파이브 아이즈 국가의 사이버·데이터 안보전략:
구조적 위치론의 시각

신승휴 (서울대학교 국제문제연구소)

목차

Ⅰ. 서론

최근 미국과 중국의 전략경쟁은 지정학적 무대를 넘어 디지털 기술 분야로까지 확산해 가는 양상을 보이고 있다. 특히 미중 간 디지털 기술패권 경쟁은 5G 네트워크 기술과 데이터 문제를 중심으로 전개되어 오고 있다. 2018년 초 미국이 자국 내에서 중국 통신장비 업체인 화웨이의 제품 사용을 금지하면서 시작된 '화웨이 사태'는 이듬해 미국 주도의 국제적인 화웨이 퇴출 운동으로 이어지면서 미중 갈등의 중심에 자리하게 되었다. 또한, 데이터의 유통과 주권을 둘러싼 문제에서도 역시 데이터의 초국적 이동을 촉진하려는 미국과 개별국가의 데이터 주권 강화를 강조하는 중국이 팽팽하게 맞서고 있다.[1] 이렇듯 미중 경쟁의 무게 중심이 5G 네트워크과 같은 첨단 기술과 데이터 안보 부문으로 빠르게 옮겨가는 가운데 미국은 우방국, 특히 '파이브 아이즈(Five Eyes)'[2] 정보동맹 국가인 영국, 호주, 캐나다, 뉴질랜드에게 화웨이 퇴출과 데이터 공유 확대를 요구하며 반중(反中) 연대에 참여를 강요해왔다.

그런데 이들 4개국은 미국의 핵심 정보동맹국이자 동지국가(like-minded)임에도 불구하고 화웨이 사태와 데이터 안보 문제에 서로 대비되는 입장과 경로를 추구하는 특성을 보여왔다. 먼저 2020년 이전까지 화웨이 장비 사용을 허가하고 이를 자체적으로 관리하겠다는 뜻을 견지해온 영국은 2020년 6월 사실상 화웨이 장비를 완전히 퇴출하기로 하였고, 미국과 함께 화웨이 퇴출에 앞장서 온 호주는 일찍이 자국 5G 네트워크 구축 사업에서 화웨이의 참여를 배제함과 동시에 나머지 파이브 아이즈 정보동맹국에게 입장을 같이할 것을 촉구해왔다. 반면에 화웨이 사태 초기 미국의 요청에 따라 멍완저우(孟晚舟) 화웨이 부회장 겸 최고재무책임자(CFO)를 체포했던 캐나다는 그 이후로 화웨이 장비 배제 결정을 유보하는 모습을 보여왔고, 뉴질랜드의 경우 화웨이에 대한 유연한 관리론을 내세워 완전한 배제도, 완전한 도입도 택하지 않는 모호한 태도를 유지해왔다.

한편, 데이터 안보 문제와 관련하여 영국은 유럽의 데이터 주권을 옹호하면서도 또 한편으론 미국과 데이터 공유 행정협정을 체결하는 모습을 보였고, 호주 역시 자국 정부와 국민의 민감한 데이터 유출을 막고자 데이터 주권 보호를 위한 제도 마련에 힘쓰면서도 미국과의 양자 간 데이터 공유만큼은 허용해왔다. 화웨이 문제에 대해 모호한 입장을 견지해온 캐나다는 데이터 이동 자유화를 지지하며 미국과 뜻을 같이해왔고, 뉴질랜드는 데이터 주권의 중요성을 강조하면서도 관리가 가능한 수준에서 데이터 이동을 허용하는 정책을 펴왔다.

이렇듯 미국의 공조 압박 속에서 비슷한 처지에 놓여있는 이들 4개국이 상이한 외교 행태를 보여온 이유는 단순히 미국의 정보동맹국으로서 이들이 갖는 '고정적 위계구조'에서의 공통된 위치나, 서방 자유민주주의 국가로서 갖는 비슷한 속성만으론 제대로 설명되지 않는다. 또한 호주처럼 대중국 경제 의존도가 높은 국가가 중국과 대립하는 양상을 보인다는 점에서 경제적 상호의존성 역시 이들 4개국 간 대응전략의 차이를 결정짓는 요인으로 보기 어렵다.

