파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 138

사이버 안보 분야에서 벌어지는 미국과 중국의 3차원 표준경쟁에 주목해야

글 | **김상배**(서울대학교 정치외교학부, sangkim@snu.ac.kr)

최근 동아시아 지역은 물론 글로벌 차원에서 21세기 세계 패권을 놓고 벌이는 미국과 중국의 경쟁에 대한 관심이 높아지고 있다. 사이버 안보는 양국이 경쟁을 벌이는 대표적인 분야 중의 하나이다. 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 핵 안보와 같은 전통 안보 못지않게 중요한 21세기 국가 전략 사안으로 부상하고 있다. 이 글은 기술, 제도, 담론의 세 가지 차원에서 벌어지는 '3차원 표준경쟁'의 시각에서 사이버 안보 분야의 미·중 표준경쟁을 살펴보고, 그러한 미·중 경쟁의 틈바구니에서 한국이 취할 표준전략의 과제를 가늠해보았다.

※ 이 글은 2014년 한국표준협회가 주관한 〈제2회 표준정책 마일스톤 연구–국가표준 거버넌스 선진화〉의 지원을 받아 수행된 연구 논문 '사이버 안보 분야의 미·중 표준경쟁: 네트워크 세계정치학의 시각'을 칼럼 형태로 재작성한 것입니다. 참고문헌은 중앙대학교 국가정책연구소(www.cauippa.re.kr)의 논문검색에서 확인할 수 있습니다.

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 140

표준경쟁으로 보는 미·중 패권경쟁

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 치열해지고 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 넘어서는 정책과 제도, 더 나아가 생각과 가치관의 표준까지도 표준화와 표준경쟁의 대상이 되고 있다. 이러한 양상은 최근 국가 간에 벌어지는 표준경쟁에서도 발견된다.

이 글에서 국가 간에 벌어지는 표준경쟁의 사례로 주목한 것은 사이버 안보 분야에서 벌어지는 미국과 중국의 경쟁이다. 2013년 6월 미국과 중국의 두 정상인 오바마 대통령과 시진핑 주석이 만나 북한의 핵 개발 문제와 더불어 사이버 안보 문제를 양국이 당면한 현안으로 거론하면서 사이버 안보는 그야말로 21세기 미·중 관계의 전면에 부상했다. 그 후 사이버 안보는 미·중 양국 간에 진행된 전략경제 대화의 현안 중 하나로서 다루어졌으며, 좀 더 구체적으로는 미·중 사이버 보안 실무그룹의 협의가 진행되기도 했다. 그러나 이러한 협력의 제스처에도 불구하고 물밑에서는 사이버 안보 분야의 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 미·중 대화를 중단하는 동시에 중국 시장에 진출한 미국 IT기업들에 대한 규제의 고삐를 죄기도 했다. 사실 사이버 안보 분야에서 벌어진 미·중 관계의 이면을 보면, 미국도 중국을 상대로 비밀스러운 정보작전을 벌인 것은 마찬가지다.

예를 들면, 2013년 6월 미국 중앙정보국(CIA) 전 직원인 에드워드 스노든(Edward Snowden)은 미국이 장기간에 걸쳐 중국을 포함한 세계 각국의 각종 데이터를 감청해왔다고 폭로한 바 있었다. 미국과 중국 간에 벌어지는 해킹과 사이버 공격에 대한 정보와 자료가 극히 제한적인 현재의 상황을 염두에 두더라도, 두 강대국 간에는 이미 수 년째 치열한 '사이버 전쟁'이 벌어지고 있음을 미루어 짐작할 수 있다.

국제정치학의 분야에서 미·중 세계 패권경쟁은 최근 국내외 국제정치학의 핵심 주제 중의 하나이다. 이러한 미·중 패권경쟁 전반의 향배(向背)

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 142

를 읽는 데 있어서 사이버 안보나 인터넷, 좀 더 포괄적으로 IT 분야에서 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 세계 경제의 선도 부문, 즉 해당 시기 첨단산업의 향배는 세계 패권의 부침과 밀접히 관련된 것으로 알려져 있다. IT 분야, 좀 더 구체적으로는 인터넷과 사이버 안보의 분야는 국제정치학적 함의를 갖는 21세기 선도 부문의 대표적인 사례이다.

