No. 106

IIRI Online Series

디지털 안보경쟁과 한국: 평가와 제언

송 태 은

국립외교원 안보통일연구부 조교수

2022. 8. 30

IIRI 일민국제관계연구원
Ilmin International Relations Institute

디지털 안보경쟁과 한국: 평가와 제언

송 태 은 | 국립외교원 안보통일연구부 조교수

디지털 안보경쟁 평가

2018년 미국에서 불거진 화웨이(Huawei) 사태부터 시작해서 2019년 12월 시작된 코로나19 감염병 팬데믹 그리고 2022년 2월 24일 러시아의 침공으로 시작된 러시아-우크라이나 전쟁은 미·중 기술패권 경쟁과 반도체 등 핵심 기술을 중심으로 한 글로벌 공급망 재편 움직임을 본격적인 궤도에 올려놓았다. 게다가 현재의 러시아-우크라이나 전쟁이 러시아와 서구권의 대리전 양상으로 전개되면서 이번 전쟁은 그동안 양측이 발전시켜온 신무기의 효과와 파괴력을 실전에서 시험해 볼 수 있는 테스트베드(test bed)가 되고 있다. 이번 전쟁으로 인해 진영 간 무기개발과 수출을 둘러싼 방산산업 경쟁은 더욱 치열해지고 있고, 구글(Google), 메타(Meta), 마이크로소프트(Microsoft), 스페이스X(SpaceX)와 같은 세계적 IT 기업들은 우크라이나의 사이버 활동을 지원하면서 디지털 안보경쟁의 승자를 가리는 진짜 주체가 누구인지 직접 보여주고 있다. 이제 고조되고 있는 미·중경쟁과 진영 간 대결 양상이 '신냉전'인지 논하는 것은 의미가 없어졌다. 이러한 상황은 그동안 미·중 사이에서 '끼인' 국가로서 어떤 외교를 펼쳐야 할지, '균형 있는' 외교를 펼치고 싶어 했던 한국에게 외교의 방향성을 놓고 머뭇거릴 시간을 주지 않고 있다.

최근 미국과 중국 간의 기술경쟁은 반도체와 배터리 부문에서 갈등이

나타나고 있다. 8월 9일 바이든 대통령은 자국의 반도체 산업을 지원하기 위한 법안인 “반도체 및 과학법(CHIPS and Science Act)”에 서명했고, 8월 16일에는 “인플레이션 감축법(Inflation Reduction Act)”에 서명하여 반도체와 배터리 부문에서 중국을 전방위로 견제할 것을 공고히 했다. 미국은 국내 법·제도적 조치와 맞물려 한국, 대만, 일본과 칩4동맹(Chip4 alliance) 논의도 본격 가동시켰다. 미·중 간 반도체와 배터리 부문에서의 경쟁은 인공지능(AI), 양자컴퓨팅, 사물인터넷(IoT), 자율무기체계(AWS), 블록체인(blockchain) 등 첨단 디지털 기술 개발 경쟁의 승자를 가리는 더 큰 대결을 자국에게 유리하게 만들기 위한 예비경기이다.

중국은 바이든 대통령이 서명한 두 법안이 세계 공급망을 왜곡하고 국제무역을 교란시킬 것이라고 반발하고 있다. 칩 설계를 자동화하는 기술은 미국 업체들이 독점하고 있고, 반도체를 제조하는 파운드리는 대만과 한국 등 미 동맹이 공급하고 있다. 하지만 중국은 미국이 주도하는 이러한 공급망 재편 조치에 대응하거나 반격할 대안을 갖고 있지 않다. 그런데 미국이 이렇게 반도체 분야에서 강력한 조치들을 취하게 된 계기가 되는 빌미는 중국이 제공했다. 애초에 미·중 간 반도체 부문에서 갈등이 시작된 것은 중국의 최대 통신장비 업체인 화웨이가 미국을 포함한 서방에서 왕성하게 펼쳐온 첩보활동 때문이었다. 일찍이 2011년 미 국방부와 하원 정보위원회는 화웨이와 중국군이 첩보활동을 긴밀히 공조하고 있고 화웨이 장비가 중국의 스파이 활동과 사이버전에 사용될 가능성을 경고한 바 있다. 호주, 스웨덴, 인도, 뉴질랜드 등 각국 통신 네트워크에 광범위하게 진입해있는 화웨이는 통신장비 소프트웨어의 백도어 기능과 도청장치를 통해 기밀정보를 중국 당국에 전달하고 있었고, 노르텔(Nortel), 모토로라(Motorola), 시스코(Cisco), 옵투스(Optus), 티모바일(T-mobile), 퀀텔(Quintel), 씨넥스(CNEX) 등은 화웨이의 그러한 정보활동의 직접적인 피해자였다.[1].