---

1) 본 논문에서 말하는 데이터 안보 문제는 개인 차원이 아닌 국가 차원에서 논의되는 데이터의 이동과 주권에 관한 것으로서, 초국적으로 이루어지는 데이터의 유통 문제와 수집된 데이터를 국가 내의 법률 및 거버넌스 구조에 종속하는 데이터 주권(data sovereignty) 문제를 두고 국가들이 벌이는 갈등과 경쟁을 의미한다. 특히 데이터 주권은 국가의 중요 데이터와 클라우드 컴퓨팅 등 데이터 관련 기술 및 산업을 보호하기 위한 데이터 지역화(data localisation)와도 관련이 있다.

2) 파이브 아이즈 정보동맹, 또는 UKUSA 안보협정은 미국, 영국, 호주, 캐나다, 뉴질랜드가 참여하는 영어권 안보협력체로서 주로 이들 국가 간 신호정보(SIGINT) 공유를 목적으로 한다. 1943년 미국과 영국 간 정보 공유를 위해 결성되었고, 이후 캐나다와 호주 그리고 뉴질랜드가 참여하게 되었다. 파이즈 아이즈 정보동맹에 대한 자세한 설명은 리처드슨과 볼(Richardson and Ball, 1990)의 연구를 참고할 것.

따라서 강대국과의 동맹관계에 초점을 둔 현실주의에 입각한 위계적 구조론이나 특정 국가군의 행태, 기질 등에 주목하는 속성론, 또는 경제적 상호의존에 입각한 자유주의 등 전통적인 국제정치이론의 시각에선 이들 국가의 상이한 대응전략을 이해하는 데에 어려움이 따른다.

이러한 문제의식을 반영하여 본 논문은 구조와 행위자를 복합적으로 엮어서 보는 '구조적 위치론'의 시각에서 화웨이 사태와 데이터 안보 문제에 대한 이들 4개국의 대응전략을 비교분석하였다. 이들 네 가지 사례의 상이한 대응전략은 각국이 대미관계, 대중관계, 주변 안보환경, 화웨이와의 관계 그리고 데이터 유통에 관한 국제규범 논의 구조에서 서로 다른 구조적 상황과 위치에 놓여있었기 때문에 비롯된 결과라 할 수 있다. 미국과 중국이 디지털 패권을 두고 경쟁하는 상황 속에서 이들 4개국은 공통적으로 화웨이 퇴출과 데이터 공유를 요구하는 미국의 동료 압박(peer-pressure)과 미중 양자택일의 압박을 받아왔지만, 대미·대중관계와 주변 안보 환경에서 각기 다른 상황적 조건에 놓여있었다. 동시에 화웨이와의 관계와 데이터 유통에 관한 국제규범 논의 구조에서도 각기 다른 상황과 위치에 처해있었다. 이러한 상이한 구조적 상황과 위치가 복합적으로 작용하면서 이들 4개국은 화웨이 사태와 데이터 안보 문제에 서로 대비되는 대응 경로를 추구하게 되었다고 볼 수 있다.

영국, 호주, 캐나다, 뉴질랜드는 파이브 아이즈 정보동맹의 주니어 파트너인가 동시에 대표적인 중견국으로서 강대국에 비해서 '구조'의 영향을 더 많이 받을 수밖에 없는 처지에 놓여있다. 따라서 이들 국가의 행동을 이해하기 위해서는 구조에 대한 좀 더 면밀한 이해가 요구된다. 이 점에서 본 논문은 국가간 관계구도와 상호작용이 만들어내는 구조적 상황과 그 안에서 발견되는 중견국의 구조적 위치에 주목하는 네트워크 이론의 개념적 자원을 원용하였다.[3] 특히, 소셜 네트워크 이론(Social Network Theory)의 '구조' 개념을 원용하여 이들 국가가 화웨이 사태와 데이터 안보를 둘러싼 갈등 국면에서 각각 당면한 구조적 상황과 그 안에서의 구조적 위치를 검토하였다. 여기서 말하는 '구조'는 단순히 행위자들을 상대적 세력의 차원이나 부의 차원을 따라 배치하는 구조가 아니라, 행위자들 간 지속적인 상호작용과 이를 통해 생성되는 관계적 구도(relational configuration)를 의미한다. 소셜 네트워크 이론은 행위자들 간 관계와 연결의 망이 유동적인 형태를 띠면서 행위자들의 행동 영역, 행동의 성격, 그리고 이들이 행사하는 권력의 크기와 형태를 결정한다고 본다.[4] 그에 따라 행위자의 행태를 설명하는 요인들을 상황적인 것으로 보고, 다른 행위자들과 관련되어 있는 각 행위자의 위치에 주목하여 이를 밝혀나간다.

