Asan Report

사이버공간의 신지정학

고명현

2020년 12월

아산정책연구원

아산정책연구원

우리 연구원은 한반도와 동아시아 그리고 지구촌 현안에 대한 깊이 있는 정책 대안을 제시하고 올바른 사회담론을 주도하는 독립 싱크탱크를 지향합니다. 특히, 통일-외교-안보, 거버넌스, 공공정책-철학 등의 분야에 역량을 집중하여 우리가 직면한 대내외 도전에 대한 해법을 모색함으로써 한반도의 평화와 통일 및 번영을 위한 여건 조성에 노력하고 있습니다. 또한 공공외교와 유관 분야 전문가를 육성해 우리의 미래를 보다 능동적으로 개척할 수 있는 역량을 키우는 데 이바지하고자 합니다.

저자

고 명 현

아산정책연구원 선임연구위원이다. 주요 연구 분야는 북한 체제의 장기지속성, 대북제재, 사이버 안보 및 사회적 정보확산이다. 미 랜드(RAND)연구소 산하 Pardee RAND Graduate School에서 정책분석학 박사학위를 취득한 고명현 박사는 2015년도 뮌헨안보회의 Young Leader, 독일 아고라 전략연구소 객원 펠로우 및 고려대학교 정보보호대학원 겸임교수이다.

감사의 글

본 보고서는 저자가 고려대학교 정보보호대학원에서 연구년을 보내며 수행한 연구의 결과물이다. 연구년 동안 조언과 지원을 아끼지 않으신 동 대학원의 이경호 교수 및 교수진과 RIMALA 랩 연구원들에게 감사의 말씀을 올린다.

* 본 보고서의 내용은 연구원의 공식 입장이 아닌 저자의 개인 견해입니다.

목차

표

서론: 사이버공간의 신지정학

오늘날 세계는 냉전 종식 이후 최대 격동기를 겪고 있다 해도 과언이 아니다. 2016년 영국의 유럽연합(EU) 탈퇴와 이를 뒤 이은 도널드 트럼프의 미 대통령 당선은 2차 세계대전 이후 미국이 구축한 자유주의 세계질서를 뿌리부터 뒤흔들었다. 지난 4년간 국제정세는 북대서양조약기구(NATO)와 유엔 등 미국 스스로 구축한 다자간 국제질서 체제를 현직 미 대통령이 앞장서 훼손하고 한미동맹을 포함해 기존 동맹관계를 부정하는 전례 없는 상황 앞에서 크게 요동쳤다. 2020년 대선에서 민주당 조 바이든 후보가 승리하면서 미국은 다시 동맹 중심의 외교안보 노선으로 복귀할 것으로 예상된다. 하지만 지난 4년간의 혼란이 야기한 국제정세의 여진은 오랫동안 계속될 것이다.

미국이 자초한 혼란 외에도 국제사회의 혼란과 갈등이 장기화될 것으로 예상되는 이유로는 정보통신기술의 발전으로 인한 안보 및 경제 패러다임이 빠르게 변하고 있다는 것이다. 중국과 러시아를 중심으로 하는 권위주의 국가들은 이러한 변화를 전략적으로 활용해 미국의 패권에 도전하고 있다. 중국은 오랫동안 축적한 과학기술과 자본력을 바탕으로 미국과 대등한 경쟁을 추구하며 러시아는 사이버공간의 개방성을 이용하는 비대칭 정보전을 벌여 서방세계의 자중지란을 유도하고 있다.

패권을 둘러싼 강대국 간의 경쟁이 야기한 국제 갈등은 과학기술이 그 촉매 역할을 하여 지정학적 영역을 넘어 다양한 분야로 확산되는 데 일조한다. 경쟁국과 초격차를 유지하려는 미국과 맹렬히 추격하는 중국은 둘 다 고도화된 과학기술을 기반으로 하는 경쟁전략을 추구한다. 미국이 첨단 군사력을 통해 군사적 우위를 유지하는 것이 목적인 3차 상쇄전략(Third Offset)을 내세운다면 중국은 "중국 제조 2025"로 상징되는 기술굴기에 집중한다. 미국이 중국의 첨단기업인 화웨이(Huawei)를 제재하는 것은 시진핑의 역점사업인 일대일로의 디지털 실크로드(Digital Silkroad)와 밀접한 관계가 있다.

아산정책연구원이 2019년 말 발간한 '아산 정세전망 2020: 신지정학'은 작금의 강대국 간 갈등이 전통적 지정학적 경쟁에서 "과학기술이 창출해낸 새로운 국경"을 따라 확산되는 하이브리드 지정학으로 진화하였다고 말한다. 즉, 기존의 지정학적 갈등이 과학기술을 통해 더욱 확대되고 심화되는 것이 신지정학이다. 신지정학적 현상은 어쩌면 당연하게도 사이버공간에서 더 쉽게 나타난다. 사이버공간에서의 충돌은 인명피해가 발생할 가능성이 낮기 때문에 무력충돌로 이어지지는 않는다. 대신 갈등의 전선은 확대되고 충돌의 유형은 다양해진다. 현재 과거 냉전 때와 같이 양 진영 간의 완전한 단절은 아직 없지만(Trenin 2014) 절대적 기술우위를 노리는 강대국 간의 치열한 경쟁으로 인해 기술, 데이터, 인터넷 거버넌스를 둘러싸고 전방위적으로 강대국 간 갈등이 심화되고 있다. 특히 이념적 갈등의 골이 깊어지며 사이버공간에서의 갈등을 "실존적 투쟁"으로 간주하는 기류가 강대국 간에 강해지고 있다.

빠르게 분쟁영역화 되고 있는 사이버공간은 강대국 간의 갈등이 확산되는 신지정학이 발현되는 공간이자 동시에 촉매제이다. 전통적인 영토 분쟁이었던 우크라이나 사태를 둘러싼 러시아와 서방세계의 충돌은 신지정학의 대표적 사례라고 할 수 있다. 2014년 우크라이나 침공으로 제재를 받는 러시아가 2016년 미 대선에 개입한 배경에는 미국과 유럽이 지지하는 개방되고 자유로운 인터넷이 실제로는 정권교체를 위한 심리전 도구라는 러시아의 강한 의구심이 작용했다.[1] 전통적 우방이던 세르비아와 우크라이나의 친러 정권들이 서방의 지지를 받는 시민혁명에 의해 전복되자 러시아가 반격 차원에서 미 대선에 개입했다는 관측이 지배적이다.

이렇듯 정보통신기술의 비약적인 발전은 인류의 사회, 문화, 경제만 변화시킨 것이 아니라 국가 간 역학관계마저 변화시켰다. 신지정학적 갈등의 구조적 원인은 4차 산업혁명으로 수렴되는 첨단과학기술을 선점하기 위한 경쟁에서 찾을 수 있다. 정보통신기술의 발전은 현대사회의 경제 구조를 탄소경제(Carbon Economy)에서 데이터경제(Data Economy)로 빠르게 전환시키며 국가전략의 우선순위도 바꿨고 강대국 간의 핵심적 갈등 요인을 영토와 천연 자원 확보에서 과학기술과 데이터로 변화시켰다. 경제발전의 핵심자원이 탄소 기반 에너지에서 무형의 데이터로 넘어가면서 오늘날 국제관계 갈등은 석유가 아닌 데이터를 둘러싸고 일어나고 있다.

이러한 패러다임 전환의 배경에는 오늘날 인류가 쏟아내고 있는 엄청난 양의 데이터가 있다. 매일 생성되는 엄청난 양의 데이터에는 동영상, SNS 메시지, 블로그 등 개인정보, 인터넷 서비스(예: 위치기반 서비스와 온라인 쇼핑) 사용 중 파생되는 메타데이터(metadata)

1. Quartz. What you need to know about Russia's election hack and why US senators say it 'should alarm every American'. December 13, 2016. https://qz.com/860706/russian-hacking-and-the-us-election-why-it-matters-what-it-means-and-whats-next/.

그리고 이제는 컴퓨터와 각종 네트워크化된 기기들이 서로 통신하면서 만들어내는 센서(Sensor) 데이터 등이 포함된다. 이른바 빅데이터로 통칭되는 이러한 데이터는 연 60% 폭증하고 있으며, 2025년도에는 2020년도 수준의 10배가 넘는 데이터 총량이 생성될 것으로 예상된다. 오늘날 가용가능한 빅데이터의 대부분은 개인정보에서 파생된다. 흔히 빅데이터로 규정되는 온라인 쇼핑, 위치기반정보, 사진과 동영상의 메타데이터가 개인정보의 범주에 들어간다. 이런 종류의 데이터들은 지난 20년 동안 인터넷 기업들의 폭발적인 성장을 뒷받침했다. 아마존, 페이스북, 구글, 인스타그램(Instagram) 등 잘 알려진 인터넷 대기업들의 사업 모형은 모두 개인정보에 기반한다.

인터넷과 빅데이터로 인해 개인정보의 경제적 가치가 급성장하면서 개인정보 보호는 단순히 사생활 보장의 차원을 넘어 중대한 경제안보적 이슈가 되었다. 2019년 미 민주당 대선 후보 경선주자였던 앤드류 양(Andrew Yang)은 인공지능 개발에 투입되는 개인정보 사용에 대한 대가를 개인이 보상받아야 한다고 주장하기도 했다.[2] 이렇듯 개인정보가 4차 산업혁명의 핵심자원으로 부상하면서 국가적 차원의 데이터 관리와 활용이 중요해졌다. 현재 각국은 사생활 보호라는 인권 차원에서 접근되던 개인정보의 경제적 잠재력을 깨닫고 이를 활용하는 전략을 수립 중이며, 최근 통과된 한국의 "데이터3법"도 사생활 보호보다는 개인정보의 상업적 활용에 방점이 맞춰져 있다.

국가 주도의 개인정보 통제와 배타적 상업적 활용은 중국과 유럽연합이 각각 "사이버 주권"과 "디지털 주권"을 내세우는 배경이기도 하다. 유럽연합이 2018년부터 시행하고 있는 "일반데이터보호규정"(GDPR: General Data Protection Regulation)과 중국의 사이버보안 관련법은 개인정보 보호를 위해 데이터의 자유로운 국외이전을 막는다. 이러한 데이터 현지화(Data Localization) 정책은 "정보의 자유로운 이동"을 추구하고 데이터 현지화를 반대하는 미국의 입장과 충돌한다. 구글과 페이스북의 사업모델은 개인정보를 비롯한 데이터의 무제한 수집을 바탕으로 하기 때문에 미국은 미국-멕시코-캐나다협정(USMCA: United States-Mexico-Canada Agreement)과 아시아-태평양 경제협력체(APEC:Asia-Pacific Economic Cooperation)에 데이터 현지화를 반대하는 규정을 삽입하였다. 중국뿐만 아니라 아니라 유럽연합의 이해와도 상충되는 미국의 데이터 정책은 경쟁국의 반발을

2. CNBC, 2019년 10월 17일. "Andrew Yang: You should get a check in the mail from Facebook, Amazon, Google for your data" https://www.cnbc.com/2019/10/17/andrew-yang-facebook-amazon-google-should-pay-for-users-data.html.

유발해 사이버공간의 주권화와 데이터 경제의 블록화로 이어지고 있다.

이 갈등은 미중 관계에서 가장 심각하게 발현된다. 미국과 자유주의적 국제질서라는 인식을 공유하는 유럽연합과는 달리 중국은 주요국가 중에서 가장 폐쇄적인 사이버 정책을 시행하고 있다. 하지만 중국의 사이버 정책은 단순히 외부정보 유입을 차단하는 것이 아니라 첨단기술 발전이 목적인 산업정책의 성격도 띈다. 중국은 페이스북 같은 세계적 IT 대기업을 자국 시장에서 밀어내고 대신 자국 기업 중심의 빅데이터 산업 생태계를 구축하였다. 바이두(Baidu), 텐센트(Tencent), 알리바바(Alibaba) 등 주요 중국 IT 기업들은 자국 시장에서 구글, 페이스북, 아마존을 각각 대체하였고 10년이 지난 현재 원조 미국 기업들을 거의 따라잡은 수준으로 성장하였다. 현재 중국 "카피" 기업들의 시가총액은 미국 "원조" 기업들 턱밑까지 따라온 상태이다.

최근 중국과 러시아는 여기서 한발짝 더 나아가 자국 인터넷을 전체 인터넷에서 분리하는 정책을 실행 중이다. 러시아는 RuNet이라는 유사시에 자국 인터넷을 전체 인터넷에서 분리할 수 있는 국내용 인터넷 도입을 완료했으며 중국은 현재 사용되는 인터넷 통신 프로토콜인 TCP/IP 대비 중앙집중적 통제를 용이케 하는 "뉴IP"이라는 새로운 인터넷 통신 프로토콜을 개발하였다. 이 신기술의 범세계적 채용을 위해 중국이 유엔기구인 국제전기통신연합(ITU: International Telecommunication Union)을 적극 활용한다는 것은 사이버 국제규범을 주도하기 위해 어떻게 중국이 국제기구를 장악하고 공공외교를 활용하고 있는지를 보여준다.

사이버공간의 분리와 국가주권화를 추진하는 중국과 러시아의 행동은 과학기술과 경제 주도권을 지키기 위해 개방된 인터넷 환경이 절실한 미국에게는 심각한 위협이 된다. 미국은 사이버 주도권에 대한 도전을 세계패권에 대한 도전으로 받아들여 국제규범, 기술, 영역을 연계하는 신지정학적 방식으로 경쟁국의 도전에 대응에 나서고 있다. 미국은 2018년 미 백악관이 발표한 "국가 사이버 전략"(National Cyber Strategy)에서 공개적으로 중국과 러시아를 사이버공간을 분열시키고 국제규범을 악용하는 국가들로 규정하였다. 특히 4차 산업혁명 관련 기술과 산업이 전무하다시피 한 러시아와는 달리 "중국 제조 2025" 등의 계획을 통해 5G, 인공지능, 첨단소재 등 분야에서 신기술을 선점해 미국을 추월하겠다는 야심을 드러낸 중국에게는 전방위 압박을 가하고 있다. 미국은 중국의 사이버공간 분리 행동에 대해 중국기업의 미국 시장 접근과 첨단기술 및 부품 이전을 차단하는 경제·기술적 디커플링(Decoupling)으로 맞대응한다.

최근 중국의 거대 IT기업인 화웨이를 둘러싼 미중 간의 충돌 또한 단순히 네트워크 보안을 둘러싼 문제가 아닌 신지정학적인 갈등의 한 예로 봐야 한다. 이를 위해 중국의 최대 전략 사업인 일대일로(BRI: Belt and Road Initiative) 계획에서 화웨이가 차지하는 위상을 이해해야 한다. 5G와 인터넷 네트워크 설비를 생산하고 기업 지배구조가 불투명한 상당수 중국 IT기업 중에서 유독 화웨이가 미국의 집중적 견제를 받는 데는 화웨이가 중국 국영기업인 차이나 텔레콤과 함께 일대일로의 사이버 버전인 디지털 실크로드를 구축하는 핵심행위자이기 때문이다. 참고로 화웨이와 차이나 텔레콤은 중국 인민해방군이 통제하는 기업이라고 미 국방부가 지목한 바 있다. 화웨이는 남아시아와 인도양 지역에서 인터넷 기간망인 해저 광케이블 부설과 일대일로 참여국들의 5G 네트워크를 구축하고, 차이나 텔레콤은 디지털 실크로드의 데이터 이동을 뒷받침하는 데이터 센터 구축을 담당한다. 미국의 입장에서 디지털 실크로드는 단순히 중국의 일대일로를 통한 정보통신 인프라 구축이 아니라 미국의 세계패권을 위협하는 신지정학적 도전인 것이다.

과학기술, 개인정보, 국제규범 등은 지금까지 전통안보와 무관하거나 하위개념으로만 여겨졌다. 이러한 인식은 역사적으로 국가 간 분쟁이 이념, 영토, 또는 석유 같은 자원을 둘러싸고 일어났었다는 점을 감안하면 놀랍지 않다. 그러나 이제는 고도화된 과학기술이 국가전략을 선도하고 정책의 우선순위를 지정한다. 여기에는 정보통신기술 특유의 유연한 스케일이 작용한다. 정보통신기술은 개인의 세세한 삶부터 초국가단위까지 포괄하는 미세성과 광범위성을 통시에 지닌다. 이러한 정보통신기술의 침투력과 확장성으로 인해 국가안보 취약성도 가늠하기 어려울 정도로 그 범위가 확대되었다. 정보전은 미국 정치의 안방까지 깊숙이 침투할 수 있고 프라이버시의 영역으로만 여겨졌던 개인정보는 빅데이터 기술 덕에 석유를 능가하는 경제적 가치를 창출하게 되었다.

이 모든 것이 불과 10년 사이에 확산된 현상이다. 정보통신기술은 경제와 사회를 근본적으로 변화시켰지만 국가 간 패권경쟁의 성격을 바꾸지는 않았다. 하지만 태동하는 4차 산업혁명과 데이터 경제의 방향과 본질을 이해해야 국제규범을 둘러싼 패권경쟁, 빅데이터와 개인정보를 둘러싼 서방진영 내 갈등, 그리고 기술패권을 둘러싼 미중 간의 충돌 등 새롭게 부상하는 갈등전선이 어떠한 지정학적 의미를 갖는지 이해할 수 있다. 사이버공간과 현실공간의 벽이 사라져 가는 오늘날 사이버공간 안팎에서 다차원적으로 발현되는 신지정학적현상을 살펴보고 한국이 나아갈 길을 제시하고자 한다.

패러다임의 전환: 탄소에서 데이터로

탄소경제의 종말

오늘날 세계경제는 석유와 같은 탄소 에너지를 기반으로 하는 탄소 경제(Carbon Economy)에서 정보통신기술 중심인 데이터 경제(Data Economy)로 변화하고 있다. 이러한 경제 패러다임의 전환은 이미 주식시장에서는 뚜렷이 드러나고 있다(표 1). 지난 20여년간의 최대 시가총액 순위 변화를 보면 2004년 시가총액 세계순위 1위 기업은 미국의 복합산업 기업인 제너럴 일렉트릭(GE)이었다. GE는 1892년 창립되어 회사 이름에 걸맞게 전기산업의 성장과 궤를 같이 한 기업이다. 나머지 시가총액 최고기업들은 3위 마이크로소프트와 9위 인텔을 제외하면 금융, 에너지, 제조업 같은 전형적인 20세기 대기업으로 구성되었다. 엑슨(Exxon)과 BP 같은 석유회사와 금융그룹인 AIG와 시티은행, 다국적 제약회사인 화이자(Pfizer), 그리고 거대 유통기업인 월마트가 10대 순위권에 포진해 있었다.

하지만 10년 뒤인 2014년부터는 경제 패러다임의 변화가 주식시장에 반영되기 시작하였다. 2014년에는 전자회사인 애플(Apple)이 시가총액 최고순위 1위을 차지하였다. 하지만 애플이 기존 제조업의 특성을 반영하는 기업이라는 점에서 아주 놀라운 변화는 아니었다. 패러다임 변화를 아주 잘 대표한 변화는 2004년에는 상장도 되지 않았던 인터넷 검색기업인 구글(Google)이 3위에 등극했다는 점이다. 2014년 당시 구글은 상위 10위권 기업 중에서 유일하게 주력 제품이 사이버공간에서 생산되고 소비되는 기업이었다. 애플과 시총 4위인 마이크로소프트(Microsoft)의 제품군은 인터넷이 없어도 사용할 수 반면 구글의 주력제품군인 검색엔진과 동영상은 순수히 네트워크상에서만 이용이 가능하다. 즉, 가상공간에서만 존재하는 서비스와 재화를 생산하는 기업이 시가총액 최고순위 3위까지 오른 것이다.

또다시 5년 뒤인 2019년에는 이 같은 추세가 더욱 뚜렷해졌다. 페이스북(Facebook)과 아마존(Amazon) 등 인터넷 기반 기업들이 최고 순위권에 추가로 진입하였고 반대로 전통적인 시가총액 상위권 기업들이었던 석유 기업들이 10위권 밖으로 밀려났다. 2019년 말 기준[3]으

3. 2020년도에는 석유기업의 쇠퇴라는 명제가 무색하게도 사우디 국영석유회사 아람코(Aramco)사가 상장되면서 애플사와 시가총액 1, 2위를 다투게 됐다. 하지만 아람코를 제외한 나머지 상위 순위는 구글, 페이스북, 아마존 등 데이터를 활용하는 기업들로 여전히 채워져 있다.