사이버 안보의 세계 정치는, 국가 간의 관계에 주목하는 기존의 전통적인 국제정치학의 안보이론이 제대로 설명하지 못하는 새로운 분야이다. 사이버 안보와 사이버 공간의 독특한 구조와 국제정치학이 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 복잡한 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 세계 정치는 전통적인 국제 정치의 게임이라기보다는, 새로운 이론적 시각을 필요로 하는 복합적인 네트워크 세계 정치의 게임이다.

이러한 맥락에서 이 글은 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 국제정치학의 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 여기에서 파생되는 양국 간의 물리적 충돌의 가능성을 논하는 차원을 넘어선다. 게다가 사이버 공간의 미·중 관계는 단순히 갈등이냐 협력이냐, 아니면 누가 승자이고 패자이냐, 그리고 더 나아가 경쟁의 주체가 누구이냐를 묻기가 무색한 복합적인 성격을 지니고 있다. 이 글은 이러한 복합적인 양상으로 전개되는 사이버 안보 분야의 미·중 경쟁을 '3차원 표준경쟁', 즉 기술표

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 144

준경쟁과 제도 표준경쟁, 담론 표준경쟁의 시각에서 분석하였다. 이러한 작업을 통해서 이 글이 목적하는 바는 미국과 중국이 벌이는 21세기 패권 경쟁을 좀 더 체계적으로 이해하고, 이를 바탕으로 향후 한국이 추구할 표준전략, 좀 더 넓은 의미에서는 외교전략의 과제를 가늠해보는 데 있다.

사이버 안보의 미·중 기술표준경쟁

2013~2014년 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 의구심 어린 움직임이 치열하게 경합하고 있다는 사실이다. 특히 중국 정부는 미국 IT 기업들이 제공하는 컴퓨터와 네트워크 장비의 보안문제를 우려한다. 인터넷 보안기술과 관련하여 중국이 미국 IT 기업들에게 너무 많이 의존하고 있으며, 혹시라도 양국 간에 문제가 발생할 경우, 이들 기업들이 미국 편을 들 것이라는 걱정이다. 사실 미국의 IT 기업들은 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 위치를 차지하고 있다. 중국은 일단 양국 간에 사이버 전쟁이 발발한다면 이들 기업들이 모두 미국 정부에 동원될 것이라고 보고 있다.

이러한 문제의식을 바탕으로 중국 정부와 기업들은 1990년대 이래 미국의 IT 기업에 대한 기술 의존을 줄이고 중국의 독자적 표준을 모색하려는 노력을 펼쳐 온 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 '맞불작전'을 하는 적극적인 형태의 전형적인 기술표준경쟁의 모습이라기보다는 지배표준을 회피하거나 또는 지배표준으로부터 자유로운 독자적 표준 공간을 확보하려는 소극적인 형태로 진행됐다는 사실이다. 구체적으로 사이버 안보 분야 미·중 기술표준경쟁은 컴퓨터 운영체계, 대규모 서버, 네트워크 장비, 모바일 운영체계 등에 구축된 미국 IT 기업들의 지배에 대한 중국의 우려에서 시작되었다.

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 IT 제품과 서비스에 대해 '인터넷 안전 검사'를 의무화하는 조치로 나타났다. 중국 정부의 보안 검사는 마이크로소프트와 IBM, 시스코, 애플 등에 집중되었다(〈매일경제〉 2014-5-23).

실제로 중국 정부는 보안강화 등을 이유로 공공기관용 PC에 마이크로소프트의 최신 '윈도 8 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 외신들

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 146

은 미국 정부가 중국군 현역 장교 5명을 사이버 스파이 혐의로 정식 기소한 것에 대한 보복이라는 해석을 내놓았다(〈아시아경제〉, 2014-7-29).

비슷한 맥락에서 중국 정부는 중국 내 은행의 IBM 서버를 중국산 서버로 대체할 것을 추진하기로 했다. 이러한 중국의 조치는 IBM 이외에도 매킨지나 보스턴컨설팅 같은 미국 기업들에게도 영향을 미쳤는데, 이는 무역기밀의 유출을 방지하기 위한 거래 단절 명령으로 볼 수 있다(〈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 IBM 서버 의존도를 낮추기 위해 자국 브랜드인 랑차오 서버로 교체해서 사용하도록 지시하기도 했다(〈아주경제〉, 2014-7-30).