이러한 관점에서 보자면, 중견국의 외교전략은 단순히 행위자의 내재적 속성과 행태에서 비롯된 정책적 결과물이 아닌, 복잡한 세계정치의 구조를 이해하는 상황 지성(contextual intelligence)과 그 안에서 자신의 위치를 파악하는 위치 지성(positional intelligence)을 바탕으로 중견국이 국익을 최대한 확보해나가는 과정이라 할 수 있다.[5] 달리 말해 중견국이 특정 이슈를 중심으로 형성된 네트워크에서 행사하는 외교전략은 해당 중견국이 어떠한 구조적 위치를 차지한다고 인식하는가에 따라 달라질 수밖에 없다. 따라서 중견국 외교전략은 전체 구조와 그 안에서 중견국이 차지하는 위치, 그리고 그러한 위치를 인식하는 중견국의 '자아 정체성'에 대한 복합적인 이해가 요구된다. 중견국의 정체성은 전체적 구조 속에서 자국의 위치에 대한 중견국의 인식을 바탕으로 형성되는 것이다.

---

3) 중견국 외교에 대한 네트워크 이론적 논의는 김상배(2014)를 참고할 것.
4) 전재성, "네트워크 이론의 관점에서 본 북핵 문제와 6자 회담" 『국가안보와 전략』 vol.14, no.2, 2014. p.63.
5) 김상배, 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』. (서울: 한울, 2014), pp. 365-369.

본 논문은 다음과 같이 크게 세 부분으로 구성되었다. Ⅱ장에서는 미중 디지털 패권경쟁과 미국의 디지털 동맹외교의 전개 양상을 살펴보았고, Ⅲ장에서는 파이브 아이즈 4개국이 화웨이 사태와 데이터 안보 문제에 접근한 방식과 그 대응 과정을 살펴보았다. 이어서 Ⅳ장에서는 구조적 위치론의 관점에서 이들 4개국의 사례를 비교분석함으로써 이들 각국이 대미·대중관계, 주변 안보 환경, 화웨이와의 관계 그리고 데이터 유통 규칙을 둘러싼 국제적 논의 구조에서 어떠한 상황과 위치에 놓여있었는지, 그러한 상황적 조건이 각국의 화웨이 사태 및 데이터 안보 대응전략에 어떠한 제약을 가하였는지를 설명하였다.

Ⅱ. 미중 디지털 패권경쟁과 미국의 디지털 동맹외교

파이브 아이즈 4개국의 화웨이 사태와 데이터 안보에 대한 대응전략을 분석하기 위해서는 디지털 영역에서의 미중 경쟁구조와 미국의 디지털 동맹외교의 전개 양상에 대한 이해가 필요하다. 사이버 질서 형성의 주도권과 첨단 디지털 기술 분야에서의 전략적 우위 그리고 데이터 자원을 두고 미중이 벌이는 디지털 패권경쟁은 사이버 공간의 탈지정학적 성격에도 불구하고 양국 간 사이버 공격-방어, 담론경쟁, 연대와 공조 등 지정학적 경쟁의 형태로 발전해왔다.[6] 이러한 상황 속에서 미국의 전략은 중국의 사이버 전력 강화와 공세적 사이버 행위 그리고 디지털 기술발전을 억제하기 위해 오프라인에서의 군사동맹을 사이버 안보 협력 관계로 발전시켜나가는 데 집중되었다. 2017년 트럼프 미국 前 대통령이 APEC 정상회의에서 인도-태평양 구상을 발표하고 본격적으로 중국과의 경쟁에 돌입할 것을 선언한 이후로 미국은 항행의 자유를 원칙으로 하는 규칙기반 질서 확립을 명분으로 세우고 우방국들과의 연대를 통해 사실상 중국을 봉쇄하려는 시도를 벌여왔는데, 이와 마찬가지로 사이버 공간에서도 동맹과 공조를 통해 중국의 영향력 팽창을 억제하려는 노력을 전개해왔다.[7] 예로, 2018년 7월 폼페이오(Mike Pompeo) 당시 미 국무장관은 워싱턴에서 열린 인도-태평양 비즈니스 포럼에서 인도-태평양 전략의 4대 목표 중 하나로 역내 국가들의 디지털 인프라 지원을 위한 '디지털 연계성 및 사이버 안보 파트너십(Digital Connectivity and Cybersecurity Partnership)' 구축을 내걸었는데, 이는 중국의 '일대일로(一帶一路)' 전략의 핵심축인 '디지털 실크로드' 구상을 견제하려는 조치였다.