로 시가총액 상위 10위권 기업 중 일곱 곳이 IT 관련 기업이며, 이 중 다섯 곳이 인터넷/데이터 산업 관련 기업이었다. 검색으로 유명한 구글 외에도 전자상거래와 클라우드 컴퓨팅을 주력 사업으로 삼는 아마존이 2위, 소셜미디어 업체인 페이스북이 5위, 중국판 아마존이라고 할 수 있는 알리바바가 7위, 그 뒤로 중국 최대 인터넷 기업이자 세계 최대 온라인 게임 회사인 텐센트가 있었다. 이미 주식시장에서는 "데이터는 21세기의 석유"[4]라는 명제가 충실히 반영되고 있는 것이다. 다른 실물경제 분야의 기업들도 IT/인터넷 기업에게 빠르게 밀려나고 있다. 제약회사(화이자, 로슈, 존슨앤드존슨), 제조업(제너럴 일렉트릭), 전통적 금융기관(웰스파고) 등 실물경제 기업들의 퇴장은 석유에너지산업의 쇠퇴와 함께 경제를 움직이는 동력이 에너지와 금융에서 데이터로 빠르게 이동하고 있음을 분명하게 보여준다.

경제 패러다임의 변화는 IT 산업 내부에서도 일어나고 있다. 상위 IT 기업들의 면모를 자세히 살펴보면 기존 IT 산업의 대표주자인 마이크로소프트와 애플도 인터넷 기업들의 영업전략을 따르고 있음을 알 수 있다. 마이크로소프트의 경우 2019년 상업 클라우드 부문이 기존 부문인 PC 컴퓨터와 기업 서비스 부문을 제치고 가장 많은 매출을 올렸다. 전자기기로 유명한 애플의 경우에도 인터넷 서비스 부문이 전체 매출액의 23%를 차지하였다.[5] 온라인 검색을 통한 광고로 수입을 올리는 구글도 클라우드 컴퓨팅 부문 매출이 급성장하고 있다.

이러한 경제 패러다임 전환은 현대 경제가 빅데이터와 인공지능(AI)으로 특징되는 제4차 산업혁명으로 진입하고 있음을 강하게 시사한다. "4차 산업혁명"이라는 표현은 2016년 다보스 포럼에서 처음 공식적으로 언급되었다. 이에 맞춰 UBS 투자은행에서 출간한 4차 산업혁명에 대한 보고서(Baweja, Donovan et al 2016)는 역대 산업혁명을 1차, 2차, 3차, 그리고 현세대의 4차 산업혁명으로 분류하면서 산업혁명의 발전과정은 자동화(automation)와 연결성(connectivity)의 지속적인 강화라고 특징지었다. 이 보고서는 1784년에 시작된 1차 산업혁명은 기계생산과 증기 에너지, 2차 산업혁명(1870)은 대량생산과 전기 에너지,

4. "데이터는 21세기의 석유"라는 표현은 영국 수학자인 Clive Humby가 2006년에 처음 언급한 것으로 알려졌다. https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294#.vjyvcwnp0.
5. Geekwire. Cloud lift: Amazon, Microsoft, Google, Apple and others find a common cushion in the crisis. May 4, 2020. https://www.geekwire.com/2020/cloud-lift-amazon-microsoft-google-apple-others-finding-common-cushion-crisis/.

[표 1] 연도별 시가총액 상위 10개 기업

시가 총액 순위	2004	2009	2014	2019
1	**제너럴 일렉트릭** General Electric 3190억불	**페트로차이나 -중국-** PetroChina 3670억불	**애플** Apple 5600억불	**마이크로소프트** Microsoft 1조 500억불
2	**엑슨** Exxon 2830억불	**엑슨** Exxon 3410억불	**엑슨** Exxon 4320억불	**아마존** Amazon 9430억불
3	**마이크로소프트** Microsoft 2820억불	**중국공상은행 -중국-** ICBC 2570억불-	**알파벳** Alphabet(Google) 3580억불	**애플** Apple 9200억불
4	**화이자** Pfizer 2700억불	**마이크로소프트** Microsoft 2120억불	**마이크로소프트** Microsoft 3440억불	**알파벳** Alphabet(Google) 7780억불
5	**시티은행** Citi 2400억불	**차이나모바일 -중국-** China Mobile 2010억불	**버크셔 해서웨이** Berkshire Hathaway 3210억불	**페이스북** Facebook 5460억불
6	**월마트** Walmart 2400억불	**월마트** Walmart 1890억불	**존슨앤드존슨** Johnson & Johnson 2770억불	**버크셔 해서웨이** Berkshire Hathaway 5070억불
7	**BP -영국-** 1970억불	**중국건설은행 -중국-** China Construction Bank 1820억불	**쉘 -영국/네덜란드-** Shell 2690억불	**알리바바 -중국-** Alibaba 4350억불
8	**AIG** 1890억불	**페트로브라스 -브라질-** PetroBras 1650억불	**제너럴 일렉트릭** General Electric 2630억불	**텐센트 -중국-** Tencent 4310억불
9	**인텔** Intel 1840억불	**존슨앤드존슨** Johnson & Johnson 1570억불	**웰스파고** Wells Fargo 2610억불	**비자** Visa 3790억불
10	**뱅크오브아메리카** Bank of America 1680억불	**쉘 -영국/네덜란드-** Shell 1560억불	**로슈 -스위스-** Roche 2560억불	**존슨앤드존슨** Johnson & Johnson 3760억불

주석:

인터넷/데이터경제 기업 | 기존 IT 기업 | 석유 기업 | 금융 기업 | 기타

출처: visualcapitalist.com, 저자 정리.

그리고 3차 산업혁명(1969)은 전자기기와 IT가 각각 자동화와 연결성을 확장하였다고 설명하였다. 가장 최근 시작된 4차 산업혁명은 인공지능과 빅데이터가 결합하게 되며, 그 확장 가능성은 1차 산업혁명에 견줄 수 있을 것으로 보았다. 궁극적으로는 4차 산업혁명을 통해 사물인터넷(IoT: Internet of Things)와 인공지능이 결합되어 실제와 가상이 통합되고 사물을 제어하는 가상물리시스템이 보편화된 시대가 도래할 것으로 예상되고 있다(이장재 2018).

빅데이터, 인공지능(AI), 클라우드 컴퓨팅

혁명적인 4차 산업혁명의 핵심 자원인 빅데이터란 무엇일까? 빅데이터에 대해선 여러 가지 정의가 있으나 보편적으로는 미 국립표준기술연구소(NIST: National Institute of Standards and Technology)의 것을 들 수 있다. NIST는 빅데이터란 "부피(Volume), 생성 속도(Velocity), 그리고 다양성(Variety) 측면에서 방대하며 저장(Storage), 조작(Manipulation), 그리고 분석(analysis)을 위해선 확장 가능한 설계(Scalable Architecture)가 필요한 데이터"라고 정의하였다(Chang, Grady 2015).

이런 정의에 해당되는 빅데이터는 바로 오늘날 인류가 매초 쏟아내고 있는 엄청난 양의 데이터들이다. 매일 생성되는 엄청난 양의 데이터에는 동영상, SNS 메시지, 블로그 등 개인정보, 인터넷 서비스(예: 위치기반 서비스와 온라인 쇼핑) 사용 중 파생되는 메타데이터(metadata),[6] 그리고 이제는 컴퓨터와 각종 네트워크化된 기기들이 서로 통신하면서 만들어내는 센서(Sensor) 데이터[7] 등 다양한 종류가 포함된다. 전 세계 빅데이터는 빠른 속도로 증가하고 있어 2025년도에는 2019년의 4배가 넘는 데이터가 생성될 것으로 예상되고 있다.[8]

빠르게 생산되고, 다양하며, 방대한 데이터인 빅데이터는 기존 정보처리 방법으로 접근하

6. 메타데이터는 데이터 관련된 정보를 의미한다. 예를 들자면 동영상이나 사진을 찍었을 때 생성되는 위치, 시간, 이미지의 종류 등의 정보가 가장 보편적인 메타데이터의 일종이다.
7. 기기 간 네트워크, 즉 사물인터넷(IoT: Internet of Things)이 생성하는 데이터를 의미한다.
8. Walker, P. AI, digital skills and data growth dominate the analytics agenda in 2020. ITProPortal. https://www.itproportal.com/features/ai-digital-skills-and-data-growth-dominate-the-analytics-agenda-in-2020/.

기가 매우 어렵다. 따라서 새로운 활용 전략에 대한 필요성이 대두된다. 여기에 클라우드 컴퓨팅과 인공지능이 역할을 하게 된다. 클라우드 컴퓨팅(Cloud Computing)은 대규모 저장장치, 메모리, 소프트웨어 등 컴퓨팅 자원을 데이터센터에 집적하여 네트워크를 통해 "가상적이지만 완결된 형태의 서비스로 제공"하는 것을 의미한다(국회입법조사처 2017). 클라우드 컴퓨팅은 분산된 네트워크상에서 병렬처리(Parallel Processing)를 통해 방대한 데이터를 조작하거나 분석할 수 있다.[9] 구글의 검색엔진이 바로 이 기술의 대표적인 응용 사례이다.

클라우드 컴퓨팅을 통해 빅데이터를 저장하고 조작할 수 있다면, 데이터의 가치를 극대화하기 위해서는 여기에 합당한 분석법이 필요하다. 여기에는 인공지능, 즉 AI(Artificial Intelligence)가 필수적이다. 인공지능은 2016년 구글 바둑 인공지능 프로그램 알파고(AlphaGo)와 이세돌 9단 간의 대국으로 국내에 잘 알려져 있다. 다만 이름이 내포하는 것처럼 인공지능은 자칫하면 인간의 지능을 재현하는 기계로 오해되기 쉬우나 반도체로 만들어진 인간형 "지능"이 절대로 아니다. 도리어 인공지능은 컴퓨터의 기계적인 부분에 매우 충실하다고 할 수 있다.

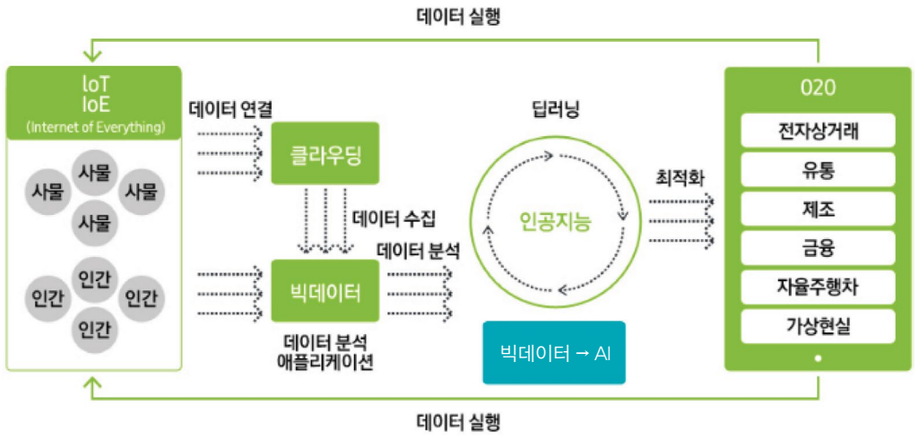
인공지능은 컴퓨터의 빠른 연산속도를 활용해 기계가 스스로 엄청난 양의 정보를 학습하여 미리 제시된 문제를 해결한다. 즉, 인공지능은 기계적 학습에 의존하기 때문에 마치 학생들이 학습량에 따라 성적이 결정되는 것처럼 인공지능의 성능은 기계학습에 투입되는 정보의 양과 비례한다. 이렇게 기계학습에 투입되는 데이터의 양이 커질수록 인공지능은 더 정교해지기 때문에 데이터의 양은 다다익선이다. 또한 인간의 지능만으로는 지금 쏟아져 나오는 빅데이터를 활용할 수 없기 때문에 인공지능의 사용은 필수이다. 결국 인공지능과 빅데이터는 불가분의 관계라고 할 수 있다.

인공지능은 방대한 학습 데이터를 필요했기 때문에 빅데이터 등장하기 이전에는 현실화가 가능한 기술이 아니었다. 하지만 빅데이터의 등장과 함께 다양한 형태로 발전하고 있다. 대표적으로 음성 및 영상 인식을 통한 안면인식과 인간 콜센터원을 흉내내는 챗봇(Chatbot) 서비스, 그리고 자율주행 자동차등에 인공지능 기술이 응용되고 있다. 인공지능을 적용한

9. 한국데이터산업진흥원. 빅데이터 분산 처리 기술의 이해. https://www.kdata.or.kr/info/info_04_view.html?field=&keyword=&type=techreport&page=14&dbnum=184943&mode=detail&type=techreporthttps://brunch.co.kr/@nsung/29.

제품들이 상용화되고 이들을 통해 더 많은 데이터가 수집되면 인공지능은 더욱 개선되는 선순환 구조가 작동한다(김대엽, 김영배 2019).

[표 2] 4차 산업혁명의 작동원리[10]



이러한 빅데이터 학습을 통한 인공지능 개발 → 인공지능이 적용된 환경에서 다시 수집된 데이터는 인공지능을 개선하는 데 쓰인다. 표 2가 보여주는 것처럼 4차 산업혁명의 작동원리는 데이터의 수집, 가공, 분석, 적용이 순차적으로 적용된다. 즉, 1) 인간과 센서가 생성하고 2) 클라우드 컴퓨팅 환경에서 수집된 3) 빅데이터를 자원으로 4) AI가 분석한 결과로 5) 각종 AI 서비스를 생산한다. AI 서비스를 소비하면서 생성되는 데이터는 다시 클라우드 컴퓨팅 환경에서 사용되어 인공지능을 개선하는 사이클을 거치게 된다. 4차 산업혁명의 기초자원인 데이터는 무한대로 재생성되어 인공지능의 잠재력을 극대화할 수 있다.

개인정보의 경제적 활용과 논란

오늘날 가용가능한 빅데이터는 대부분 개인정보에서 파생된다. 개인이 직접 생산하는 정보도 있지만(예: 이메일, 동영상, 사진, 온라인 쇼핑, 인터넷 검색) 위치기반정보, 사진과 동영상의 메타데이터 등 개인의 인지 없이 기기가 수집하는 정보 또한 개인정보의 범주에

10. 삼성 뉴스룸. 4차 산업혁명, 세계 각국과 기업은 어떻게 준비하고 있을까? 2017년 5월 18일. https://news.samsung.com/kr/4차-산업혁명-세계-각국과-기업은-어떻게-준비하고-있.

들어간다. 개인정보는 기본적으로 정보의 채굴, 즉 "정보化" 되었을 때 경제적 가치가 부여되기 때문에 빅데이터/개인정보의 상업적 가치를 창출하기 위해서는 기계학습 등 새로운 분석기법이 필요하다. 인공지능은 절대 정보화가 될 수 없을 것으로 여겨졌던 범주의 개인정보에 대한 정보화를 가능케 하였다. 4차 산업혁명은 빅데이터를 통한 인공지능 개선을 통해 궁극적으로는 인간의 지능까지 대체하려고 한다(장필성 2016).

지난 20년간 인터넷 기업들은 개인정보 활용을 통해 폭발적으로 성장하였다. 아마존, 페이스북, 구글, 인스타그램 등 일반에도 잘 알려진 인터넷 대기업들의 사업모델은 개인정보에 기반하고 있다. 하지만 4차 산업혁명에 필수자원인 개인정보의 산업적 활용은 두 가지 측면에서 논란이 된다. 첫째는 개인정보의 보호와 활용의 균형 문제이다. 개인정보의 무단 활용은 개인의 사생활(프라이버시)를 침해할 여지가 다분하기 때문에 취급이 민감할 수밖에 없다. 그래서 데이터경제가 부상하기 전까지는 개인정보는 인격권 보호차원에서만 논의되었다. 하지만 개인정보의 "정보화"가 가능해지면서 경제적 가치가 부각되고 개인정보를 제3자인 기업이 국가의 통제 아래서 활용하는 것에 대한 논의가 활발한 상태이다(김미리, 권헌영 2017).

실제로 개인정보가 빅데이터로 집적되어 AI로 분석하는 방식으로 사회적 가치를 창출해 낼 수 있다. 예컨대 신용평가 등을 위해 정형화된 정보가 아닌 개인정보를 활용하여 금융 사각지대에 있는 이들이 제도권 금융 접근을 가능케 하는 것이다. 금융위원회 권대영 금융혁신기획단장은 "금융서 데이터라는 것은 평가이자 추천이다. 개인의 금융 거래와 소비 등 경제활동을 하면서 쌓이는 데이터"이라며 "금융데이터에 통신과 위치, 결제 등 비금융데이터를 결합해 제도권 금융을 이용하지 못하는 1천107만 명(씬 파일러)과 소상공인 600만 명이 제대로 평가받고 사회적 전체로 긍정적 효과를 낼 수 있다"고 강조했다.[11]

사실 개인정보를 인격권 차원으로 한정하는 것은 개인정보의 활용을 원천적으로 막는다는 점에서 비판의 여지가 있었다. 대부분의 개인정보 보호법의 취지는 개인의 의사에 반하는 식별을 막는 것이다. 하지만 다채로운 데이터 분석 기법과 고성능의 컴퓨터가 등장하면서 서로 상이한 데이터를 결합하여 개인을 식별하는 게 실제로 가능해지고 있어 개인정보에 대한 통제를 확산하는 것보다는 활용에 더 방점을 두기 위해 개인정보 보호법들이 전 세계

11. ZDNet 코리아. 데이터 3법, 데이터=재산권으로 보는 논의 필요. 2019년 11월 20일. https://zdnet.co.kr/view/?no=20191120084719.

적으로 개정되고 있다. 한국의 "데이터3법"과 유럽연합의 일반데이터보호규정(GDPR)이 개인정보 활용을 위해 개정된 대표적인 개인정보 보호법제이다.

두 번째로 개인정보 활용을 둘러싸고 논란이 되는 부분은 데이터 주권과 이전 부분이다. 데이터의 탈영토성(Un-territoriality)으로 인해 데이터化된 개인정보에 전통적인 주권 개념을 적용하는 것이 어려워졌다(Daskal 2015). 국가 주권이란 기본적으로 영토를 기반으로 하나 국경이 없는 사이버공간에 저장된 개인정보는 무한대로 분할, 이전, 혼합이 가능하며 지리적 구애에서 자유롭다. 데이터 처리자(Controller)가 데이터를 클라우드 컴퓨팅을 통해 전 세계로 분산해 놓을 경우 통제가 사실상 불가능해지는 상황이 구글과 페이스북 같이 수억 명의 사용자를 보유한 초거대 인터넷 기업들이 등장하면서 더욱 두드러지고 있다. 실제로 클라우드 컴퓨팅은 개인정보 저장과 처리를 분리하여 저장은 국내에서 처리는 국외에서 각각 수행될 수 있기에 법률 적용이 더더욱 복잡해지는 측면이 있다(권헌영 2015).

매일 어마어마한 규모의 개인정보 빅데이터가 국외로 이전되고 있고, 이러한 데이터 흐름의 최대 수혜자는 미국의 거대 인터넷 기업들이기 때문에 이들과 상대할 수 있는 주체는 국가가 될 수밖에 없다. 그러나 아직까지 국내에서는 개인정보를 전략자산으로 취급해야 한다는 인식이 부족하다. 한국의 경우 현재 개인의 동의 여부만 충족되면 국내 개인정보의 국외이전이 가능하고,[12] 대부분의 인터넷 사용자가 개인정보의 중요성을 인식하지 못하여 자신의 정보의 해외 이전에 대한 거부감이 없다. 당장 2019년 한 해 동안 성인 인구의 30%가 페이스북을 사용했고 전 국민이 매월 평균 884분의 유튜브(YouTube) 동영상을 시청하나[13] 기술발전의 속도를 따라가지 못해 데이터에 대한 통제를 포기한 상황이다. 새로운 접근법이 필요하지만 국내 개인정보 보호법을 해외 데이터 처리자에게 강제할 경우 역외적용 문제부터 국제무역 위축까지 수많은 문제가 발생할 수 있어 이를 포괄적으로 접근하는 장치에 대한 요구가 커지고 있다(이창범 2016).

이러한 문제들은 데이터의 탈영토성에서 파생되는 문제들이다. 데이터의 중요성은 나날이 높아지고 있지만 관할권, 안보, 산업정책 등의 정책 우선 순위가 혼재되어 각국의 대처 수준은 상이하다. 한국의 경우 빅데이터와 클라우드 컴퓨팅이라는 변화에 대응하기 위해 "데이터3법"을 통과하였지만 해당 법안이 개인정보 보호나 국외이전 제한, 즉 데이터 주권보다는 신산업 육성을 위한 익명화된 개인정보 활용에 더 방점을 두었다는 우려가 강하다.[14] 반대로 미국과 경쟁하는 중국과 유럽연합의 경우 각자 역내 데이터 경제 주도권을 지키기 위해 데이터 보호주의(Data Protectionism)를 추구하는 모습을 보인다. 데이터를 핵심 자원으로 간주하여 잠재적 경쟁국의 접근을 막고, 국가가 만들어준 보호막 아래서 자국의 디지털 생태계를 배양하려 한다. 강대국 간의 경쟁이 사이버공간으로 확산되는, 전형적인 신지정학적 국가 간 갈등을 보여주고 있다.