이미 부시 행정부 시기에 드러난 중국 기업의 문제는 트럼프 행정부 시기인 2018년 8월 중국 정부가 소유, 통제하거나 실질적으로 그렇게 운영되는 중국 기업의 통신장비와 서비스를 미국의 행정기관이 조달, 계

1) Rohit Dube, “Huawei’s role in Chinese espionage and information operations,” March 27, 2022,https://www.researchgate.net/publication/359582343_Huawei%27s_role_in_Chinese_espionage_and_information_operations 참조.

약하는 것을 금지하는 2019년 국방수권법이 통과되면서 공격적으로 다뤄지기 시작했다. 1년 뒤인 2019년 5월 미국은 “국제긴급경제권한법(IEEPA: International Emergency Economic Powers Act)”을 발동하여 국가 안보를 침해하고 미국 기업의 기술을 유출하는 타국 IT 기업과의 거래를 금지했다. 급기야 미국은 2020년 5월 미국산 장비와 소프트웨어를 사용하는 반도체 업체가 화웨이에 반도체를 공급할 경우, 사전 승인을 받을 것을 담은 수출관리규정(EAR: Export Administration Regulations)을 개정하기에 이르렀다. 이렇게 4년에 걸쳐 차근차근 강화된 미국의 화웨이에 대한 견제는 한때 전 세계 스마트폰 시장 점유율 1, 2위였던 화웨이가 현재 6위의 시장 점유율이라는 결과로 나타났다. 되짚어보면, 애초에 반도체 부문에서 미국의 중국 견제를 촉발한 직접적인 계기는 이미 화웨이가 20년 가까이 깊숙이 공조해온 중국 정부와의 첩보활동이다.

민주주의 대 권위주의: 신기술 경쟁과 함의

현재 미국의 대중국 견제는 단순히 기술, 경제, 군사 분야에서의 위협 인식 때문만이 아니다. 주지하다시피 2016년 미국 대선을 비롯하여 2017년 이후 유럽 각국의 거의 모든 선거철 소셜미디어 플랫폼에서 러시아가 전개한 허위조작정보 유포 활동은 전시(wartime) 심리전을 방불케 할 정도로 위협적이었고 ‘로보트롤링(robo-trolling)’과 같은 AI의 정보커뮤니케이션 기술까지 동원되었다. 즉 미국이 화웨이에 칼을 빼 든 시점은 러시아와 이란 등 권위주의 국가들이 서구권 선거에 은밀하게 개입하는 사이버 심리전에 대한 미국과 서구권의 경각심이 최고조에 이르렀던 때이다. 현재의 미·중 패권경쟁의 핵심은 ‘기술’을 둘러싼 양국 간 대결이지만 이 경쟁과 맞물려 일어나는 미·중 간 갈등은 경제·산업과 군사부문에 한정되지 않고 정치체제와 가치·이념까지 확장되고 있는 것이 오늘날 디지털 안보경쟁의 본질을 이해하는 중요한 관전 포인트이다.

지금의 미·중 간 패권경쟁은 디지털 기술을 중심으로 진행되고 있고, 그러한 기술경쟁의 승자를 결정하는 분야는 다양한 신기술의 발전을 견인하고 있는 인공지능(AI) 분야이다. AI는 반도체, 양자컴퓨팅, 바이오, 첨단 네트워크의 발전을 견인하는 가장 중요한 범용기술(General Purpose Technology)이자 ‘기술 중의 기술(the field of the fields)’이

다. 현재까지 미국의 AI 기술 경쟁력은 전반적으로는 중국에 비해 우위에 있으나 양국 간 격차는 빠르게 좁혀지고 있고, 현재의 추세가 지속되면 중국은 미국의 기술패권을 10년 이내에 앞지를 수 있다. 그런데 현재 미국이 AI 분야에서 중국에 대해 느끼는 위협은 기술의 차원을 넘어 정치체제, 사회심리 차원과 가치와 이념 영역에서의 위협도 포함한다. 즉 미국은 중국의 AI 기술력이 안보, 경제, 정치, 가치 모든 차원에서 미국의 국익을 위협하고 있다고 인식한다. 바로 이 지점에서 한국의 선택이 단순히 미·중 사이의 아슬아슬한 균형 잡기의 차원에서 끝나기 어려운지 말해준다.