이러한 문제와 관련해서는 미국의 반응도 별반 다르지 않았다. 2014년 6월 미국 정부도 자국 기술이 중국으로 유출될 수 있다는 국가안보의 문제를 우려해서 중국 기업인 레노버가 IBM의 x86 서버 사업을 인수하는 것을 지연시켰다. 레노버가 IBM 서버 사업부를 인수할 경우 펜타곤이 중국 해커의 공격으로부터 취약해질 수 있다는 이유였다. 사실 미국 정부가 IBM-레노버 간 거래에 대해 우려를 표명한 것은 이번이 처음이 아니었다. IBM은 2005년에 자사 PC 사업부를 레노버에 매각했는데, 당시 익명의 미군 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 금융 업계에서 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 등의 업계에서 60% 이상의 점유율을 차지하고 있다. 심지어 인터넷 업계에서도 중국 내 상위 20개 인터넷 기업들에서 시스코 제품이 차지하는 비율이 약 60%에 해당되고, 방송국과 대중매체 업계에서는 80% 이상이다. 인터넷랩의 창시자인 팡싱둥(方兴东)은, "시스코가 중국 경제의 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 도청·감청 프로그램을 운용하며 시스코의 설비를 활용했다는 사실이 폭로된 것이 화근이었다. 중국 내 유관기관의 검증 결과 시스코의 라우터 제품에 히든백도어를 삽입한 문제가 밝혀졌다. 그 무렵 미국 정부가 ZTE와 화웨이의 설비 구매를 금지한다고 발표한 사건도 중국 정부와 기업들이 노골적으로

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 148

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-7'의 '자주 가는 위치(frequent location)' 기능이 중국의 경제상황이나 국가기밀 정보에까지 접근할 수 있다며 '국가안보에 위협적인 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 〈블룸버그〉에 의하면, 중국 정부는 2014년 8월 해킹과 사이버 범죄를 둘러싼 중국과 미국 간 긴장이 고조되는 가운데 정부 조달 품목에서 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, 에너지 효율성이 있는 컴퓨터 제품군 정부 조달 목록에서 마이크로소프트도 제외시켰다. 〈블룸버그〉는 이와 같은 중국 정부의 해외기업에 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 구성 부분이다. 중국 정부는 인터넷 정보안전을 보다 강화해 나갈 것이다. 우리는 대외개방정책을 고수하고 있고, 계속하여 해외기업들의 중국 투자와 경영을 환영하며, 앞으로도 적극적으로 해외와의 협력을 지속해 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 잘 보여준다.

사이버 안보의 미·중 제도표준경쟁

기술과 시장에서 나타난 미국 IT 기업들과 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

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 150

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 IT 기업들은 중국 정부가 시장 접근을 위한 조건으로서 제시한 자체 검열의 정책을 수용하고 나서야 중국 시장에 진출할 수 있었다. 구글도 2006년에 중국 시장에 진출할 당시 미국의 다른 IT 기업들과 마찬가지로 정치적으로 민감한 용어들을 자체 검열하라는 중국 정부의 요구를 수용하였다.

이러한 중국의 인터넷 검열 정책에 대한 미국 IT 기업들의 반발이 없을 리 만무했다. 2010년 1월 12일 구글은 자사 이메일 서비스에 대한 해킹과 지적재산권 침해를 이유로 중국 시장에서 철수하겠다고 발표하여, 중국과 미국뿐만 아니라 국제사회에서 많은 논란을 일으켰다. 이러한 일련의 사태에 대해 중국 정부는 국제적인 인터넷 기업이 중국 내에서 기업 활동을 하려면 중국의 국내법을 따라야 한다는 주장을 폈다. 구글 사건이 주는 의미는, 단순히 미국의 IT 기업과 중국 정부의 갈등이라는 차원을 넘어서, 양국의 정치경제 모델의 차이를 보여주었다는 데 있다. 이 사건에서 나타난 구글의 행보가 미국 실리콘밸리에 기원을 두는 인터넷 자유 담론을 바탕에 깔고 있다면, 이를 견제한 중국 정부의 태도는 중국의 정치체제에 친화적인 정책적 주권 담론에 기반을 둔다.

