는 인식을 넘어서, 미국의 글로벌 스탠더드에 대항하는 '중국형 정보화 모델'을 추구하였다. 예를 들어, 중국 정부는 인터넷상의 불건전하고 유해한 정보를 차단하고 검열하는 것은 주권국가의 정부가 취하고 있는 법적 관행이라고 주장하였다. 게다가 이러한 규제와 검열은 서구 국가들이 사이버 공간을 통해 서구적 정치모델과 가치관 및 생활양식을 중국에 쏟아 붓는 데 대한 정당한 대응이라고 반박했다. 따라서 국내외 기업을 막론하고 중국 법에 따라 자체 검열하는 것이 불가피하며, 밖으로부터 세계적 차원의 인터넷 자유의 논리를 내세워 중국의 정책과 제도를 비판하는 것은 주권국가에 대한 내정간섭이라는 것이다.

이러한 맥락에서 중국 정부는 중국 내의 인터넷 서비스 제공자들이 자체 검열을

수행하도록 요구했으며 이러한 방침은 외국 기업들에게도 예외가 아니었다. 예를 들어, 시스코, 야후, 마이크로소프트 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 ICT기업들과 마찬가지로 정치적으로 민감한 용어들을 자체 검열하라는 중국 정부의 요구를 수용하였다. 그만큼 미국 ICT기업들에게 거대한 규모의 중국 시장은 더할 나위 없이 매력적인 카드였는데, 중국의 인터넷 사용자라는 규모의 힘에 대해 순응적으로 포섭되었다.

중국 시장에 진출한 이후 구글이 받아든 성적표는 세계시장에서 차지하는 비중에 비해서 그리 인상적이지 않았다. 구글은 중국 검색시장에서 현지 맞춤형 서비스를 개발하는 등 많은 노력에도 불구하고 2위에 머물러 있었다. 2008년 3/4분기 현재 중국 토종기업 바이두의 시장점유율이 63.3퍼센트인데 비해, 구글은 27.8퍼센트의 시장점유율을 기록하였으며, 3위는 야후가 4.7퍼센트를 차지하였다. 구글은 중국 정부의 인터넷 검열 방침을 수용한다는 비판과 중국 정부와의 잦은 마찰이 있었음에도 불구하고, 중국 정부가 제시한 표준 내에 잔류하면서 검색 서비스를 제공하였다.

그러던 것이 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 해킹당했다는 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, 새로운 '끊고 맺기'를 시도한 것으로 풀이되는 구글의 철수 결정은 중국과 미국뿐만 아니라 세계사회에서 많은 논란을 불러 일으켰다(배영자, 2011; 김상배, 2012).

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.

이렇듯 표면적으로는 구글이 다시 중국의 방침을 수용하고 굽히고 들어간 것으로 보이지만, 구글 사건의 승자가 누구인지를 판단하기는 쉽지 않다. 앞서 살펴본 마이크로소프트의 사례에 비추어 볼 때 단순히 눈에 보이는 현상에만 주목하여 판단할 수는 없다. 사실 PC시대의 패권을 마이크로소프트가 쥐고 있었다면, 현재 전개되고 있는

인터넷 시대의 강자는 단연코 구글이다. 앞으로 벌어질 경쟁에서 구글은 다른 어느 행위자들보다도 IT분야의 향배를 좌지우지할 영향력을 가지고 있다. 구글은 인터넷의 표준과 규범을 정의할 수 있는 몇 안 되는 행위자 중의 하나임에 불명하다. 사실 승패 여부를 판단하는 것을 떠나서 14억 인구에 달하는 중국을 상대로 일개 다국적 기업이 대결을 벌여서 6개월여 간 세계의 이목을 집중시켰다는 사실은 그냥 가볍게 볼 일이 아니다.

게다가 구글 사건이 주는 의미는, 단순히 미국의 IT기업과 중국 정부의 갈등이라는 차원을 넘어서, 양국의 정치경제 모델의 차이와도 관련된다. 이 사건에서 나타난 구글의 행보가 미국 실리콘밸리에 기원을 두는 기업-정부 관계를 바탕에 깔고 있다면, 이를 견제한 중국 정부의 태도는 중국의 정치경제 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 소위 워싱턴 컨센서스와 베이징 컨센서스로 알려져 있는 미국과 중국의 정치경제 모델의 경쟁 또는 제도표준의 경쟁을 성격을 바탕에 깔고 있었다.

3. 인터넷 이념과 정체성의 표준경쟁

2010년의 구글 사건은 양국의 정책과 제도의 차이를 넘어서는 경쟁의 면모를 지니고 있었다. 이 사건의 결말은 구글이 고개를 숙이고 다시 중국 시장으로 돌아감으로써 일단락된 것처럼 보이지만, 이미지의 세계정치라는 시각에서 보면 권위주의적 인터넷 통제정책을 펴는 중국 정부에 대해서 일종의 도덕적 십자군으로서 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 갖고 있는 생각의 표준을 놓고 벌인 경쟁이기도 했기 때문이다.

가장 포괄적인 의미에서 볼 때, 구글 사건은 자유롭고 개방된 인터넷의 담론과 통제되고 폐쇄된 인터넷의 담론 사이에 벌어진 표준경쟁으로서 이해된다. 구글로 대변되는 미국의 IT기업들(그리고 미국 정부)이 중국 정부(또는 중국의 네티즌)를 상대로 해서 반론을 제기한 핵심 문제는 인터넷 자유주의라는 보편적 이념의 전파를 거스르는 중국 정치사회체제의 특성이었다. 이러한 점에서 구글 사건은 '이념의 표준경쟁'의 일면을 지니고 있었다. 이러한 이념의 표준경쟁은 앞서 살펴본 제도의 표준경쟁과 밀접히 연관되어 있다. 그럼에도 불구하고 미국과 중국이 벌이고 있는 표준경쟁을 온전히 이해하기 위해서는 양자를 나누어 이해하는 것이 유용하다. 특히 양국 간의 이념의 차이가 발생하는 것은, 일차적으로는 양국 국내체제의 제도와 정책, 그리고 역사문화적 전통과 연관되겠지만, 미국과 중국이 세계체제에서 각각 패권국과 개도국으로서 차지하고 있는 국가적 위상과 밀접히 관련이 있기 때문이다. 이러한 점에서 미중경쟁

은, 용어 자체가 조금 어폐가 있지만, '정체성의 표준경쟁'이라고 부를 수 있다.

이념과 정체성의 표준경쟁이라는 관점에서 볼 때, 미국은 인터넷 자유주의의 확산과 그 지원체계 구축을 위한 노력을 기울여 왔다. 특히 미국의 인권 단체, 정부관리, 각계 전문가 등을 중심으로 중국에 대해서 인터넷 검열기술을 제공하는 것을 금지하고 더 나아가 인터넷 자유주의 확산을 위한 법적·제도적 지원을 펼치는 것이 필요하다는 문제제기가 지속적으로 이루어졌다. 이러한 취지에서 중국과 같이 권위주의 국가의 영토 내에는 서버를 설치하거나 또는 이메일 서비스를 제공하고 검열기술을 판매하는 것을 제한해야 한다는 주장도 제기되었다. 이러한 문제제기를 반영하여 미국은 2000년대 초반부터 중국에서 인터넷 자유주의를 부추기는 차원에서 디지털 공공외교를 다각도로 펼쳤다. 특히 2010년 상반기의 구글 사건은 인터넷 자유의 확산에 대한 미국 정부의 관심을 제고시켰다(김상배, 2012).