먼저 미국을 비롯한 자유주의 진영이 중국, 러시아, 이란 등 권위주의 진영의 AI 기술을 민주주의 제도에 대한 위협으로 보고 사회심리적 차원에서도 대응하게 된 가장 큰 계기는 이들 권위주의 국가들이 내러티브(narrative) 구사와 스토리텔링(storytelling) 기술을 구비한 AI의 정보생산 및 대규모 정보의 전달 기술을 이용하여 서구권 여론을 교란한 행위였다. 즉 서구권 민주주의 국가들은 이러한 정보활동의 궁극적인 목적이 여론을 왜곡하는 수준을 넘어 민주주의 정부의 정치적 정당성(political legitimacy)을 훼손하고 사회 내 분열과 극단주의 세력을 자극하여 전복적인 움직임을 조성하는 것이라고 보고 있다. 서구권은 권위주의 진영의 사이버 심리전 혹은 디지털 프로파간다(digital propaganda) 활동을 '주권'과 '민주주의 제도'에 대한 직접적인 도전으로 인식하기 때문에 군사적 차원에서 대응하고 있는 것이다.

권위주의 국가가 사용할 때 더욱 증대될 수 있는 AI와 관련된 정치적 위협 중 민주주의 진영이 주목하고 있는 이슈는 알고리즘의 편향성(bias) 문제와 더불어 '디지털 권위주의(digital authoritarianism)의 확산' 문제이다. 중국의 일대일로를 통해 개발도상국으로 이식되고 있는 중국식 국가 감시체제는 중국의 권위주의 체제를 이식시키는 효과와 더불어 중국 기술 수용국의 안보와 보안이 중국에 대해 취약해지는 결과도 가져오기 때문이다. 중국의 AI 감시기술이나 '만리방화벽(Great firewall)'과 같이 광범위한 검열과 자동화된 감시 시스템을 갖춘 폐쇄적 디지털 인프라와 플랫폼이 개발도상국에 이식되면서 중국식 사회통제와 언론검열 수단이 함께 이식되고 있는 것이다. 중국의 AI 감시기술은 케냐, 라오스, 몽골, 우간다, 우즈베키스탄, 남아프리카공화국, 보츠와나,

나이지리아, 짐바브웨와 같이 첨단기술이 부재한 국가가 중국의 일대일로에 참여하거나 화웨이가 이러한 국가와 추진하는 스마트시티 개발 사업을 통해 확산되고 있다. 코로나19 팬데믹을 계기로 국가의 강화된 방역 정책의 필요성은 개인에 대한 프로파일링(profiling)과 사회 전체를 대상으로 하는 전방위 감시체계 구축을 정당화하고 공고화시키는 계기가 되었으므로 이러한 문제는 민주주의 국가도 예외가 아니다. 다만 민주주의 사회에서는 국가의 감시체제가 초래할 인권침해에 대해 정당과 언론, 시민사회가 끊임없이 문제를 제기할 수 있으나, 인권을 보장할 법·제도적 장치가 부재하거나 취약한 권위주의 국가는 그러한 감시체제를 더 쉽게 악용할 수 있다.

미국은 중국발(發) 디지털 권위주의의 확산을 저지하기 위해 AI 기술의 개발과 사용에 있어서 민주주의 국가가 기업들과 공조하여 국내적으로는 민주주의 제도와 시민사회를 보호하고, 민주주의 동맹국들이 서로 연대하는 전략을 모색하고 있다. 또한, 미국은 AI를 포함한 다양한 신기술에 대한 비민주주의적 접근법을 저지하기 위해 국제사회의 규범 형성 과정에서 민주주의 국가들과 협력하고 권위주의 국가와는 직접 대화와 협상을 도모하고 있다. 지속적인 AI 기술의 발전을 위해서라도 미국은 AI의 개발과 사용에 있어서 민주주의 모델을 추구하고 대중의 신뢰를 얻는 것을 중시하고 있다. 요컨대 AI 기술을 사용하는 방식이 정치와 인권에 끼치는 영향에 있어서도 미·중 기술경쟁은 격렬하게 충돌하고 있다.

고도로 발전하고 있는 신기술 무기와 관련해서도 미국을 비롯한 민주주의 진영은 권위주의 진영이 자율무기의 군사적 의사결정을 인식하는 방식에 대해 우려하고 있다. 인간과 달리 알고리즘은 전장의 상황을 산술적으로 판단하고 오로지 양적 효율성 차원에서 군사적 의사결정에 이를 수 있으므로 자율무기의 의사결정 과정에 인간이 개입하지 않을 경우, 기계가 내릴 결과는 '예측불가능성'의 문제를 갖는다. 전쟁이라고 해도 전황에 대한 평가는 종합적인 판단 즉 법률적, 정치적, 외교적 판단을 필요로 하나, 현재 AI의 발전 수준은 그러한 능력을 결여하고 있기 때문이다. 미국은 중국이 전장에서 전투속도와 파괴력의 우위를 점하기 위해 자율무기의 완전한 자율성에 대해 민주주의 국가에 비해 보다 개방적인 접근법을 취하고 있는 것으로 인식하고 있다. 그러면, 현실은 어떠한가? 이번 전쟁에서 러시아는 우크라이나 민간인들을 대량 학살하고 화

