

# 화웨이 사태와 미중 기술패권 경쟁: 선도부문과 사이버 안보의 복합지정학\*

김상배 | 서울대학교 정치외교학부 교수

최근 복잡다단해지고 있는 미중경쟁의 단면을 가장 극명하게 보여주는 사례 중의 하나가 ‘화웨이 사태’이다. 중국의 통신장비 업체인 화웨이의 제품에 심어진 백도어를 통해서 미국의 국가안보에 큰 영향을 미칠 정도로 중요한 데이터가 유출될 우려가 있다는 것이 쟁점이다. 이러한 인식은 화웨이 제품에 대한 전략적 수출입 규제와 이에 수반되는 양국 간의 통상마찰을 낳고 있으며, 이러한 과정에서 동맹국들을 동원해서라도 화웨이를 견제하겠다는 외교전의 양상까지 나타나고 있다. 이러한 사태 전개에 기저에 5G 이동통신으로 대변되는 선도부문의 기술패권 경쟁이 깔려 있음도 놓쳐서는 안 된다. 미국은 중국의 ‘기술굴기’를 견제하고 화웨이와 같은 기업들을 지원하는 중국의 정책과 법·제도를 비판한다. 이러한 맥락에서 볼 때, 화웨이 사태는 미래 글로벌 패권을 놓고 벌이는 미중 양국의 ‘지정학적 경쟁’을 방불케 한다. 이 글은 이렇게 복합적인 양상으로 전개되고 있는 화웨이 사태를 이해하는 이론적 분석틀로서 ‘복합지정학(Complex Geopolitics)’의 시각을 제안하였다. 복합지정학은 지정학의 유용성을 인정하면서도, 최근 변화된 세계정치의 양상을 제대로 이해하기 위해서는, 단순히 기존의 전통 지정학으로의 회귀가 아닌, 좀 더 복합적으로 이론화된 ‘새로운 지정학’의 시각이 필요함을 역설한다. 이러한 복합지정학의 시각에서 본 화웨이 사태는, 선도부문의 기술패권 경쟁을 배경으로 하여 사이버 안보 논란과 정책·제도 마찰, 사이버 연대외교 등의 쟁점이 복합적으로 연계되는 미중경쟁의 사례이다.

주제어: 화웨이, 미국, 중국, 기술패권 경쟁, 선도부문, 사이버 안보, 복합지정학

\* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A3A2924409)

## I. 머리말

최근 복잡다단해지고 있는 미중경쟁의 단면을 가장 극명하게 보여주는 사례 중의 하나가 '화웨이 사태'이다. 미국 내에서 중국의 통신장비 업체인 화웨이와 관련된 사이버 안보 논란은 오래 전부터 제기되었지만, 미중 양국의 외교적 현안으로까지 불거진 것은 2018년 들어서의 일이다. 2018년 2월 CIA, FBI, NSA 등 미국의 정보기관들이 일제히 화웨이 제품을 사용하지 말라고 경고하고, 8월에는 미 국방수권법이 화웨이를 정부 조달에서 배제하기로 하더니, 12월에 이르러서는 화웨이 창업자의 맏딸인 멩완저우 부회장 겸 최고재무책임자(CFO)가 체포되는 사건이 발생했다. 2019년 초에는 미국이 우방국들에게 화웨이 제품을 도입하지 말라고 압박을 가하는 외교전이 벌어지더니, 5월에는 트럼프 대통령의 행정명령으로 국가비상사태를 선포하고 민간 기업들에게도 화웨이와의 거래 중지를 요구하는 데까지 나아갔다.

이러한 일련의 과정에서 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.

그러나 이러한 안보담론 경쟁의 이면에 현실 국제정치의 이권 다툼이 자리 잡고 있음을 놓쳐서는 안 된다. 사실 화웨이를 둘러싼 미중 갈등의 기저에는 미래 선도부문(leading sector) 중의 하나인 5G 이동통신 부문을 중심

으로 벌어지는 양국의 기술패권 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 나타나며, 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.

이 글은 이렇게 복잡하게 전개되고 있는 화웨이 사태의 구조와 동학을 국제정치(경제)학 분야의 이론적 시각을 원용하여 체계적으로 이해하는 것을 목적으로 한다. 특히 기존 연구에서 기술패권 경쟁을 분석하는 데 활용되었던 네 가지의 이론적 논의를 이 글에서 제안하는 분석틀 개발의 디딤돌로 삼았다. 첫 번째는 국제정치이론 분야의 선도부문과 세계정치 리더십의 ‘장주기’(Long-cycle) 이론이고, 두 번째는 국제안보론 분야의 ‘코펜하겐 학파’에서 제시하는 ‘안보화’(Securitization) 이론이고, 세 번째는 1980-90년대에 (정치)경제학 분야에서 출현한 ‘전략무역’(Strategic Trade) 이론이며, 마지막은 ‘행위자-네트워크 이론’(Actor-Network Theory, ANT)을 바탕으로 개발된 네트워크 외교전략에 대한 이론적 논의이다. 이 글이 궁극적으로 의도하는 바는 이들 논의를 유기적으로 엮어내는 이론적 분석틀을 마련하는 데 있다.

이를 위해 이 글은 ‘복합지정학’(Complex Geopolitics)의 시각을 제시한다(김상배, 2015). 복합지정학은 지정학의 유용성을 인정하면서도, 오늘날 세계정치를 제대로 이해하기 위해서는, 전통 지정학을 넘어서 다양한 시각을 엮어내야 한다고 주장한다. 아무리 영토국가들의 자원권력 경쟁에 주목하는 현실주의적 ‘(고전)지정학’이 득세하더라도, 초국적 자본이 추동하는 지구화의 추세에 주목하는 자유주의적 ‘비(非)지정학’의 시각은 여전히 유용하다. 오늘날의 국가안보 문제에서 전통적 군사안보의 위협은 여전히 실재하지만, 비전통 영역의 안보위협이 지정학적 위기로 창발되는 담론정치의 과정을 보여주는 구성주의적 ‘비판지정학’의 시각도 필요하다. 게다가 탈(脫)지리적 공간으로서 사이버 공간을 매개로 전개되는 4차 산업혁명과 5G 이동통신 부문의

경쟁과 협력을 이해하기 위해서 이른바 ‘탈(脫)지정학’의 시각도 있어야 한다.

이러한 복합지정학의 시각에서 본 화웨이 사태는, 지정학적 경쟁의 양상에 비지정학과 비판지정학 및 탈지정학의 성격을 지닌 다양한 요소들이 연계되는 과정이다. 화웨이 사태에서 가장 눈에 띄는 것은 탈지정학적 성격을 지닌 5G 이동통신 부문에서 기술패권 경쟁이라는 명목으로 두 강대국 간의 지정학적 갈등이 발생하고 있다는 점이다. 이러한 지정학적 양상은 지구화의 상호의존 과정에서 구축된 글로벌 생산 네트워크의 변화라는 비지정학적 차원의 구조변동과도 연계되는데, 구체적으로 보호주의적 수출입 규제가 전략적으로 활용되고 기술·산업 정책 및 제도가 국제적으로 통상마찰의 원인이 된다. 이렇게 복합적인 양상을 보이는 화웨이 사태는 기술문제를 국가안보 차원으로 안보화하는 비판지정학적 담론정치에 의해 추동된다. 더 나아가 이러한 안보담론은 미국이 주도하는 ‘해양세력’과 중국이 앞장 서는 ‘대륙세력’의 지정학적 대립구도를 탈지리적 공간인 사이버 공간으로 확대·강화시키고 있다.