2010년 구글 사건에 표명된 중국 정부의 태도는 2013~2014년 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 아는 상식을 의미 한다"며 "세계에 그 어떤 만병통치약도 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 다루어졌다기 보다는, 넓은 의미에서 본 인터넷 거버넌스의 일부로서 논의되어 왔다. 이러한 인터넷 거버넌스를 지배한 것은 미국을 기반으로 활동하는 인터넷 전문가들과 민간사업자들의 자율적인 거버넌스 체계였다. 이를 잘 보여주는 사례는 초창기부터 인터넷을 관리해온 미국 소재 민간 기관인 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 있다

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 152

는 비판으로부터 자유롭지 못했다.

이러한 기존의 인터넷 거버넌스 모델에 대해서 최근 개발도상국들이 반론을 제기하고 있다. 개발도상국들은 인터넷 분야에서 미국의 패권을 견제하려면 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 지금까지 용인되었던 관리방식의 정당성을 문제 삼을 수밖에 없다는 것이었다. 특히 이러한 움직임은 인터넷 초창기에는 상대적으로 뒤로 물러서 있던 국가 행위자들이 인터넷 거버넌스에서 고유한 활동영역(예를 들어 글로벌 정보 격차나 사이버 안보)을 찾아가는 과정과 맞물렸다. 특히 인터넷 거버넌스의 운영과정에 국가 행위자들의 영토주권이 좀 더 적극적으로 인정되어야 한다는 것이다.

이상으로 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 개발도상국 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 필요 시 정보통제도 가능한 공간이므로 기존의 인터넷 거버넌스를 주도해온 서방 진영의 주장처럼 민간 중심의 거버넌스에 의해서 사이버 공간을 관리할 수는 없다고 주장한다.

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 개발도상국들이 제기하는 '대항의 표준'이 맞선다. 여기에 이해당사자들이 형성해온 '민간표준'과 국가 행위자들이 주도하는 '국가표준'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 구도에서 대체로 미국이 전자의 논리를 취한다면 중국은 후자의 논리에 기반을 두고 있다.

사이버 안보의 미·중 담론 표준경쟁

가장 추상적인 차원에서 볼 때 사이버 안보의 미·중 표준경쟁은 사이버 안보 담론의 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

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 154

중국 간에 벌어지는 논쟁점은 기본적으로 사이버 안보의 대상이 무엇이며, 그 문제를 해결하는 주체가 누구인가를 규정하는 담론의 차이에서 비롯된다. 이렇게 보면 미국과 중국 사이에서 인터넷과 관련된 보안기술(또는 기술표준)이나 인터넷 정책과 규범 등과 관련하여 벌어지고 있는 경쟁은 모두 사이버 공간의 안보 담론을 선점하려는 경쟁과 밀접히 관련된다. 이는 단순히 관념의 차이가 아니라 이를 통해서 구성될 미래의 방향을 놓고 벌이는 이익 규정의 차이에 기반을 두고 있기 때문이다.

미국의 사이버 안보 담론은 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 '중국 해커 위협론'을 펼쳤다. 중국의 해커들이 중국 정부와 군의 지원을 받아 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 IT 기업들을 목표로 하여 중국 해커들이 벌인 일이라는 것이다. 2010년 구글 사건 당시에도 중국의 해커들이 적극적인 역할을 한 것으로 알려졌다.

게다가 이들 사이버 공격 대상이 미국 기업들의 지적재산권이라는 점에서 심각한 문제로 다가왔다. 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 투자자산 회사의 사이버 보안 대책 마련에 적극 나서야 할 것이라고 강조했다(〈조선일보〉, 2014-7-30). 이러한 안보 담론은 자연스럽게 미국의 인권 단체, 정부관리, 각계 전문가 등을 중심으로 중국에 대한 인터넷 검열기술의 제공을 금지해야 한다는 문제를 제기하기에 이르렀다. 이러한 취지에서 중국의 영토 내에 서버를 설치하거나 또는 이메일 서비스를 제공하고 검열기술을 판매하는 것을 제한해야 한다는 주장도 제기되었다.