이에 비해 인터넷 분야의 이념 표준경쟁에서 중국은 민족주의의 독자표준을 추구하고 있는 것으로 판단된다. 사실 초국적으로 작동하는 인터넷이 만들어내는 공간에서 국가 단위에 기반을 둔 민족주의의 이념이 득세한다는 것은 다소 역설적일 수 있다. 그러나 IT와 인터넷의 공간이 단순한 기술의 공간이 아니라 사회적으로 구성되는 공간이라는 점을 상기하면 그리 이상할 것도 없다. 실제로 중국에서 인터넷의 공간은 민족주의의 공간으로 구성되고 있는데, 이러한 현상은 인터넷에 대한 중국 정부의 권위주의적 통제나 개도국으로서 중국이 세계체제에서 차지하고 있는 위상 등의 변수와 미묘하게 연결되어 있다. 다시 말해 중국 지도부가 그들의 정통성을 강화하고 대외적 압력에 대항하려는 의도나 급속한 경제적 성장과 함께 형성된 중국인들의 국민적 자부심 등이 인터넷상에서의 민족주의와 결합하였다. 이렇게 중국의 특수성을 내세우는 구상은 인터넷에 대한 보편주의를 내세우는 미국의 그것과 충돌할 수밖에 없었다.

이러한 인터넷 이념과 정체성의 충돌이 발견되는 분야 중의 하나는 지적재산권과 불법복제의 문제이다. 여기서 지적하려는 것은 실제로 중국에서 불법복제가 행해지고 있고 이 문제가 얼마나 심각하냐의 '현실'은 아니고, 불법복제와 관련된 이념과 정체성의 표준경쟁이다. 사실 불법복제의 문제와 관련하여 중국은 국제적으로 성숙한 선진국의 이미지보다는 아직 '문명화되지 않는' 개도국의 이미지를 벗어나지 못하고 있다. 다시 말해, 미국이 신자유주의를 전파하는 보편적 규범의 수호자로서 이미지를 유지한다면, 중국은 국제규범으로부터 다소 일탈적인 이미지를 갖고 있는 것이 사실이다. 소프트웨어나 기타 디지털 콘텐츠의 지적재산권 문제와 관련하여 중국 정부는 '책임 있는 대국'의 이미지를 구현하기 위해서 노력하기보다는 다분히 불법복제의 관행을 방조하는 정책적 태도를 취해왔다.

이러한 시각에서 보면, 중국은 보편적 원리에 충실한 이미지보다는 자국의 특수성을 주장하는 이미지로 그려진다. 이에 비해 미국은 인터넷 세상의 질서와 규범을 수호하는 이미지이다. 비유컨대, 마치 일탈행위를 하는 '사이버 해적'과 이를 단속하려는 '디지털 보안관'의 경주를 본다고나 할까? 그런데 중국이 좀 더 '책임 있는 대국'으로서 이미지를 구축하고 싶다면, 이러한 불법복제와 해킹을 지원하는 국가로서의

이미지는 큰 부담이 아닐 수 없다. 사실 이 분야에서 중국의 관련 법규는 명목상으로는 존재하지만 실제로는 집행되지 않는 '그림 속의 호랑이'라는 인식이 강했다. 이러한 상황에서 관건이 되는 것은 중국이 자국의 특수성을 주장하는 독자 표준의 차원을 넘어서 세계시민들까지도 설득하는 보편적인 표준을 추구하느냐의 여부이다.

이러한 연속선상에서 볼 때, 최근 중국이 미국에 대해서 벌이고 있는 패권경쟁의 양상은 기술과 제도 및 이념의 표준을 놓고 벌인 3차원의 표준경쟁의 분석틀을 활용하여 이해할 수 있다. 우선, 중국의 리눅스 지원정책과 마이크로소프트의 중국 시장 진출 사례를 통해서 살펴본 미국과 중국의 경쟁은 기술표준경쟁의 대표적인 사례이다. 둘째, 2010년 상반기 미국의 인터넷 기업 구글의 중국 시장 철수 결정을 통해서 드러난 미국과 중국의 갈등은 양국의 정책과 제도의 표준을 놓고 벌인 복합적인 경쟁이었다. 끝으로, 가장 포괄적인 차원에서 보면 미국과 중국이 불법복제와 해킹의 문제를 놓고 벌인 논란은 정보화시대의 이념과 정체성의 표준을 놓고 벌인 경쟁으로 해석될 수 있다.

Ⅲ. 사이버 공간의 미중 표준경쟁

이 장에서 미중 표준경쟁의 구체적 사례로서 주목하는 분야는 사이버 안보이다. 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.

1. 사이버 안보의 미중 기술표준경쟁(1): 초기 사례

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 것이

라는 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 장의 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.

앞서 다루었다시피, 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 '훙치(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 훙치리눅스의 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 훙치리눅스'라고 불리면서 중국산 운영체계의 대표 브랜드로 발돋움했다. 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 전환

을 추진하고 있다.

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 보안 검사는 마이크로소프트와 IBM, 시스코, 애플 등에 집중되었다. 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.

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 서버로 교체해서 사용하도록 지시하기도 했다.

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) 인터넷보안연구소장에 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 중국

시장 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.

2. 사이버 안보의 미중 기술표준경쟁(2): 화웨이 사태

최근 복잡다단해지고 있는 사이버 공간의 미중경쟁의 단면을 가장 극명하게 보여주는 사례 중의 하나가 ‘화웨이 사태’이다. 미국 정부는 화웨이 문제를 산업의 문제가 아닌 안보의 관점에서 봐야 한다고 강조했다. 화웨이 제품에 심어진 백도어를 통해서 미국의 사이버 안보에 큰 영향을 미칠 데이터가 빠져나간다는 것이었다. 이런 점에서 화웨이 문제는 ‘실재하는 위협’으로 부각되었으며, 이러한 담론에 근거해서 대내외적으로 화웨이 제재의 수위를 높여갔다. 이에 대해 화웨이와 중국 정부는 화웨이 제품에 대한 미국 정부의 의심과 경계는 객관적인 근거가 없으며, 오히려 주관적으로 위협을 과장함으로써 이를 통해 달리 얻고자 하는 속내가 있다는 논리로 맞섰다. 화웨이 제품의 사이버 안보 문제를 놓고 벌이는 미중 간의 ‘말싸움’은 앞으로 ‘창발’(創發, emergence)할 가능성이 있는 미래의 안보위협을 놓고 벌이는 담론정치의 전형적인 양상을 보여주고 있다(김상배, 2019).