12. 김현경. [W포럼] '데이터3법'의 통과와 남겨진 숙제들. 아시아경제 2020년 3월 6일. https://www.asiae.co.kr/article/2020030611323058682.
13. 중앙일보. 월간 442억분 보는 유튜브···SNS는 인스타 빼고 사용 줄었다. 2020년 1월 28일. https://news.joins.com/article/23691005.
14. 디지털 데일리. [데이터3법④] 걸음마는 뗐지만··· 데이터3법, 후속 과제는? 2020년 3월 5일. http://m.ddaily.co.kr/m/m_article/?no=192607.

주요국의 개인정보정책

개인정보와 빅데이터의 경제적 중요성에 대한 인식이 높아지면서 사이버공간에 대한 국가의 주권 강화 노력도 강화되고 있다. 현재 미국, 중국, 그리고 유럽연합(EU)은 사이버공간의 안보와 빅데이터에 대해 매우 상이한 접근을 보여준다. 빅데이터, 인공지능, 클라우드 컴퓨팅이라는 4차 산업혁명의 주요 분야에서 절대적인 우위를 가진 미국은 국가 안보 측면을 제외하면 최소한의 개입을 지향한다. 반대로 후발 주자인 중국과 유럽은 자국 데이터 국외이전의 통제라는 방향성에서는 동일하나 방법론에 있어서는 중국은 폐쇄적이며 유럽은 개방적으로 서로 상반된 입장을 취한다.

미국: 데이터 이동의 자유

미국의 경우 인터넷 종주국 답게 사이버공간에 대한 국가 개입을 꺼리는 편이다. 국내총생산에서 데이터 경제와 디지털 무역의 비율이 가장 빠르게 성장하고 있는 미국은 개인정보 보호를 경제적 관점에서 접근하여 국가 개입으로 인해 (자국) 기업 활동이 저해되는 것을 막으려는 성향이 강하다. 그 결과 국가 단위의 개인정보 보호정책이 없으며 기준 또한 주(state)별로 다르다. 예를 들어 가장 강력한 개인정보 보호정책을 펴는 미 국가기관은 연방정부가 아니라 캘리포니아 주정부로 2020년 1월 1일부터 시행된 캘리포니아 소비자 프라이버시 보호법(CCPA: California Consumer Privacy Act)은 2018년 5월부터 시행된 유럽연합의 일반데이터보호규정(GDPR)급의 역외 관할권을 주정부에 부여하여 GDPR과 유사하게 CCPA 규정 위반 시 벌금을 부과할 수 있다.[15]

미국이 주도하는 여러 국제 협약의 개인정보 규범들을 살펴보면 미국은 개인정보 보호보다는 기업 활동을 위한 데이터의 자유로운 이전을 최대한 보장하려 한다는 것을 알 수 있다. 미국이 탈퇴했으나 최종적으로는 재가입할 것으로 예상되는 포괄적-점진적 환태평양동반자 협정(CPTPP: Comprehensive and Progressive Trans-Pacific Partnership)은 원활한 데이터 무역을 위해 데이터 현지화를 금지한다. 아시아-태평양 경제협력체(APEC)의 국경 간 프라이버시 규정(CBPR: Cross-border Privacy Rules)은 회원국 간의 자유로운

15. 강태욱. 캘리포니아 소비자 프라이버시 보호법(CCPA). 법률신문. 2020년 1월 13일. https://m.lawtimes.co.kr/Content/Opinion?serial=158664.

데이터 이전 원칙 아래서 데이터 처리나 기기의 지리학적 제한을 두면 안된다고 명시한다. 기존 북미무역협정(NAFTA)를 대체하는 미멕캐협정(USMCA) 경우 CPTPP의 反데이터 현지화 원칙과 APEC의 CBPR 같은 개인정보보호 내용을 채택하였다(박지영, 김선경 2019).

미국은 일반적으로 시장에는 개입을 꺼려하지만 국가안보와 치안에 있어서는 매우 적극적으로 국가 권한을 행사한다. 이는 개인정보보호 부문에서도 유사하여 미국은 클라우드법(CLOUD Act: Clarifying Lawful Overseas Use of Data Act)을 유럽연합의 GDPR이 발효되기 2달 전인 2018년 3월부터 시행하였다. 이 법안의 중요 특징은 미 정부가 미국에 위치한 기업에게 해외에 위치한 개인정보를 요구하면 이를 정부에 제출하도록 강제한다는 점이다. 즉, 미 정부는 미 IT 기업들이 향유하는 우월한 시장지위를 활용해 자국법의 관할권을 사이버공간 전역으로 확대하였다. 이러한 미국의 정책은 유럽연합의 GDPR 규정이 지향하는 역내/외 구분 없이 유럽시민의 개인정보를 보호하려는 목적과 상충되기 때문에 우방 간의 마찰이 계속되고 있다.[16]

중국: 국가가 통제하는 개인정보

중국의 데이터 주권 개념은 일당독재 체제를 위협할 수 있는 외부 정보 유입과 비판적 정보 확산을 막기 위해 구축한 "방화장성"(Great Firewall of China)의 존재에 기인한 바가 크다. 방화장성은 외부 정보의 유입을 막았을 뿐만 아니라 중국 내 해외 IT 기업들이 중국 당국의 통제를 받도록 하였다. 중국은 개인정보 보호를 국제 규범으로 인정하지 않으며, 외국기업이 자국 시장에 진출하기 위해서는 "데이터 현지화"(Data Localization)를 요구하기 때문에 이에 불응한 페이스북과 구글은 2009년과 2010년에 각각 중국 시장에서 철수하였다.

중국 당국의 이러한 조치는 당시에는 폐쇄적이라는 비판을 받았다. 하지만 구글과 페이스북이 중국 시장에서 철수하면서 역설적으로 중국은 자국 기업 중심의 빅데이터 산업 생태계를 구축할 수 있게 되었다. 바이두, 텐센트, 알리바바 등 중국기업은 중국의 13억 인구

16. Irish Times. Wilbur Ross warns Schrems II ruling could have 'severe consequences' for EU-US trade. Nov 3, 2020. https://www.irishtimes.com/business/economy/wilbur-ross-warns-schrems-ii-ruling-could-have-severe-consequences-for-eu-us-trade-1.4399039.

[표 3] 미-중-EU 데이터 정책 특징

	미국	중국	유럽연합
정책 방향	자유시장	국가통제	상호 적정성
개인정보/데이터 국외 저장 및 처리	가능	불가능(정부 허가 있을 시 예외)	적정성 결정 통과 시 가능
국내법 역외적용	미 기업이 데이터를 관리하며 치안/국가안보 관련 경우 가능	불투명	가능(GDPR 규정 위반 시 벌금)
데이터 현지화	불필요	필수("핵심정보기반시설사업자 및 네트워크 사업자"에게 해당)	불필요
사법기관의 국외 개인정보 접근	미 기업이 저장/처리하는 데이터이며 치안/국가안보 관련 경우 가능	불가능	해당 없음. 치안과 국가안보 관련 사항에는 GDPR이 적용되지 않음

시장에서 구글, 페이스북, 아마존을 각각 대체하였고, 10년이 지난 현재는 원조 미국 기업들을 따라잡는 수준으로 성장하였다. 현재 중국 "카피" 기업들의 시가총액은 미국 "원조" 기업의 턱밑까지 따라온 상태다(표 1). 중국 정부의 폐쇄적인 정책 덕분에 시장에서 독점적 지위를 누릴 수 있게 된 중국 인터넷 기업들은 당국의 강력한 인터넷 검열 정책에 협조적이며[17] 공산당 지도부를 정책적으로 보좌한다.[18] 다만 이러한 중국 기업들과 정부의 밀착은 부메랑이 되어 최근 미국이 중국 인터넷 기업들을 제재하는 근거가 되었다.

17. Bloomberg. China Protectionism Creates Tech Billionaires Who Protect Xi. 7 March 2018. https://www.bloomberg.com/news/articles/2018-03-06/how-china-protectionism-creates-tech-billionaires-who-protect-xi.
18. South China Morning Post. Tech entrepreneurs replace real estate tycoons as political advisers in China's push for IT edge. 4 March 2018. https://www.scmp.com/business/companies/article/2135642/tech-entrepreneurs-replace-real-estate-tycoons-political-advisers.

개인정보 보호에 있어서 중국은 매우 보수적으로 접근한다. 중국은 자국민 개인정보에 관해서 폐쇄적인 데이터 운영정책을 적용하고 중국 내 데이터의 국외이전을 사실상 불허한다. 2017년 6월에 발효된 "사이버보안법"은 이러한 정책적 방향을 더욱 확고히 하였다. 이 법에 따르면 중국 내 IT 기반시설 운영자는 국내에서 수집한 개인정보 및 중요데이터를 국내에 저장하는 것뿐만 아니라 처리도 해야 하는 의무가 있으며, 개인정보 등의 국외이전은 정부의 평가와 승인이 있어야만 가능하다. 즉, 중국은 해외기업이라도 데이터 서버가 자국 내에 위치해야 하는 "데이터 현지화" 정책을 실시한다. 특히 국가안보에 방점을 두었기 때문에 데이터를 관리하는 주체는 중국 정부가 요구할 경우 암호화된 정보를 해제해야 한다. 중국의 개인정보보호법은 국가의 권력 남용 위험에 노출되어 있어 명목상 취지인 개인정보 보호가 아니라 데이터 현지화와 정부 사찰을 용이케 하는 것이 사실상 목적이라는 비판을 받는다.[19]

중국의 데이터 정책은 경제적으로도 한계가 있다. 중국은 보호주의적 정책을 통해 자국만의 디지털 생태계를 형성하는 것은 성공했지만 동시에 확장성도 포기하였다. 표 3은 중국 당국이 데이터의 해외 반출을 금지하고 주요 기업들의 데이터 현지화를 강제하고 있음을 보여준다. 하지만 이러한 보호정책 때문에 중국 기업들의 자유로운 데이터 이동에도 제한이 생기게 되었다. 사이버안보법의 관할권은 중국으로 국한되나 자국의 안보가 위협받을 경우 국외에서도 적용될 가능성을 열어 놓는 등 불투명한 부분이 있다.[20]

유럽연합: 개인정보를 보호하는 데이터 무역

역사적으로 유럽연합은 개방적인 사이버 정책을 시행했다. 유럽은 사이버공간을 경제적 가치보다는 보편적 표현과 정보의 자유의 관점에서 접근하였다. 그러나 이러한 정책적 방임으로 인해 유럽 사이버공간은 미국의 기술적·경제적 영향권에 거의 종속된 상태이다. 세계 20대 인터넷 기업 중에서 유럽 기업은 전무하며, 그 결과 유럽시민들의 개인정보 대부분을 구글과 페이스북이 소유하고 있다. AI와 클라우드 컴퓨팅 등 빅데이터 기반 4차 산업혁

19. Dickinson, S. China Cybersecurity: No Place to Hide. China Law Blog. October 11, 2020. https://www.chinalawblog.com/2020/10/china-cybersecurity-no-place-to-hide.html.
20. Linklaters. Data Protected - People's Republic of China. Last updated March 20, 2020. https://www.linklaters.com/en/insights/data-protected/data-protected---prc#:~:text=There%20is%20currently%20no%20comprehensive,of%20the%20National%20People%27s%20Congress.

명 분야에서 유럽의 존재감은 미미하다.

유럽연합은 사이버공간에서 유럽이 주도권을 되찾기 위해 보호주의적 정책이 절실함을 인지하고 있다. 우르줄라 폰데라이엔(Ursula von der Leyen) EU 집행위원장은 향후 5년간 EU 유럽집행위원회(EU Commission)의 중요 지침으로 유럽의 첨단기술 분야에서의 자주성 확보를 내세웠고,[21] 인공지능, 암호화폐, 양자컴퓨터 등에서 "디지털 주권을 회복"해야 한다고 역설하였다. 같은 맥락에서 독일 앙겔라 메르켈(Angela Merkel) 총리는 유럽연합이 더욱 적극적으로 역내 기업들을 지원해야 하고, 특히 첨단기술 분야에서 미국과 중국의 기업들과 경쟁하기 위해 유럽 스스로 전기차 배터리와 반도체를 생산해야 한다고 주장하였다.[22]

산업정책적 배경 외에도 유럽연합이 강력한 개인정보보호 정책을 추진하게 된 또 다른 요인은 2013년 전직 미 정보분석가인 에드워드 스노든(Edward Snowden)에 의한 미 국가안보국 기밀문서 폭로였다. 이를 통해 미 정보기관들이 독일 메르켈 총리를 포함해 다수의 유럽 지도자들을 수년간 감청했다는 사실이 드러났고, 이는 유럽 정부와 시민사회에 엄청난 충격을 주었다. 이 사건으로 인해 유럽시민의 개인정보를 보호하고 타국으로의 이전을 막자는 여론에 더욱 힘이 실리게 되었고, 유럽의회(European Parliament)가 더 강력한 개인정보보호 법안을 추진하게 되는 중요한 계기가 되었다(Coyne 2019).

개인정보에 대한 유럽연합의 데이터 보호주의 전략은 유럽 내 개인정보에 대한 통제를 강화하는 동시에 데이터 경제와 디지털 무역에 대한 활성화를 대비하는 모습을 보인다. 유럽연합의 디지털 전략의 산물이 바로 2018년 발효된 "일반데이터보호규정"(GDPR)이다. 사이버공간에서 유럽시민의 개인정보를 보호하기 위해 입안된 GDPR은 해킹 등 불법적 행위보다는 개인정보의 역외이전에 초점을 맞춘 법안이며, 특히 법안의 관할권을 정보의 위치에 국한시키지 않고 정보주체, 즉 유럽연합 시민과 거주자로 정의한다. 따라서 유럽연합 밖에 사업체가 위치하더라도 유럽시민과 거주자의 개인정보를 취급하면 유럽연합의 GDPR이 적용된다고 봐야 한다.

21. "Political Guidelines for the Next European Commission 2019-2024" https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.
22. "Angela Merkel warns EU: 'Brexit is a wake up call'" Financial Times, 16 Jan 2020. https://www.ft.com/content/a6785028-35f1-11ea-a6d3-9a26f8c3cba4.

만약 역외 기업이 GDPR 규정을 준수하지 않을 경우 연 매출액의 4% 또는 최대 2천만 유로의 벌금이 부과되는 강력한 처벌 조항도 포함되어 있다. 이는 일종의 자국법의 역외적용으로 보일 수 있는 행태이며, 미국이 흔히 사용하는 "세컨더리 보이콧"과 유사하다. 미국의 제재조치들을 역외 관할권 남용이라고 비판하던 유럽이 유사한 행태를 보인다는 점은 역설적이라고 할 수 있다. GDPR 탄생 배경에는 안보적 목적과 역외 기업들의 유럽시민 개인정보 사용을 통제하여 미국의 이른바 "FAANG"[23]이라고 약칭되는 글로벌 IT 공룡기업들을 견제하며 유럽의 IT 기업 경쟁력을 제고하는 목적도 있다.

하지만 데이터의 역외이전을 기본적으로 막고 있는 중국과는 달리 유럽연합의 경우 제3국이 GDPR 수준의 개인정보보호 조치를 갖췄다고 평가되면 적정성 결정(Adequacy Decision)[24]을 통해 추가적인 조치 없이 데이터의 자유로운 역외이전을 허용한다. 이는 데이터 경제와 국제 디지털 무역의 성장을 촉진하되 동시에 유럽의 주권을 보존하고 개인보호 규범을 전 세계로 확산하려는 정책의 일환이다. 개방적인 적정성 결정은 다음과 같은 기준을 충족할 경우 가능하다(김현경 이경준 2019).

- 개인정보보호 관련 직·간접적 제도와 개인정보의 제3국 이전 관련 제도의 존재:
  -법치주의, 인권, 기본권 보장 등 보편적 가치를 유럽연합과 공유
  -정보주체의 개인정보 보호권리에 대한 보장수단과 권리 침해 시 구제수단이 있음
- 개인정보보호를 관할하는 적절한 집행력을 가진 독립적인 감독기관의 존재
- 개인정보보호 관련 국제협약, 법적 구속력 있는 조약 가입, 다자간/지역 기구 참여

일단 GDPR은 유럽연합 회원국과 유럽경제지역(European Economic Area) 회원국에 바로 적용되었고 추가적으로 미국,[25] 캐나다, 아르헨티나, 안도라, 이스라엘, 일본, 우루과이, 뉴질랜드, 스위스 등이 유럽연합과 적정성 협약을 체결하여 EU 회원국들과의 자유로운 데

23. Facebook - Apple - Amazon - Netflix - Google.
24. Article 45 of EU Regulation 2016/679.
25. 미국과 유럽은 적정성 결정과 유사한 Privacy Shield 협정을 체결해 기업의 미-유럽 간 데이터 이전을 허용하였다. 하지만 2020년 7월 유럽연합법원(European Court of Justice)은 이 협정이 유럽시민의 개인정보를 충분히 보호하지 않는다고 결정하고 Privacy Shield 협약을 무효화하였다. 이에 따라 미국 기업은 대신 유럽연합이 개별적으로 승인해야 하는 표준계약조항(Standard Contractual Clause)을 통해서만 데이터를 이전할 수 있게 된다. 이는 기업에게 추가적인 시간과 비용을 의미한다.

이터 이동이 가능하게 되었다. 유럽연합의 GDPR은 한국이 데이터3법을 개정하는 데도 영향을 주었다. 한국 기업의 유럽 시장 진출을 위해서는 유럽연합의 적정성 결정을 받는 것이 필요하나 2020년 8월 현재 아직 통과되지 않은 상태이다. 적정성 결정이 늦춰지는 중요한 이유는 "적절한 집행력을 가진 독립적인 감독기관"에 대한 유럽연합의 의구심 때문이다(이양복 2020). 이를 개선하기 위해 개인정보보호위원회는 중앙 행정기관으로 격상되고 행정안전부, 방송통신위원회, 금융위원회 등 3개 부처에 나뉘어 있던 개인정보 관리·감독 업무를 통합 관리하게 되었다.

적정성 결정 조건은 유럽연합이 추구하는 외교안보전략의 특성을 잘 보여준다고 할 수 있다. 특히 법치주의와 인권을 중요시하며 국제협약 및 다자간 기구 참여가 적정성 협약의 중요 조건이라는 점은 국제법과 다자간 외교를 바탕으로 하는 국제관계를 중심으로 하는 유럽연합의 글로벌 전략을 잘 보여준다.[26] 뒤집어 말하면 유럽연합은 고유의 규범과 가치를 유럽 디지털 시장으로의 접근을 원하는 국가들이 수용하도록 GDPR을 통해 유도하고 있다. 즉, 시장지배력에 기반한 "소프트파워"로도 볼 수 있다. 유럽연합의 GDPR은 개인정보와 빅데이터를 둘러싼 강대국 간 경쟁이 어떻게 신지정학의 전선을 구성하는지 잘 보여주는 사례이다.

중국과 유럽연합: 디지털 주권의 등장

유럽연합과 중국이 추구하는 사이버 전략은 미국이 주도하고 개방적인 사이버공간의 시대가 종말을 고하고 있다는 것을 시사한다. 유럽연합은 전통적으로 사이버공간에서 주권을 강조하던 중국과 러시아에 비해 국가의 개입을 최소화하고 대신 자율적 규제와 사용자의 권리 보호에 더 비중을 두었다. 하지만 개인정보의 경제적 가치가 부각되고 국가 간의 기술경쟁이 첨예해지면서 개인정보 보호와 산업발전 사이의 균형을 추구한다.

미국은 전반적으로 특정 개인정보(개인 진료정보와 금융정보)를 제외하면 개인정보와 데이터 이전에 대해서 상당히 시장친화적으로 접근한다. 반대로 중국과 유럽은 일당독재주의와 자유민주주의라는 서로 상이한 정치체제를 가지나 4차 산업혁명의 전략적인 중요성과 여기에 투입되는 개인정보의 역외이전에 대해 경계하는 인식은 유사하다. 거대 인터넷

26. European External Action Service. A Global Strategy for the European Union. 18 October 2018. https://eeas.europa.eu/topics/eu-global-strategy/49323_en.

기업을 보유한 미국이 데이터의 자유로운 이동을 추구한다면 중국과 유럽은 데이터에 "주권" 개념을 적용하여 자국 내 데이터의 역외이전을 제한한다. 일종의 비관세장벽으로서 무역 보호주의를 통해 자국 시장을 보호하고 선두 국가를 추격하는 것은 아이러니하게도 미국이 취했던 경제발전 전략이기도 하다(Chang 2002).