이 글은 크게 네 부분으로 구성되었다. 제2장은 선도부문의 기술패권 경쟁을 보는 기존 이론들을 소개하고 이들을 엮어서 보는 이론적 분석틀로서 복합지정학을 제시하였다. 제3장은 화웨이 통신장비의 사이버 안보 위협을 강조하는 미국의 안보화 담론정치와 미국의 기술패권에 대항하여 독자표준을 모색하려는 중국의 주권담론을 살펴보았다. 제4장은 화웨이 사태의 이면에 깔린 미중 기술패권 경쟁의 양상을 중국의 기술추격을 견제하는 미국의 행보와 이에 대항하는 중국의 정책 및 법·제도를 살펴보았다. 제5장은 화웨이 사태의 전개과정에서 나타난 미중 양국의 외교전 양상을 미국의 우방활용 전략과 중국의 국제연대 전략을 대비하여 살펴보았다. 맺음말에서는 이 글의 주장을 종합·요약하고, 화웨이 사태가 미중 패권경쟁 전반에 주는 의미를 살펴보았으며, 아울러 한국이 취할 전략의 방향도 간략히 짚어 보았다.

## II. 기술패권 경쟁의 복합지정학적 이해

### 1. 기술패권 경쟁의 이론적 이해

이 글이 기술패권 경쟁과 세계정치 변화를 분석하는 데 디딤돌로 활용한 국제정치(경제)학 분야의 논의들을, 기존 연구에 대한 검토를 겸해서, 살펴보면 다음과 같은 네 가지 이론을 들 수 있다. 이들 이론은 로버트 콕스(Robert Cox)가 제기한 권력의 세 가지 범주인 ‘물질적 능력’, ‘관념’, ‘제도’ 변수의 상호작용과 그 외중에 형성 및 변화하는 역사적 구조로서의 ‘세계질서’라는 프레임워크에서 각기 하나의 개념적 층위를 다루는 것으로 이해할 수 있다(Cox, 1981). 콕스의 프레임워크가 주는 유용성은 ‘물질적 능력’의 변화가 새로운 ‘사회세력’을 형성하고, ‘국가형태’의 변화를 초래하며, ‘세계질서’의 구조를 바꾸는 역사적 구조의 변화 메커니즘을 담아낸다는 데 있다. 이 글은 이러한 네 차원의 프레임워크에 근거해서 기술패권 경쟁과 세계정치 변환의 역사적 사례를 이해하고, 이를 오늘날 미중경쟁의 사례에도 적용하였다.

첫째, 국제정치이론 분야에서 진행된 선도부문과 세계정치 리더십의 장주기를 탐구한 조지 모델스키(George Modelski)와 윌리엄 톰슨(William Thompson)의 이론적 논의이다(Modelski and Thompson, 1996). 역사적으로 선도부문에서 진행된 기술경쟁은 패권국과 도전국의 운명을 갈랐고, 이는 궁극적으로 국제정치의 구조변동을 야기했다. 20세기 전반 영미경쟁이 그랬고, 20세기 후반 미일경쟁이 그랬으며, 오늘날 미중경쟁도 그러할 것이다. 이러한 점에서 볼 때, 오늘날의 선도부문은 4차 산업혁명 분야로 대변되는 정보통신기술 부문인데, 그 중에서도 인공지능, 빅데이터, 클라우드 컴퓨팅, 사물인터넷, 그리고 이 글의 주제와 관련된 5G 이동통신이 해당된다. 장차 이 분야의 ‘물질적 능력’ 확보 경쟁은 강대국들의 ‘상대적 지위변화’를 유발함으로써 글로벌 패권의 항배에 지대한 영향을 미칠 것으로 예견된다.

둘째, 국제안보론 분야에서 배리 부잔(Barry Buzan)으로 대변되는 ‘코펜하

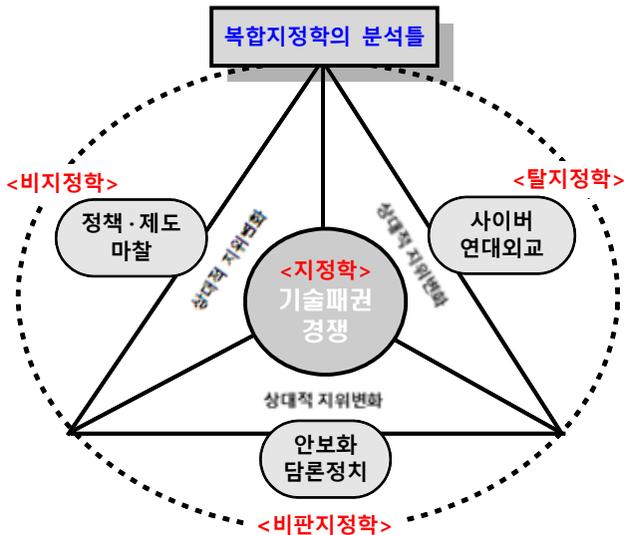
겐 학파'에서 제시한 '안보화' 이론이다(Buzan and Hensen, 2009). 탈냉전과 탈근대 시대의 국제안보는 객관적으로 실재하는 위협인 동시에 주관적으로 구성되는 위협이라는 시각에서 연구되어 왔다. 기술안보 분야에서도 선도부문 경쟁의 결과로 나타나는 강대국들의 '상대적 지위변화,' 특히 패권국의 기술경쟁력 하락은 안보화의 담론정치를 유발했다. 가장 비근하게는 1990년대 초반 미일 패권경쟁이 화두였던 당시에도 일본의 미사일용 반도체나 잠수함용 무음기술 등과 같은 이른바 민군겸용기술(dual-use technology)의 우위는 군사안보적 관점에서 심각한 위협으로 안보화 되었으며, 당시 미국이 선도부문의 육성을 위한 산업정책을 채택하는 이례적 행보를 낳았다. 오늘날 미중 경쟁에서도 이러한 기술 안보화의 '관념'이 작동하고 있음은 물론이다.

셋째, 국제(정치)경제학자인 폴 크루그먼(Paul Krugman)이나 로라 타이슨(Laura D. Tyson) 등의 논의에서 발견되는 '전략무역정책'에 대한 논의이다(Krugman, ed. 1986; Tyson, 1992). 선도부문 경쟁의 결과로 나타나는 '상대적 지위변화'는 도전국뿐만 아니라 패권국도 무역정책의 기초를 전략적으로 활용케 하는 변화를 야기하는데, 이는 국가별로 상이하게 채택되는 정책과 법·제도의 마찰로 귀결된다는 것이다. 1980~90년대 미일경쟁에서도 이러한 전략무역정책이 등장했는데, 일본의 기술추격을 경계하여 미국 정부는 일본 산업정책의 불공정성을 문제 삼았다. 대외적으로는 일본 시장의 개방에 대한 요구를 표출하였고, 대내적으로는 미국의 산업 육성을 위한 정책을 구사하였다. 이러한 '국가형태'와 '제도' 변환의 양상은 오늘날 미중경쟁에서도 드러나는데, 미국이 중국의 기술굴기를 견제하는 차원에서 '중국제조 2025'나 <인터넷안전법(網絡安全法)>을 비판하는 과정에서 나타나고 있다.

끝으로, '행위자-네트워크 이론'(Actor-Network Theory, ANT)의 대표적 논자 중의 하나인 미셸 칼롱(Michel Callon)이 제시한 '내편 모으기'와 '표준 세우기'에 대한 이론적 논의이다(Callon, 1986; 김상배, 2014, 제1장). 기술 패권 경쟁이 야기하는 국가 간의 '상대적 지위변화'는 국제정치의 관계적 구조(즉 구조)를 비집고 들어가서 주변국들의 국제적 지지를 획득하고 이를 반영한 보편적 표준을 세우는 '네트워크 전략'의 필요성을 낳는다. 1990년대 미일경쟁의 사례에서도 보면, 미국은 자국의 이익을 반영한 국제제도와 규범을

관철시킴으로써 미국 주도의 세계질서를 유지하고자 시도하였다. 이러한 양상은 오늘날에도 나타나는데, 정치군사적으로는 동맹국이었던 미일 기술패권 경쟁에 비해서, 미국과 중국이 사이버 공간을 매개로 벌이는 ‘내편 모으기’와 ‘표준 세우기’의 과정은 좀 더 넓은 범위에 걸쳐서 좀 더 본격적으로 경쟁하는 ‘사이버 동맹·연대 외교’의 양상을 보이고 있다(蔡翠红, 2012).