그러나 이러한 안보담론 경쟁의 이면에 현실 국제정치의 이권 다툼이 자리 잡고 있음을 놓쳐서는 안 된다. 사실 화웨이를 둘러싼 미중 갈등의 기저에는 미래 선도부

문(leading sector) 중의 하나인 5G 이동통신 부문을 중심으로 벌어지는 양국의 기술 패권 경쟁이 있다. 실제로 최근 화웨이 견제에서 나타나는 미국의 행보는 중국의 '기술굴기'에 대한 견제의식을 노골적으로 담고 있다. 또한 이러한 기술굴기를 부당하게 지원하는 중국의 정책과 법·제도에 대한 강한 반감도 숨기지 않고 있다. 이러한 인식은 국가안보를 명분으로 내세운 전략적 수출입 규제와 이에 수반된 양국 간의 통상마찰로 나타났으며, 이례적으로 우방국들을 동원해서라도 화웨이 제품의 확산을 견제하려는 '세(勢) 싸움'의 양상으로 드러났다. 이런 점에서 화웨이 사태는 미래 글로벌 패권을 놓고 벌이는 미중 양국의 '지정학적 경쟁'을 방불케 한다.

화웨이 사태 관련 논란은 2010년대 초중반으로까지 거슬러 올라간다. 중국의 사이버 안보 위협에 대한 미국의 안보화 담론은 2010년대 초반의 '중국 해커 위협론'에서 2010년대 후반의 '중국 IT보안제품 위협론'으로 이행했다. 이러한 담론이행의 핵심에 중국의 통신장비 업체인 화웨이가 있다. 미국과 화웨이(또는 ZTE) 간의 갈등의 역사는 꽤 길다. 2003년 미국 기업 시스코는 자사의 네트워크 장비 관련 기술을 부당하게 유출했다는 의혹을 제기하면서 화웨이를 고소했다. 2012년 미 하원 정보위원회는 화웨이 통신장비들이 백도어를 통해서 정보를 유출하고 랜섬웨어 공격을 가한다며 안보 위협의 주범으로 지적했다. 2013년 미국 정부도 나서서 중국산 네트워크 장비 도입이 보안에 위협이 될 수 있음을 인정했는데, 2014년에는 화웨이와 ZTE 설비의 구매를 금지한다고 발표가 있었다. 2016년에는 미국 내 화웨이 스마트폰에서 백도어가 발견되는 사건이 발생하기도 했다.

이러한 분위기는 2018년 들어 급속히 악화되었다. 2018년 1월 미국 업체인 AT&T가 화웨이의 스마트폰을 판매하려던 계획을 전격 취소했다. 2월에는 CIA, FBI, NSA 등 미국의 정보기관들이 일제히 화웨이와 ZTE의 제품을 사용하지 말라고 경고했다. 3월에 FCC는 화웨이 등 중국 업체들에 대해 '적극적 조치'를 취하겠다고 발표했다. 4월에는 ZTE가 대(對)이란 제재 조치를 위반했다는 혐의로 미국 기업들과 향후 7년간 거래 금지라는 초강력 제재를 받았다가 6월에 구사일생했다. 7월에는 차이나모바일의 미국 시장 진입이 불허됐다. 8월에는 미국 정부는 '2019년 국방수권법'을 통과시키며 화웨이와 ZTE 등 5개 중국 기업의 제품을 정부 조달품목에서 원천 배제하기로 했다. 12월에는 화웨이 부회장 겸 최고재무책임자(CFO)인 멍완저우가 대(對)이란 제재 위반 혐의로 체포됐다. 2019년 2월 마이크 펜스 미국 부통령은 뮌헨안보회의에서 미국의 동맹국들이 화웨이 제품을 사용하지 말 것을 촉구했다.

이렇게 전세계적 이목을 끈 화웨이 사태는 2019년 5월 14일 트럼프 대통령의 행정명령으로 새로운 국면에 접어들었다. 미국 당국은 국가안보를 위협한다는 이유로, 화웨이를 거래제한 기업목록에 올렸고, 주요 IT기업들에게 거래 중지를 요구했다. 따라서 구글, MS, 인텔, 퀄컴, 브로드컴, 마이크론, ARM 등이 화웨이와 제품 공급계약을 중지하고 기술계약을 해지했다(*Economist*, May 20, 2019). 이러한 조치는 화웨이 제품의 수입중단 조치와는 질적으로 다른 파장을 낳을 것으로 예상되었다. 그도 그럴 것이 화웨이가 글로벌 공급망에 크게 의존하고 있는 상황에서 부품 공급차질에

따라 장비와 소프트웨어의 업데이트 등이 막힌다면, 화웨이는 미국의 의도대로 5G 이동통신 시장에서 완전히 축출될 가능성도 배제할 수 없기 때문이다. 게다가 2019년 6월에는 중국에서 설계·제작되는 5G 장비를 미국 내에서 사용 금지하는 방안의 검토가 보도되었는데, 이러한 방안이 현실화된다면 미국의 통신장비 공급망이 완전히 새롭게 짜이는 것을 의미한다는 점에서 파장이 컸다.

전문가들은 이러한 수출입 규제조치의 여파가 예상했던 범위를 넘어설 것으로 우려했다. 일각에선 트럼프 행정부의 압박이 오히려 중국의 보호주의적 대응을 초래하고 자체 기술개발을 촉진시킬 것이란 전망도 나왔다. 중국이 반도체, 항공기술, 로보틱스의 자급화를 모색함으로서 글로벌 공급망의 분절화(fragmentation)가 초래될지도 모른다고 우려되었다(Luce, 2018). 이러한 경향이 지속되면 기업들은 각기 상이한 시장을 놓고 상이한 제품들을 생산하는, 이른바 '기술의 발칸화'(balkanization)가 발생할지도 모른다고 경계되었다(Knight, 2019). 이러한 지적들은 미국의 제조업과 긴밀히 연결된 수천 개 중국기업들 중의 하나인 화웨이만을 염두에 둔 근시안적 조치가 낳을 부작용을 우려했다(Rollet, 2019). 특히 이러한 행보가 미국과 중국이 지난 수십년 동안 긴밀히 구축해 온 글로벌 공급망을 와해시키고 경제와 기술의 '신냉전'을 초래할지도 모른다는 경고가 제기되었다(Lim, 2019).

그럼에도 최근의 사태전개는 화웨이 장비의 보안 문제를 넘어서 정치군사적 함의를 갖는 여타 기술 분야로 확산될 조짐마저 보이고 있다. 2019년 하반기에 접어들면서 미국은 화웨이에 이어 드론 업체인 DJI와 CCTV 업체인 하이크비전에 대한 제재 카드를 다시 꺼내 들었다. 2019년 5월 20일 미 국토안보부는 중국의 드론이 민감한 항공 정보를 중국 본국으로 보내고 있다고 폭로했다. 이는 2018년 9월 특허 침해 논란이 있었던 중국의 드론 업체인 DJI를 염두에 둔 발표로 해석되었다. 한편 2017년 11월 미국 시장 진출에 대한 우려를 제기한 바 있었던 CCTV 업체 하이크비전에 대해서도 제재를 검토한다는 보도가 나왔다. 2019년 5월 22일 하이크비전을 상무부 기술수출 제한목록에 올리는 것을 검토 중이라고 했다. CCTV가 중국 정부의 소수민족과 반체제 세력에 대한 감시도구로 활용되는 상황에서 하이크비전에 대한 압박은 천안문 사태 30주년을 맞이하여 미국이 중국의 인권 문제를 겨냥했다는 해석을 낳았다.