유럽연합과 중국의 데이터 국외이전 제한은 "데이터 보호주의"라는 개념에서는 유사하지만 실제 정책면에서는 상이하다. 유럽연합이 국가 간 합의 아래 데이터의 상호호혜적 "데이터 자유무역"을 표방한다면 중국은 일방적으로 자국 데이터의 국외이전을 차단하고 내부적으로는 완전히 통제할 수 있는 "데이터 블록"을 지향한다(박지영, 김선경 2019). 이러한 개념적 차이는 실질적 정책 차이로 이어진다. 중국의 데이터 정책이 데이터의 국외이전을 사실상 불허하는 폐쇄적인 정책이라면, 유럽연합의 개인정보보호 정책은 개인정보 보호, 자국 데이터 산업 보호, 그리고 데이터 이동의 자유라는 세 마리 토끼를 잡았다고 볼 수 있다.

미래 성장동력을 위한 전략자원인 개인정보를 둘러싸고 강대국 간의 데이터 보호주의가 확산되고 있으며, 여기에는 미국의 우방인 유럽연합도 동참하고 있다. 유럽연합은 데이터 보호주의를 "디지털 주권"이라는 개념으로 향상시켰고[27] 이는 미국의 사이버공간에 대한 국가개입을 반대하는 입장과 대비된다. 유럽의 디지털 주권은 단순히 4차 산업혁명의 주도권 확보 차원뿐만 아니라 사이버 안보와 이념 차원에서도 작동한다는 점에서 중국과 러시아가 주장하는 "사이버 주권"과 일맥상통하는 부분이 있다. 중국과 러시아는 서방세계의 탈국가적 인터넷 거버넌스 규범을 국가주권 중심의 규범으로 대체하기 위해 꾸준히 노력해 왔다. 미국의 거대 인터넷 기업에 대항할 수 있는 주체가 국가밖에 없다는 점에서 "주권" 개념은 진지하게 고려되어 한다. 하지만 국가주권은 개방되고 자유로운 사이버공간 개념과 상충하며 최악의 경우 사이버공간의 파편화로 이어질 수 있다. 최근 파행하고 있는 국제사회의 사이버 국제규범 논의를 보면 이러한 우려가 기우가 아님을 알 수 있다.

27. European Parliament Think Tank. Digital sovereignty for Europe. July 2, 2020. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651992.

사이버공간의 이념 갈등

사이버공간의 불안정성: 강대국 간의 갈등

인터넷으로 대표되는 사이버공간은 일반적으로 국가 통제에서 자유로운 것으로 인식된다. 30여년간 인터넷[28]이 보여준 놀라운 발전의 이면에는 학계 및 기업, 그리고 개인들의 혁신과 노력이 있었다. 성향상 이들은 중앙 중심적 통제보다는 행위자 간의 자발적인 협치(governance)를 선호하였고 인터넷 자체가 분산된 네트워크라는 속성을 가지고 있기 때문에 통제의 분산화 또한 개방적인 사이버공간의 특성을 잘 나타냈다. 여기에 인터넷의 실질적 종주국이라고 할 수 있는 미국은 정보의 자유로운 이동을 선호하였기 때문에 국가 불간섭 원칙이 오늘날 인터넷 거버넌스에 대거 반영되었다. 미국과 유럽연합이 추구하는 "자유롭고, 개방되고, 안전한" 사이버공간 개념이 이를 잘 대변한다.[29]

그러나 정보의 디지털화가 가속되고 정보산업의 경제적 비중도 커지면서 사이버공간에 대한 국가의 개입도 따라 늘어났다. 특히 인터넷의 구조적 취약성 때문에 창궐한 사이버 범죄 문제 때문에 국가가 주도하는 사이버 보안대책의 필요성이 대두되었고, 중국과 러시아 등 권위주의 국가들은 인터넷으로 인한 체제 위협과 사회통제능력 상실에 대한 불안감 때문에 사이버공간에 대한 통제와 검열을 강화하였다. 이러한 국가의 개입은 수치로도 드러난다. 미국 싱크탱크인 프리덤 하우스(Freedom House)가 2018년 발표한 "네트워크상의 자유"(Freedom on the Net) 보고서에 따르면 사이버공간에서의 정보의 자유는 지속적으로 악화일로를 걷고 있으며 특히 이러한 추세는 중국과 러시아 등 권위주의 국가에서 더욱 두드러진다.

28. 인터넷(Internet)은 1965년 미 국방부 ARPA가 스탠포드 대학과 캘리포니아 주립대학교-로스앤젤레스(UCLA) 사이를 연결한 첫 컴퓨터 연결망인 ARPANet(아파넷)를 기반으로 한다. 이후 90년대 영국 출신 과학자인 Berniers-Lee가 하이퍼텍스트(Hyper-text)를 개발함으로써 현재 우리에게 익숙한 인터넷이 만들어졌다.
29. 미 정부의 2018년 사이버 국가전략(National Cyber Strategy of the United States) 보고서와 유럽연합의 2013년 사이버 안보 전략(Cybersecurity Strategy of the European Union)은 자유롭고 안정되고 개방적인 인터넷을 핵심 개념으로 삼았다. 즉, 사이버공간에 대한 국가 개입을 최소화하고 자유민주주의적 가치인 정보와 표현의 자유를 보호하는 것이 목적이다.

사이버공간에 국가 간 갈등이 심해지는 원인에는 사이버공간의 구조적 익명성과 개방성에 있다. 오늘날 인터넷은 공통의 통신표준과 프로토콜인 TCP/IP를 가지면 연결이 가능하나 네트워크를 구성하는 인터넷 IP주소가 간단한 숫자로 구성되어 있어 쉽게 위조가 가능하여 외부의 침투에 취약하다(신영웅 2017). 이러한 사이버공간의 구조적 익명성은 공격자에게 유리한 전략적 환경을 조성한다. 익명성은 사이버 공격의 은닉성을 강화하며 이는 공격의 귀속 확인을 어렵게 한다. 즉, 사이버공간은 구조적으로 공격자에게 유리한 비대칭적 공간인 것이다.

비대칭성과 함께 사이버 공격이 선호되는 또 다른 이유는 인명피해가 없는 저강도 사이버 공격에 대한 국가 간 해결 메커니즘이 전무하다는 사실이다. 이는 특정 국가가 사이버 공격의 배후라는 것을 증명하더라도 실질적인 군사적 반격을 불가능케 하는 부작용을 낳고, 그 결과 사이버 공격에 대한 대응은 규탄이나 제재 정도에 머무르게 된다(김소정, 김규동 2017). 사이버 공격은 피해자 측에서 강력한 대응을 할 가능성이 낮기 때문에 공격이 실패하거나 발각되더라도 후환이 적다.

국경 없는 영역이었던 사이버공간이 점차 분쟁영역화 되는 현상은 최근 대두되는 사이버 주권 개념과 맞물려 있다. 2011년 중국, 러시아, 타지키스탄, 그리고 우즈베키스탄은 유엔에 공식 서한을 보내는 형태로 사이버공간상의 국가 권리와 책임을 강조하고, 동시에 사이버 영역에 대한 국가 간 상호불간섭을 공식적으로 언급하였다.[30] 중국과 러시아를 위시한 권위주의 국가들은 사이버공간을 소통과 경제 활동의 영역보다는 안보적 관점에 바라보는 경향이 강하며, 서방세계가 인터넷 "정보전"을 통해 체제 전복을 도모한다는 의심을 공유한다. 따라서 미국 주도의 인터넷 환경에서 국가가 온전히 통제하는, 즉 사이버 주권을 행사하는 독자적인 영역을 확보하려는 것이다. 이들 국가들의 사이버공간에서 주권 확보 노력은 외부정보의 차단이라는 방어적 정책과 사이버공간 전반에 대한 공세적인 전략으로 나뉘어 발현된다.

사이버공간에서 대해 상당히 방어적인 정책을 운영하는 중국은 인터넷의 초창기인 1998년부터 해외 인터넷 사용을 검열하는 정책을 실시할 정도로 서방세계의 신기술을 불신하

30. NATO CCDCOE. An Updated Draft of the Code of Conduct Distributed in the United Nations - What's New? https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/.

였다.[31] 중국과 러시아의 국내와 외부 인터넷 환경을 분리하는 정책은 성공할 것으로 보인다.[32] 특히 중국은 검열과 필터링이 조합된 방호벽을 구축하면서 동시에 페이스북과 트위터는 웨이보(Weibo), 위챗(WeChat) 및 큐큐(QQ), 유튜브는 요우쿠(Youku) 등 해외 인기 웹서비스의 대체재를 제공하는 방식으로 자국민이 해외 인터넷에 접속하지 않고 유사한 서비스를 즐길 수 있도록 하였다. 중국 당국은 방화장성(The Great Firewall) 바탕의 인터넷 검열 정책에 유화책을 겸비하는 방식으로 통제정책에 대한 사회적 불만을 상쇄하는데 성공한 것으로 평가받는다(김진용 2017).

중국과 러시아는 자국 인터넷을 해외망과 물리적으로 단절하는 것이 아닌 중국식 검열과 필터링이 조합된 방호벽을 구축하거나 러시아처럼 자체 도메인 서버를 구축해 러시아 내 인터넷 트래픽이 외부로 이동하지 않고 자국 내 머물도록 하는 방법을 모색하고 있다.[33] 중국처럼 국내 대체재에 기댈 수 없는 러시아는 국내 인터넷과 외부 인터넷망을 유사시에 분리할 수 있는 자체 도메인(Domain) 서버 정책을 추진하고 있다. 여기에는 RuNet이라고 불리는 자체 도메인 서버를 사용하는 내부망, 즉 인터넷이 아닌 인트라넷(Intranet)이 사용된다.[34] 도메인 서버란 웹 브라우저 주소창에 입력되는 .com, .org, .edu 등으로 끝나는 인터넷 주소로 방문자를 연결해 주는 역할을 하며, 전 세계 인터넷 도메인은 지금까지 미국 기관인 국제인터넷주소관리기구(ICANN: Internet Corporation for Assigned Names and Numbers)가 관리하였다. ICANN은 1998년에 설립된 미 정부의 감독을 받는 준 국가기관이었다가 미 정부의 지나친 영향력을 우려한 국제사회의 여론이 커지면서 2016년에야 비로소 미 정부에서 독립하였다. 러시아 입장에서 볼 때 인터넷 주소를 관리하는 도메인 서버를 자국 내에 묶어 두면 유사시 외부 인터넷을 차단하더라도 국내 인터넷은 부분적이라도 사용할 수 있게 된다.

내부적으로는 국내외 인터넷 환경을 분리하는 방어전략을 수행하는 중국과 러시아는 반대

31. Hong Kong Free Press. The evolution of China's Great Firewall: 21 years of censorship. September 3 2017. https://hongkongfp.com/2017/09/03/evolution-chinas-great-firewall-21-years-censorship/.
32. BBC. The global internet is disintegrating. What comes next?. 2019년 5월 15일. https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.
33. 조선일보. 푸틴, '러시아 독자 인터넷망' 법안 서명…인터넷 검열 강화되나. 2019년 5월 2일. https://news.chosun.com/site/data/html_dir/2019/05/02/2019050203233.html.
34. TechCrunch.com. Russia starts testing its own internal internet. December 27, 2019. https://techcrunch.com/2019/12/26/russia-starts-testing-its-own-internal-internet/.

로 서방권에 대해서는 공세적인 자세를 취한다. 2018년 미 백악관이 발표한 "국가 사이버 전략"(National Cyber Strategy)은 중국과 러시아가 각각 사이버공간에서 불안을 조성하고 불법적 경제 이익을 추구한다고 성토하였다. 트럼프 행정부는 미국의 인터넷 종주국 역할이 "개방된 인터넷의 수혜자지만 동시에 자국민들의 인터넷 접근은 제한하며, 국제포럼에서 적극적으로 인터넷의 개방성 원칙을 저해하는" 국가들의 도전을 받는다고 주장하였다. 주 원인제공자로는 "무모한 사이버 공격"을 자행하는 러시아, 이란, 북한, 그리고 "사이버 산업스파이 활동을 하고 수조 달러의 지적재산권을 탈취하는" 중국을 지목하였다(White House 2018). 비록 미 정부의 관점이지만 중국과 러시아의 사이버 전략을 간략하게 잘 요약하였다고 볼 수 있다.

분쟁영역이 된 사이버공간: APT와 정보전

중국과 러시아를 중심으로 권위주의 국가들은 사이버공간을 체제 위협의 원천이기도 하지만 동시에 상대방에 대한 비대칭적 전술을 구사할 수 있는 전략적 영역으로 간주한다. 사이버 상의 국가 간 충돌은 수치상으로도 나타난다. 미 전략국제문제연구소(CSIS)에서 전 세계에서 보고되는 국가기관, 방산업체, 첨단기술 기업 및 미화 1백만불 이상 피해를 입힌 사이버 사건들을 취합해 만드는 "중대 사이버 사건"(Significant Cyber Incidents)[35] 데이터베이스에 의하면 심각한 사이버 공격은 2016-2017년을 기점으로 그 빈도가 빠르게 늘어나는 추세를 보인다(표 4).

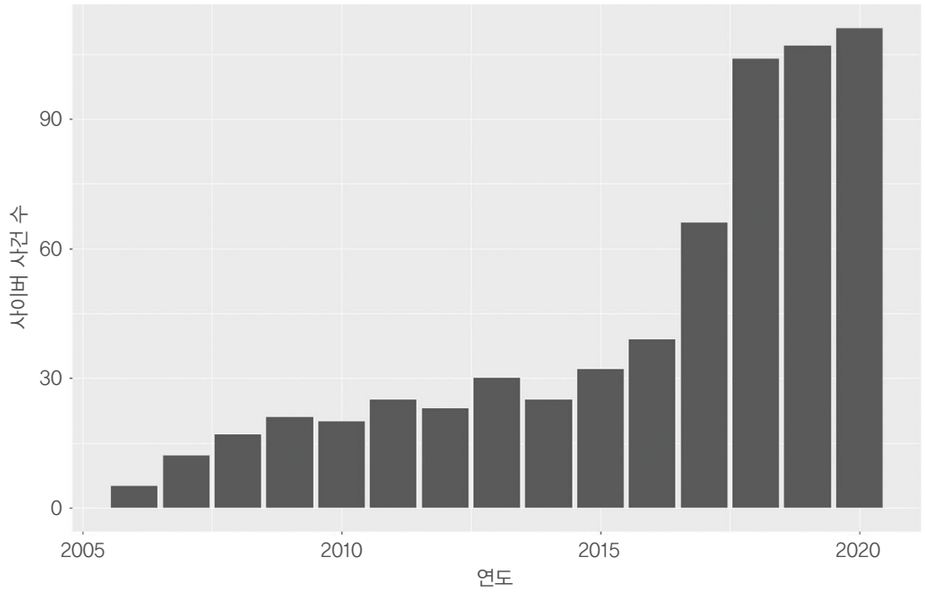
심각한 사이버 공격은 주로 핵심 기술을 탈취하거나 핵심 인프라를 공격할 때 나타난다. 사이버 보안체제가 잘 구축된 국가기관 및 대기업에 대한 사이버 공격은 일개 범죄단체나 개인이 자행하기에는 상당히 고도화된 기술과 최소 수 개월에서 수 년의 기간의 준비 기간이 필요하다. 이 정도의 기술력과 계획능력을 갖출 수 있는 공격조직은 고차원의 기술력을 필요로 하기 때문에 국가 차원의 지원이 필요한 경우가 대부분이다. 심각한 사이버 공격은 사실상 "국가지원 사이버 공격"(State-sponsored cyber-attacks)으로 간주해야 한다.

국가지원 사이버 공격을 자행하는 공격집단은 일반적으로 "지능적 지속적 위협"(APT: Advanced Persistent Threat)이라고 불린다. 분류체계에 따라 다르지만[36] 일반적으로 중

35. Center for Strategic and International Studies. Significant Cyber Incidents. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

국, 러시아, 북한, 이란 등이 이들 APT 배후[37]에 있는 것으로 추정된다(이민호, 박창욱 외 2020). 아직까지 86%의 사이버 공격은 개인이나 범죄집단에 의해 영리목적으로 자행되고 있으나 APT 집단의 활동이 늘어나면서 사이버 공격의 유형 또한 영리 목적보다는 정보 취득 및 유무형의 자산 파괴가 목적인 경우가 많아지고 있다(Verizon 2020).

[표 4] CSIS 중대 사이버 사건 연도별 추이



출처: CSIS "중대 사이버 사건"(Significant Cyber Incidents) 데이터베이스. 저자 재구성.

중국의 경우 APT가 사이버 공격을 실행하는 주체인 것으로 추정된다. 현재까지 알려진 APT 집단 중에서 국가기관과의 관계가 가장 명확하게 드러난 APT1은 중국의 인민해방군 소속인 "제61398부대"일 정도로 APT는 중국 사이버 전력의 핵심이라고 할 수 있다.[38]

36. 특정 APT의 배후국가를 100% 증명하는 것은 매우 어려운 일이기 때문에 IT 보안전문업체들은 APT의 공격 전술과 기술의 특정 패턴을 구별해 내는 자신들만의 고유 노하우를 사용한다. 그 결과 업체에 따라 APT의 분류가 달라질 수 있다.
37. 권위있는 사이버보안 업체인 미 FireEye사는 APT와 배후국가를 다음과 같이 분류한다: APT 1/3/10/12/16/17/18/19/30/40/41(중국); APT 28/29(러시아); APT 32(베트남); APT 33/34/39(이란); APT 37/38(북한).

미 군사연구기관 MITRE의 분류에 따르면 2020년 7월 현재 전체 식별된 117개의 APT 집단 중에서 최소한 30개가 중국과 관련되어 있다.[39] 중국 APT는 주로 미국의 연구기관, 우주항공산업 및 기타 첨단기업을 표적으로 삼아 이들이 소유한 상업 비밀과 지적재산권을 탈취한다.[40]

미국과 러시아는 군사적 목적으로 타국에 대한 사이버 공격을 감행한다. 러시아의 경우 2007년 에스토니아와의 외교적 마찰 중 에스토니아 전산망에 대한 대규모 디도스(DDOS) 공격을 감행하여 기간시설인 통신 인프라를 마비시켰고, 2008년 그루지야 공화국과 분쟁에서 재래식 공격과 사이버 공격을 병행하는 등 사이버 공격이 현대 군사 교리의 범주에 포함하게 되는 데 일조하였다. 미국은 이스라엘과 공조하여 2010년 스턱스넷(Stuxnet)이라는 컴퓨터 바이러스를 이용해 이란 나탄즈(Natanz)에 위치한 우라늄 농축시설 제어시스템을 공격하였으며(신경수, 신진 2018), 이는 악성코드가 무기화된 첫 사례라고 할 수 있다.[41] "올림픽 작전"(Operation Olympic Games)이라고 명명된 이 작전은 후에 미 오바마 대통령이 직접 지시했던 것으로 밝혀졌다(Sanger 2012). 북한도 국가 차원에서 타 국가를 공격한다. 북한 APT인 라자루스(Lazarus)그룹은 2014년 소니 픽처스(Sony Pictures)와 2016년 방글라데시 중앙은행을 해킹하였고, 또 다른 북한 APT 그룹인 김수키(Kimsuky) 경우 2014년 한수원 해킹의 배후로 지목되었다.[42] 미 오바마 행정부는 소니 픽처스 해킹 사건을 북한의 국가 차원 공격으로 규정하고 북한에 대한 제재조치를 취하기도 했다.[43]

중국이 APT를 통한 핵심정보와 데이터 탈취에 집중한다면 러시아는 사이버공간의 구조적 비대칭성을 활용하는 "회색지대전략"(Gray Zone Strategy)을 적극적으로 구사한다.

38. 보안뉴스. 사이버 전쟁을 주도하는 국가정보기관: 중국. 2020년 3월 23일 https://www.boannews.com/media/view.asp?idx=87114.
39. MITRE- Groups https://attack.mitre.org/groups/.
40. The Register. China cuffs hackers at US request to stave off sanctions. 9 Oct 2015. https://www.theregister.com/2015/10/09/china_cuffs_hackers_at_us_request/.
41. 안철수연구소 보안 이슈. 악성코드의 새로운 패러다임, Stuxnet. 2010년10월19일. https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=16852.
42. 중앙일보. '한수원 유출' 북한 해커조직 소행…'코드 네임 kimsuky(김수키)' 헉. 2015년 3월 17일. https://news.joins.com/article/17375096.
43. The Wall Street Journal. U.S. Targets North Korea in Retaliation for Sony Hack. Jan 3, 2015. https://www.wsj.com/articles/u-s-penalizes-north-korea-in-retaliation-for-sony-hack-1420225942.