학무기와 진공폭탄 등 국제사회가 사용을 금지한 무기를 무차별적으로 사용하여 서구의 그러한 우려를 강화시켜주고 있다. 러시아가 취하고 있는 군사행동은 인간의 판단이 기계보다 더 합리적이고 도덕적이라고 볼 수 없게 만드는 사례를 만들어주었다. 결국 2022년 4월 7일 유엔의 긴급 특별총회는 러시아의 유엔 인권이사회 이사국 자격을 정지하는 결의안을 통과시켰고, 러시아는 안보리 상임이사국 중 유일하게 유엔 산하 기구에서 자격을 정지당한 국가가 되었다. 러시아는 이번 전쟁에서 전개한 사이버 공격에 있어서도 교육기관과 보건기관 등에 대해 무차별로 공격을 수행하여 러시아의 제안으로 조직된 유엔 정보안보전문가그룹(UN GGE: UN Group of Governmental Experts)과 개방형워킹그룹(OEWG: Open-Ended Working Group) 등에서 발휘한 러시아 리더십의 진짜 목적이 무엇인지 의문을 갖게 한다. 아무리 전시라고 하여도 러시아는 그동안 진행되어온 사이버 공간에 대한 국제사회의 거버넌스 논의를 완전히 무용지물로 만들어버렸기 때문이다.

특히 해킹이나 멀웨어(malware) 공격과 같은 사이버 범죄와 사이버 공격 행위에 대한 규범 구축, 즉 사이버 공간의 거버넌스와 관련된 이슈들은 이번 러시아-우크라이나 전쟁 이전부터도 민주주의 진영과 권위주의 진영 간 첨예하게 대립한 주요 문제였다. 그동안 전 세계적인 랜섬웨어(ransomware) 공격의 주요 진원지는 러시아, 중국, 북한, 이란으로서 주로 서방과 외교적 갈등 관계에 있는 권위주의 국가들이었기 때문에 사실상 사이버 공간은 미·중 경쟁과 진영화의 폐해가 가장 심각한 공간이었다. 2021년 10월 14일 미국이 유럽과 아시아의 30여 개국 장관들과 '랜섬웨어 대응 이니셔티브 회의'를 발족시키며 발표한 공동선언문은 각국의 핵심 인프라, 에너지 및 보건기관 등에 대한 랜섬웨어 공격과 금전적 이익을 위한 랜섬웨어 공격을 규탄했다. 러시아는 동 회의에 참석하지 않았는데, 2022년 1월부터 우크라이나에 대한 대규모의 사이버 공격을 수행했고, 2월 전쟁 개시와 함께 미국과 유럽의 많은 국가가 러시아 사이버 공격의 주요 대상이었다는 점을 보면 당연한 일일 것이다.

한국의 고려사항

정리해보면, 디지털 안보경쟁의 주요 이슈들은 모두 공통적으로 안보, 경제, 기술, 정보, 커뮤니케이션, 정치체제, 가치가 서로 연계되어 있다.

문제는 미국과 중국을 중심으로 한 양 진영이 디지털 기술의 사용 방식과 목적 및 거버넌스 등 거의 모든 관련 이슈에서 충돌하고 있는 점이다. 이러한 상황에서 우리의 선택은 무엇인가?

먼저 민주주의 국가로서 한국은 미국이 이끄는 신기술동맹과 민주주의 연대에 공조하는 것이 AI를 비롯한 다양한 디지털 기술에 대한 우리의 자연스러운 정책적 선호이다. 그렇기 때문에 한국은 신기술동맹의 추진에 있어서 자연스럽게 미국과 서방 민주주의 진영의 중요한 파트너로 여겨지고 있다. 그럼에도 불구하고 우리는 왜 민주주의 가치와 모델이 우리의 디지털 기술 정책에서 우리가 관철해야 할 국익인지 스스로 확인하고(define), 그러한 인식을 국가 차원에서 선언하는 작업이 필요하다. 우리의 과학기술외교 전개에 있어서 우리가 강조할 가치와 우리가 취할 규범적 접근법을 실제 정책에 반영할 때, 우리의 접근법이 국제사회와 인류의 안녕에도 기여한다는 것을 강조할 필요가 있다.