이상에서 살펴본 화웨이 사태의 이면에는 일종의 '화웨이 포비아(phobia)'가 미국형 안보화 담론정치의 일환으로 작동하였다(*Economist,* Jan 31, 2019). 화웨이의 장비를 쓰는 것이 위험하다는 공포감의 근거는, 백도어라는 것이 지금은 아니더라도 언제든지 심어 넣을 수 있는 미래의 위협이기 때문이다. 특히 5G 시스템은 공급업체가 제공하는 소프트웨어 갱신에 크게 의존하기 때문에 언제든지 악성코드를 심는 것이 가능하다는 것이었다. 게다가 화웨이라는 기업의 성장배경이나 성격을 보면, 이러한 미국 정부의 주장은 나름대로의 '합리적 의심'이었다. 특히 미국은 화웨이라는 기업의 뒤에 중국 정부가 있다는 사실을 의심했다. 2017년 7월 시행된 중국의 <인터넷안전법>에 따르면, 중국 정부가 정보제공을 요청하면 민간 기업은 이를 거부할 수 없기 때문에 더욱 그러했다. 이러한 상황에서 화웨이가 5G 이동통신망을 장악할 경우 이는

미국의 핵심적인 국가정보를 모두 중국 정부에게 내주는 꼴이 될 것이라는 우려가 제기되었다.

사실 중국이 5G와 중국표준에 각별한 관심을 가진 이유는, 과거 3G 시장에 뒤늦게 진출해 표준설정 과정에서 배제되고 통신장비 및 단말기 산업에서 뒤진 경험 때문이었다. 또한 4G LTE 시장에서도 중국이 부진한 사이 미국 등 주요 선진국들이 선두사업자로서 큰 수혜를 누리는 것을 감수해야만 했다. 이러한 맥락에서 중국 업체들의 선제적 투자와 중국 정부의 정책적 지원이 5G 분야에서 이루어졌으며, 이를 바탕으로 화웨이와 같은 중국 업체가 글로벌 기술경쟁력을 갖추게 되었다. 스마트시티, 원격의료, 자율주행차 등과 같이 중국이 주력하고 있는 4차 산업혁명 시대의 인프라 구축과정에서 5G 이동통신 기술이 지니는 전략적 가치에 대한 인식도 중국이 이 분야에서 먼저 치고 나가는 동기부여가 되었다.

이러한 맥락에서 볼 때, 안보화의 담론정치에서 나타나는 중국의 관심은 미국 기업들의 기술패권으로부터 독자적인 표준을 지키고 자국시장을 수호하는 데 있었다. 중국형 안보화의 내용적 특징은, 하드웨어 인프라의 사이버 안보를 강조한 미국의 경우와는 달리, 소프트웨어와 정보 콘텐츠 및 데이터에 대한 주권적 통제를 확보하는 것으로 나타났다. 이러한 중국의 인식은 중국 시장에 진출하여 사업을 하는 미국의 다국적 기업들에 대한 규제정책에 반영되었다. 표면적으로는 인터넷 상의 유해한 정보에 대한 검열 필요성을 내세웠지만, 대내적으로는 중국 정부에 정치적으로 반대하는 콘텐츠를 걸러내고, 대외적으로는 핵심 정보와 데이터가 국외로 유출되는 것을 막으려는 주권적 통제의 의도가 깔려 있었다.

최근 중국의 인터넷 정책은 데이터의 국외이전에 대한 규제에 집중되고 있는데, 이러한 과정에서 적극 원용되는 것이 2017년 7월 1일 시행된 <인터넷안전법>이다. <인터넷안전법>은 외국 기업들의 반발로 2019년 1월 1일로 그 시행이 유예되기도 했다. 이 법은 핵심 기반시설의 보안 심사 및 안전 평가, 온라인 실명제 도입, 핵심 기반시설 관련 개인정보의 중국 현지 서버 저장 의무화, 인터넷 검열 및 정부당국 개입 명문화, 사업자의 불법정보 차단 전달 의무화, 인터넷 관련 제품 또는 서비스에 대한 규제 등을 내용으로 한다. <인터넷안전법>은 미국 기업들에 맞서서 정보주권 또는 데이터 주권을 지키려는 중국의 안보화 담론을 그 바탕에 강하게 깔고 있었다. 표면적으로는 개인정보 보호 강화 및 국가와 국민의 안전을 목표로 내세웠지만, 사실상 사이버 보안시장의 국산화, 자국 산업 보호, 인터넷 뉴스 정보활동의 통제, 기업체 검열 강화 등이 진짜 의도라는 의혹이 제기되었다(손승우. 2019).

그럼에도 미국의 IT기업들은 중국의 <인터넷안전법> 시행을 수용하지 않을 수 없는 처지였다. 특히 애플의 행보가 주목을 끌었는데, <인터넷안전법> 시행 이후 애플은 중국 내에 데이터센터를 건설하였으며, 2018년 3월부터는 아이클라우드 계정의 암호 해제에 필요한 암호화 키도 중국 당국에 넘겼다. 이는 중국 내 1억 3천만 명이 넘는 애플 이용자의 개인정보가 담긴 아이클라우드 계정이 데이터 주권의 행사라는 명목 하에 중국 국영 서버로 넘어가는 것으로 의미했는데, 이에 따라 중국 정부는 직권

으로 아이폰 사용자들을 모니터링하고 통화내역·메시지·이메일 등을 검열할 수 있게 되었다. 이는 중국 내에서 수집된 자국민의 데이터를 반드시 국내에서만 사용해야 한다는 규정을 따른 조치였지만, 중국 이용자들이 인터넷 검열에 노출되는 것은 불을 보듯 뻔한 일이었기에 많은 우려가 제기된 것은 당연했다. 미국 당국의 테러 수사에도 협력을 거부했던 애플이었지만, 매출의 20%를 차지하는 중국 시장에서 퇴출당하지 않기 위해서 '불가피한 결정'을 내렸다.

3. 사이버 안보의 미중 제도표준경쟁: 5G 기술표준 경쟁의 이면

중국 기업인 화웨이의 통신장비가 미국의 국가 사이버 안보에 실제 위협인지에 대해서는 논란의 여지가 있을지 몰라도, 화웨이로 대변되는 중국 기업들의 기술추격이 5G시대 미국의 기술패권에 대한 위협임은 분명하다. 5G는 기존의 4G LTE에 비해 속도가 최대 100배가 빠르고, 10배 이상의 기기를 한 번에 사용할 수 있으며, 응답속도가 현저히 빨라진다. 5G 환경의 구축을 바탕으로 하여 다양한 4차 산업혁명 시대의 기술들이 구현될 수 있고, 사물인터넷으로 연결되고 클라우드 환경을 배경으로 하여 빅데이터와 인공지능을 활용하는 수많은 기기들이 제대로 작동할 수 있다. 그야말로 5G는 생활환경을 바꾸고 새로운 서비스를 가능하게 만드는 패러다임 전환의 기술이 아닐 수 없다. 이러한 5G 기술의 표준을 장악하기 위한 기업 간, 그리고 국가 간 경쟁은 이미 시작됐다. 그런데 문제는 미국이 제대로 준비가 되기 전에 화웨이가 치고 나왔다는 점이다(Johnson and Groll, 2019).