회색지대전략이란 일반적으로 국력이 상대적으로 열세인 국가가 구사하는 전략으로 긴장의 수위를 무력충돌의 임계점 밑으로 유지하며 상대국을 정치-경제-외교-군사적 면에서 복합적으로 압박하는 것을 말한다(Morris, Mazarr et al. 2019). 전쟁과 평화 사이의 모호함을 활용하는 회색지대전략은 러시아의 하이브리드전에서 특히 빛을 발한다. 러시아의 하이브리드전(hybrid warfare) 특징은 물리력 사용을 최소화하고 대신 표적국가에 대한 심리전과 사이버전을 지속적으로 수행해 자중지란을 유도하는 것이다(Chivvis 2017).

하이브리드전의 핵심은 사이버 공격과 사이버공간을 활용하는 정보전(information warfare)이다. 하이브리드전 개념을 확립한 것으로 인정받는 현 러시아군 총참모장인 발레리 게라시모프(Valery Gerasimov)는 "아랍의 봄" 시기 견고해 보였던 북아프리카 국가들이 인터넷과 소셜미디어를 통한 정보전에 의해 단기간에 붕괴된 점을 상기시키면서 미래전에는 전통적인 군사 수단 대비 정보전을 비롯한 비군사적 수단의 활용비율이 4대 1에 도달할 것으로 예상하였다(Gerasimov 2016). 러시아의 정보전은 90년대부터 2010년대 사이 중동, 중앙 아시아, 동유럽에서 일어난 "색깔 혁명"(Color Revolution)을 서방권의 체제전환 전략으로 이해한 러시아가 이를 대서방권 공세를 위한 전략으로 재해석한 것으로 봐야 한다.

러시아의 정보전 철학 저변에는 자신이 서방권의 정보 공세에 포위되어 있다는 강박관념이 기본전제로 깔려 있다. 서방권과의 갈등이 단기간 내에 끝나지 않을 실존적 투쟁이라는 보는 관점은 사이버공간에서 충돌을 불사하는 공격적 대응으로 이어진다(Connell, Vogler 2017). 이는 러시아가 국가 차원에서 2014년 우크라이나 대선, 2016년 미 대선, 그리고 2017년 독일 총선에 개입한 배경이 된 것으로 여겨진다. 민주주의의 근간인 선거 과정을 저해한 러시아의 도발은 서방 세계와의 대립을 심화시켰다. 러시아의 미 대선 개입을 조사한 미 국가정보장실(Office of Director of National Intelligence)은 푸틴 대통령이 직접 미 대선 개입을 명령했음을 분명히 하였고, 러시아의 선거 개입을 조사한 뮬러 특별검사는 러시아군 정보기관(GRU) 요원 12명을 미 민주당 하원선거위원회(DCCC)와 전국위원회(DNC)를 해킹한 혐의로 기소하였다(Galante, Shaun 2018). 러시아는 미국 중앙정치 내부까지 깊숙이 침투해 자유민주주의의 근간인 선거의 무결성(Integrity)을 훼손했고 미국은 이를 자국에 대한 실존적 위협[44]이라고 간주하여 대대적인 보복에 착수하였다. 미국의 대응은 오바마 행정부의 임기가 끝나는 시점이었기 때문에 러시아 외교관 35명을 추방하고 관련자를 제재하는 선에서 끝맺었다. 비록 미 행정부의 후속 조치는 러시아와의 관계 개선을 우선시하는 트럼프 행정부 정책 때문에 최소화되었지만 뮬러 특검 조사를 통해 방대하고 심각한 수준의 러시아의 사이버 공격 행위가 공식적으로 확인되었기 때문에[45] 언젠가 재개될 가능성이 높다.

사이버 외교와 국제협력: 사이버 규범 도출의 실패

2007년에 일어난 에스토니아 DDOS 공격은 한 국가가 타 국가에게 사이버 공격을 한 첫 사례라는 점에서 분수령 같은 사건이었다. 북대서양조약기구(NATO) 회원국인 에스토니아가 러시아로 추정되는 국가의 사이버 공격으로 인해 3주 이상 국가 기간시설이 마비되었으나 NATO는 끝내 대응하지 못했다. 문제는 단순한 해킹 수준을 넘는 국가 주도 사이버 공격에 대한 교전수칙이 없었기 때문이었다. 일단 러시아가 배후라는 증거가 불충분했고, 사이버 공격으로 야기된 무형의 피해를 근거로 NATO 헌장 5조에 명시된 집단적 방위권을 발동할 수 있을지가 불분명했기 때문이다.[46]

에스토니아 사태 이후 서방 세계는 사이버 공격에 대한 억지력 제고를 위한 방안을 강구하였다. 이 노력의 첫 결실은 NATO 산하 사이버방위협력센터(CCDCOE: Cooperative Cyber Defense Center of Excellence)가 준비한 탈린 매뉴얼(Tallinn Manual)이었다. 탈린 매뉴얼은 2009년부터 2013년까지 20여 명의 국제법 전문가가 모여 진행한 연구로 2013년 첫 출간되었다. 탈린 매뉴얼의 대표적 성과는 사이버 공격으로 인해 인명 피해가 발생할 경우 공격자에 대한 군사적 보복이 가능하고 이를 지원한 국가 또는 단체들도 기존 국제법과 전쟁법을 적용해 책임을 물을 수 있음을 확인했다는 점이라 할 수 있다.

그러나 탈린 매뉴얼의 자체적 한계도 명확하였다. 비록 NATO의 후원을 받았지만 탈린 매뉴얼은 민간 전문가 집단의 권고 사항일 뿐이며 공식 지위를 갖지 못했다. 또한 탈린 매뉴얼이 실제로 사이버 공격 상황에서 법적 효용을 가지려면 전쟁법(jus in bello)인 국제인도법의 추가 개정이 필요하였다(박노형, 정명현 2014). 사이버공간상에서 국제인도법이 정의하는 "공격"이 성립되려면 최소한 "기능적 피해"(functional damage)[47]가 확인되어야

44. CNBC. Intelligence boss Clapper: Russia poses 'existential threat' to the United States. Janunary 5, 2017. https://www.cnbc.com/2017/01/05/sen-mccain-everyone-should-be-alarmed-by-russia-hacks.html.
45. Time. The Mueller Report Made It Clear: America's Response to Russia Has Been Far Too Weak. March 3, 2019. time.com/5582867/mueller-report-trump-russia-sanctions.
46. BBC. How a cyber attack transformed Estonia. 27 April 2017 https://www.bbc.com/news/39655415.

한다는 점, 사이버 공격이 전쟁법상 공격에 해당하는지에 대한 학계 컨센서스가 없다는 점 등은 탈린 매뉴얼의 저자들조차 인정하였다.[48] 파괴 또는 폭력이 수반되지 않는 데이터 탈취, 즉 해킹이나 정보전을 벌이는 것은 국제인도법상 "공격"에 해당되지 않으며(Schmitt 2012 June), 고로 해킹이나 정보전에 대한 국가차원의 대응을 제한하는 효과를 가지게 된다. 탈린 매뉴얼이 사이버 "공격"에 대한 무력대응을 국제법 차원에서 정당화하였다고 알려진 것과는 달리 실제 억지력 효과는 다분히 제한적이었던 것이다.

하지만 미국 중심의 서방국가들의 관점에서 탈린 매뉴얼은 완벽하지는 않지만 일단 사이버공간의 충돌에 대한 국제법 적용에 대한 가능성을 열어 놓았다는 데 의의가 있었다. 미국은 탈린 매뉴얼이 자위권 발동이 가능한 사이버 공격의 범주를 재산 및 인명피해를 야기할 수 있는 것으로 좁게 정의하여 군사적 대응을 지나치게 제한한다고 보았다(Schmitt 2012). 이런 한계에도 불구하고 미국은 탈린 매뉴얼이 사이버공간에서 전쟁법 적용에 대한 국제기준을 제시하였다고 평가했고,[49] 탈린 매뉴얼의 핵심 함의인 사이버공간에 대한 개전법(jus ad bellum)과 전쟁법(jus in bello) 등 기존 국제법 적용을 자국 사이버 외교의 주요 의제로 삼았다. 미국은 사이버공간에 대한 국제법 적용을 "양자간, 지역별, 다자간" 외교대화를 통해 설득하려 하였고,[50] 특히 사이버 안보에 대한 유일무이한 다자간 논의의 장인 유엔 정부전문가그룹(UN GGE: UN Group of Governmental Experts)을 활용하기를 기대하였다.

아이러니하게도 사이버공간의 안보적 특성과 문제점을 인지하고 다자간 논의의 필요성을 처음으로 제기한 국가는 러시아였다. 1998년 러시아는 유엔에 "국제안보적 배경에서 정보통신 부문의 발전"에 대한 공개적 논의를 시작할 것을 요청하였고, IT기술이 국제안보 및 국가안보에 위협이 될 수 있다는 러시아 입장에 동조하는 다른 유엔 회원국들의 지지 아래

47. 예시: 사이버 공격으로 인한 대규모 정전(blackout).
48. Council of Europe Parliamentary Assembly. Legal challenges related to hybrid war and human rights obligations. Report | Doc. 14523 | 06 April 2018 https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24547&lang=en.
49. Federal Computer Week. What does international law mean for cyber warfare? April 2, 2013. https://fcw.com/articles/2013/04/02/cyber-engagement-international-law.aspx.
50. Harold Hongju Koh, Legal Advisor of the Dep't of State, International Law in Cyberspace. Address to the USCYBERCOM Inter-Agency Legal Conference. Sept. 18, 2012. https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

2004년 1차 유엔 GGE[51] 회의가 소집되었다. 첫회 15개국의 정부 대표로 구성되었던 유엔 GGE[52]는 현재 25개국이 참여 중이며 국제법과 규범, 신뢰구축조치, 글로벌 역량강화 등에 대한 국가 간 협의체의 틀을 가진 유일한 논의의 장이다(김소정, 김규동 2017). 유엔 GGE는 2004년(1차), 2009년(2차), 2011년(3차), 2013년(4차), 2015년(5차) 다섯 차례에 걸쳐 소집되어 1차와 5차를 제외하고는 공동보고서를 제출하는 데 성공하였다. 2019년 6차 GGE가 소집되어 현재 논의를 진행 중이다.

2010년에 출간된 2차 GGE 보고서는 정보통신기술이 점차 무기화되고 사이버공간에서의 국가 간 일치된 행동 규범의 부재 문제를 지적하는 선에서 결론을 맺었다. 2013년에 출간된 3차 GGE 보고서는 처음으로 사이버공간의 일치된 "규범, 규칙 및 원칙"의 필요성을 상기시키고 동시에 유엔 헌장과 국제법이 사이버공간에서의 국가 행동에도 적용된다는 점을 적시하였다. 서방 국가들뿐만 아니라 중국, 러시아, 인도 등도 이런 내용이 포함된 보고서 출간에 합의했다는 점에서 3차 GGE 보고서는 비록 원론적이지만 국제법의 사이버공간 적용 여부를 주요국들이 모두 확인하였다는 점에서 의미가 크다고 할 수 있다. 2015년 출간된 4차 GGE 보고서는 더 진일보하여 3차에서 원론 차원에서만 다뤘던 국제법 적용 여부를 예시를 들어 좀 더 구체화하였다. 또한 사이버 주권을 강조하는 중국과 러시아의 입장을 고려하여 사이버공간에서도 내정 불간섭 및 주권 존중 원칙이 지켜져야 한다는 점을 강조하였다(Henriksen 2019). 추가적으로는 지역-국제적 차원의 신뢰구축조치(CBM: confidence building measures)와 자발적 규범과 원칙의 적용방법에 관련해 상당한 진전을 이루었다.

4차 보고서의 성공을 바탕으로 2015년에 소집된 5차 유엔 GGE에서는 국제법 적용 여부에 대한 좀 더 명확한 합의를 도출하려 시도하였다. 서방 국가들은 2013년 발간된 탈린 매뉴얼의 기조를 이어 개전법과 전쟁법을 사이버공간에 적용하고자 하였으나 중국과 러시아를 설득하는데 끝내 실패하였고, 결국 5차 유엔 GGE는 공동보고서 없이 2017년 해산하였다. 비록 후속 회기인 제6차 유엔 GGE가 2019년 소집되어 2021년까지 활동할 예정이지만 국제사회에서는 유엔 GGE 체제가 사실상 실패로 끝났다는 비관적 의견이 지배적이다.[53] 당장 중국과 러시아가 유엔 GGE에 대한 대안으로 제안한 정보안보 개방형 워킹그룹(OEWG:

51. 러시아의 요구를 반영해 설립된 기구이기 때문에 UN GGE의 공식 명칭은 "국제안보 관점에서 정보통신 분야의 발전상에 대한 정부전문가그룹"이다.
52. https://www.un.org/disarmament/group-of-governmental-experts/.

Open-Ended Working Group on Information Security)이 채택되어 2019년 첫 회의가 열렸다. OEWG는 서방 국가 중심의 유엔 GGE가 밀실처럼 운영되었다는 러시아와 중국의 비판을 반영하여 193개 유엔 회원국 전체에 문호가 개방되어 있다는 점에서 기존 유엔 GGE와 차별성을 가진다. 동시에 유엔 GGE와 마찬가지로 국제법의 사이버공간 적용 문제 논의를 이어간다는 점에서 국제사회 노력의 연속성을 나타낸다.

문제는 유엔 GGE와 OEWG의 목적이 겹친다는 점이다. 유엔이 두 기구에 부여한 임무는 동일하게 사이버공간에서 책임감 있는 국가 행동을 위한 "규범, 규칙, 원칙"을 수립하는 것이고 각각 2021년과 2020년 유엔 총회에 진전 사항을 보고해야 하는 의무가 있다. 실질적으로 같은 활동을 하는 두 개의 기구가 존재하며 서로 어떤 방식으로 협력을 하고 정책적 중복을 피할 것인지에 대해 아직 논의된 바가 없다는 점은 우려되는 부분이다(Stauffacher 2019). 유엔 GGE와 OEWG를 미국과 러시아가 각각 주도한다는 사실은 이 두 유엔 공식 기구가 사이버공간의 국제법 적용에 대해 서로 상충되는 결론을 내리는 전례 없는 결과로까지 이어질 수 있다.

결국 사이버공간 안정화를 위해 일치된 국제규범을 만들려던 국제사회의 노력은 2017년 5차 유엔 GGE의 실패로 인해 수포로 돌아갔다. 더욱 우려되는 것은 유엔 GGE의 실패가 중국과 러시아가 보여주고 있는 기존 국제규범을 대체하려는 행동 중 하나의 사례일 뿐이라는 점이다. 같은 맥락에서 중국과 러시아는 현재 유일무이한 사이버공간 국제조약인 유럽사이버범죄협약(The Convention on Cybercrime of the Council of Europe)의 무력화를 꾀하고 있다. 2001년 헝가리 부다페스트에서 유럽평의회(Council of Europe) 회원국들에 의해 조인되었기 때문에 부다페스트협약으로도 알려진 이 조약은 사이버 범죄와 관련된 법적으로 구속력을 갖는 최초의 국제협약으로서 사이버 범죄행위 규정 및 조사 관련 국가 간 협력 등에 대한 내용을 담고 있다. 하지만 유럽평의회 회원국이기도 한 러시아는 부다페스트협약이 국가주권을 침해한다는 이유로 가입을 거부하고 있다. 러시아가 특별히 문제 삼는 조항은 협약의 제32조b항 "저장된 컴퓨터 데이터에 대한 초국경적 접근"으로 정부의 별도 허가가 없더라도 데이터 소유주가 자발적으로 동의할 경우 범죄를 조사하는 국가로의 데이터의 이전을 허용하는 부분이다. 이는 국가주권을 우선하는 최근 중국과 러시아의 입장과 배치된다.

53. Soesanto, S. & D'Incau, F. The UN GGE is dead: Time to fall forward. European Council of Foreign Relations. https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

2017년 중국과 러시아는 부다페스트협약을 대체하는 유엔 차원의 사이버범죄협약을 제안하였다.[54] 중국과 러시아가 주도해 유엔총회 제3위원회에 제출한 유엔사이버범죄협약안은 기존 부다페스트협약과 유사하게 당사국 간의 원활한 사법공조와 데이터 이전을 보장한다. 그러나 본질적 차이점은 바로 표현 및 정보의 자유와 관련되어 있다. "정치범죄"가 관련되었을 경우 사법공조를 거부할 권리를 조인국들에게 보장한 부다페스트협약과는 달리 중국과 러시아의 제안은 "정치범죄"가 공조를 거부할 근거가 되지 않음을 못박아 놓았다.[55] 또한 이 제안은 사이버범죄를 모호하게 정의하여 국가의 권력 남용 가능성을 열어 놓아 정보와 표현의 자유가 심각하게 침해되는 것을 우려하는 국제사회와 인권단체들의 비판을 받는다.[56]

54. Agenda item 107, The rule of law at the national and international levels, A/RES/67/97(14 December 2012), available : https://undocs.org/en/A/74/701.
55. "Draft United Nations Convention on Cooperation in Combating Cybercrime" in 2017(A/C.3/72/12),: https://undocs.org/A/C.3/72/12.
56. CircleID. U.N. Approves Resolution to Combat Cybercrime Despite Opposition From E.U., the U.S. and Others. December 30, 2019. http://www.circleid.com/posts/20191230_un_approves_resolution_to_combat_cybercrime_despite_opposition/.

사이버 외교의 지정학

사이버 규범의 전장: 국제기구와 지역 기구

중국과 러시아의 사이버 외교 목표는 기존 서방세계가 구축한 국제사회의 사이버 거버넌스 체제를 대체하는 것이다. 여기에는 기존 사이버 거버넌스 체제가 보장하는 정보와 표현의 자유가 자신들의 체제를 실존적으로 위협한다는 뿌리 깊은 위기 의식이 자리 잡고 있다. 실제로 미 정부의 2018년 사이버 국가전략(National Cyber Strategy of the United States)[57]과 유럽연합의 2013년 사이버 안보 전략(Cybersecurity Strategy of the European Union)[58]은 자유롭고 안정되고 개방적인 인터넷을 핵심 개념으로 삼는다. 사이버공간에 대한 국가 개입을 최소화하고 자유민주주의적 가치인 정보와 표현의 자유를 보호하는 미국과 유럽연합의 사이버 전략은 중국과 러시아가 지향하는 국가주권 중심의 사이버 거버넌스 전략과 완전히 배치된다.

현재 사이버 외교지형은 점차 이원화·양극화되는 추세이다. 중국과 러시아는 서방세계가 구축해 놓은 사이버공간 국제규범에 대항하는 새로운 국제규범 체제를 형성하기 위해 기존 국제기구와 체제에 대해 일대일 맞대응하는 대안들을 만들어내고 있다. 유엔 GGE를 통한 논의를 매개체로 탈린 매뉴얼의 함의인 국제법의 사이버공간 적용을 국제규범화 하려던 미국과 서방권의 의도를 OEWG를 발족시켜 좌절시킨 것이 한 예다. 마찬가지로 중국과 러시아는 유엔에 사이버범죄협약을 상정하여 미국과 유럽 중심의 부다페스트협약에 대응한다.

중국과 러시아는 단순히 제도적으로만 서방세계와 대립하는 것이 아니다. 서방세계가 주도해 온 사이버 공공외교 분야에서도 중국과 러시아는 사이버 주권 개념을 강조한다. 인터넷 거버넌스에 관련된 가장 오래된 다자간 논의 기구는 인터넷 거버넌스 포럼(IGF: Internet Governance Forum)이었다. IGF는 자발적 협치를 강조하는 90년대 인터넷 거버넌스 문

57. White House.(2018). National Cyber Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
58. European Commission.(2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. adopted February, 7. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206225%202013%20INIT.

화를 수용한 유엔이 학계와 민간분야 전문가과 활동가들의 의견을 대폭 반영하기 위해 다중이해당사자(multi-stakeholder) 협의체로 2006년 출범한 회의이다. 하지만 중국은 유엔이 주도하는 공식 인터넷 거버넌스 논의기구가 민간분야 중심으로 운영되는 것을 반대하였고, 결국 2011년 IGF를 민간분야가 주도하는 수평적 논의기구가 아닌 국가 간 협의체로 전환하는 것에 대한 다른 유엔 회원국의 동의를 얻는 데 성공하였다(Mueller 2011).

중국이 추구하는 사이버공간에서의 주권 강조는 곧 사이버 외교의 분열로 이어졌다. 서방세계는 현재 영국이 주도적으로 설립한 사이버공간총회(Global Conference on Cyberspace)를 중심으로 논의를 이어가고 있다. 국제사회의 일치된 사이버 규범 형성을 위해 설립된 이 회의는 2011년 런던에서 처음 개최되었으며, 2012년 부다페스트, 2013년 서울, 2015년 헤이그, 그리고 가장 최근에는 2017년 뉴델리에서 개최되었다. 사이버공간총회는 유엔 GGE 활동을 보조하고 국가그룹과 시민사회 및 민간기업을 잇는 가교 역할을 하였고, 같은 맥락에서 2013년 서울 회의에서는 같은 해 발간된 3차 유엔 GGE 보고서의 결론인 사이버공간의 일치된 "규범, 규칙 및 원칙"의 필요성을 재확인하여 사이버공간의 규범화에 힘을 실어주기도 하였다.