사이버 공간의 국제규범과 국제제도를 설정하는 문제, 달리 말해 사이버 질서를 구축하는 게임에서도 미국은 전략적 우위를 선점하려는 노력을 보여왔다. 2018년 발표된 『국가사이버전략』에서 미국은 전략 구축의 핵심 원칙 중 하나로 사이버 공간에서의 영향력 증대를 꼽으며, 이를 위해 국가 중심의 인터넷 거버넌스에 반대하는 '다중이해당사자 모델(multi-stakeholder model)'을 내세웠다. 이는 중국과 러시아 등으로 대표되는 비서방·비자유민주주의 진영 국가들이 지향하는 국가중심적 사이버 안보 거버넌스와 상충하는 모델로서 그 이면에는 단연 중국에 대한 견제가 존재한다. 즉, 미국은 사이버 공간에 다중이해당사자

6) 김상배, "사이버 안보와 미중 기술패권 경쟁: 그 진화의 복합지정학," EAI 특별기획논평 시리즈: 미중 경쟁과 세계 정치 경제 질서의 변환 - 기술편, 2019a.

7) Nirmal Ghosh, "Mike Pompeo announces $154m in US initiatives for Indo-Pacific," *The Straits Times,* July 31 2018. https://www.straitstimes.com/world/united-states/pompeo-announces-154m-in-us-initiatives-for-indo-pacific (검색일: 2019.7.5.)

주의에 기초한 안보 거버넌스를 구축함으로써 지정학적 차원에서와 마찬가지로 사이버 질서를 구성하는 경쟁에서도 중국을 따돌리고자 한 것이다.

이러한 맥락에서 미국은 국가중심적 사이버 거버넌스를 추구하는 국가들, 특히 중국이 개방적이고 자유로우며 안정된 사이버 공간을 구축하려는 노력을 와해한다는 인식을 가져왔다. 그러한 인식을 토대로 미국은 중국이 배타적 국익을 추구하는 과정에서 악의적 사이버 활동을 후원함으로써 사이버 안보 환경을 어지럽힘은 물론이거니와 미국과 미국의 우방국들을 직간접적으로 위협한다는 '중국해커위협론'을 펼쳤다. 미국은 2007년 중국 정부가 배후에 있는 것으로 추정되는 해커들이 미국 국방부 전산망을 공격했다고 주장한 바 있으며, 2015년에는 미국 연방 공무원 신상자료에 대한 중국의 대규모 사이버 절도 사건이 있었다고 밝히기도 하였다.[8] 이와 관련하여 당시 미국 재무장관은 미중 전략경제대화에서 중국 고위 관리들에게 미국을 겨냥한 중국의 국가 주도적 대규모 사이버 절도에 대한 우려를 노골적으로 표하기도 하였다.

물론 중국은 미국의 중국해커위협론이 모두 조작된 것이라고 주장하면서 일련의 해킹 사건과 중국 정부의 관련성을 전면 부인해왔다. 더 나아가 자국이야말로 외부적인 사이버 공격의 피해국임을 주장해왔는데, 특히 인터넷과 정보통신 분야에서 오랫동안 기술패권을 장악해온 미국이 중국의 기술발전과 정보주권을 위협한다는 '미국기술패권경계론'을 앞세워 미국의 담론적 공격에 대항하는 모습을 보였다. 사이버 국제질서 구축을 위한 전략에서도 중국은 다중이해당사자 거버넌스를 지향하는 미국과 반대로 국가중심적 시각에서 국가사이버 안보전략을 수립하고 "정보콘텐츠의 정치안전과 인터넷에 대한 검열과 규제를 수행할 수 있는 국가 정책적 권리"를 보장하는 사이버 거버넌스를 구축함으로써 국가 지배력과 국제적 영향력을 강화하고자 노력해왔다.[9]

이러한 상황에서 디지털 안보 분야 미중 간 경쟁과 갈등이 정점에 이르게 된 것은 2018년 초 미국이 자국 내에서 중국 통신장비 업체인 화웨이의 제품 사용을 금지하고 이듬해 국제적 차원에서 화웨이 퇴출 운동을 주도하게 되면서부터이다. 2018년 2월 미국의 주요 정보기관들이 화웨이 제품의 악용 위험성을 경고하고, 그해 8월 미 예산관리국(OMB)이 국방수권법에 따라 화웨이를 미 연방정부 물품 조달 대상에서 배제하면서 시작된 화웨이 사태는 2019년 중반 트럼프 대통령이 민간 기업들에게 화웨이와의 거래 중지를 요구하는 행정명령을 선포하고, 우방국들에게도 화웨이 퇴출 압박을 가하게 되면서 미중 경쟁의 중심에 자리하게 되었다.