화웨이는 4G LTE 시절부터 저가경쟁을 통해 몸집을 키운 뒤 늘어난 물량을 바탕으로 기술력을 키우는 전략을 통해 이제는 가격도 경쟁사보다 20~30% 저렴한 것은 물론 기술력도 세계 최고의 수준을 자랑하게 되었다. 2018년 현재 화웨이의 글로벌 이동통신 장비 시장점유율은 28%로 세계 1위이다. 화웨이는 이동통신 장비 시장에서 2012년 에릭슨을 누르고 최대 매출을 올리는 회사로 성장했고 2016년에는 에릭슨 매출의 2배 규모에 이르렀다. 에릭슨과 시스코의 연합이 원천기술을 보유하고 있으면서도 시장이 형성되지 않아 머뭇거리고 있던 사이, 화웨이는 중국 정부의 지원에 힘입어 초기 투자를 집중하여 '선발자의 이익'을 누리게 되었다. 2018년 4월 미국 이동통신산업협회(CTIA)의 '글로벌 5G 경쟁' 보고서에 따르면, 주요국의 5G 이동통신 주파수 분배와 정부 정책, 상용화 수준 등에서 미국이 중국에 뒤져 있다고 한다.

이러한 점에서 화웨이 사태의 이면에 중국의 5G 기술굴기에 대한 미국의 견제의식이 강하게 깔려 있음을 쉽게 추측할 수 있다(Harrell, 2019). 미국의 불만은, 중국이 기술기밀을 훔치거나 기술이전을 강요하는 행태를 보이면서 성장했다는 데 있다. 특히 중국이 5G 상용화 경쟁에서 가장 앞선 이유로 '중국제조 2025'와 같이 강력한 정부 주도 정책에 주목한다. 2018년 12월 마이크 폼페이오 국무장관, 윌버 로스 상무장관, 존 디머스 법무부 차관보, 빌 프리스탭 FBI 방첩본부장, 크리스포퍼 크렙스 국토안보부 사이버·기반시설보안국장 등이 '중국제조 2025'에 대해 일제히 퍼부은 비난

은 이러한 인식을 잘 반영한다. 이들이 내세운 일관된 메시지는 '중국제조 2025는 제조업 업그레이드를 추구하는 기술굴기가 아니라 국가 차원의 기술 도둑질인 범죄'라는 것이다. 이는 미국 외교·산업·사법·방첩 당국이 망라돼 '중국제조 2025'의 성격을 규정한 것이라고 할 수 있다(이길성. 2018).

또한 미국은 자국 기업에 악영향을 미치는 중국의 <인터넷안전법>을 미중 무역협상의 주요 의제로 정할 정도로 민감하게 반응했다. 이와 관련하여 2019년 2월 로버트 라이트하이저 미 무역대표부(USTR) 대표와 스티븐 므누신 재무장관이 중국 베이징에서 류허 중국 부총리와 만나 담판했다. 중국에서 개인정보를 취급하는 기업에 대해 데이터 서버를 반드시 중국 내에 두도록 하는 <인터넷안전법>의 조항이 문제시되었다. 그 이전 2019년 1월 워싱턴 DC에서 열린 미중 고위급 협상에서 중국은 그동안 '국가안보 문제여서 논의 불가'라고 했던 일부 사안을 논의할 수 있다고 입장을 바꾸었는데, <인터넷안전법>은 새로이 논의대상에 포함된 의제 중 하나였다. 미중 무역협상이 계속되면서 논의 불가 항목이 상당 부분 줄어들었지만 <인터넷안전법>은 여전히 미중 간 이견이 큰 항목으로 꼽혔었다(강동균. 2019).

이러한 과정에서 흥미로운 점은, 미국에서는 5G 네트워크 구축에 정부개입과 통신망 국유화의 가능성이 거론될 정도로 5G에 대한 민감한 반응이 나왔다는 사실이다. 2018년 1월 백악관 국가안보회의(NSC) 관계자는 미 정부 고위관료와 관련 정보기관에 중국의 사이버 안보와 경제 위협에 대응하기 위한 장치로서 트럼프 대통령 첫 임기 말까지 5G 통신망을 국영화하는 방안을 보고했다고 한다. 시장경제의 본국을 자처하는 미국의 컨트롤타워에서 '산업 국유화'가 거론됐다는 것은 그 자체가 매우 이례적인 일이었다. 이러한 뉴스가 유출된 2018년 초만 해도 미 상·하원 의원들은 정부가 민간 부문에 개입해서는 안 된다는 원론적인 입장만을 내놨지만, 2018년 중후반을 거치면서 5G 네트워크 구축 문제는 미국 '산업정책'의 중요 이슈로 자리 잡아 갔다(심재훈·김연숙, 2018).

미국 정부의 규제와 견제에 맞서 중국 정부도 미국의 다국적 IT기업들을 향한 압박을 가하기는 마찬가지였다. 특히 <인터넷안전법>에 의거하여, 중국 내에서 확보한 데이터를 중국 내에만 보관하고 국외로 반출하려면 당국의 허가를 받도록 의무화함으로써 미국 기업의 중국 내 서비스를 검열하고 통제하려 했다. 그런데 이른바 인터넷 안전검사와 데이터 현지화의 기준과 적용 범위가 매우 모호해 오남용의 우려가 제기되었다. 이에 미국 정부와 기업들은 법 개정을 요구하고 있지만 중국 정부는 꿈쩍도 하지 않고 있다. 예를 들어 '인터넷 안전 등급제도'에 따라 등급별로 보호 의무를 부과하는데, 문제는 그 기준이 매우 모호하다는 점이었다. 특히 중국 내 데이터 현지화와 인터넷 안전검사의 의무를 지는 최상위 등급의 '핵심 정보 인프라 운영자'의 선별 기준 등이 논란거리였다(손승우, 2019).

그럼에도 미국 IT기업들은 이 법을 수용할 수밖에 없었다. 2017년 7월 31일 애플은 중국 앱스토어에서 인터넷 검열시스템을 우회하는 가상사설망(VPN) 관련 애플리케이션 60여 개를 삭제했으며, 아마존웹서비스(AWS)는 2017년 11월 중국사업부 자

산을 매각했다. 2018년 초 MS와 아마존도 자사 데이터를 각기 베이징과 닝샤의 데이터센터로 옮겼다. 또한 <인터넷안전법> 시행 직후 애플은 중국 내 사용자들의 개인정보와 관리권을 모두 중국 구이저우 지방정부에 넘겼으며, 2018년 2월에는 제2데이터센터를 중국 네이멍 자치구에 건설할 계획을 발표했다. 2018년 12월에는 멍완저우 부회장 체포에 대한 보복으로 중국 내 애플의 아이폰 7개 기종에 대해 판매금지 처분을 내려지기도 했다. 중국 법원은 미국 기업인 퀄컴이 애플을 상대로 한 특허 소송에서 퀄컴이 요청한 판매금지 요청을 받아들이는 형식을 취했다.