요컨대, 이장에서 제시한 이론적 논의를 콕스의 프레임워크에 입각해서 설정된 범주와 그 귀결에 대한 논의를 적용해서 보면, 선도부문에서 미중이 벌이는 기술패권 경쟁은 안보화의 담론정치와 양국의 정책 및 법·제도의 마찰을 유발하고, 좀 더 넓은 의미에서 오프라인 및 사이버 공간의 동맹·연대 외교를 통해서 세계질서를 주도하려는 복합적인 양상으로 그려진다(〈그림 1〉 참조). 이러한 과정에서 특히 주목할 변수는 패권국과 도전국의 ‘상대적 지위변화’가 경쟁에 임하는 양국의 대응전략 변화에 미치는 영향이라고 할 수 있다. 그런데 이렇게 다소 복잡하고 난삽하게 느껴질 수도 있는 이들 변수의 관계에 대한 논의를 좀 더 유기적으로 엮어내는 이론적 분석틀을 마련해 볼 수는 없을까?



〈그림 1〉 기술패권 경쟁의 복합지정학

## 2. 복합지정학 시각의 도입

첫째, 새로운 이론적 분석들은 5G 이동통신 부문의 미증경쟁을 전통 지정학의 시각에서 해석하여 '기술패권 경쟁'의 성격을 부각시키는 데서 출발한다 (Eurasia Group, 2018; Gu, et al., 2019). 전통 지정학은, 권력의 원천을 자원의 분포와 접근성이라는 물질적 또는 지리적 요소로 이해하고 이러한 자원을 확보하기 위한 경쟁이라는 차원에서 국제정치를 이해하는 현실주의 국제정치이론의 시각과 통한다(Mead, 2014). 최근 세계경제 분야에서도 기술발전과 상호의존을 바탕으로 한 지구화의 추세에도 오히려 자국 중심의 이익을 내세워 보호무역을 강화하고 민족주의를 부추기는 현상이 나타나고 있다. 그러나 지정학적 시각이 부활하더라도 과거 국제정치 현실에서 잉태된 시각을 미래 세계정치에 그대로 적용할 수는 없다.

둘째, 기술패권 경쟁의 지정학은 지구화의 추세 속에 지리적 공간을 넘어서 구축되는 상호의존 질서에 주목하는 비(非)지정학과의 관계 속에서 이해되어야 한다. 비지정학의 시각은 영토국가의 경계를 넘어서 이루어지는 자본과 정보 및 데이터의 흐름을 통해서 발생하는 '상호의존'과 글로벌 거버넌스를 강조하는 자유주의자들의 담론과 일맥상통한다. 최근 들어 지구화를 지탱하던 물질적 기반과 사회적 합의가 흔들리면서 '지정학의 부활'이 거론되기도 하지만, 자유주의 국제정치이론가들은 여전히 '지정학의 환상'(the illusion of geopolitics)을 경계하는 논지를 옹호한다(Ikenberry, 2014). 지정학으로의 완전 회귀라기보다는 지구화 시대의 문제들을 좀 더 정의롭게 풀어갈 새로운 글로벌 거버넌스를 설계해야 한다는 것이다.

셋째, 기술패권 경쟁의 지정학은 주관적 공간구성에 주목하는 비판지정학 시각을 곁들여서 보완되어야 한다. 1980년대에 등장한 비판지정학의 시각은 구성주의와 포스트모더니즘의 영향을 받아 기존의 지정학이 원용하는 담론을 해체하는 데서 시작한다. 비판지정학의 시각에서 지정학적 현실은 단순히 존재하는 것이 아니라 재현되고 해석되는 대상으로 이해된다(Ó Tuathail, 1996). 이러한 시각에서 보면 지정학적 현상은 담론적 실천을 통해서 현실을

재편하려는 권력투사의 과정이다. 이러한 비판지정학의 시각은 기술문제를 국가안보 차원으로 안보화하는 담론정치와 통하는 바가 크다. 사실 화웨이 사태는 객관적으로 '실재하는 위협'만큼이나 '구성되는 위협'의 성격을 지니고 있다(Hansen and Nissenbaum, 2009).

끝으로, 기술패권 경쟁의 지정학은 탈지리적 공간으로서 사이버 공간에 주목하는 탈지정학적 시각으로 보완될 필요가 있다. 5G 이동통신 부문의 경쟁에서 탈영토적 '흐름의 공간'(space as flows)으로서 사이버 공간은 매우 중요한 의미를 갖는다(Steinberg and McDowell, 2003). 사실 사이버 공간은 새로운 기술공간의 의미를 넘어서 주요 행위자들이 서로 관계를 맺는 세계정치 공간의 부상을 의미한다. 최근의 양상은 지정학 시각에서 본 전통 공간의 동맹과 연대가 사이버 공간으로 확장되면서 새로운 질서를 모색하려는 모습을 보이고 있다. 이러한 과정에서 미국 중심의 서방 진영과 중국 주도의 비서방 진영의 지정학적 대립구도가 사이버 공간의 거버넌스에서 나타나고 있음에 주목해야 한다(鲁传颖, 2013).

요컨대, 오늘날 선도부문의 기술패권 경쟁은 전통 지정학 시각만으로는 제대로 파악할 수 없는 복합지정학적인 양상을 드러내며 전개되고 있다. 선도 부문인 4차 산업혁명 분야 또는 5G 이동통신 부문의 승패는 미래 글로벌 패권의 향배를 가늠하는 잣대이다. 이러한 이유 때문에 선도부문 경쟁의 결과로 발생하는 상대적 지위변화는 국가안보의 논리를 내세워 대응할 정도로 위중한 사안으로 인식된다. 게다가 이러한 기술패권 경쟁은 전통적인 국가 간 경쟁의 양태를 넘어서 글로벌 차원으로 활동 범위를 넓히고 있는 민간 행위자들의 경쟁과 협력이라는 차원에서 이해되어야 한다. 이러한 과정에서 미중이 벌이는 기술패권 경쟁의 결과는 패권국과 도전국 간의 단순한 '세력전이'가 좀 더 복잡한 세력재편의 양상을 예견케 된다.

### III. 사이버 안보 논란과 미중 안보화 담론정치

#### 1. 화웨이 사태와 미국의 수출입 규제 담론

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 안보위협的主범으로 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 멩완저우가 대(對)이란 제재 위반 혐의로 체포됐다. 2019년 2월 마이크 펜스 미국 부통령은 민헨안보회의에서 미국의 동맹국들이 화웨이 제품을 사용하지 말 것을 촉구했다.

이렇게 전 세계적 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, 2019d). 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(송경재, 2019). 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(김치연, 2019).

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(조진형, 2018). 중국이 반도체, 항공기술, 로봇틱스의 자급화를 모색함으로써 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 수십 년 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

하이키비전에 대한 제재카드를 다시 꺼내 들었다. 2019년 5월 20일 미 국토 안보부는 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 하이키비전에 대해서도 제재를 검토한다는 보도가 나왔다. 2019년 5월 22일 하이키비전을 상무부 기술수출 제한목록에 올리는 것을 검토 중이라고 했다. CCTV가 중국 정부의 소수민 족과 반체제 세력에 대한 감시도구로 활용되는 상황에서 하이키비전에 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(홍성현, 2019; *Economist*, 2019a). 화웨이의 장비를 쓰는 것이 위험하다는 공포감의 근거는, 백도어라는 것이 지금은 아니더라도 언제든지 심어 넣을 수 있는 미래의 위협이기 때문이다(유성민, 2019). 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.