2019년 5월 16일 미국은 연방 수출관리규정(Export Administration Regulation, EAR)을 개정하여 화웨이와 그 계열사 68개를 수출 블랙리스트라 할 수 있는 엔티티 리스트(Entity List)에 등재함으로써 자국 정부의 승인 없이는 자국 기업이 반도체를 비롯한 EAR 적용대상 품목을 화웨이에 수출하거나 제3국에서 자국 기업의 기술 및 소프트웨어가 일정 비율(25%) 이상 포함된 외국제품을 화웨이에 수출할 수 없도록 했다. 2020년 5월에 내려진 추가 제재는 여기에 더해 EAR의 일반금지(General Prohibition) 항목에 규정되어 있는 해외 직접생산품 규칙(Foreign produced Direct Product Rule)을 개정하여 화웨이 및 계열사 등 엔티티 리스트 등재 기업에 대한 수출 통제를 대폭 확대하는 내용을 포함시켰다.[10] 미국의 이러

---

8) 성연철, "중국, 미국 공무원 400만명 자료 해킹," 『한겨레』 June 5 2015. http://www.hani.co.kr/arti/international/china/694516.html (검색일: 2019.5.26.)

9) 김상배, "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각," 『국제지역연구』 26권 3호, 2017, pp.83-86.

10) 박영욱, 화웨이 제재를 위한 미국의 법적 조치, KISA Report vol. 9, 한국인터넷진흥원, 2020.

한 행보는 중국 정부가 화웨이의 5G 네트워크 장비에 심어진 백도어(backdoor)를 통해 미국과 그 우방국들의 중요하고 민감한 데이터를 탈취할 위험이 크다는 위협인식을 바탕으로 하였고, 실제로 미국 정부는 화웨이를 실재하는 위협으로 구성하기 위한 안보 담론을 생산하고 이를 기반으로 국제적 차원의 반(反)화웨이 연대를 구축하는 데 주력하였다.

물론 미국의 전략은 화웨이뿐만 아니라 중국 정부와 기업 전체를 대상으로 전개되었다. 2019년 4월 미 상원에서는 북한과 중국 등의 사이버 위협에 대한 인도-태평양 국가들의 공동 대응을 모색하는 '인도-태평양 국가 사이버 리그(CLIPS)' 법안이 발의되었고, 2020년 8월에는 미 행정부가 중국 공산당을 '악의적 행위자(malign actor)'로 규정하고 이로부터 자국민의 개인정보와 기업의 지적재산 등 국가 자산을 보호한다는 목적 아래 '클린 네트워크(Clean Network)'라는 포괄적 사이버 안보 전략구상을 발표하였다. 특히 클린 네트워크는 반중 연대와 동맹을 구축하고자 하는 미국의 전략적 사고가 명확히 드러나는 계기가 되었다. 해당 전략구상은 중국 통신사업자가 미국 통신 네트워크에 접근할 수 없도록 하는 '클린 캐리어(Clean Carrier)'; 미국 모바일 앱스토어에서 신뢰할 수 없는 앱을 삭제하도록 하는 '클린 스토어(Clean Store)'; 미국 기업이 개발한 앱을 중국 스마트폰 업체가 사용할 수 없도록 하는 '클린 앱(Clean Apps)'; 미국 국민의 개인정보와 미국 기업의 지적재산에 대한 외국 기업의 도난을 방지하고, 악의적 공격자가 접근할 수 있는 클라우드 기반 시스템 사용을 피하도록 하는 '클린 클라우드(Clean Cloud)'; 미국의 네트워크와 연결된 해저 케이블이 중국 정부의 대규모 정보 수집 행위에 악용되지 않도록 하는 '클린 케이블(Clean Cable)'; 그리고 미국 외교시설에 송수신하는 5G 네트워크 트래픽에 대한 안전한 경로를 보장하는 '클린 패스(Clean Path)' 등 6개 분야로 세분된다.[11]