한편 2019년 5월 24일 미국의 화웨이 제재가 정점으로 치닫던 시기, 중국의 인터넷 감독 기구인 국가인터넷정보판공실은 미국의 수출입 규제 조치에 맞불을 놓는 성격의 새로운 규제 방안을 발표했다. 그 내용은, 중국 정부가 자국 내 정보통신 인프라 사업자가 인터넷 관련 부품과 소프트웨어를 조달할 때 국가안보에 위해를 초래할 위험 여부를 점검하여 문제가 있다고 판단되면 거래를 금지할 수 있다는 것이었다. 이는 미국 첨단기술 제품의 중국 수출을 막을 수 있다는 신호를 보낸 것이었다. 이어서 유사한 조치를 내놓았는데, 2019년 5월 29일 중국 국가인터넷정보판공실은 국가안보를 이유로 국내 인터넷 이용자에 대한 데이터를 국외로 보내는 것을 금지하는 내용의 규정 초안을 공개하기도 했다. 새 규정은 위반 시 사업 허가를 취소하거나 심지어 형사 책임을 물리는 등 무거운 처벌 조항을 담았다. 이는 미국의 화웨이 제재에 대한 대응조치로서 향후 구글, MS, 아마존 등과 같은 많은 미국 기업에 영향을 미칠 것으로 해석되었다(김윤구, 2019).

이렇듯 주권담론에 입각한 중국의 정책적 행보는 향후 미중관계의 미래 쟁점과 관련하여 본격적인 데이터 통상마찰의 가능성을 예견케 한다. 현재 데이터의 초국적 유통을 위한 국제규범 형성과 관련해서는 미국과 중국이 각기 다른 입장을 취하고 있다. 미국의 인터넷 기업들이 초국적 데이터의 자유로운 유통을 보장하는 디지털 경제 규범의 수립을 옹호한다면, 중국은 경제적 재화로서 가치가 증대된 데이터의 국외유출에 대해 대해서 이른바 데이터 주권에 입각해서 경계론을 펴고 있다. 이러한 입장 차이를 염두에 두고 보면, 오프라인 무역에서와 마찬가지로 온라인 무역에서도 자유무역과 보호무역 간의 논쟁이 재현될 가능성이 있다. 실제로 최근의 양상을 보면, 양자협력뿐만 아니라 지역규범과 다자규범의 모색 차원에서 초국적 데이터 유통을 규제하는 디지털 경제규범의 내용에 대한 논란이 진행되고 있다.

4. 사이버 안보의 미중 담론표준경쟁: 안보화 담론

가장 추상적인 차원에서 볼 때 사이버 안보의 미중 표준경쟁은 사이버 안보담론의 표준을 놓고 벌이는 경쟁이다. 사실 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). 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, 이른바 '중국해커위협론'을 펼쳤다. 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. 2010년 구글 사건 당시에도 중국의 해커들이 적극적인 역할을 한 것으로 알려졌다.

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. 이러한 안보담론은 자연스럽게 미국의 인권 단체, 정부 관리, 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.

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

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 특명전권 군축대사 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 본 체"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 형성과

정에서 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. 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.

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)패권주의적·민족주의적인 국가주권의 안보담론이다.

Ⅳ. 미중 3차원 표준경쟁과 한국

이상에서 살펴본 사이버 안보의 미중경쟁은 기술경쟁의 문제일 뿐만 아니라 사이버 공간의 새로운 질서와 국내외 제도 및 규범 형성을 놓고 벌이는 담론과 법제도 경쟁의 문제라고 할 수 있다. 미중의 '사이버 전쟁'은 실제로 해킹 공격이 가해지고 이를 막기 위한 방책을 고안하는 차원을 넘어서는 좀 더 추상적인 경쟁의 양상으로 나

타난다. 이 장은 이러한 사이버 경쟁을 3차원적인 표준경쟁, 즉 기술-제도-담론의 표준경쟁이라는 시각에서 이해하였다. 최근 미국과 중국 사이에서 중견국으로서 외교전략 또는 표준전략을 고민하고 있는 한국의 입장에서 볼 때, 이러한 복합적인 양상으로 전개되고 있는 사이버 안보 분야 미중경쟁의 동향을 제대로 파악하는 것은 중요한 사안이 아닐 수 없다.

1. 미중 사이버 기술표준경쟁 사이의 한국

사이버 안보 분야에서 벌어지는 미국과 중국의 경쟁은 미국이 주도하고 있는 인터넷과 사이버 안보 분야의 기술패권에 대항하는 중국의 독자적인 표준전략에서 발견되는 기술표준경쟁으로서 이해할 수 있다. 사실 PC시대부터 정보통신산업 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 우려사항이었다.

한국은 사이버 안보 분야에서 경합하는 미국과 중국의 상이한 기술표준 사이에서 기회와 도전에 동시에 맞닥뜨릴 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.

사실 화웨이는 미중 사이버 안보 갈등에서 미묘한 위치에 놓여 있다. 화웨이는 스마트폰뿐만 아니라 안테나와 무선 송수신기기 등 통신장비를 생산하는데, 중국 정부가 이를 이용해 미국에서 첩보활동을 한다는 논란이 2012년부터 일었다. 당시 미국 하원 정보위원회가 중국의 스파이 활동에 화웨이가 협조한다는 의혹을 제기한 뒤 미국 행정부에 화웨이 통신장비 구매금지를 요구했다. 미 CIA 전직 국장이 하원에 출석해 “화웨이가 세계 각국에서 구축한 통신시스템 비밀 정보를 중국 당국과 공유해왔다”고 증언한 후, 미국뿐만 아니라 유럽과 캐나다에서도 화웨이 통신장비 규제론이 제기된 바 있었다. 100여 개국에 통신장비를 수출하는 화웨이는 스웨덴 에릭슨과 함께 세계 최대 통신장비 공급업체로 꼽힌다(김상배. 2019).

한국에게 이러한 종류의 선택이 부과된다는 것은 쉽지 않은 일인데, 외교적 문제와 관련되는 경우 더욱 그러하다. 예를 들어, 사이버 안보 분야에서 한국은 한미동맹

을 고수할 것이냐 아니면 한중협력을 강화할 것이냐의 선택에 놓일 수도 있다. 참으로 이러한 선택은 한편으로는 새로운 관계를 수립하고 다른 한편으로는 기존의 관계를 끊는 '맺고 끊기' 또는 비대칭적 관계조율의 과정을 의미한다. 이러한 관계의 연결과 단절의 과정은 중개외교의 핵심인데, 간혹 중개의 과정은 네트워크의 구조를 바꾸고 완전히 새로운 네트워크 환경을 만들어 네트워크 게임의 의제 자체를 바꾸기도 한다. 그러나 이렇게 한국이 미국과 중국 사이에서 비대칭적 관계조율을 추구하는 중개외교를 모색함에 있어서 두 나라를 허브로 하는 강대국 간의 망제정치에서 호환성을 잃지 말아야 함을 명심해야 할 것이다.