## 2. 중국표준의 모색과 데이터 주권의 담론

역사적으로 중국은 미국 기업들의 기술패권에 대항하여 자국표준을 확보하려는 대항적 행보를 보여왔다(王正平·徐铁光, 2011). 예를 들어, 1990년

대 말부터 MS 컴퓨터 운영체계의 지배표준에 대항하여 독자표준을 모색하였는데, 이는 오픈소스 소프트웨어인 리눅스에 대한 정책적 지원으로 나타났다. 중국 정부가 리눅스를 지원한 배경에는 경제적 동기 이외에도 MS의 플랫폼 패권에 대한 민족주의적 경계가 큰 몫을 차지했다. 그러나 중국의 리눅스 실험은 MS와의 관계에서 기대했던 것만큼의 성과를 거두지는 못했다. 결국 MS는 중국 시장에서 살아남아 자사의 컴퓨터 운영체계 표준의 지배력을 유지하는 성과를 거뒀다. 그러나 MS는 이에 대한 반대급부로 중국 정부가 요구하는 인터넷 검열정책이나 여타 ‘비(非)기술표준’을 수용해야만 했다(김상배, 2014: 426-428).

중국표준의 필요성에 대한 인식은 5G 이동통신 부문에도 반영되었다. 사실 중국이 5G에 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 선두 사업자로서 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(정명섭, 2018).

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.

이러한 중국의 인터넷 정책이 미국 기업들과 갈등을 유발한 초기의 대표적 사례로는 2010년 1월의 ‘구글 사태’를 들 수 있다. 당시 구글은 중국 해커들이 지메일 계정을 해킹하고 구글의 지적재산권을 침해한다는 이유로 중국 시장에서 철수한다고 발표했다. 이러한 발표의 이면에 중국 정부의 정보검열에 대한 반대 입장과 인터넷 자유에 대한 이념의 차이가 존재했다. 이러한 과정에서 중국 정부는 인터넷에서 유통되는 정보를 차단하고 검열하는 것은 각국 정부가 취할 수 있는 당연한 법적 권리라고 주장하였다. 따라서 국내의 기업을 막론하고 중국 국내법을 따르는 것은 불가피하며, 미국이 인터넷 자유의 논리를 내세워 이러한 중국의 행보를 비판하는 것은 주권을 가진 국가의 내정에 간섭하는 행위라는 것이었다(王世伟, 2012).

실제로 중국 정부는 이러한 논리를 내세워 중국 내에서 비즈니스를 하는 미국의 인터넷 서비스 제공자들에게 자체적으로 정보 검열을 수행하도록 요구했다. 예를 들어, MS, 시스코, 야후 등과 같은 미국의 다국적 IT기업들이 중국 시장에 진출하기 위해서는 중국 정부가 시장접근을 위한 조건으로서 제시한 자체검열의 정책을 수용해야만 했다. 구글도 중국 시장에 처음으로 진입하던 2006년에는 다른 기업들처럼 정치사회적으로 민감한 용어들을 자체 검열해야만 한다는 중국 정부의 요구를 수용하지 않을 수 없었다. 그만큼 미국 IT기업들에게 거대한 규모의 중국 시장은 더할 나위 없이 매력적인 카드였는데, 중국 시장에 진출하려는 어느 기업도 예외가 아니었다(김상배, 2014: 429).

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(강동균, 2019). 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 직권으로 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(안호균, 2018).

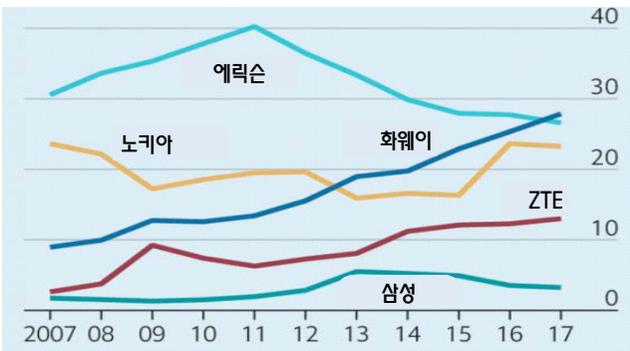
#### IV. 5G 기술경쟁과 미중 정책·제도 마찰

##### 1. 중국의 ‘기술굴기’에 대한 미국의 견제

중국 기업인 화웨이의 통신장비가 미국의 국가 사이버 안보에 실제 위협 인지에 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 기기

를 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 나왔다라는 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(〈그림 2〉 참조). 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(원병철, 2018). 2018년 4월 미국 이동통신산업협회(CTIA)의 ‘글로벌 5G 경쟁’ 보고서에 따르면, 주요국의 5G 이동통신 주파수 분배와 정부 정책, 상용화 수준



출처: IHS Markit; Economist(Dec 15, 2018)에서 재인용

〈그림 2〉 글로벌 이동통신 장비 시장점유율(%)

등에서 미국이 중국에 뒤져 있다고 한다(조진형, 2018).

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 프리스텝 FBI 방첩본부장, 크리스토퍼 크렙스 국토안보부 사이버·기반시설보안국장 등이 ‘중국제조 2025’에 대해 일제히 퍼부은 비난은 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 브누신 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).

## 2. <인터넷안전법>과 다국적 기업의 규제

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 선별기준 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 자산을 매각했다. 2018년 초 MS와 아마존도 자사 데이터를 각기 베이징과 닝샤의 데이터센터로 옮겼다(오주환, 2018). 또한 <인터넷안전법> 시행 직후 애플은 중국 내 사용자들의 개인정보와 관리권을 모두 중국 구이저우 지방정부에 넘겼으며, 2018년 2월에는 제2데이터센터를 중국 네이명 자치구에 건설할 계획을 발표했다. 2018년 12월에는 명완저우

부회장 체포에 대한 보복으로 중국 내 애플의 아이폰 7개 기종에 대해 판매 금지 처분을 내리자기도 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(차대운, 2019). 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 경제규범의 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.

## V. ‘내편 모으기’와 미중 사이버 연대외교

### 1. 미국의 사이버 동맹외교와 그 균열

2018년 초부터 미국은 오프라인 첩보동맹을 맺고 있는 영국, 캐나다, 호주, 뉴질랜드 등, 이른바 ‘파이브 아이즈’(Five Eyes) 국가들에 화웨이 통신장비를 도입하지 말라고 요청했다. 이에 따라 영국 정부는 2018년 초 중국산 통신장비의 보안취약성 문제를 제기하였으며, 캐나다의 경우도 2018년 초 의회가 나서서 캐나다 업체들이 화웨이와 교류하는 것을 자제하도록 요청했으며, 캐나다 정부도 사이버 보안에 필요한 조치를 약속하였다. 호주는 미국에 대해 화웨이에 대한 행동을 촉구했다고 알려질 정도로 적극적인 입장을 취했는데, 2018년에는 5G 장비입찰에 화웨이 도입을 반대했을 뿐만 아니라 남태평양 국가들이 장거리 해저 케이블망 부설 사업의 계약자로 화웨이를 선택하지 말라고 압력을 행사했다. 이밖에 독일과 프랑스도 미국의 화웨이 견제 전선에 동참하였다(김대호, 2018).

2018년 들어 트럼프 행정부는 동맹국들에 대한 화웨이 제재의 요구를 강화하였다. 영국은 대형 통신업체인 BT그룹이 화웨이와 ZTE 제품을 5G 사업에서 배제하려는 움직임을 보였다. 캐나다는 중국과의 무역마찰을 무릅쓰고 미국의 요청에 따라 화웨이의 부회장인 명완저우를 체포했다. 호주와 뉴질랜드는 5G 이동통신 사업에 중국 업체가 참가하지 못하도록 하는 방침을 내렸다. 여기에 일본까지 가세해서, 정부 차원의 통신장비 입찰에서 중국 화웨이와 ZTE를 배제하기로 결정했으며, 일본의 3대 이동통신사도 기지국 등의 통신설비에서 화웨이와 ZTE 제품을 배제하기로 했다(고성혁, 2018). 이러한 행보를 보고 기존의 ‘파이브 아이즈’에 일본, 독일, 프랑스 등 3개국이 합류한 ‘파이브 아이즈+3’의 출현이 거론되기도 했다(박세진, 2019).