클린 네트워크가 발표된 이후로 미국의 대중국 안보화는 더욱 거세졌는데, 2020년 말에 들면서 폼페이오 국무장관은 언론을 통해 중국 공산당을 '약탈자(predator)', '군국주의 깡패(jackbooted thug)', '우리 시대의 주된 위협(central threat of our time)'으로 묘사하며 맹렬히 비난하기 시작하였고, 중국 정부와 기업을 적으로 바라보는 미국의 이러한 시각을 우방국들에 전달하고자 하였다. 동시에 클린 네트워크에 대한 우방국들의 참여를 강력히 요구하였는데, 일례로 2020년 12월 6일 미 의회의 상하원은 '2021 회계연도 국방수권법안(NDAA)'을 발의하면서 해당 법안에 자국 병력이나 군사장비를 해외에 배치할 때 주둔 대상 국가가 화웨이 등 중국 통신기업의 5G 장비를 도입하였는지 여부를 고려하는 조항을 넣었다. 해당 법안에는 '위험을 줄 수 있는 업체'로 중국의 화웨이와 ZTE 등이 명시되었다.[12] 즉 미국의 클린 네트워크 참여 압박은 우방국에게 정부뿐만 아니라 민간기업들까지도 5G 네트워크, 모바일 애플리케이션, 해저 케이블, 클라우드 시스템 등에서 화웨이를 포함한 모든 중국 기업의 제품 및 서비스의 사용을 완전히 배제할 것을 강요하는 것으로서, 이는 당장 우방국이 중국과의 외교관계 악화는 물론이고 경제성이 높은 중국 기업의 제품 및 서비스를 포기하거나 기존에 이미 설치된 제품을 철거함으로써 발생하는 막대한 경제적 손실 역시 감수해야 함을 의미한다는 점에서 우방국들에게 큰 압박으로 작용해왔다.

미국의 디지털 안보 전략에서 또 하나 눈여겨볼 점은 중국을 겨냥한 데이터 안보화 논리이다. 전술한 바와 같이, 미국의 화웨이 배제론은 화웨이를 포함한 모든 중국 기업의 통신장

11) '클린 패스'는 2020년 4월 새롭게 추가된 것이다.; 이승용, "미국과 중국의 5G 사이버보안 최신 정책 동향," KISA Report vol.9, 한국인터넷진흥원, 2020년 9월.

12) 유재동, 이건혁, 美의회 '미군 해외배치때 화웨이 사용여부 고려', 『동아일보』 2020년 12월 7일. https://www.donga.com/news/Inter/article/all/20201207/104314856/1 (검색일:2021.5.3.)

비가 자국의 중요하고 민감한 데이터 유출의 원인이 될 수 있다는 안보적 논리에 기반한 것이었다. 이러한 논리는 중국 기업 바이트댄스의 동영상 공유 플랫폼 '틱톡(TikTok)'을 둘러싼 갈등에도 그대로 적용되어 2020년 8월 1일 트럼프 행정부는 틱톡이 미국 내 사용자 개인정보를 중국 정부에 제공할 수 있다는 안보적 이유로 틱톡 사용을 금지하는 행정명령을 내리기도 하였다. 미국이 클린 네트워크 전략구상에 자국민의 개인정보와 자국 기업의 지적재산 등 중요 데이터가 중국 기업의 클라우드 시스템에 저장되는 것을 방지하는 '클린 클라우드' 조치를 포함시킨 것 역시 이 같은 데이터 안보화 논리에서 비롯된 것이다.

그러나 한가지 짚고 넘어갈 점은 미국의 데이터 안보화, 또는 데이터 보호주의는 클라우드 기술에 대한 의존도가 빠르게 증가하는 상황을 고려하여 중국이 빅데이터 경쟁력이 강화되는 것을 견제하기 위한, 어디까지나 '중국만을 겨냥한' 조치라는 사실이다. 오히려 데이터 안보에 대한 미국의 기본적인 입장은 '프라이버시에 영향을 미치는 아주 민감한 분야를 제외하고는 데이터의 초국적 이동을 자유롭게 하자는 것'으로서 '글로벌 차원에서 데이터의 가치를 극대화하려는 미국 다국적 기업들의 이해관계를 대변'한다.[13] 이는 데이터 현지화나 보호주의에 반대하는 입장으로서 개별국가의 자주적인 데이터 관리권을 옹호하는 중국의 입장과 상충한다. 미국은 2019년 6월 오사카 G20 정상회의에서 일본과 함께 초국적 데이터 유통 담론을 강화하기 위해 '오사카 트랙'을 제안하였고, 2020년 7월 1일 멕시코, 캐나다와 체결한 USMCA 무역협정에 '국경 간 자유로운 데이터 이동 및 서버의 설치'에 대한 규정을 포함하는 등 데이터의 초국적 이동 자유화와 데이터 지역화 금지를 디지털 통상의 국제 표준으로 추진하려는 노력을 꾸준히 전개해오고 있다.