그렇다면 미중 간의 사이버 안보 관련 논란에서 한국이 할 만한 일이 얼마나 있느냐가 관건이다. 예를 들어 소니 영화사에 대한 북한의 사이버 공격 이후 미국이 북한의 소행임을 입증하는 과정에서 한국이 정보를 제공했던 사례를 들 수 있다. 그러나 한국이 긴히 필요한 것은 첨단 사이버 공격 및 방어 기술이지만, 이와 관련된 한미협력은 원활치 못하다. 게다가 군사적 용도를 전제로 한 사이버 기술을 미국으로부터 도입하는 것에 대해서 중국이 반길 리 만무하다. CERT 차원의 한중 협력은 잘 진행되고 있는 것으로 알려져 있다. 그런데 한국이 정작 필요로 하는 것은 북한의 사이버 공격과 관련된 경유지 정보인데, 이 부분에서는 한국과 중국 두 나라 간의 협력이 쉽지 않다. 게다가 최근 미국은 한국이 중국과 너무 가까워질까 봐 우려하고 있다.

2. 미중 사이버 제도표준경쟁 사이의 한국

사이버 안보 분야에서 벌어지는 미국과 중국의 표준경쟁은 사이버 안보와 관련된 인터넷 정책과 제도를 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.

미중 사이에서 사이버 안보 문제가 한국의 중개외교에 부과하는 기회와 도전은 양국의 인터넷 관련 정책과 규제제도, 즉 인터넷 거버넌스 상의 차이에서도 발견된다. 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 상황이다. 이는 사이버 안보 분야에서 양국이 국내 정책과 제도모델을 모색하는 과정의 차이와도 연결된다. 이러한 와중에 한국은 어느 쪽의 손을 들어 주어야 할 것인가? 미국이 주창하는 민간 주도의 이해당사자주의 모델인가, 아니면 중국이 고수하려고 하는 국가 주도의 인터넷 통제 모델인가? 만약에

사이버 안보 분야에서 워싱턴 컨센서스나 베이징 컨센서스와 같은 정치경제 모델을 설정할 수 있다면, 그 사이에서 중견국으로서 한국이 추구할 사이버 안보 분야의 새로운 모델을 제시하는 것이 가능할까?

인터넷 거버넌스 모델을 세움에 있어서 한국의 선택은 미국이 추구하는 민간 주도 모델과 중국이 지지하는 국가 개입 모델을 복합하는 방향으로 갈 수밖에 없다. 그렇다면 한국은 일견 호환되지 않는 양국의 인터넷 거버넌스 모델 사이에서 중개의 역할을 할 가능성이 있는가? 이 대목에서 중개자로서 중견국의 역할은, 완전히 새로운 모델을 창출하는 것보다는, 기존 모델들을 결합하고 복합하는 전략과 친화성에 있다는 사실에 주목할 필요가 있다. 이 장은, 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 발휘할 수 있다. 중개자의 역할이 매력적이냐 아니냐의 문제는 그 나라가 채택한 전략의 콘텐츠 문제가 아니라, 기존의 다양한 콘텐츠들을 어떻게 통합하고 엮어서 주변 국가들이 무난하게 수용하게 만들 수 있느냐에 달려 있다.

이른바 '서울 컨센서스'로 대변되는 한국의 정치경제 모델은 이와 관련된 좋은 사례를 제공한다. 정치경제 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. 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 간주되는 현실은 이러한 시나리오의 실효성을 떨어뜨리는 큰 한계로 작용한다.

3. 미중 사이버 담론표준경쟁 사이의 한국

사이버 안보 분야의 미중 표준경쟁은 사이버 위협의 원인이 무엇이고 사이버 안보의 대상과 주체가 무엇인지에 대한 담론을 둘러싸고 벌어지는 표준경쟁이다. 현재 미국과 중국 간에 벌어지는 사이버 안보와 관련된 논점의 차이는 문제 자체를 보는 시각의 차이에서 비롯된다. 미국의 사이버 안보담론은 미국 내뿐만 아니라 글로벌 차원의 물리적 네트워크 인프라의 안정성을 확보하는 데 주 관심을 두는데, 그 이면에는 인터넷 자유와 프라이버시의 보호에 대한 관심이 있다. 이에 비해 중국은 반(反)패권주의적이고 민족주의적인 국가주권의 안보담론을 펼치고 있는데, 사이버 공간을 국가 차원의 정보인프라 위에 구축된 공간으로 간주하고 그 안에서 이루어지는 활동은 국

가주권의 관할권 하에 있는 것으로 인식하고 있다.

사이버 안보 분야 한국의 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. 이러한 상황을 이해하고 타개하는 데 있어 한국의 공식적인 입장은 유엔, ITU, OECD, ICANN 등이 주도하는 글로벌 인터넷 거버넌스에 대해 개방적이고 유연한 자세를 취하여 모두 참여하고 모두 지지하는 '망라(網羅)형 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.

이러한 연속선상에서 볼 때, 서방과 비서방 진영, 좀 더 구체적으로는 미국과 중국 사이에서 어느 쪽을 선택해야 할까? 한국의 전략적 선택으로 먼저 생각해 볼 수 있는 것은 미국식 민간 주도 모델을 지지하고 커뮤니티와 전문 활동가를 활성화하는 것이다. 그런데 영미권의 사회문화에 기반을 둔 미국식 인터넷 거버넌스 모델을 다른 사회문화권에 속하는 한국에서 구현하기란 쉽지 않다. 오랫동안 정부가 주도하는 정책 모델에 익숙한 한국에서는 민간 중심의 의사결정권을 강조하는 다중이해당사자주의 모델이 정착하기도 쉽지 않다. 다중이해당사자주의 담론과 이를 추진하는 사회경제세력 사이의 괴리 문제도 간단치 않다. 글로벌 스탠더드로서 미국 모델에 마음은 가지만, 한국의 현실에서는 실제로 몸이 따라가지 못하는 상황이 발생하곤 한다.

그렇다면 생각해 볼 수 있는 한국의 대안적 선택은 국가 모델 또는 국가간다자주의 모델의 지지이다. 지난 산업화와 정보화의 역사를 되돌아보면, 한국은 정부 중심의 프레임 짜기에 익숙한 것이 사실이다. 이러한 역사에서 한국에서는 이른바 이해당사자들이 이미 '존재'해 있었다기보다는 정부에 의해서 위로부터 그 이해관계가 '구성'되고 '동원'된 측면이 없지 않다. 인터넷 거버넌스나 사이버 안보 분야의 국제적 해법을 모색함에 있어서도 정부가 나서서 한미 또는 한중의 정부간 협의를 활용하려는 경향이 강하다. 그러나 한국이 이러한 접근을 지속할 경우 국제적으로는 국가중심 접근의 경향을 추수할 가능성이 크다, 그러나 인터넷 거버넌스와 사이버 안보 분야에서 '국가간다자주의'의 표방은 '안보 변수'를 근간으로 하는 한미관계를 불편하게 만들 가능성이 있다. 이러한 선택은 중국식 글로벌 인터넷 거버넌스 모델의 지지, 유엔과 같은 전통 국제기구 중심 사이버 외교 추진, 사이버 공간에서 국가주권의 역할 강조 등을 의미할 것이기 때문이다.