이러한 상황에서 중국은 서방국가들이 주도하는 사이버 공공외교에 대항하기 위해 두 가지 전략을 구사하는 중이다. 첫째는 공공외교 강화이다. 중국은 사이버공간총회와 유사한 정부, 기업, 민간전문가를 망라하는 다중이해당사자(multi stakeholder) 중심 기구인 세계인터넷대회(World Internet Conference)를 2014년부터 중국 우전(Wuzhen)에서 개최하고 있다. 2015년 회의에는 시진핑 본인이 개회사에서 사이버공간의 주권화를 직접적으로 언급하기도 하는 등 중국은 이 회의를 통해 사이버공간에서도 국가의 주권적 통제가 필요하다는 주장을 일관되게 펼치고 있다.

둘째는 유엔과 같은 기존 다자간 기구에서의 영향력을 확대하는 것이다. 중국은 2020년 현재 미국에 이어 두 번째로 큰 유엔 기여금을 내는 국가이며, 유엔 관료조직 내 요직을 다수 차지한다.[59] 주로 배후에서 실무를 담당하는 자리지만 다른 회원국들의 이해에 영향을 줄 수 있다는 점에서 보이지 않는 영향력을 갖는다. 이미 사이버 거버넌스 측면에서 중국

59. The Economist. In the UN, China uses threats and cajolery to promote its worldview: some countries are pushing back China. December 7th 2019. https://www.economist.com/china/2019/12/07/in-the-un-china-uses-threats-and-cajolery-to-promote-its-worldview.

은 유엔을 통해 상당한 영향력을 가진다. 현재 중국은 미국 중심의 TCP/IP 기반 인터넷에 대한 대안으로 자국이 주도하는 이른바 "뉴IP"를 내세웠고,[60] 이에 대한 긍정적인 여론을 국제사회에서 확산시키기 위해 유엔기구인 국제전기통신연합(ITU: International Telecommunication Union)을 적극 활용한다. 이미 중국은 2000년대부터 ITU 내에 활동하는 자국 출신 유엔 관료들을 통해 인터넷 주소, 즉 도메인 서버를 관리하는 ICANN의 권한을 개별 국가에게 부여하는 방안을 꾸준히 추진해왔다(Mueller 2011). 이는 최근 러시아가 밀고 있는 RuNet와 위에서 언급된 "뉴IP" 정책과 연결되며, 중국과 러시아가 얼마나 일관되게 사이버공간 통제를 위한 국제 기술기준과 행동 규범을 구축하고 있는지를 보여준다.

사이버 규범의 진영별·지역별 파편화에도 지정학적 요인이 작용한다. 2001년 중국과 러시아, 우즈베키스탄, 카자흐스탄, 키르기스스탄 및 타지키스탄이 결성한 지역협력체제인 상하이협력기구(SCO: Shanghai Cooperation Organization)는 태초부터 국가안보에 방점을 둔 지역 기구로서 "테러리즘, 분리주의, 극단주의"에 대한 집단적 대응과 협력을 목적으로 두었다. 또한 주권과 내정불간섭 원칙을 강조하며 인권과 정치적 자유 같은 보편적 가치와 분명한 거리를 두고 서방세계가 대립각을 세웠다. 초기 SCO는 90년대의 혼란을 극복한 러시아와 서부 변경 지대의 안정을 원하던 중국의 이해가 맞아 떨어졌기에 출범한 중앙아시아 지역안보 체제였으나 2005년 인도와 파키스탄이 옵서버 지위를 획득하고 2017년 두 국가가 가입하면서 초대형 지역협력기구로 진화하였다.[61]

SCO가 안보에서 지역협력기구로 성장하면서 협력분야도 다양해졌다. 특히 중국과 러시아는 SCO를 통해 사이버공간에서 자신들이 추구하는 국가 중심의 사이버 규범을 설파한다. 2009년 공표된 "상하이협력기구 회원국 간의 국제 정보안보 협력 합의문" 제2조는 해킹과 IT 인프라 공격 등 일반적인 사이버 위협 범주 외에도 "사이버공간에서의 우월한 지위를 이용해 타국의 이익과 안보를 저해하는 것" 과 "타국의 사회정치 및 사회경제 구조와 영적, 도덕적, 문화적 환경에 위해를 가할 수 있는 정보를 확산하는 것"을 명시하여[62] 사이버공간을 독점적으로 주도하는 미국과 서방세계가 강조하는 정보와 표현의 자유를 정확히 겨냥한다.

60. FT Magazine. Inside China's controversial mission to reinvent the internet. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f.
61. 연세대 중국연구원. 최근 상하이협력기구 확대의 함의와 우리의 대처 방. 2017년7월 1일. https://yonsei sinology.org/archives/2153.

[표 5] 2020년 현재 활동 중인 국제 인터넷 거버넌스 체제 및 논의기구

다자간 사이버 안보 및 신뢰구축 논의 조직			
조직	**설립연도**	**주 회원국**	**목적**
유엔 정부전문가그룹 **UN Group of Governmental Experts**	2004	25개 유엔 회원국	유엔 공식 조직; 사이버공간의 책임 있는 국가행동에 대한 국제규범, 규칙 및 원칙 도출; 신뢰구축조치(CBM) 제시
정보안보 개방형 워킹그룹 **Open Ended Working Group on Information Security**	2018	유엔 회원국	유엔 공식 조직으로 유엔 GGE와 목적이 겹침
탈린 매뉴얼 **Tallinn Manual**	2009-2013; 2017 (개정판)	NATO가 후원한 국제법 연구그룹	전통적인 국제법(전쟁법)의 사이버공간에 대한 적용: 특히 사이버 공격에 대한 교전수칙 적용 및 비례적 무력사용에 대한 규칙 제시
유럽사이버범죄협약 **"부다페스트협약"** **The Convention on Cybercrime of the Council of Europe "Budapest Convention"**	2001	67개 조인국: 유럽, 미주, 일본, 호주 및 뉴질랜드; 한국은 기존 법제와 충돌로 가입하지 않음	사이버범죄 수사의 국제공조; 핫라인을 통한 신속한 정보 공유
상하이협력기구 **정보보안전문가 그룹** **Shanghai Cooperation Organization Information Security Experts Group**	2006	중국, 러시아, 카자흐스탄, 키르기스스탄, 타지키스탄, 우즈베키스탄, 인도, 파키스탄 (총 8개국)	정보안보 강조; 사이버공간 내 체제 위협과 테러리즘에 대한 공동 대처; 사이버공간에 대한 국가의 주권적 통제
인터넷 거버넌스 포럼 **Internet Governance Forum**	2006	유엔 회원국, 학계, 기업, 민간단체	유엔의 공식 다자간-다중이해당사자 국제회의
사이버공간총회 **Global Conference on Cyberspace**	2011	100여 개 국가정부, 기업, 민간단체 등 다중이해당사자 중심 기구 (multistakeholder)	사이버공간의 공동 규칙과 원칙 로드맵 수립; 민관대화
세계인터넷대회 **World Internet Conference**	2014	중국 주도 다중이해당사자 중심 기구	사이버공간에 대한 국가주권 강조

유럽연합이 지역연합기구로서 국제사회에서 상당한 영향력을 발휘하듯 SCO 회원국들도 국제사회에서 단일화된 목소리를 내 영향력을 높인다. 특히 서방세계의 자유주의 이념이 사이버공간을 통해 확산되는 것에 대한 두려움이 있는 국가들에겐 중국과 러시아의 사이버 규범은 매력적일 수밖에 없다. 중국과 러시아는 SCO를 매개체로 유엔 내 지지세를 확장해 국가 중심의 사이버 규범을 보편화 하려고 한다. 이를 위해 SCO의 2009년 사이버 안보 협약을 바탕으로 하는 "정보보안 국제공통수칙"[63]을 2011년과 2015년에 각각 원안과 개정안의 형태로 유엔에 제출해 서방세계가 추진하는 자유주의적 사이버 규범의 대안으로 제시하였다. 이 같은 노력은 부다페스트협약의 대안으로 제안된 유엔사이버범죄협약안의 경우처럼 중국과 러시아가 유엔을 통해 자신들의 사이버 규범에 당위성과 구속력을 부여하려는 전략의 일환으로 여겨진다.[64]

SCO가 지정학적 집합이라는 점은 중국과 러시아의 사이버 영역 확대에 도움이 되기도 한다. SCO는 2017년 "세계 최대 민주주의 국가"인 인도를 파키스탄과 함께 신규 회원국으로 맞아들였다. 미국의 인도 태평양 전략의 근간이 되는 "쿼드"(Quad)의 일원인 인도가 권위주의 국가들의 집합인 SCO 회원국이 된 배경에 대해선 중앙아시아에서 중국의 영향력을 견제하려는 인도와 러시아의 이해가 맞았기 때문이라는 관측이 지배적이다.[65] 반대로 중국의 입장에서 인도의 가입은 SCO의 국제적 위상을 높이고 자국의 사이버 규범을 보편화 할 수 있는 기회가 된다(McKune, Ahmed 2018).

SCO는 중국이 야심차게 추진 중인 일대일로와 지정학적으로 겹친다. 일대일로의 핵심 목표가 중국을 중앙아시아와 인도양을 거쳐 유럽과 연결하는 것이라는 점을 감안하면 SCO를 통한 지역안보 확립이 중국에게 장기적으로 필요할 수밖에 없다. 다만 안보적 측면에서 있어서 중앙아시아에서 러시아의 영향력이 절대적이기 때문에 현재 중국은 경제적 이해에 더 집중하는 모습이다. 대신 중국은 첨단기술분야에서의 상대적 우위를 활용해 중앙아시아

62. Shanghai Cooperation Organization(SCO). Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO. http://eng.sectsco.org/load/207508/.
63. United Nations Digital Library. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. 22 Jan 2015. https://digitallibrary.un.org/record/786846?ln=en.
64. McKune S. An Analysis of the International Code of Conduct for Information Security. September 28, 2015. https://citizenlab.ca/2015/09/international-code-of-conduct/.
65. Pantucci, R. (2015). India and SCO: the real benefit. *Gateway House, Indian Council on Global Relations*, *9*.

와 일대일로 지역 국가들의 보안 및 정보통신 수요를 담당한다. 이를 선도하는 기업들이 중국의 화웨이, ZTE, 그리고 감시 및 보안장비업체로 유명한 하이크비전(Hikvision)이다. 모두 미국의 제재리스트에 올라있는 중국 기업들이다. 이는 미국과 중국의 기술패권을 둘러싼 갈등이 단순히 첨단기술 선점뿐만 지정학적 충돌의 한 단면이라는 것을 보여준다.

사이버 외교의 갈등전선: 기술패권

4차 산업혁명에 관련된 첨단기술들은 사이버공간의 신지정학을 움직이는 동력이다. 빅데이터는 4차 산업혁명을 움직이는 핵심 자원이지만 이를 최대한 활용하기 위해서는 5G, 인공지능 및 클라우드 컴퓨팅 기술 개발이 필수적이다. 중국 APT 그룹들의 주요 해킹 대상이 전 세계 주요 첨단기술 기업들이라는 점은 중국이 첨단기술 확보에 수단과 방법을 가리지 않는 점을 잘 보여준다. 또한 중국은 일대일로와 디지털 실크로드를 바탕으로 자국의 첨단기술과 경제력으로 묶여진 거대한 영향권을 중앙아시아와 인도양 영역에 구축하고 있다. 중국의 신지정학적 전략인 일대일로의 양대 축은 첨단기술과 경협이다. 중국의 주변국과 투자와 무역을 확대하는 것은 미국이 막을 수 없지만 첨단기술 분야는 아직 기술적으로 서방세계에 뒤떨어져 있는 중국에게는 아킬레스건이다. 미국은 수출통제규정의 확대적용과 자국 기업에 대한 인수합병을 금지하는 방식으로 일대일로의 약한 고리를 공략한다. 특히 중국의 핵심 첨단기업들을 겨냥해 중국의 첨단기술과 시장에 대한 접근을 차단하는 전략을 피고 있다.

중국이 미국의 견제를 겪게 된 배경에는 시진핑 집권 이후 중국이 보이는 패권 지향적인 자세가 자리한다. 시진핑은 2013년 "중화민족의 위대한 부흥"이라는 중국몽(中國夢)을 국가 비전으로 선포하였고, 이로서 중국이 더 이상 내부 발전에만 집중하지 않고 대외적으로도 힘을 발휘할 것임을 선언하였다(최경식 2014). 중국은 지도자의 중국몽 비전에 걸맞게 팽창주의적 전략의 일환으로 일대일로(一帶一路)라는 거대 국가 프로젝트를 시작하였다. 일대일로 프로젝트는 명목상 중국의 낙후된 서부지역 대개발계획을 유라시아와 아프리카 대륙으로 확대하는 것이 그 배경으로, 일대일로 중 일대(一帶)는 중국 서부 지역에서 중앙아시아와 동유럽을 통해 서유럽까지 이어지는 거대한 육로이며 일로(一路)는 남중국해를 통해 인도양, 동아프리카, 북아프리카, 남유럽을 거쳐 서유럽까지 이어지는 거대한 해로이다. 중국은 일대일로를 통해 단순히 경제의 과잉공급 문제를 해결하는 것뿐만 아니라 중국과 경제적으로 관련 있는 국가들과 정치, 경제, 금융, 군사 등 분야에서 협력을 도모하는 협력 플랫폼으로 추진되고 있다(서종원 2016).

일대일로 프로젝트는 중국경제가 겪는 과대공급 문제를 국제경제의 변방이라고 할 수 있는 중앙아시아와 아프리카의 교통과 경제 인프라 건설을 통해 해소하는 것으로 해석될 수 있다. 하지만 시간이 지나면서 일대일로는 중국이 지정학적 영역뿐만 아니라 과학기술과 군사[66] 영역에서도 미국을 능가하는 세계 최첨단 산업국가로의 도약하려는 종합 국가개발 계획의 면모를 드러내고 있다. 특히 사이버 영역에 대한 집중은 크게 "과학기술 굴기"와 "디지털 실크로드"로 구현된다.

중국은 건국 1백주년인 2049년까지 "과학기술혁신강국"으로 도약하여 중화민족 부흥의 꿈을 뒷받침하겠다는 "과학기술 굴기"를 2016년 선포하였다(KISTEP 2018). 이를 뒷받침하는 것이 2015년 리커창 총리가 발표한 "중국 제조 2025"라는 첨단기술 개발 및 혁신 중심의 제조업 육성 계획이다. 독일의 제조업 혁신 계획인 "Industrie 4.0"를 본뜬 "중국 제조 2025"는 차세대 정보기술, 로봇, 항공 우주, 해양 공학, 고속철도, 고효율·신에너지 차량, 친환경 전력, 농업 기기, 신소재, 바이오 등 10대 핵심산업들을 21세기 중국 경제를 견인하는 동력으로 삼으려는 계획이다. 중국은 첨단과학기술국의 지위를 달성하기 위해 2000년대 GDP의 0.9%에 불과했던 R&D 투자를 2019년에는 2.5%까지 끌어올렸다.[67]

중국의 전방위적 대국 굴기는 사이버공간에서 더 활발하다. 디지털 실크로드[68](Digital Silk Road)로 불리는 사이버공간의 일대일로는 지정학적 경로를 따라 IT 인프라를 병행 구축하여 중앙아시아와 아프리카 국가들을 중국의 영향권 안에 단단히 묶어 두려는 목적을 띠고 있다. 시진핑이 2017년 처음 열린 일대일로 국제협력 정상포럼에서 디지털 실크로드 구축을 위해 디지털 경제, 인공지능, 빅데이터, 클라우드 컴퓨팅, 스마트 시티 개발을 강조했을 정도로[69] 디지털 실크로드는 중국의 중요한 전략사업이다.

중국은 디지털 실크로드를 구축하기 위해 관련국 ICT(Information and Communication Technology) 인프라 건설에 박차를 기하고 있다. 중국은 일대일로 참여국가에 차관을 제

66. 이상국(2015).
67. 서울경제. 中, GDP 2.5% R&D투자…기초연구 대폭 늘려 '美 추격'. 2019년 3월 11일. https://www.sedaily.com/NewsView/1VGJR5GHIJ.
68. 아주경제. "中, 일대일로에 '디지털 실크로드' 구축"...美와 경쟁 치열해진다. 2019년 10월 21일. https://www.ajunews.com/view/20191021105454694.
69. People's Daily. Construction of digital Silk Road lights up BRI cooperation. 24 April 2019. http://en.people.cn/n3/2019/0424/c90000-9571418.html.

공하고 반대급부로 화웨이와 ZTE가 5G 네트워크 구축을 맡도록 한다. 특히 화웨이는 국제 통신망부터 국내 이동통신망까지 구축하며 디지털 실크로드 인프라 건설에 있어서 핵심적 역할을 한다.

디지털 실크로드에서 가장 눈에 띄는 사업은 방대한 지상-해저 광케이블망으로 일대일로 참여국들을 서로 연결하는 계획이다. 광케이블망은 5G 네트워크 구축에 필수적으로 필요한 인프라이나 아프리카와 중앙아시아에는 대규모 데이터 전송망이 부족한 상황이다. 중국의 디지털 실크로드 사업이 시작되면서 중국 기업들의 해저 케이블 부설사업 참여율은 2012-2015년 기간 동안 7%였던 것이 2016-2019 기간에는 20%로 3배가량 증가하였다(Shen 2018). 일대일로를 따라 건설되고 있는 중국의 대표적인 광케이블망 프로젝트로는 현재 2019년에 완성된 중국과 파키스탄을 잇는 연장 820km의 광케이블망과 2020년 중 완공 예정으로 화웨이 마린(Huawei Marine)이 주도하는 총 연장 12,000km의 파키스탄-동아프리카 광케이블망 건설 사업 등이 있다.[70]

중국은 광케이블망으로 연결된 국가들 내 5G 네트워크 구축에도 참여한다. 화웨이는 현재 세르비아, 러시아, 캄보디아와 나이지리아에서 5G 네트워크 사업을 진행하고 있다.[71] 화웨이의 광케이블망과 5G 네트워크로 구축된 ICT 인프라를 뒷받침하는 데이터 센터 확장에도 중국 기업이 참여한다. 현재 중국의 국영통신업체인 차이나 텔레콤(China Telecom)의 계열사인 차이나 텔레콤 글로벌은 홍콩과 싱가포르에 디지털 실크로드를 지원할 데이터 센터를 구축 중이다. 참고로 차이나 텔레콤은 2015년과 2017년도에 한국과 미국, 캐나다를 오가는 인터넷 트래픽을 가로채 정보를 들여다보았다는 의심을 받는다.[72]

데이터는 네트워크 성능과 용량을 감안해 최적 궤적으로 전달된다. 이는 중국이 중국 바깥에 깔려 있는 광케이블 기간망의 일부라도 통제할 수 있다면 국제 인터넷을 감시할 수 있는 능력이 생기는 것을 의미한다. 특히 오늘날 대륙 간 데이터 트래픽의 95%를 담당하는

70. Center for Strategic and International Studies(CSIS). China Doubles Down on Its Digital Silk Road. November 19. 2019. https://reconnectingasia.csis.org/analysis/entries/china-doubles-down-its-digital-silk-road/.
71. 각주 25번과 같음.
72. ZDNet Korea. 오라클 "중국 '인터넷 트래픽 가로채기' 확인". 2018년 11월 7일. https://zdnet.co.kr/view/?no=20181107160756.

해저 케이블망에 대한 통제가 초미의 관건이다.[73] 중국이 자국 기업을 통해 구축하고 있는 동유럽, 중동, 아프리카, 중앙아시아를 아우르는 거대한 해저 광케이블망이 완성되면 해당 지역뿐만 아니라 서방세계의 인터넷 데이터도 중국이 관할하는 제3의 국가 인터넷망을 통해 감청할 수 있는 능력이 생기게 된다.[74]

특히 이들 사업에 간여하는 핵심 회사인 화웨이 마린이 화웨이 계열사였다는 점이 이러한 우려를 증폭시킨다. 2019년 중반 화웨이는 화웨이 마린의 자사 지분 51% 전부를 다른 중국 회사인 헝퉁(Hengtong)에 매각하였으나 아직까지 미 정부는 의심의 눈초리를 거두지 않고 있다.[75] 화웨이 마린은 세계 해저 광케이블 부설 시장의 10%정도를 차지하는 것으로 추정되지만 향후 일대일로 사업을 통해 점유율을 크게 늘릴 것으로 예상된다.[76]

미국의 반격: 수출통제체제를 통한 대중제재

중국의 디지털 실크로드와 이에 대한 미국의 견제는 사이버공간에서의 충돌이 지정학적 영역으로 확대되는 현상이라고 볼 수 있다. 최근 미중 간의 무역전쟁은 미국이 천문학적인 대중무역 적자를 상쇄하려는 이유도 있지만 실제 핵심 목표는 IT 통신기술, 지적재산권, R&D 등 첨단기술 분야에서 중국과의 격차를 벌리고 신지정학적 갈등의 요인이 되는 중국의 디지털 실크로드를 견제하는 것이다. 미국이 기술적으로 중국에게 월등히 앞서 있기 때문에 거의 모든 기술 분야에서 미국은 선도자고 중국은 추격자인 입장이다. 이를 감안해 미국은 중국이 선진기술을 획득하는 경로를 차단해 중국과의 기술적 격차를 유지하려고 한다.