이러한 작업이 중요한 것은 민주주의 국가로서 한국이 AI 및 디지털 기술 분야에서 미국의 가치외교와 규범외교에 동참하고 협력하는 것이 양자 택일 압력에 의한 수동적 선택이 아니라, 우리의 국익과 우리가 중시하는 가치 때문임을 당당하게 공식화할 수 있고, 국제사회에서 신기술 분야 우리 외교의 자율성과 규범적 우위 확보에도 유용하기 때문이다. 즉 우리가 미국의 동맹이라는 이유만으로 미국의 기술동맹과 민주주의 연대에 동참한다기보다 민주주의 규범과 가치를 중시하는 방식으로 디지털 기술을 개발하고 사용하는 민주주의적 접근법이 우리의 기술정책 규범과 국익에 부합한다는 논리를 펼 수 있기 때문이다. 이와 같은 논리는 인권을 보호하고 신뢰할 수 있는 기술 개발과 이용을 추구하는 민주주의 유사입장국들(like-minded countries)의 기술에 대한 접근법이 곧 우리가 선호하는 접근법이라는 명분을 만들어준다. 더불어, 기술에 대한 우리의 민주주의적 접근법을 적극적으로 드러내는 것은 개발도상국이나 신생 민주주의 국가가 디지털 기술의 협력 파트너로서 한국을 선택하는 것이 그들 국가의 대중에게도 합리적인 명분을 제공하는 효과가 있다.

이제 우리의 디지털 기술정책은 동맹과 파트너 국가 및 국제사회에서 어떤 협력을 추구하고 연대외교를 펼쳐야 하는지 구체적인 목표와 세부 과제 및 외교전략을 제시할 수 있어야 한다. 또한, 디지털 기술 분야에

서 우리의 국익을 최대화하면서 미국과의 기술동맹 협력에서 무엇을 얻어내고 기여할 것인지 포괄적인 협력의 목표와 전략이 조속히 마련되어야 한다. 현재 디지털 기술과 관련된 우리의 외교 의제는 신기술·신흥안보 분야에서의 국제규범 형성과정에 한국이 참여하고 기여하는 중견국 외교와 반도체 공급망 문제 등 경제안보 문제에 집중되어 있으나, 더 나아가 우리 정부는 다양한 첨단 디지털 기술을 아우르며 종합적인 국가 목표를 제시할 수 있어야 한다. 우리 정부는 디지털 경제 및 안보와 관련된 각 부처가 경제, 안보, 정치·규범적 차원에서 우리의 국익을 달성하기 위해 어떻게, 누구와, 어떤 분야에서 협력할 것인지 치밀한 계획과 차근차근 단계를 밟아나가는 중장기 전략을 빨리 마련해야 한다. 즉 우리가 동맹 및 파트너 국가들과 디지털 기술의 어떤 분야에서 우리의 기술력을 압도적으로 내세우고 우위를 다지며 협상력을 키울 것인지, 어떤 분야에서 중점적으로 협력하고 교류할 것인지, 그리고 디지털 기술과 관련하여 해외 정부기관 및 연구기관 파트너와 어떤 네트워크를 만들 것인지 구체적인 전략을 마련할 필요가 있다.

/끝/

저자 소개

송태은 교수는 성균관대 정치외교학과 학사, 美 University of California, San Diego(UCSD) 국제관계학 석사, 서울대에서 외교학 박사학위를 받았다. 현재 국립외교원 안보통일연구부 조교수, 한국국제정치학회 연구이사, 정보세계정치학회 총무이사, 국회도서관 의회정보자문위원이다. 서울대 국제문제연구소 선임연구원, 국립외교원 외교전략센터 연구교수로 재직했고, 연구 분야는 신기술, 사이버전, 하이브리드전, 정보전, 심리전, 전략커뮤니케이션과 위기대응 및 글로벌 커뮤니케이션 이슈이다. 주요 저서와 보고서는 『디지털 안보의 세계정치』(공저, 2021), 『4차 산업혁명과 신흥 군사안보』(공저, 2020), “러시아-우크라이나 전쟁의 사이버전”(2022), “러시아-우크라이나 전쟁의 정보심리전”(2022), “바이든 행정부의 인공지능 국가정책”(2022), “신기술 무기의 안보적 효과와 주요 쟁점”(2021), “디지털 시대 하이브리드 위협 수단으로서의 사이버 심리전의 목표와 전술”(2021), “인공지능 기술을 이용한 국가의 사회감시 체계 현황과 주요 쟁점”(2020) 등이다. (Email: tesong22@mofa.go.kr)