이러한 '중국 해커 위협론'에 대해서 중국은, 미국이 해커의 공격으로부터 가장 피해를 보는 나라라는 인식을 스스로 조장하고 있다며 맞섰다. 또한 미국이 중국 해커 위협론을 조장하여 여론의 우위를 점해 중국의 사이버 군사기술의 발전을 억누르려 한다고 했다. 또한 미국이 중국 해커 위협론을 유포하는 이면에는 경제무역 측면에서 중국 기업의 부상을 도전으로 인식하고, 사이버 안보를 빌미로 자국 기업을 보호하려는데 미국 정부의 진짜 속내가 있다고 평가했다. "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 상반되게 하고 있다"는 것이었다(〈参考消息网〉, 2014-1-03).

아울러 중국이 사이버 안보 담론에서 중시하는 것은 소위 '정치안전'

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 156

에 대한 위협이었다. 중국 인터넷정보판공실 부주임 왕슈쥔(王秀军)에 따르면, 현재 중국이 "관심을 가지고 있는 인터넷 안전은 의식형태의 안전, 데이터 안전, 기술 안전, 응용 안전, 자본 안전, 루트 안전 등이 포함되는데, 총괄적으로 보면 정치 안전이 근본이 된다"라고 하였다. 그에 의하면, "현재 외부 세력들이 인터넷을 중국에 대한 침입과 파괴의 주요 루트로 삼는데, '인터넷 자유'라는 미명하에 계속하여 중국에 대한 공격을 가하면서 중국의 사회안정과 국가안전을 파괴하려 시도하고 있다"는 것이다. 특히 "인터넷 신기술은 일부 인사들의 새로운 전파도구로 사용되어 불법정보와 유해정보"를 퍼뜨리고 있기에, '인터넷상의 의식형태 영역에 대한 침투와 반(反)침투의 투쟁에서 승리를 취득하느냐의 여부'는 많은 부분에서 중국의 미래에 중요하다는 것이다(〈大公网〉, 2014-5-18).

한편 미국과 중국의 사이버 안보 담론의 경쟁은 안보의 대상과 주체에 대한 인식의 차이로도 나타났다. 국내적인 의미의 '국가' 차원에서 본 미국의 사이버 안보 담론은 개방된 공간으로서 인터넷상에서의 개인의 권리와 표현의 자유라는 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 것'이라고 밝혔다.

이러한 주장의 연속선상에서 볼 때, 앞서 살펴본 2010년 구글 사건은 미국과 중국의 인터넷 정책의 차이를 넘어서 인터넷에 담긴 정치 담론의 차이, 즉 자유롭고 개방된 인터넷의 담론과 통제되고 폐쇄된 인터넷의 담론을 놓고 벌인 표준경쟁의 성격을 갖고 있었다. 당시 구글로 대변되는 미국의 IT 기업들(그리고 미국 정부)이 중국 정부(또는 중국의 네티즌)를 상대로 해서 반론을 제기한 핵심 문제는 인터넷 자유라는 보편적 이념의 전파를 거스르는 중국 정치사회 체제의 특성이었다. 이러한 점에서 구글 사건은 '정치이념의 표준경쟁'이기도 했다. 양국 간에 이러한 차이가 발생하는 것은, 일차적으로는 양국 국내 체제의 제도와 정책, 그리고 역사·문화적 전통과 연관되겠지만, 미국과 중국이 세계 체제에서 각각 패권국과 개발도상국으로서 차지하고 있는 국가적 위상과도 관련이 있다.

이러한 미국의 사이버 담론에 대해서 중국은 인터넷을 검열하고 규제하는 정책적 자율성을 정당화하는 논리를 폈다. 중국이 중시하는 것은 '개인 차원의 인터넷 자유'라기 보다는 '국가 차원의 인터넷 자유'이다. 2010년 구글 사건에 대한 중국 정부의 대처방식도 국가의 권리라는 차원에서 정당화된다. 이러한 중국의 눈으로 볼 때, 미국의 인터넷 자유에 대한 담론은 보편적 가치라기 보다는 미국이 자국의 패권을 투영하는 수단에 불과하다. 특히 미국이 일부분의 반정부 세력들에 자금을 지원해주어 백도어 프로그램을 개발, 중국의 사회모순과 민족 관계의 부정적 측면을 주객관적으로 확대 해석한 것은 중국의 국가안보에 위협이 된다는 것이다. 미국과 중국이 '인터넷 자유'를 두고 벌이는 게임은 양국의 의식형태와 가치관의 분쟁이 사이버 공간으로 연장된 것이고, 양국이 주권과 인권,

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 158

주권과 안보를 두고 벌이는 분쟁이 정보화 시대에 반영된 것이라는 인식이다.