73. The Wall Street Journal. America's Undersea Battle with China for Control of the Global Internet Grid. March 12, 2019. https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466.
74. Washington Post. Huawei Marine is being sold. That's unlikely to change the threat it poses. June 5, 2020. https://www.washingtonpost.com/politics/2019/06/05/huawei-marine-is-being-sold-thats-unlikely-change-threat-it-poses/.
75. The Washington Post. Huawei Marine is being sold. That's unlikely to change the threat it poses. June 5, 2019. https://www.washingtonpost.com/politics/2019/06/05/huawei-marine-is-being-sold-thats-unlikely-change-threat-it-poses/.
76. Nikkei Asian Review. Undersea cables -- Huawei's ace in the hole. May 28, 2019. https://asia.nikkei.com/Spotlight/Comment/Undersea-cables-Huawei-s-ace-in-the-hole+&cd=11&hl=en&ct=clnk&gl=kr.

미 정부의 중국 첨단기업에 대한 제재는 동시다발적으로 적용되고 있다. 화웨이와 ZTE에 대한 미 정부의 견제가 가시화된 것은 2012년 미 하원 정보위원회에서 "중국기업 화웨이와 ZTE의 미 국가안보에 대한 위협 조사보고서"[77]를 발표하면 서다. 미국 기업 인수합병을 통해 미국 시장 진출을 노리고 있던 화웨이는 미 하원의 조사에 적극 협조했지만 미 하원 보고서는 화웨이와 ZTE는 중국 공산당이 통제하는 회사라고 결론을 내렸다. 미 의회가 화웨이와 ZTE의 대미투자를 사실상 보이콧하면서 국산 통신장비의 미국 시장 진출은 좌절되었다.

8년이 지난 오늘날 미국의 대중제재는 중국기업의 대미투자를 막는 차원을 넘었다. 미국의 대중제재는 기술이전을 막기 위한 수출통제, 해당기업의 제품 유통 금지, 그리고 최근에는 중국기업의 미 국민의 개인정보 수집을 차단하기 위한 앱 퇴출로 이어지고 있다. 제재의 범위도 국제적으로 확대되었다. 미국의 수출통제체제는 광범위한 관할권을 가진다. 여기에는 대부분의 원천첨단기술을 미국이 개발하였고 현재에도 첨단 신기술이 가장 활발히 개발되고 있는 나라라는 배경이 있다. 미국은 일정 비율의 미국산 원천기술이나 부품이 사용된 제품을 미국산으로 규정하여[78] 자국의 수출통제규정을 적용한다. 예컨대 한국의 삼성전자가 생산한 반도체에도 미국산 원천기술이 일정비율 이상 적용되었기 때문에 제재대상으로 지정된 화웨이에 반도체를 수출할 경우 미 수출통제체제를 관할하는 미 상무부의 승인을 받아야 한다. 즉, 미국 수출통제체제의 관할권은 전 세계 첨단기술과 제품을 포괄한다고 봐도 무방하다.

화웨이를 비롯한 중국기업을 국제적으로 퇴출하기 위해 미 정부가 사용하는 또 다른 전략은 네트워크 보안성 위협에 따른 중국산 통신장비에 대한 사용금지 요청이다.[79] 이는 주로 미국과 안보협력관계가 있는 동맹국들에게 미국이 요구하는 사항이다. 여기서 언급되는 부분이 화웨이가 제작한 5G 네트워크 장비를 통한 미 정부 기밀 유출 위험성이다. 즉, 미국이 해당국 정부와 공유하는 정보가 화웨이가 자사 통신기기에 심어 놓은 백도어(Backdoor)

77. Rogers, M., & Ruppersberger, C. D.(2012). Investigative report on the US national security issues posed by Chinese telecommunications companies Huawei and ZTE: a report. US House of Representatives.
78. 여기에는 미 정부가 규정한 "De minimis" 기준이 적용된다.
79. The Wall Street Journal. Washington Asks Allies to Drop Huawei. November 23, 2018. https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105.

를 통해 유출될 수 있다는 이유로 해당국 네트워크에서 화웨이와 기타 중국 통신기기를 제외달라는 것이다. 이미 미국의 정보공유체계인 "파이브 아이즈"(Five Eyes)에 속해 있는 캐나다, 뉴질랜드와 호주가 화웨이 제품을 퇴출했고 가장 최근에는 영국도 이에 동조하였다. 하지만 미 동맹국인 일본, 독일, 그리고 프랑스는 현재 구축되고 있는 5G 네트워크에서 아직 화웨이 제품을 완전히 퇴출하지 않은 것으로 알려져 있다.[80]

가장 최근에는 중국 소셜미디어 앱인 틱톡과 위챗이 미 국민의 개인정보를 중국으로 유출할 수 있다는 점을 들어 미국시장에서 퇴출시키는 행정명령을 내렸다. 이는 미 인터넷 기업인 구글과 페이스북이 중국에서 활동하지 못하는 것에 대한 대응이며 동시에 미 국민의 개인정보가 중국 빅데이터 산업발전에 도움이 되는 것을 막고자 하는 조치이기도 하다. 개인정보 유출을 막기 위해 틱톡과 위챗을 퇴출하라는 이 행정명령은 데이터는 21세기의 석유라는 명제를 증명해 주는 사례로도 볼 수 있다.

미국의 대중제재조치 중에서 특히 두드러지는 부분은 화웨이에 대한 미 정부의 집요한 압박이다. 화웨이는 중국에서 가장 시가총액이 큰 기업도 아니며[81] 논란이 되고 있는 5G 네트워크 기술면에서 일부 분야에서는 경쟁사인 ZTE가 앞서기도 한다. 그럼에도 2019년 미 정부가 화웨이와 계열사 68곳을 동시다발적으로 제재한[82] 것처럼 미 정부가 화웨이에 집중하는 이유로는 두 가지 요인이 있는 것으로 알려져 있다. 하나는 미 국방부에서 2020년 6월 밝힌 것처럼 중국 인민해방군이 화웨이를 지배하고 있다는 점과 백도어 등을 심어놓아 5G 네트워크 안정성에 위협이 된다는 점이다.

하지만 덜 부각되기는 하지만 미국의 반화웨이 정책의 핵심요인이라 할 수 있는 것은 화웨이가 위에서 언급되었던 것처럼 일대일로 참여국의 5G 네트워크 구축과 인터넷 기간망인 해저 케이블 부설까지 망라하는 디지털 실크로드의 핵심 기업이라는 점이다. 화웨이는 이집트와 알제리에 데이터 센터를 건설 중이며 아프리카 23개국의 통신시장에 진출해 아프

80. CHANNELe2e. Huawei: Banned and Permitted in Which Countries? Updated Nov 6, 2020. https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/.
81. 알리바바와 텐센트가 중국기업 중 시가총액으로 각각 1위와 2위이며 화웨이는 7위임.
82. Bureau of Industrial Security. Addition of Certain Entities to the Entity List(final rule). May 16, 2019. https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019.

리카 LTE 네트워크의 70%를 점유하고 있다.[83] 중국이 사이버공간 장악을 위해 추진 중인 "뉴IP"도 화웨이가 개발 중인 기술이다. 만약 화웨이가 문을 닫을 경우 중국의 디지털 실크로드 계획과 사이버공간 장악 시도는 큰 차질을 겪을 수밖에 없다.

따라서 미국은 바로 화웨이의 취약점인 반도체 수급을 겨냥해 화웨이를 고사시키려는 것으로 보인다. 미 정부는 이미 2018년도에 반도체 및 미국산 첨단부품 공급을 막아 화웨이의 경쟁사인 ZTE를 폐업 직전까지 몰고 간 전례가 있다.[84] 하지만 화웨이는 이를 대비해 이미 2019년부터 대만 TSMC에서 최소한 1년치의 반도체 제품을 미리 구비해 놓은 것으로 알려졌다. 화웨이는 미리 쌓아 놓은 부품을 바탕으로 중국 내 고객기업들에게 2021년까지 차질없이 5G 기지국 구축에 투입될 통신기기를 공급할 것을 약속했다고 보도되기도 했다.[85]

제재의 성공 여부를 떠나 화웨이와 기타 중국기업을 겨냥하는 미국의 궁극적 목표는 일차적으로는 신지정학적 경쟁에서 중국을 압도하고 궁극적으로는 미국과 중국 간의 경제와 기술적 디커플링을 노리는 것으로 보인다. 미 정부가 광범위한 관할권을 가진 수출통제체제를 활용해 중국기업들에 대한 첨단부품 및 기술 판매를 막는 것은 미국시장에서뿐만 아니라 세계시장에서 중국기업들의 실질적 퇴출을 의도하는 것이다. 특히 오락성이 강한 틱톡을 안보위협으로 규정하여 미국 시장에서 퇴출시키도록 한 트럼프 대통령의 행정명령의 목적은 미 국민의 개인정보의 중국으로 이전을 차단하여 미중 간 데이터 무역 가능성을 아예 막기 위한 것이다. 이렇게 미중 공급망과 데이터 이동이 제한되는 것이 바로 디커플링이기 때문에 미중 간 디커플링은 트럼프 행정부의 조치들이 장기간 유지될 경우 결국 실현될 수밖에 없다.

트럼프 행정부가 추진한 대부분의 정책을 폐기할 것으로 예상되는 바이든 행정부도 중국 첨단기업에 대한 미국 기술과 첨단물자에 대한 차단은 유지할 것으로 보인다. 이미 중국기

83. 매일경제. 화웨이 앞세워 '디지털 중국夢'…中, 아프리카 23개국 통신망 장악, 2020년 1월 2일. https://www.mk.co.kr/news/world/view/2020/01/6346/.
84. Forbes. How the U.S. Export Ban Effectively Bankrupts China's Telecom Giant ZTE: Analysis. April 17, 2018. https://www.forbes.com/sites/jeanbaptiste/2018/04/17/how-the-u-s-export-ban-effectively-bankrupts-chinas-telecom-giant-zte/?sh=3a78eee0720c.
85. Huawei Outhustles Trump by Hoarding Chips Vital for China 5G. October 22, 2020. https://www.bloomberg.com/news/articles/2020-10-22/huawei-outhustles-trump-by-stockpiling-chips-needed-for-china-5g.

업들에 대한 미 정부의 제재조치의 시발점이 된 미 하원 정보위원회의 화웨이와 ZTE에 대한 보고서가 초당적 협력의 산물이기 때문이다. 즉, 미 조야에는 중국 첨단기업이 지적재산권을 갈취하고 ICT제품에 백도어 같은 보안위협을 심는다는 트럼프 행정부의 주장에 대한 초당적 동의가 있음을 의미한다. 미 정부의 대중제재 정책이 행정부 교체 시에도 유지될 것으로 예상되는 이유이다.

결론: 사이버공간의 지정학화(Geo-politicization)

20세기 후반부터 시작된 정보통신 분야의 비약적인 발전은 사이버공간이라는 새로운 영역을 열었다. 특히 2020년 코로나바이러스 대유행으로 인해 많은 현실공간 내 활동이 사이버공간으로 빠르게 흡수되고 있다.[86] 기술의 발전을 넘어 경제구조 자체의 패러다임이 달라지는 변곡점에 도달하면서 안보 분야 또한 예외가 아니게 되었다. 이렇게 현실공간의 정보통신기술에 대한 의존이 커질수록 사이버공간이 제기하는 외교안보적 도전은 더욱 복잡해질 전망이다.

외교안보적 측면에서 정보통신기술의 발전은 기존 갈등 구조를 확대하는 촉매제 역할을 한다. 과학기술의 발전은 기존 안보 개념을 송두리째 뒤바꿔 놓았다. 미국이 오늘날 가장 우려하는 러시아의 위협은 핵무기가 아니라 사이버 댓글 부대의 선거 개입이다.[87] 미국은 중국이 보안을 무력화하기 위해 정보통신기기 회로에 백도어를 심어 놓았다고 주장한다.[88] 중국과 러시아는 반대로 미국이 사이버공간을 이용해 체제 전복을 시도한다고 의심한다.[89] 미국은 중국이 추진 중인 지정학적 영향권 확대 전략인 일대일로 프로젝트보다 이에 부속된 계획인 디지털 실크로드에 더 민감하게 반응한다.

즉, 신지정학은 현실공간에 뿌리를 두지만 동력은 사이버공간과 이를 뒷받침하는 정보통신기술에서 나온다. 기존 경제 및 외교안보 개념이 사이버공간과 정보통신기술과 맞닥뜨리게 되면 새로운 모습으로 변화한다. 예컨대 사이버공간에서 도발은 전통적인 군사력으로는 쉽게 대응할 수 없는 비대칭적 위협이다. 프라이버시의 영역으로만 여겨지던 개인정

86. Financial Times. How Covid-19 is accelerating the shift from transport to teleport. March 30, 2020. https://www.ft.com/content/050ea832-7268-11ea-95fe-fcd274e920ca.
87. The Business Insider. These are the biggest threats to the US in 2020. Jan 4, 2020. https://www.businessinsider.com/here-are-the-biggest-threats-to-the-us-in-2020-2019-12.
88. Bloomberg. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Oct 4, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
89. Chicago Tribune. Kremlin convinced U.S. is intent on regime change in Russia, intel report says. Jun 28, 2017. https://www.chicagotribune.com/nation-world/ct-russia-united-states-tensions-20170628-story.html.

보는 빅데이터 기술로 인해 이제는 석유처럼 중요한 핵심 경제자원으로 취급된다. 트럼프 행정부에 따르면 미국의 국가안보, 외교 및 경제를 위협하는 심각한 위협 중 하나는 다름이 아니라 전 세계 청소년들이 15초에서 1분 이내 동영상을 제작해 공유할 수 있게 해 주는 틱톡이라는 소셜미디어 앱이다.

극단적으로 보일 수 있는 이러한 신지정학적 현상의 배경에는 전통적인 이념적 갈등이 도사리고 있다. 서방세계는 사이버공간을 자유주의적 국제질서의 보루라고 여기고 중국과 러시아는 반대로 사이버공간이 제공하는 정보와 표현의 자유가 권위주의적 체제에 대한 실존적 위협이라고 간주한다. 냉전 종식 후 역사의 종말을 맞았어야 하는 체제경쟁은 중국의 부상과 러시아의 부활 덕분에 다시 되살아나고 있다. 강대국 간의 갈등은 핵무기로 이룬 공포의 균형이 아직 유지되는 현실세계와는 달리 직접적 인명피해 가능성이 낮은 사이버공간에서 더 자유롭게 발현한다. 하지만 정보통신기술은 경쟁에서 승리한 쪽이 모든 것을 독식하도록 허락한다. 그 결과 4차 산업혁명 기술과 사이버 국제규범의 주도권을 쥐는 쪽이 체제경쟁의 승패를 결정할 것이라는 위기 의식이 두 진영 내 팽배해 있다. 이는 갈등을 다시 증폭시키는 악순환으로 이어진다.

현재 신지정학적 갈등은 세 가지 전선에서 관찰되고 있다. 빅데이터와 AI 개발의 밑바탕을 이루는 개인정보의 확보와 배타적 활용, 자유주의 대 국가주권으로 이원화된 사이버 거버넌스 규범, 그리고 신지정학적인 현상인 중국의 디지털 실크로드 계획과 기술굴기에 대한 미국의 견제다. 이 모두 4차 산업혁명의 주도권을 사이에 두고 미국과 (유럽연합을 포함하는) 경쟁국들 사이에 형성된 전선들이다. 이 저변에는 사이버공간이 사실상 미국에 의해 만들어져 미국의 이해를 위해 작동하는 미국의 영역이라는 경쟁국들의 불만과 우려가 깔려 있다.

미국이 주도하는 사이버공간에 대한 도전을 특징짓는 개념은 사이버/디지털 주권이다. 사이버 주권은 중국과 러시아가 2010년대 공식화한 개념으로 사이버 인프라의 보호뿐만 아니라 사이버공간의 데이터와 서비스를 모두 국가가 통제해야 한다는 개념이다. 디지털 주권은 유럽연합이 개인정보보호와 데이터 무역에 적용하는 개념으로 아직까지는 중국과 러시아의 것보다 인권과 산업정책적 측면에 좀 더 무게를 둔다. 하지만 사이버공간에 대한 국가 통제를 부분적으로나마 강조한다는 점에서는 둘 다 유사하다. 중국, 러시아, 그리고 유럽연합이 사이버공간상의 국가주권에 대해 궤를 같이 한다는 점은 최소한 경제적 측면에서 향후 사이버 경제에 대한 국가 통제가 심화될 것이며, 특히 데이터 무역에서는 더욱 두드러질 것이 분명하다. 다자간 합의를 통해 국가 간 데이터의 자유로운 이전을 용이케 할 세계데이터기구(WDO: World Data Organization)의 설립은 시간문제로 보인다.

하지만 사이버/디지털 주권을 바탕으로 2010년대 이후 점차 불안정해지고 있는 사이버공간을 안정화하기에는 어려울 것이다. 2010년대 들어 국가지원 사이버 공격의 빈도와 피해 규모가 기하급수적으로 늘어나고 있으며 정보전 성격의 사이버 공격도 자행되고 있다. 대표적인 사례로 미국 민주주의 근간을 뒤흔든 심각한 수준의 공격으로 취급되는 러시아의 2016년 미 대선 개입을 들 수 있다. 심화되는 사이버공간에서의 갈등을 완화하고 지속가능한 안정을 위해서는 주요 행위자 간 일치된 행동규범이 절실하다. 하지만 이와 관련된 UN GGE 같은 국제논의는 당사국들이 사이버 안보 규범 관련 합의 도출에 실패하면서 사실상 중단되었다.

국제논의가 파행된 배경에는 중국과 러시아가 추진하는 새로운 사이버 규범들이 있다. 중국과 러시아는 사이버 범죄 관련해 유일한 국제사법공조 조약인 부다페스트협약을 대체하는 가칭 “유엔사이버범죄협약안”을 유엔총회에 제안해 놓은 상태이다. 이 협약안은 정치범죄에 대한 수사공조도 회원국들에게 강제할 수 있는 조항이 삽입되어 있어 인권침해 소지가 크다. 자유민주주의 국가들에게는 거부감이 큰 국가 중심의 사이버 규범에 대한 국제여론의 지지를 얻기 위해 중국은 공공외교에 힘쓰고 있다. 중국은 2014년부터 중국 우전에서 매년 세계인터넷대회(World Internet Conference)를 개최하고 있으며 2015년에는 시진핑 주석이 개회사에서 직접 사이버 주권을 언급하기도 하였다. 중국의 공공외교는 여기에 그치지 않고 유엔과 국제기구를 장악해 자신들의 사이버 규범 채택을 종용하고 이 과정에서 정보통신기술 관련 국제표준을 마련하는 유엔 산하의 국제전기통신연합(ITU)를 적극 활용하고 있다.

하지만 국제규범과 데이터 이전을 둘러싼 강대국 간의 갈등은 국가 존망을 결정하는 중대한 지정학적 위협은 아니다. 오늘날 세계질서를 뒤흔드는 가장 지대한 신지정학적 위협 중 하나는 지정학과 첨단기술이 복합적으로 융합되어 있는 중국의 디지털 실크로드 계획이라고 할 수 있다. 디지털 실크로드는 명목상 중앙아시아와 유럽을 육로와 해상으로 잇는 거대 인프라 개발 계획인 일대일로의 부수적 사이버 인프라 개발계획일 뿐이다. 하지만 중국은 디지털 실크로드를 통해 신지정학적 요충지를 선점하고 궁극적으로 미국이 향유하는 사이버 주도권을 약화시키려 한다.

중국은 일대일로를 활용해 세계 기술표준 경쟁에서도 우위를 점할 수 있다. 중국은 인프라 투자와 기술 지원에 대한 반대급부로 60여개국이 넘는 일대일로 참여국들에게 자국 기술 표준과 통신설비 채용을 종용한다. 사실상 아프리카와 아시아의 개발도상국에게는 중국을 제외하고는 IT인프라 투자를 제공할 국가가 없기 때문에 중국의 요구를 수용하는 상황이다.[90] 현재 일대일로 참여국의 총 합산 인구는 전 세계 인구의 60%, 경제규모는 세계 GDP의 30%에 육박한다.