한편, 2018년 3월 미국은 자국 사법기관이 테러리즘을 포함한 심각한 중범죄의 예방, 탐지, 수사, 기소 등 합당한 이유가 있을 때 자국 영내나 해외에 저장된 자국 기업의 데이터를 합법적으로 요구할 수 있도록 하는 <클라우드법(Clarifying Lawful Overseas Use of Data Act, CLOUD)>을 통과시킴으로써 역외 데이터에의 접근에 대한 법률적 근거를 마련하였다. 해당 법에는 외국 정부가 미국과 행정협정을 체결할 경우 그 국가의 정부기관이 미국 기업에 데이터를 직접 요청할 수 있도록 하는 규정 역시 포함되었다. 미국의 이러한 조치는 일차적으로 자국의 역외 데이터 접근권한을 강화하고, 나아가 신뢰할 수 있는 우방국들과의 국제적사법공조를 위한 데이터 공유를 증진하려는 의도에서 비롯된 것이라 할 수 있다. <클라우드법>은 미국 정부가 자국 기업에 데이터 접근을 요청하는 과정에서 외국의 법률을 위반할 소지가 있거나 데이터 접근의 대상자가 미국인이 아닌 경우, 해당 기업이 미국 정부의 데이터 접근요청을 거부하거나 조정할 수 있다는 조항을 포함하고 있는데, 본 조항의 적용 대상국이 '자격을 갖춘 외국 정부(qualifying foreign government)'에 국한된다는 점에서 이러한 자격을 갖추지 못한 외국 정부는 자국민 데이터에 대한 미국의 광범위한 접근을 제지하는 데 어려움을 겪을 수밖에 없다.[14] 이 점에서 <클라우드법>은 미국의 우방국들에게 미국과의 데이터 공유 강화를 강요하는 법제적 장치로 작동하게 되면서 또 다른 디지털 안보 연대의 압박을 가해왔다.

---

13) 김상배, "미중 데이터 규범경쟁과 한국: 유럽연합의 '데이터 주권론'이 주는 함의," EAI 특별기획논평 시리즈, 동아시아연구원, 2019b년 10월 28일.

14) 송영진, "미국의 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점," 『형사정책연구』 29권 2호, 2018. pp.159-160.

Ⅲ. 화웨이 사태와 데이터 안보에 대한 파이브 아이즈 국가의 대응

1. 영국: '화웨이 배제 결정'과 '데이터의 관리된 유통 모색'

화웨이에 대한 영국의 초기 입장은 경제적 이해관계와 외교안보적 이해관계 사이에서 균형을 모색하는 방향으로 설정되었다.[15] 영국은 5G 네트워크 기술과 관련하여 2010년대에 이미 경제성이 높은 화웨이의 장비를 '필요악'으로 간주하고 이를 도입함으로써 화웨이가 자국 통신망 시장에서 주도적인 위치를 점하는 것을 사실상 용인하였다. 2018년 7월 영국의 화웨이 사이버보안평가센터(Huawei Cyber Security Evaluation Centre)가 화웨이 장비의 보안 문제를 지적하는 보고서를 발표하면서 국내적으로 화웨이 배제 필요성이 대두되기도 하였지만, 그 이듬해인 2019년 2월 영국 국가사이버보안센터(National Cyber Security Centre)가 5G 네트워크에 화웨이 장비를 사용하더라도 보안 위험을 완화하고 관리할 방법이 있다고 발표함으로써 화웨이에 대한 영국의 수용적 입장은 크게 바뀌지 않았다.[16]