그런데 2019년 2월말을 넘어서면서 미국의 압박에 동참했던 영국과 뉴질랜드 등 ‘파이브 아이즈’ 국가들이 ‘사이버 동맹전선’에서 이탈하는 조짐을 보

였다. 영국 국가사이버보안센터(NCSC)는 화웨이 장비의 위험을 관리할 수 있어 그 사용을 전면 금지할 필요는 없다는 잠정 결론을 내렸다. 미국의 요청에 따라 화웨이를 배제했던 뉴질랜드도 저신다 아던 총리가 직접 나서 화웨이를 완전히 배제하지 않았다는 점을 분명히 했다. 이밖에도 독일 역시 특정 업체를 직접 배제하는 것은 법적으로 가능하지 않다는 점을 밝혔고, 프랑스도 특정 기업에 대한 보이콧은 하지 않겠다는 입장을 내놨으며, 이탈리아도 화웨이를 5G 네트워크 구축 사업에서 배제하지 않겠다는 보도를 부인했다. 또한 일찍이 화웨이 장비의 배제 입장을 내놓았던 일본 역시 그러한 제한은 정부기관과 공공부문 조달에만 해당되며, 5G 네트워크 구축에는 포함되지 않는다고 한발 빼기도 했다(Economist, 2019c).

이들 국가들이 입장을 변화한 이유는, 화웨이를 배제한 채 자체 기술로 5G 네트워크를 구축하는 것이 현실적으로 어려운 상황이 작용한 때문으로 해석되었다. 만약에 이들 국가들이 화웨이 장비를 도입하지 않는다면 5G 출범이 2년가량 지체되는 차질을 빚을 것이라는 전망도 나왔다. 역설적으로 미국이 제기한 ‘미국 우선주의’의 영향을 받아 이들 국가들이 자국 우선주의로 돌아섰다는 분석이다(이성민, 2019). 여기에 더해서 2019년 초 파리평화회담과 뮌헨안보회의 등을 거치면서 미국이 이들 동맹국들을 무리하게 밀어붙인 것도 반발을 초래했다. 2019년 2월 마이크 폼페이오 미 국무부 장관은 “만약 어떤 나라가 화웨이 장비를 채택하고 중대한 정보를 넣는다면 우리는 그들과 정보를 공유할 수 없다. 우리는 그들과 함께 일할 수 없을 것”이라고 경고했다. 또한 리처드 그리넬 독일 주재 미국대사도 올라프 숄츠 독일 재무장관에게 “독일이 5G 네트워크를 구축하면서 화웨이 또는 다른 중국 기업의 설비를 사용할 경우 미국의 정보를 얻지 못할 것”이라는 서한을 보냈다(Economist, 2019b).

화웨이의 5G 장비 도입을 금지하는 ‘사이버 동맹전선’이 흔들리면서 트럼프 행정부는 몇 가지 추가조치를 취했다. 표면적으로는 초강경 자세를 다소 완화하는 제스처를 보였는데, 2019년 2월 21일 트럼프 대통령은 자신의 트위터에 “미국이 가능한 한 빨리 5G, 심지어 6G 기술을 원한다”며 “미국 기업들이 노력하지 않으면 뒤처질 수밖에” 없으니, “더 선진화된 기술을 막기

보다는 경쟁을 통해 미국이 승리하길 바란다”고 적었다(조슬기나, 2019). 이는 트럼프 대통령이 화웨이에 대한 입장을 바꿀 조짐으로 해석되기도 했으나, 2019년 5월에 이르러서는 오히려 더 강경한 대응전략을 채택하는 양면 전술을 드러냈다. 게다가 화웨이 제재의 ‘사이버 동맹전선’이 흔들리는 조짐을 보이자, 트럼프 대통령은 화웨이 통신장비의 국내 도입 금지뿐만 아니라 5G 네트워크 구축에 필요한 핵심 부품을 제공해온 미 기업들의 화웨이에 대한 수출을 금지하는 행정명령을 내리기에까지 이르렀다(우은식, 2019).

사이버 안보를 내세운 미국의 동맹결속 전략은 미국의 인도·태평양 전략에서도 나타났다. 2019년 4월에는 미국을 위협하는 북한과 중국의 사이버 공격에 대응하기 위한 국제협력체 신설을 골자로 하는 ‘인도·태평양 국가 사이버 리그(CLIPS)’ 법안이 상원에서 발의됐다. 이 법안에 따르면, 클립스(CLIPS)에는 인도·태평양 지역의 미국 동맹국과 파트너 국가들이 참여한다.(이조은, 2019). 한편 미 국방부는 2019년 6월 1일 공개한 ‘인도·태평양 전략보고서’에서 중국의 일대일로(一帶一路) 전략에 맞서 인도·태평양 전략을 강화하였으며, 화웨이 사태를 ‘하이브리드 전쟁’의 개념을 빌어 이해하는 모습을 보였다. 하이브리드 전쟁은 핵무기를 사용하기 힘든 상황에서 재래전뿐만 아니라 정치, 경제 등 비군사적 요소와 사이버전, 심리전 등을 포함하여 전방위로 전개하는 새로운 개념의 전쟁을 의미한다(정충신, 2019).

## 2. 화웨이의 항변과 중국의 일대일로 연대

화웨이 사태가 불거지기 전부터 ‘파이브 아이즈’로 대변되는 미국의 우방국들은 화웨이 통신장비를 사용하고 있다. 영국은 2005년 유럽에서 처음으로 화웨이 통신장비를 도입했으며, 현재 영국의 양대 통신사인 BT그룹과 보다폰은 화웨이 장비를 사용한다. 영국이외에도 캐나다, 호주, 뉴질랜드 등도 화웨이 장비를 사용한다(황준호, 2018). 이들 국가들이 화웨이 장비를 도입한 이유는 경쟁사 대비 저렴한 가격과 앞선 기술력 때문이다. 린정페이 화웨이 창업자 겸 회장은 2019년 1월 CCTV와의 인터뷰에서 “5G와 마이크로파 통

신 장비를 동시에 가장 잘 만드는 회사는 세계에서 화웨이가 유일합니다. 기술은 경쟁입니다. 다른 국가들이 화웨이 제품을 사지 않고 배길 수 있을까요?”라고 말한 바 있다(『인민망 한국어판』, 2019년 1월 28일).

이러한 상황에서 화웨이는 “사이버 보안 강화를 위해 최선을 다하고 있으며, 보안과 관련해 의혹을 제기 받은 사안은 단 한 번도 없다”는 입장을 취했다. 또한 화웨이는 “현재 전 세계 주요 이동통신사, 포춘(Fortune) 500대 기업, 170여 개 이상 국가의 소비자들이 화웨이의 제품과 솔루션을 사용하고 있다. 화웨이는 ‘글로벌 가치사슬’ 전반에 걸쳐 전 세계 기업들의 신뢰를 얻은 파트너로 자리매김한지 오래”라며 자신감을 보였다. 아울러 화웨이는 “전 세계 선도적인 글로벌 ICT 솔루션 제공업체로서 비즈니스를 운영하는 해당 지역의 관련 법과 규정을 준수”하고 있으며, “미국뿐만 아니라 유엔과 유럽 연합을 비롯한 국제사회에서 공포된 수출 규제 조치를 따르는 데 최선을 다하고 있다”는 입장을 보였다(원병철, 2018).