결국 한국의 전략적 선택은 미국식과 중국식 논의에 동시에 참여하는 복합외교 전략 또는 좀 더 적극적으로 말해 중개외교 전략일 수밖에 없다. 현재 한국은 사이버 안보와 관련된 중개외교에서 글로벌 거버넌스 모델과 국제기구를 모두 모색하는 개방적이고 유연한 접근(open and flexible approach)을 취하고 있다. 이는 사이버 안보의 미중경쟁과 세계정치 과정에서 위치잡기를 하기 위한 기본적인 전제이다. 그러나

한발 더 나아가 현재 한국의 사이버 안보 외교전략에서 필요한 것은 이 분야에서 경합을 벌이고 있는 양국의 관계를 조율하는 중개외교의 발상이다. 이를 실현하기 위해서 한국은 진화하는 사이버 안보 분야의 구조적 조건 하에서 다층적으로 형성되는 비대칭적인 관계를 조율하는 외교적 능력을 발휘해야 한다. 이를 통해서 한국은 단순한 연결자가 아니라 상이한 행위자들 간의 관계에 상호작동성과 호환성을 제공하는 적극적 중개자로서 행동할 수 있을 것이다.

Ⅴ. 맺음말

이 장은 사이버 안보의 세계정치를 표준경쟁의 국제정치학이라는 시각에서 살펴보았다. 사이버 안보는 기술적인 문제일 뿐만 아니라 사이버 공간의 새로운 질서와 국내외 규범 형성을 놓고 벌이는 담론과 법제도의 문제로서 국제정치학의 분야에서도 중요한 연구주제로서 주목받고 있다. 최근 미국과 중국 사이에서 중견국으로서 외교전략의 진로를 고민하고 있는 한국의 입장에서 볼 때도 이러한 사이버 안보의 문제는 북한의 핵무기 개발 문제를 둘러싼 전통안보의 문제에 못지않게 중요한 안보문제이다. 이러한 문제의식을 바탕으로 이 장은 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 사이버 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.

이렇게 사이버 안보 분야에서 복합적으로 벌어지는 미국과 중국의 표준경쟁은 단순히 두 나라의 관계에만 그치는 것이 아니라, 동아시아와 세계정치에 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 대외환경의 변화이다. 이 장의 논의를 바탕으로 볼 때, 사이버 안보 분야에서 벌어지고 있는 미·중 3차원 표준경쟁은 한국의 표준전략, 또는 표준경쟁의 관점에서 본 국가전략에 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 개발할 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 지닌 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 학계의

연구 실정을 고려할 때, 이렇게 미국과 중국의 사이에서 헤쳐 나갈 한국의 표준전략의 내용을 묻는 질문에 적절한 답을 제시하는 것은 쉽지 않은 일이다. 그럼에도 지금 이 시점에서 미국과 중국의 표준경쟁을 올바로 이해하고 이에 대응하는 미래전략의 방향을 수립하는 작업이 시급히 필요하다. 이 장에서 살펴본 사이버 안보 분야의 미·중 표준경쟁에 대한 논의가 이에 대응하는 한국의 표준전략에 대한 후속 연구를 유발하기를 기대해 본다.

<참고문헌>

강동균. 2019. “기업 검열하는 中 ‘사이버 보안법’ 손본다.”『한국경제』, 2월 7일.

김상배. 2007.『정보화시대의 표준경쟁: 윈텔리즘과 일본의 컴퓨터 산업』한울.

김상배. 2010.『정보혁명과 권력변환: 네트워크 정치학의 시각』한울.

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

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

김상배. 2019. “화웨이 사태와 미중 기술패권 경쟁: 선도부문과 사이버 안보의 복합지정학.”『국제·지역연구』28(3), pp.125-156.

김윤구. 2019. “中, 인터넷 이용자 데이터 국외 반출 금지…미국 기업 겨냥.”『연합뉴스』, 5월 29일.

『뉴시스』, 2014-08-07. “중국 정부, 애플제품 정부 조달 품목서 제외.” <http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140807_0013095370&cID=10808&pID=10800> (검색일: 2014년 8월 8일).

배영자. 2011. “미국과 중국의 IT 협력과 갈등: 반도체 산업과 인터넷 규제 사례.”『사이버커뮤니케이션학보』28(1), pp.53-88.

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

손승우. 2019. “중국의 사이버보안 규제와 新보호주의 확산.”『아시아경제』, 2월 27일.

심재훈·김연숙. 2018. “美정부, 중국발 보안위협 우려에 5G망 국영화 검토.”『연합뉴스』, 1월 29일.

이길성. 2018. “美 ‘중국제조 2025는 기술 굴기 아닌 범죄’.”『조선닷컴』, 12월 14일.

이희진·오상조. 2008. “중국의 정보통신기술 표준 전략: 한국의 정보통신산업에 주는 함의.”『정보화정책』15(4), pp.55-68.

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).

Economist. Jan 31, 2019. "How to Handle Huawei."

Economist. May 20, 2019. "Holding out on Huawei."

Economy Insight, 2014-1-1. "스노든 사태로 날벼락 맞은 시스코." <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.

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

Harrell, Peter. 2019. "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation." *Testimony before the United States Senate Committee on the Judiciary,* Center for a New American Security.

Johnson, Keith and Elias Groll. 2019. "The Improbable Rise of Huawei. How did a Private Chinese Firm Come to Dominate the World's Most Important Emerging Technology?" *Foreign Policy,* Apr 3.

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, pp.177-195.

Lim, Darren. 2019. "Huawei and the U.S.-China Supply Chain Wars: The Contradictions of a Decoupling Strategy." *War on the Rocks.* May 30.

Luce, Edward. 2018. "The New Era of US-China Decoupling." *Financial Times.* Dec 20.

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.

Rollet, Charles. 2019. "Huawei Ban Means the End of Global Tech." *Foreign Policy.* July 7.

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 사이버안보문제에서 중국을 겨누는가).”『时事报告(시사보고)』第7期.
蔡翠红(차이추이훙). 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. pp.107-121.
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)』, 2014-5-18. “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: 2014년 7월 18일).
『网易科技(망역과기)』, 2009-05-13. “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)” <http://tech. 163.com/09/0513/15/5971ICO9000915BD.html> (검색일: 2014년 5월 15일)
『环球网科技(환구망과기)』. 2014-05-29. “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: 2014년 7월 18일).
『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: 2014년 7월 25일).
『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 인터넷정보안전의 강화를 위한 정책을 연구 중이다)”. <http://news.xinhuanet. com/world/2014-05/28/c_1110904778.htm> (검색일: 2014년 7월 16일).
『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: 2014년 7월 16일).