사실 이상에서 언급한 미국의 사이버 안보 담론은 글로벌 패권 담론을 바탕에 깔고 있다. 인터넷이 전 세계적으로 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 패권 담론은 앞서 언급한 국제규범의 형성 과정에서 나타나는 미국의 입장과 일맥상통하는 바가 크다.

이에 대해 중국은 반(反)패권주의적이고 민족주의적인 국가주권의 안보 담론을 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 주석의 연설은 시사점이 큰데, 시 주석은 "비록 인터넷이 고도의 글로벌화라는 특징을 가지고 있지만 각 국가의 정보 영역의 주권이익은 침범당해서는 안 되며, 인터넷 기술이 발달하더라도 타국의 정보 주권을 침범해서는 안 된다"라고 주장했다. 또 시 주석은 "각국은 모두 자국의 정보안보를 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).

한국의 표준전략에 던지는 과제

사이버 안보 분야에서 벌어지는 미국과 중국의 경쟁은, 예전에 국제정치에서 출현했던 패권경쟁과는 달리 복합적인 권력게임을 벌이는 다층적인 행위자들의 네트워크 게임으로 이해해야 한다. 이렇게 사이버 안보 분야에서 복합적으로 벌어지는 미국과 중국의 표준경쟁은 단순히 두 나라의 관계에만 그치는 것이 아니라, 동아시아와 세계 정치 전반에 광범위한 영향을 미친다. 21세기 세계패권을 놓고 자웅을 겨루는 두 나라의 경쟁이 야기하는 변화의 소용돌이로부터 한국도 자유로울 수는 없다. 특히 중견국으로서 새로운 외교 방향을 모색하고 있는 최근의 한국 상황에서 사이버 안보의 미·중 경쟁은 미래전략의 차원에서 고민해야 하는 중요한 구조적 환경의 변화이다. 이 글의 논의를 바탕으로 할 때, 사이버 안보 분야에서 벌어지고 있는 미·중 3차원 표준경쟁은 한국의 표준전략, 또는 표준경쟁의 관점에서 본 외교전략에 적어도 다음과 같은 세 가지의 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

파트1 1차_레이아웃 1 14. 11. 19. 오후 6:09 페이지 160

진영에 편입할 것인가, 아니면 중견국으로서 한국의 독자 표준을 개발할 것인가? 그리고 이러한 표준 선택의 상황이 단순한 기술과 산업 분야가 아닌 한·미 동맹과 한·중 협력의 재조정 문제라는 외교문제로서 다가올 경우는 어떻게 할 것인가?

둘째, 인터넷과 사이버 안보 분야의 국내 정책과 제도 모델(좀 더 구체적으로는 표준 거버넌스 모델)을 모색함에 있어서 한국이 추구할 방향은 어디인가? 미국이 주창하는 민간 주도의 이해당사자주의 모델인가, 아니면 중국이 고수하려는 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 안보 담론의 경쟁을 벌이는 와중에 한국이 제시하는 담론의 내용은 무엇인가? 미국이 전파하고 있는 인터넷 자유의 보편주의적 안보 담론인가, 아니면 중국이 지키려고 하는 사이버 주권의 민족주의적 안보 담론인가? 그 사이에서 중견국으로서 한국이 새로운 안보 담론을 생성할 여지는 없는가? 예를 들어, 강대국들이 추구하는 힘의 논리에 기반을 둔 안보 담론이 아닌, 규범과 윤리를 강조하는 사이버 공간의 담론을 구성할 수는 없을까?

최근 중견국으로서 외교전략의 진로를 고민하고 있는 한국의 입장에서 볼 때 이러한 질문에 대해 답을 찾는 것은 매우 중요한 국가전략적 과제가 아닐 수 없다. 이러한 과정에서 표준경쟁과 표준전략에 대한 논의는 중견국 외교전략 연구에 매우 유용한 이론적 틀을 제공할 것이다. 지금 이 시점에서 사이버 안보 분야, 그리고 좀 더 넓게는 21세기 세계 정치 전반에서 미국과 중국이 벌이는 표준경쟁의 전개 양상을 올바로 이해하고, 이에 대응하는 표준전략 또는 외교전략의 방향을 수립하는 작업은 시급하다 하겠다.