미국이 우방국들을 동원하여 화웨이 제품을 도입하지 말라는 압력을 목소리를 높여가는 와중에, 화웨이는 보안 강화를 위한 20억 달러 투자 계획을 발표했고, 보안을 최우선 강령으로 내세우겠다고 했다(홍성현, 2019). 이와 더불어 화웨이는 자사가 스페인의 정보보안 평가기관인 E&E (Epoche and Espri)에서 ‘CC(Common Criteria)인증’을 받는다는 사실을 강조하는 등 자사 통신장비가 보안에 문제가 없다는 점을 적극적으로 소명하고 있다. E&E는 통신 장비 설계·개발을 포함해 실제 고객사에 납품되는 최종 장비에 이르기까지 모든 범위에 대해 보안 평가를 수행하는데, 그 중 대표적인 것이 CC인증이다. CC인증은 IT 장비의 보안을 검증하고 인증을 발급하는 과정을 말한다(안별, 2019).

또한 화웨이는 사이버 보안의 국제표준에 부합하는 조치를 위한 일환으로, 2019년 3월 5일 벨기에 브뤼셀에 사이버안보연구소를 개설했다. 화웨이가 다른 곳이 아닌 유럽연합 본부가 있는 브뤼셀에 관련 연구소를 연 것은 자사 통신장비가 중국 정부에 기밀을 빼돌리는 스파이 행위에 이용될 수 있다는 미국의 주장에 적극적으로 대응하기 위한 조치로 풀이된다. 화웨이는 유럽연합의 정책 담당자들을 상대로 미국이 제기하는 보안논란을 불식시키

는 데 초점을 맞춰 왔다. 화웨이는 이미 2018년 11월 독일 본에 브뤼셀과 비슷한 연구소를 개설했으며, 영국 정부가 구성한 화웨이 사이버보안평가센터(HCSEC·Huawei Cyber Security Evaluation Centre)를 지원하기도 했다(권성근, 2019).

화웨이는 미국에 국방수권법에 대해서도 적극적으로 문제제기했다. 화웨이는 2019년 3월 4일 자사 제품 사용을 금지한 미국 정부에 소송을 제기할 예정이라고 밝혔다. 소송 내용은 2018년 미국 연방정부가 ‘심각한 안보 위협’을 이유로 자사제품 사용을 금지한 방침이 부당하다는 것이다. 미 국방수권법 제889조는 미국 정부가 화웨이, ZTE 등 중국 통신장비 업체들의 기술을 이용하거나, 이들 기업의 기술을 이용하는 다른 사업체와 거래하는 것을 금지하는 규정을 담고 있다. 화웨이는 이 법안이 헌법 위반이라고 주장할 것이며, 재판 없이 개인이나 단체를 처벌하는 법안을 의회가 통과시켜서는 안 된다는 주장을 펼친다는 것이다(김영정, 2019).

미국의 화웨이 견제에도 불구하고 중국 정부는 일대일로 추진 차원에서 해외 통신 인프라 확충을 가속화하고 있다. 2018년 4월 시진핑 중국 국가주석은 일대일로 건설을 계기로 관련 국가들, 특히 개도국에 인터넷 기반시설을 건설하고 디지털 경제와 사이버 보안 등 다방면에서 협력을 강화하여 ‘21세기 디지털 실크로드’를 건설해야 한다고 강조한 바 있다(오광진, 2018). 이러한 맥락에서 보면 동남아 국가들이 화웨이를 선호하는 조치를 취한 최근의 행보를 이해할 수 있다. 태국은 2019년 2월 8일 5G 실증 테스트를 시작하면서 화웨이의 참여를 허용했으며, 말레이시아, 싱가포르, 인도 등도 화웨이 장비로 5G 테스트를 진행할 계획을 밝혔다.

이밖에도 화웨이와 중국 정부는 서방국가들에 대한 우호적 공세도 진행했다. 2018년 2월초 테레사 메이 영국 총리는 쏘 야팡 화웨이 회장과 면담을 가졌고, 3월 화웨이는 영국에 향후 5년간 30억 유로(42억 달러)를 투자하겠다고 선언했다. 화웨이는 2019년 2월 캐나다에서 연구개발 투자를 확대하고 일부 지적재산권을 넘기겠다고 밝히는 등 주요국들을 설득하기 위한 여론전에도 나섰다. 2019년 3월 25일에는 시진핑 주석이 이탈리아와 일대일로 양해각서를 체결했다. 한편, 유럽연합의 집행기관인 EC는 화웨이가 사이버 보

안을 위협한다는 미국의 주장이 근거가 없다고 발표했다. 특히 EC는 이러한 발표를 시진핑 주석이 파리에서 에마뉼엘 마크롱 프랑스 대통령, 앙겔라 메르켈 독일 총리, 장 클로드 융커 EU 집행위원장과 회동하는 행사에 맞춰서 진행했다(최예지, 2019; 박형기, 2019).

이러한 행보에 힘입은 덕분인지 유럽의 이동통신사들은 여전히 화웨이 장비를 선택하는 추세이다. 화웨이는 2019년 6월 말 기준으로 전 세계에서 50건의 5G 장비 공급 계약을 맺은 것으로 알려졌다. 이 가운데 28건은 유럽에서 맺은 계약으로 전체 56%에 달한다. 같은 기간 화웨이의 경쟁사인 노키아와 에릭슨은 각각 43건, 22건의 계약을 맺었다. 화웨이의 중국 경쟁자인 ZTE는 25건의 계약을 체결했다. 화웨이는 2018년 최대 시장인 유럽·중동·아프리카에서 모두 2,045억 위안(약 34조 9347억 원)의 매출을 올렸으며 이는 전체 매출 가운데 28.4%를 차지하는 금액이다. 해당 금액은 미국과 아시아·태평양(중국 제외) 시장의 매출을 모두 합한 것보다 많다(『미주 한국일보』, 2019년 7월 22일).

## VI. 맺음말

최근 화웨이 통신장비의 사이버 안보 문제를 놓고 벌어지고 있는 미중갈등, 즉 이른바 ‘화웨이 사태’는 복잡다단하게 전개되고 있는 양국의 관계를 단적으로 보여주는 사례이다. 이 글은 지정학적 시각을 원용하여 선도부문에 벌어지는 미중 기술패권 경쟁이라는 맥락에서 화웨이 사태의 구조와 동학을 체계적으로 분석하기 위한 시도를 펼쳤다. 특히 이 글은 기존의 전통 지정학의 시각 이외에도 비판지정학, 비지정학, 탈지정학 등과 같은 다양한 이론적 논의들을 원용하여 ‘복합지정학’의 분석틀을 제안하였다. 이러한 복합지정학의 시각에서 본 화웨이 사태는 선도부문에서의 기술력 변화와 연동하여 발생하는 관념과 제도 및 세계질서의 복합적인 변동으로 이해된다.

첫째, 안보화의 비판지정학 시각에서 보는 화웨이 사태는 선도부문 기술의

국가안보적 중요성을 강조하는 미국과 중국의 담론 경쟁이다. 특히 화웨이 사태를 촉발하고 확장시킨 핵심 논란거리는 화웨이 장비가 야기할 것이라고 주장되는 사이버 안보위협이었다. 여기서 주목할 것은 잠재적 안보위협을 파악하는 미국과 중국의 안보화 담론의 내용적 차이이다. 미국이 인프라 장비의 보안문제를 내세워 ‘화웨이 포비아’를 들먹인다면, 중국은 소프트웨어와 데이터 분야의 ‘주권 침해’에 대해서 민감하게 반응한다. 미국이 사이버 안보 위협을 내세워 화웨이 제품에 대한 수출입 규제를 벌인다면, 중국은 기술 및 데이터 주권의 시각에서 중국 시장에 진출한 미국의 다국적 기업들을 규제하고 압박한다.