일대일로의 규모를 생각하면 중국은 기술표준뿐만 아니라 정보와 표현의 자유 중심의 현 사이버 거버넌스 규범을 국가통제 중심으로 개편하기가 매우 수월해진다. 이를 위해 중국과 권위주의 이념 및 반미주의 성향을 공유하는 상하이협력기구(SCO) 국가들이 중국의 전략을 뒷받침하는 핵심 블록을 형성한다. 중국이 기술 및 인프라 투자를 바탕으로 개발도상국의 개인정보를 확보하게 된다면 중국은 서방세계를 제치고 AI와 빅데이터 기술을 선도하는 데 유리한 고지를 차지할 수 있다. 특히 중국이 최근 ITU에 제시한 뉴IP는 현존하는 TCP/IP 인터넷 통신 프로토콜보다 정보에 대한 국가통제를 용이하게 한다. 만약 일대일로 참여국들이 중국의 뉴IP를 채택하면 미국과 서방세계의 인터넷과는 완벽하게 단절된 중국 지배의 사이버 공간이 만들어진다. 디지털 실크로드를 통해 중국 중심의 거대 경제-사이버 블록이 탄생하는 것이다.

미국의 입장에서 디지털 실크로드는 단순히 중국의 일대일로를 통한 정보통신 인프라 구축이 아니라 미국의 세계패권을 위협하는 복합적인 도전이다. 디지털 첨단기술은 미국이 예상치 못한 곳에서 새로운 지정학적 요충지를 만들어 냈다. 대표적으로 남아시아와 아프리카를 연결하는 해저케이블망이 있다. 인터넷 인프라가 빈약한 이 두 지역을 연결하는 것은 경제적 가치가 크지 않았기 때문에 지금까지 선진국 기업들은 관심을 가지지 않았다. 중국이 이런 빈틈을 파고 들면서 전 세계 인터넷의 한 모퉁이를 차지할 수 있게 되었다. 중국이 일대일로를 따라 부설하고 있는 해저케이블망과 데이터 센터가 완성되면 중국은 인터넷을 마음대로 들여다볼 수 있는 능력을 갖추게 된다.

중국의 기술굴기와 디지털 영역 확장을 견제하기 위해 미국은 광범위한 관할권을 가진 수출통제체제를 활용하고 있다. 여기서 중국이 유형적 척도인 GDP에서는 미국을 따라잡을

90. Chipman, J. China's long and winding Digital Silk Road. IISS. Jan 25th, 2019. https://www.iiss.org/blogs/analysis/2019/01/china-digital-silk-road.

수 있을지 모르지만 무형적 자산인 원천기술 등에서는 미국에 비해 한없이 열세임을 알 수 있다. 미국은 이를 이용해 첨단기술과 부품의 중국기업으로의 이전을 제한하여 중국기업의 세계시장에서의 퇴출을 자연스럽게 유도하고 있다. 이는 자연스럽게 미중 간의 경제·기술적 디커플링으로 이어질 수밖에 없다. 특히 디지털 실크로드의 핵심기업인 화웨이에 제재를 집중하는 것은 미국이 명목상 주장하는 5G 네트워크의 보안성 문제보다는 신지정학적 경쟁에서 중국을 압도하려는 목표가 있기 때문이다.

미국은 중국의 팽창주의 전략의 발현인 일대일로 프로젝트에 대해서는 별다른 견제를 하지 않았지만 디지털 실크로드 참여기업과 4차 산업혁명 선두기업들에 대해서는 강경한 입장을 취한다. 뚜렷이 대비되는 미국의 반응에서 지정학적인 요인과 사이버공간이 상호작용하면서 기존의 강대국 간 갈등이 신지정학적인 갈등으로 확대되는 것을 알 수 있다. 특히 중국기업에 대한 공급망 차단과 시장 퇴출을 집요하게 압박하고 있는 미국의 정책은 미중 간 디커플링으로 이어져 궁극적으로는 사이버공간의 파편화까지 이어질 것이다. 이미 미 재계는 미래 인터넷이 미국과 중국이 주도하는 개별 인터넷 공간으로 각각 분리될 것을 예상하고 있다.[91] 현실공간에서의 갈등이 사이버공간에까지 이어지면서 사이버공간이 빠르게 지정학화(geo-politicization)되고 있는 것이다.

한국에 대한 함의

신지정학 시대의 한국은 두 가지 도전에 당면해 있다. 첫째는 정보통신혁명으로 인한 경제패러다임의 급진적 변화로 개인정보가 가지는 위상과 함의가 완전히 달라졌다는 점이다. 둘째는 미중 간의 알력다툼이 남중국해와 인도양 영역으로 국한된 지정학적 갈등을 넘어 과학기술과 사이버공간으로 인해 심화된 포괄적인 신지정학적 갈등이라는 것이다. 즉, 신지정학의 시대에는 국제적 갈등에서 한국은 결코 안전하지 않다는 점을 인지하고 이에 합당한 대비를 해야 한다.

선제적으로 취해져야 할 조치는 개인정보 데이터의 해외이전을 통제하여 개인정보의 안보적 중요성을 정책에 반영하는 것이다. 최근 개정된 데이터3법은 개인정보에 대한 산업적

91. CNBC. Former Google CEO predicts the internet will split in two — and one part will be led by China. September 21, 2018. https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

활용의 문을 열어주었다. 동시에 유럽 데이터 시장 진출에 필수적인 GDPR의 적정성 평가 통과를 위해 국내 개인정보보호법을 재정비한 측면도 있다. 문제는 GDPR과는 달리 데이터3법은 개인정보의 산업적 활용은 허용하지만 개인정보의 국외이전에 대한 보호조치는 유명무실하다는 점이다. 여기에는 불가피한 측면도 있다. 한국은 데이터 현지화를 금하고 개인정보를 포함한 데이터의 자유로운 국외이전을 요하는 APEC의 국경 간 프라이버시 규정(CBPR)을 추종하기 때문에 개인정보의 국외이전 규제는 미국과의 통상 마찰로 비화될 수 있다. 하지만 개인정보보호 법제의 최근 추세는 GDPR과 미국 캘리포니아 주의 캘리포니아 소비자 프라이버시 보호법(CCPA)가 보여주듯이 개인정보의 산업적 활용을 용이케 하면서 동시에 개인의 프라이버시 권리도 강화하는 것이다.

통상적 측면에서도 데이터의 국외이전에 대한 제한은 향후 한국의 협상력을 높일 수 있다. 유럽연합의 GDPR은 디지털 주권 개념이 향후 데이터 무역에 확대적용될 것임을 시사한다. 데이터 시장은 데이터의 자유로운 국외이전에 대한 제약으로 인해 향후 무역블록별로 분할될 것으로 예상되며, 유럽의 적정성 평가 같이 상호호혜적 협약을 맺은 국가의 기업들만이 데이터의 자유로운 이전의 혜택을 향유할 것이 확실하다. 만약 국내 개인정보의 조건 없는 국외이전이 가능하다면 구지 한국과 데이터 무역 관련 협상을 할 필요성이 사라지게 된다. 향후 WTO 같이 데이터 무역 부분에서도 다자간 데이터 무역기구(가칭 WDO)가 등장할 경우를 대비해 협상력 제고 측면에서도 개인정보의 국외이전 규제는 절실하다.

안보적 측면에서 개인정보의 무분별한 국외이전은 주변국의 정보전을 용이케 하는 중대한 위협으로 이어질 수 있다. 빅데이터와 관련 분석 기법의 발전은 5천만 한국 국민의 개인 성향에 대한 전수 분석도 이론적으로 가능케 한다. 이미 특정 집단이나 개인에 대한 표적특정 허위정보 캠페인(Targeted Disinformation Campaign)이 벌어지고 있는 상황이다. 2020년 미 대선 직전 러시아 해커 포럼에서 미국 미시건 주, 아칸소 주, 코네티컷 주, 플로리다 주, 노스캐롤라이나 주 유권자의 이름과 생년월일 같은 개인식별정보가 공유되기도 했다.[92] 이는 구글과 페이스북이 사용자 맞춤형 광고를 보여주듯이 해외 해커들이 표적이 된 유권자에게 정교한 피싱 공격부터 투표 방향을 바꾸는 맞춤형 허위정보 공격까지 실행하는 것이 가능함을 의미한다. 개인정보 국외유출이 계속되면 정교한 허위정보 캠페인을 통해 주변국들이 국내 정치에 개입할 수 있는 여지가 커지게 된다. 개인정보의 국외유

92. 보안뉴스. 러시아 해커 포럼에 미국 유권자 개인정보 무료로 공개돼. 2020년 9월 2일. https://www.boannews.com/media/view.asp?idx=90897&kind=14.

출에 무방비로 노출된 한국 사회는 주변국의 허위정보 캠페인에 특히 취약함을 정부와 시민사회는 인식하고 대비해야만 한다.

하지만 앞으로 한국을 괴롭힐 안보위험은 미중 간의 신지정학 갈등으로 인한 경제·기술적 디커플링이다. 이는 단순히 국제 공급망의 붕괴를 넘어 관련 표준과 규범의 이분화를 의미한다. 미국은 포괄적 수출통제체제를 수단으로 삼아 중국기업과 과학기술 생태계를 세계경제에서 분리시키려고 한다. 그 결과 미국에 이어 반도체 시장 세계 2위인 한국 반도체 기업들은 중국기업과의 거래 중단으로 인해 막대한 피해를 입을 것이 자명하다. 경제적 측면에서만 본다면 한국은 미중 갈등에서 중립을 지키는 것이 이성적인 선택이다. 하지만 작금의 미중 갈등이 신지정학적 현상이라는 점을 감안하면 선택은 달라진다.

미국의 대중제재를 단순히 기존 패권국이 경쟁국의 추격을 방해하려 저지르는 "사다리 걷어차기"의 일환으로 치부하면 안된다. 미국에 대한 중국의 도전은 복합적이며 지정학적 면과 첨단기술 면이 융합되어 있다. 중국은 사이버 공간이 가치중립적이지 않다는 점을 잘 인식해 인터넷 초창기부터 강력한 사이버 검열체제를 구축한 국가이다. 중국은 개방된 사이버공간을 중대한 체제위협으로 인식한다. 사실 사이버공간을 뒷받침하는 기술표준에는 중앙집중화를 지양하고 익명성을 보장하는 미국의 자유주의 가치가 충실히 반영되어 있다. 중국의 사이버 전략은 개방된 사이버공간을 국가통제가 가능한 영역으로 탈바꿈하는 것이다. 그래서 중국이 중앙집중적 통제가 가능한 기술표준과 거버넌스 규범을 채택하도록 국제사회에 종용하는 것이다.

중국은 사이버공간을 미국과의 경쟁에서 우위를 점할 수 있는 전략적 영역으로 간주해 전방위적으로 공략하고 있다. 중국이 추진 중인 디지털 실크로드 프로젝트도 이러한 노력의 일환이다. 디지털 실크로드가 성공하면 중국 주도의 기술표준, 국제규범, 첨단기술 등이 바탕이 되어 형성되는 거대한 정치-경제-기술 블록이 출현하게 된다. 현재 일대일로 참여국의 총 합산 인구는 전 세계 인구의 60%, 경제규모는 세계 GDP의 30%에 육박한다. 일대일로 참여국들이 평균적으로 인구는 서방세계보다 젊고 자원은 더 풍부하다는 점을 감안하면 향후 중국이 일대일로 블록을 바탕으로 세계 패권을 쟁취하는 것을 어렵지 않게 예상할 수 있다.

"안미경중"의 대표적인 수혜국인 한국은 미중 간 갈등이 심화되면 가장 큰 피해를 볼 국가 중 하나이다. 그럼에도 불구하고 5G 네크워크 보안성 논란으로 화웨이가 세계시장에서 퇴

출되면 도리어 한국기업에게 반사 이익이 돌아올 것이라는 안이한 시각 또한 존재한다. 이러한 반응은 미중 간의 갈등이 극단적으로 치닫지는 않을 것이라는 희망 섞인 기대가 저변에 깔려 있기 때문이다. 하지만 미중 간의 신지정학적 갈등의 원인은 4차 산업혁명 기술과 사이버 국제규범의 주도권을 쥐는 쪽에서 패권을 독점한다는 위기의식에서 나온다. 이러한 인식은 두 강대국을 실존적 "제로섬" 경쟁으로 내몬다. 이 같은 경쟁에서 안전지대는 없다. 한국은 선택을 해야만 한다.

참고문헌

김대엽, 김영배. 2019. 4 차 산업혁명 시대의 핵심 ICT 기술: 빅데이터, 인공지능, 클라우드 기술 동향. *정보처리학회지*, *26*(1), 7-17.

김미리, 권헌영. 2017. 빅데이터 변화 이후에도 개인 정보의 재산권적 성격은 타당한가? 개인 통제와 명확성. *경제규제와 법*, *10*(2), 223-235.

김상배. 2015. 사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계. *국제지역연구*.

김상배. 2017. 사이버 안보 국제규범의 세계정치: 글로벌 질서변환의 프레임 경쟁. *국가전략*, *23*(3), 153-180.

김소정, 김규동. 2017. UN 사이버안보 정부전문가그룹 논의의 국가안보 정책상 함의. *정치정보연구*, *20*(2), 87-122.

김현경. 2019. '데이터 주권'과 '개인정보 국외이전' 규범 합리화 방안 연구. *성균관법학*, *31*, 587-631.

김현경, 이경준. 2019. EU의 'GDPR 적정성결정'을 위한 입법과제. *성균관법학*, *31*(3), 1-56.

국회입법조사처. 2017. *클라우드 컴퓨팅의 현황과 과제*.

권헌영. 2015. 클라우드 컴퓨팅 서비스와 개인정보보호. *토지공법연구*, *71*, 297-312.

박노형, 정명현. 2014. 사이버전의 국제법적 분석을 위한 기본개념의 연구: Tallinn Manual의 논의를 중심으로. *국제법학회논총*, *59*(2), 65-93.

박지영, 김선경. 2019. 디지털 무역 경쟁과 데이터 보호주의. 이슈브리프. 아산정책연구원.

서봉교. 2019. 미-중 국제금융 헤게모니 경쟁과 중국의 디지털 국제금융 도전. *미래성장연구*, *5*, 35-55.

서의경. 2017. 중국의 개인정보보호 입법에 관한 연구-사이버보안법을 중심으로. *중국연구*, *72*, 131-155.

서종원. 2016. 일대일로와 유라시아 이니셔티브 연계를 통한 북한 교통 인프라 개발전략. *KDI 북한경제리뷰*. 2016년 2월호. 33-46.

신경수, 신진. 2018. 국제사회와 사이버공간의 안보문제. *국제지역연구* 27(3). 27-5

신범식, 윤민우. 2020. 러시아 사이버안보 전략 실현의 제도와 정책. *국제정치논총*, *60*(2), 167-209.

신영웅. 2017. 국가안보에 대한 사이버 위협과 새로운 국제 사이버안전규범의 제안. *국가*

정보연구, *10*(2).

이민호, 박창욱, 김완주, 임재성. 2020. CAAM-국가 수준 사이버 공격 귀속성 모델. *정보과학회논문지*, *47*(1), 19-26.

이상국. 2015. 시진핑 시기 중국의 '강군몽'(强军梦) 구상과 군사안보적 함의. *국방정책연구*, *31*(3), 9-35.

이양복. 2020. 데이터 3 법의 분석과 향후과제. *비교사법*, *27*, 423-465.

이장재. 2018. 제4차 산업혁명의 현상과 분석틀. 한국기술혁신학회 학술대회, 361-380.

이창범. 2016. 한국의 개인정보 국외이전 법제 현황과 개정방향. *법학논총*, *36*(3), 373-409.

연원호, 나수엽, 박민숙, 김영선. 2020. 첨단기술을 둘러싼 미-중간 패권 경쟁 분석. *대외경제정책연구원(KIEP) 오늘의 세계경제*. Vol. 20, No. 18. 2020년 6월 24일.

장필성. 2016. 2016 다보스포럼: 다가오는 4 차 산업혁명에 대한 우리의 전략은?. *과학기술정책*, *26*(2), 12-15.

최경식. 2014. 칼럼 2: 무엇이 중국몽(中國夢) 인가? *군사논단*, *78*, 9-19.

한승조, 신진. 2019. 제4차 산업혁명과 제3차 상쇄전략 추진 시 극복해야 될 군사적 이슈. *융합보안논문지*, *19*(1), 145-152.

Arsène, S. 2012. The impact of China on global Internet governance in an era of privatized control. *Paper presented at CIRC 2012*, available online. http://hal.archivesouvertes.fr/docs/00/70/41/96/PDF/circ_14mai.pdf.

Bailes, A. J. 2007. The Shanghai Cooperation Organization: *SIPRI Policy Paper No. 17*.

Baweja, B., Donovan, P., Haefele, M., Siddiqi, L., Smiles, S. 2016. Extreme automation and connectivity: The global, regional, and investment implications of the Fourth Industrial Revolution. In *UBS White Paper for the World Economic Forum Annual Meeting* (Vol. 18).

Bruni, M. 2019. The Belt and Road Initiative. Demographic trends, labour markets and welfare systems of member countries (No. 300). *GLO Discussion Paper*.

Chang, W. L., & Grady, N. 2015. *NIST Big Data Interoperability Framework: Volume 1, Big Data Definitions. NIST SP-1500-1*.

Chang, H. J. 2002. Kicking away the ladder: An unofficial history of capitalism, especially in Britain and the United States. *Challenge*, *45*(5), 63-97.

Chivvis, C. S. 2017. *Understanding Russian hybrid warfare*. Rand Corporation.

Connell, M., & Vogler, S. 2017. *Russia's Approach to Cyber Warfare(1Rev)*. Center for Naval Analyses.

Coyne, H. 2019. The Untold Story of Edward Snowden's Impact on the GDPR. *The Cyber Defense Review*, *4*(2), 65-80.

Daskal, J. 2015. The un-territoriality of data. *Yale lJ*, *125*, 326.

Fjäder, C. 2014. The nation-state, national security and resilience in the age of globalisation. *Resilience*, *2*(2), 114-129.

Galante, L., & Shaun, E. 2018. Defining Russian Election Interference: An analysis of select 2014 to 2018 cyber enabled incidents. *Washington, Atlantic Council*.

Gerasimov, V. 2016. The Value of Science is in the Foresight. *Military Review*, *96*(1), 23.

Henriksen, A. 2019. The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, *5*(1).

Irwin, D. A. 2002. Interpreting the tariff-growth correlation of the late 19th century. *American Economic Review*, *92*(2), 165-169.

KPMG China. 2017. *Overview of China's Cybersecurity Law*. Available online at: https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

McKune, S., & Ahmed, S. 2018. Authoritarian practices in the digital age| the contestation and shaping of cyber norms through China's internet sovereignty agenda. *International Journal of Communication*, *12*, 21.

Menière, Y. A. N. N., Rudyk, I., & Valdes, J. 2017. *Patents and the Fourth Industrial Revolution: The Inventions Behind Digital Transformation*. European Patent Office.

Morris, L. J., Mazarr, M. J., Hornung, J. W., Pezard, S., Binnendijk, A., & Kepe, M. 2019. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. The RAND National Defense Research Institute.

Mueller, M. L. 2011. China and global Internet governance: A tiger by the tail. *Access contested: Security, identity, and resistance in Asian cyberspace*, 177-194.

Ruhl, C., & Ruhl, C. 2020. Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads. *URL: https://carnegieendowment.org*.

Sanger, D. E. 2012. Obama order sped up wave of cyberattacks against Iran. *The New York Times*, *1*(06), 2012.

Schmitt, M. N. 2012. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal*, *54 (13)*.

Schmitt, M. N. 2012, June. "Attack" as a term of art in international law: The cyber operations context. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*.

Stauffacher, D. 2019. UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes. *Jeju 2019 Peace Forum*. Available online at: https://ict4peace.org/activities/ict4peace-at-the-jeju-peace-forum-how-to-live-with-two-concurrent-un-cybersecurity-processes/.

Trenin, D. 2014. Welcome to Cold War II. *Foreign Policy*, March *4, 2014*. https://foreignpolicy.com/2014/03/04/welcome-to-cold-war-ii/.

Walker, S. 2019. *Cyber-insecurities? A guide to the UN cybercrime debate*. The Global Initiative Against Transnational Organized Crime. Available online at: https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf.

Verizon. 2020. *Data Breach Investigations Report*. Available online at: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

ASAN
REPORT

사이버공간의 신지정학

발행일 2020년 12월
지은이 고명현
펴낸곳 아산정책연구원
주소 (03176) 서울시 종로구 경희궁1가길 11
등록 2010년 9월 27일 제 300-2010-122호
전화 02-730-5842
팩스 02-730-5849
이메일 info@asaninst.org
홈페이지 www.asaninst.org
편집 디자인 EGISHOLDINGS

ISBN 979-11-5570-219-2 93340 비매품