둘째, 지구화의 비지정화 시각에서 보는 화웨이 사태는 미국의 기술경쟁력 하락이라는 상대적 위치변화가 촉발시킨 미중 간의 통상마찰 문제이고, 더 나아가 양국(특히 중국)이 채택하고 있는 정책과 법을 놓고 벌이는 제도마찰이다. 이러한 양상은 양국 모두에서 전략무역 정책이 가미된 보호주의적 대응으로 나타났는데, 그 양상의 차이에 주목할 필요가 있다. 미국이 사이버 안보를 내세운 수출입 규제를 통해서 화웨이의 5G 기술굴기를 견제하고 ‘중국 제조 2025’나 <인터넷안전법>과 같은 중국의 제도적 편향성을 문제시한다면, 중국은 인터넷 안전검사와 데이터 현지화의 논리를 내세워 자국 시장에서 활동하는 다국적 기업들을 기술·경제적으로 뿐만 아니라 정치·사회적으로도 통제하려고 시도한다.

끝으로, 사이버 공간의 탈지정화 시각에서 보는 화웨이 사태는 ‘내편 모으기’의 네트워크 전략 차원에서 오프라인의 동맹과 연대를 사이버 공간의 안보 문제로 확대하려는 미중 간 외교전의 양상으로 나타나고 있다. 미국이 사이버 안보를 내세워 오프라인의 첩보동맹인 ‘파이브 아이즈’ 국가들의 지지를 동원하고 있다면, 중국은 화웨이의 기술력과 자금력을 앞세워 동남아와 유럽 국가들의 국제연대를 모색한다. 이러한 사이버 동맹·연대의 과정은, 최근 미국이 추구하는 인도·태평양 전략으로 연계되고 있을 뿐만 아니라, 중국이 추진해온 일대일로 구축의 맥락에서 ‘디지털 실크로드’를 지향하는 양상으로 나타나고 있다. 이는 마치 해양세력과 대륙세력의 지정학적 경쟁이 사이버 공간으로 옮겨가는 양상을 방불케 한다.

이렇게 복합적 양상으로 진행되는 화웨이 사태의 세계정치는 미래 패권경쟁의 일 단면을 보여준다는 점에서 이론적 의미가 있다. 무엇보다도 국가 간의 '대칭적 경쟁'을 통해서 패권경쟁의 결과를 가늠했던 근대 국제정치 지평을 넘어서 미래 패권경쟁의 '비대칭성'을 예견케 한다. 사실 최근 벌어지고 있는 미중 기술패권 경쟁은 MS나 구글 등과 같은 미국의 다국적 기업과 중국 정부가 대결하는 양상이며, 또한 역으로 화웨이라는 중국 기업과 미국 정부가 맞서는 비대칭 경쟁의 모습을 보이고 있다. 게다가 이들이 벌이는 권력 경쟁의 성격도 전통 지정학에서 상정하는 '자원권력 게임'만이 아니라 복합지정학의 시각으로 보는 '네트워크 권력 게임'의 양상을 띠고 있다. 이러한 점에서 보면, 미중이 벌이는 패권경쟁의 결과도 과거와 같은 '제로점 게임적인 세력전이'의 질서변환이 아닐 수도 있다.

이렇게 복합지정학의 시각에서 이해된 미중 기술패권 경쟁이 한국의 미래 전략에 미치는 영향을 무엇일까? 한국과 같은 중견국의 입장에서 특히 고민스러운 것은, 화웨이 사태로 대변되는 미중 기술패권 경쟁의 결과가 두 개의 호환되지 않는 표준의 진영을 출현시킬 가능성이 있다. 예를 들어, 현재 진행되는 5G 기술패권 경쟁의 지정학적 양상은 상호 분리된 두 개의 글로벌 생산 네트워크를 창출할 가능성이 없지 않다. 실제로 화웨이 사태에서 엿보는 최근의 양상은 미국의 다국적 기업들이 주도하는 '초국적 질서'의 비전과 중국 기업과 정부가 모색하는 '주권적 질서'의 비전이 사이버 공간을 매개로 하여 충돌하는 모습이다. 그런데 만약에 이러한 두 네트워크가 '디지털 신(新)냉전'의 세계질서를 거론케 할 정도로 상호작용성과 호환성이 결여된 모습으로 향후 구축되어 간다면, 두 네트워크의 가장자리에 위치한 중견국인 한국으로서는 난감한 상황이 아닐 수 없다.

게다가 이러한 구도가 한국에게 기술·경제적 선택뿐만 아니라 지정학적 차원의 전략적 선택까지도 요구한다면 어떻게 해야 할까? 미중이 벌이는 5G 시대 안보화 담론정치의 외중에 한국이 추구할 기술담론의 내용은 무엇일까? 저렴하고 경쟁력 있는 기술과 장비의 도입인가, 아니면 한반도의 안보환경을 염두에 둔 국가 사이버 안보 또는 데이터 안보일까? 또한 5G 부문에서 보호 무역주의를 내세우고 있는 미중 사이에서 한국이 지향할 정책과 법제도 모델

은 무엇일까? 미국식으로 초국적 데이터 유통을 보장하는 개방과 자유의 모델인가, 아니면 중국식의 국가주도형 기술지원과 인터넷 통제의 국가주권형 모델인가? 끝으로, 미중이 벌이는 사이버 동맹·연대 외교 사이에서 한국이 취할 전략적 선택은 무엇일까? 미국의 사이버 동맹진영에 동참할 것인가, 아니면 중국과의 기술경제적 협력을 강화할 것인가? 이러한 고민들은 단순히 관련 사업을 하는 기업의 몫으로만 남겨놓을 수는 없는 국가전략의 난제들이 분명하다.

투고일자: 2019-08-11 심사일자: 2019-09-06 게재확정일자: 2019-09-09

## 참고문헌

- 강동균. 2019. 「기업 검열하는 中 ‘사이버 보안법’ 손본다」. 『한국경제』, 2월 7일.
- 고성혁. 2018. 「美 중국 화웨이 제품 퇴출은 안보전쟁」. 『미래한국』, 12월 26일.
- 권성근. 2019. 「화웨이, 벨기에 브뤼셀에 사이버안보 연구소 개설」. 『뉴시스』, 3월 6일.
- 김대호. 2018. 「중국 화웨이는 위험한 기업’ 교류·협력 중단 전세계 확산…미국+ 캐나다, 호주, 영국 등 ‘화웨이 주의보」. 『글로벌이코노믹』, 3월 23일.
- 김상배. 2014. 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』. 서울: 한울.
- 김상배. 2015. “사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계.” 『국제·지역연구』(서울대학교 국제학연구소) 24권 3호 pp. 1-40.
- 김영정. 2019. 「화웨이의 반격…美, 화웨이 보이콧 부당’ 제소 방침」. 『이투데이』, 3월 5일.
- 김윤구. 2019. 「中, 인터넷 이용자 데이터 국외 반출 금지…미국 기업 겨냥」. 『연합뉴스』, 5월 29일.
- 김치연. 2019. 「미국, 중국에서 만든 5G장비 미국 내 사용금지 검토」. 『연합뉴스』, 6월 24일.
- \_\_\_\_\_. 2019. 「화웨이, 미국 압박에도 5G 시장 석권」. 『미주 한국일보』, 7월 22일.
- 박세진. 2019. 「中 견제 美 중심 새 정보동맹 ‘파이브 아이즈+3’ 출범」. 『연합뉴스』, 2월 4일.
- 박형기. 2019. 「시진핑 유럽에 돈 뿌리자 유럽도 선물 하나 줬다」. 『뉴스1』, 3월 27일.
- 손승우. 2019. 「중국의 사이버보안 규제와 新보호주의 확산」. 『아시아경제』, 2월 27일.
- 송경재. 2019. 「화웨이 규제 보복엔 中이 더 타격…부품 막히면 퇴출될 수도」. 『파이낸셜뉴스』, 5월 17일.
- 심재훈·김연숙. 2018. 「美정부, 중국발 보안위협 우려에 5G망 국영화 검토」. 『연합뉴스』, 1월 29일.

- 안별. 2019. 「[MWC 2019] 스페인 보안연구소 ‘화웨이, 5G 보안 인증 올 가을 결론’. 『조선닷컴』, 2월 28일.
- 안호균. 2018. 「다르게 생각하라 딘 애플, 중국에선 다를 수 없는 이유?’. 『뉴시스』, 2월 27일.
- 오광진. 2018. 「美 ZTE 제재에 시진핑, ‘중국 IT 핵심기술 돌파 가속’. 『조선닷컴』, 4월 22일.
- 오주환. 2018. 「국민 개인정보 지켜라’ 미·중 치열한 ‘안보전쟁’… 한국은?’. 『국민일보』, 3월 12일.
- 우은식. 2019. 「美, ‘反화웨이 동맹’ 흔들리자 통신부품 수출금지 추진’. 『뉴시스』, 3월 8일.
- 원병철. 2018. 「세계 최초 5G 상용화와 화웨이 장비 보안성 논란’. 『보안뉴스』, 7월 26일.
- 유성민. 2019. 「미국은 왜 화웨이만 콕 집어 두들겨 팰까?’. 『신동아』, 3월호.
- 이길성. 2018. 「美 ‘중국제조 2025는 기술 굴기 아닌 범죄’’. 『조선닷컴』, 12월 14일.
- 이성민. 2019. 「미국 고립주의와 유럽 열국의 반응’. 『이코노믹리뷰』, 2월 20일.
- 이조은. 2019. 「미 상원 인도태평양 사이버 연합체 ‘클립스’ 설립 법안 발의…‘북한 범죄 지속 가능성’’. *Voice of America*, 4월 9일.
- 인민망 한국어판. 2019. 「런칭페이 화웨이 회장, 中 CCTV 인터뷰 동영상 전격 공개!’. 『인민망 한국어판』, 1월 23일.
- 정명섭. 2018. 「中 5G 굴기…보안 문제로 꺾이나. 『아주경제』, 7월 23일.
- 정충신. 2019. 「기술·자원·무역 ‘모든 것을 무기로’… 美·中, 이미 ‘3차대전’’. 『문화일보』, 6월 7일.
- 조슬기나. 2019. 「[주말에 읽는 글로벌 뉴스] 화웨이 사태. 『아시아경제』, 2월 23일.
- 조진형. 2018. 「미국이 중국에 뒤진 미래 먹거리… 5G 통상전쟁 2라운드. 『중앙일보』, 4월 23일.
- 차대운. 2019. 「中, IT인프라 부품 도입때 ‘국가안보위해’ 심사 예고…美에 맞불. 『연합뉴스』, 5월 25일.
- 최예지. 2019. 「中언론 ‘일대일로, 유럽에 긍정적’…‘트로이목마’ 우려 불식에 나서. 『아주경제』, 3월 25일.
- 홍성현. 2019. 「서방 떨게하는 ‘화웨이 포비아’의 실체는?’. 『중앙일보』, 1월 13일.
- 황준호. 2018. 「다섯개의눈’과 손잡은 화웨이…커지는 미국의 우려. 『아시아경제』, 2월 25일.
- Buzan, Barry and Lene Hensen. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.
- Callon, Michel. 1986. “Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay.” in John Law ed. *Power, Action and Belief: A New Sociology of Knowledge*. London: Routledge and Kegan Paul, pp.196-233.
- Cox, Robert W. 1981. “Social Forces, and World Orders: Beyond International Relations Theory.” *Millennium*, 10(2): 126-155.

- Economist*. Dec 15, 2018. "Can Huawei Survive an Onslaught of Bans and Restrictions Abroad?"
- \_\_\_\_\_. 2019a. "How to Handle Huawei." Jan 31.
- \_\_\_\_\_. 2019b. "Are Security Concerns over Huawei a Boon for its European Rivals?" Mar 21.
- \_\_\_\_\_. 2019c. "Britain Strikes an Artful Compromise on Huawei and 5G." Apr 27.
- \_\_\_\_\_. 2019d. "Holding out on Huawei." May 20.
- Eurasia Group. 2018. "The Geopolitics of 5G." *Eurasia Group White Paper*, Nov 15.
- Gu, Xuewu, et al. 2019. "Geopolitics and Global Race for 5G." *CGS Global Focus*, Center of Global Studies, Bonn University.
- Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53(4): 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.
- Ikenberry, G John. 2014. "The Illusion of Geopolitics: The Enduring Power of the Liberal Order." *Foreign Affairs*, 93(3): 80-90.
- 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.
- Knight, Will. 2019. "Trump's Feud with Huawei and China could Lead to the Balkanization of Tech." *MIT Technology Review*, May 24.
- Krugman, Paul R. ed. 1986. *Strategic Trade Policy and the New International Economics*. Cambridge: MIT Press.
- 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.
- Mead, Walter Russell. 2014. "The Return of Geopolitics: The Revenge of the Revisionist Powers." *Foreign Affairs*, 93(3): 69-79.
- 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.
- Ó Tuathail, Gearóid. 1996. *Critical Geopolitics*. Minneapolis, MN: University of Minnesota Press.
- Rollet, Charles. 2019. "Huawei Ban Means the End of Global Tech." *Foreign Policy*, July 7.
- Steinberg, Philip E., and Stephen D. McDowell. 2003. "Global Communication and the Post-Statism of Cyberspace: A Spatial Constructivist View." *Review of International Political Economy*, 10(2): pp. 196-221.

- Tyson, Laura D'andrea. 1992. *Who's Bashing Whom? Trade Conflict in High-Technology Industries*. Washington DC: Institute for International Economics.
- 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. pp. 48-54.
- 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 문화발전전략)” 『图书情报工作』 第6期, pp. 8-13.
- 王正平(왕정평) 徐铁光(취테광). 2011. “西方网络霸权主义与发展中国的网络权利(서방의 사이버 패권주의와 개발도상국의 사이버 권리).” 『思想战线(사상전선)』, 第2期 第37卷. pp. 105-111.
- 蔡翠红(차이추이홍). 2012. “网络空间的中美关系竞争, 冲突与合作(사이버 공간에서의 미중관계: 경쟁, 충돌과 협력).” 『美国研究(미국연구)』 第3期. pp. 107-121.

# The Huawei Incident and U.S.-China Technological Hegemony Competition: The Complex Geopolitics of Leading Sectors and Cyber Security

Sangbae Kim

Professor, Seoul National University

The so-called Huawei Incident is one of the most typical examples of the U.S.-China competition in recent years. The issue is that the backdoor planted in the products of Huawei, a Chinese mobile telecom equipment maker, could leak data that is so important as to have a significant impact on U.S. national security. This perception creates strategic import and export restrictions on Huawei products and the accompanying trade friction between the two countries, and the U.S. is deploying a kind of “diplomatic war” to block Huawei even by mobilizing its allies. We should also note that the U.S.-China technology hegemony competition in the leading sectors represented by 5G mobile communications is at the root of this Incident. The U.S. checks China’s “technological rise” and criticizes China’s government policies and domestic laws that support companies like Huawei. In this context, the Huawei Incident means a “geopolitical rivalry” between the U.S. and China over future global hegemony. This paper proposed the perspective of “Complex Geopolitics” as a new theoretical framework for understanding the Huawei Incident in such a systematic manner. Complex geopolitics recognizes the usefulness of existing classical geopolitics, but stresses the need to seek a more complex understanding of geopolitics, not merely a return to traditional geopolitics, in order to properly understand the recent transformation of world politics. From this perspective of complex geopolitics, the Huawei Incident is an example of the U.S.-China competition for technology hegemony in the leading sector. in which such issues as cyber security, system friction, and allied diplomacy are inter-linked.

Keywords: Huawei, United States, China, Technological Hegemony Competition, Leading Sectors, Cyber Security, Complex Geopolitics

김상배, 서울대학교 정치외교학과 교수  
서울특별시 관악구 관악로 1  
서울대학교 사회대학교 정치외교학과  
E-mail\_sangkim@snu.ac.kr