그러나 이러한 입장은 2018년부터 조금씩 변화의 조짐을 보이기 시작하였는데, 2018년 10월 영국 정부는 정보통신 공급망에 대한 포괄적 검토에 착수해 2020년 1월 고위험 공급업체(high-risk vendor)에 관한 정부 지침을 최종적으로 발표하였다.[17] 이 조치는 화웨이 장비를 전면 배제하진 않더라도 네트워크를 핵심(core)과 가장자리(periphery)로 구분하고 후자에만 화웨이를 제한적(가장자리 네트워크의 35%)으로 용인함으로써 자국 통신기업의 손해를 가능한 한 최소화하려는 의도가 반영된 것이었다. 그리고 2020년 7월 14일 영국 정부는 자국 통신업체가 2020년 12월 31일부터 화웨이의 5G 네트워크 장비를 구매할 수 없도록 하고, 2027년까지 자국 5G 네트워크에서 화웨이 장비를 완전히 퇴출하기로 결정하였다.[18]

한편, 데이터 안보 문제에 대한 영국의 대응은 큰 틀에서 유럽연합의 데이터 주권론에 발을 맞추는 방식으로 전개되어왔다. 영국은 2018년 5월 25일부터 유럽연합의 <일반개인정보보호법(General Data Protection Regulation, GDPR)>과 자국의 <데이터보호법(Data Protection Act 2018)>[19]을 시행해왔다. 2018년 5월 시행된 GDPR은 유럽연합 회원국 간 개인정보의 자유로운 이동을 보장하고 정보주체인 개인의 개인정보보호 권리를 강화하는 한편 자국민 데이터의 해외서버 이전은 엄격히 제한하고자 제정된 통합 규정이다. GDPR은 데이

---

15) 전혜원, "영국의 화웨이 정책: 관리에서 퇴출까지," 서울대학교 국제문제연구소 이슈브리핑, 121호, (2021.1.20.), pp. 1-2.

16) 영국 정부는 2010년부터 NCSC와 HCSEC를 통해 화웨이를 집중적으로 감시하는 맞춤형 보안 전략을 실행함으로써 그 잠재적 위험을 관리할 수 있다고 자신하였고, 그러한 맥락에서 자국 네트워크에 화웨이 장비를 사용하더라도 정보동맹국들과 민감한 정보를 공유하는 데에 문제가 없다고 주장하였다.; House of Commons, 'The Security of 5G', Defence Committee, Second Report of Session 2019-21, HC 201, October 8, 2020, p. 4, https://committees.parliament.uk/publications/2877/documents/27899/default/ (검색일: 2021.4.25.)

17) 전혜원, 2021, pp. 4-5.

18) National Cyber Security Centre, *Summary of the NCSC analysis of May 2020 US sanction,* December 14, 2020. https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction (검색일: 2021.5.2.)

19) 1998년 제정된 영국의 정보보호법은 민감한 개인정보보호를 위한 기본법으로 몇 차례 개정을 거쳤고 가장 최근으로는 2018년 12월 17일 개정되었다. 정보보호법은 보호대상 개인정보 및 기타, 개인정보 관리자의 통보의무, 국가보안, 범죄 및 과세, 보건 교육 및 사회적 작업, 언론 문학 및 예술 관련 개인정보보호 예외 조항, 개인정보보호 효력 등에 대해 규정하고 있다(한국인터넷진흥원 2019).

터의 국외이전을 유럽연합 회원국 또는 적정성 평가를 통과한 제3국에게만 허용하는 등 유럽시민의 데이터 주권 보호를 강조하고 있는데, 이러한 맥락에서 최근 프랑스와 독일 등 주요 유럽연합 국가들은 미국의 대형 IT기업들의 데이터 독점에 대항하는 차원에서 '유럽형 클라우드 서비스' 구축과 데이터 현지화를 추진하는 등 디지털 보호주의적 행보를 보여왔다.[20]

2020년 1월 31일 공식적으로 유럽연합을 탈퇴(BREXIT, 이하 '브렉시트')한 영국은 데이터 안보와 관련해서는 브렉시트 이후에도 자국의 <데이터보호법>에 GDPR을 흡수하겠다는 뜻을 밝혔고, 그에 따라 국내법이 GDPR과 유사한 수준의 데이터 보호를 시행하도록 수정에 착수하였다. <브렉시트 협정법안(EU Withdrawal Agreement Bill)>에 따라 영국은 GDPR 제5장의 목적하에서 사실상 제3국이 되었기 때문에 데이터 국외이전에 관한 적정성 평가를 받게 되었고, 2021년 2월 19일 유럽위원회(European Commission)는 영국이 유럽연합 차원의 개인정보 보호수준을 충족한다는 적정성 결과 초안(draft data adequacy decisions)을 발표하였다.[21] 아직 최종 결과는 발표되지 않았지만, 영국이 유럽연합과의 자유로운 데이터 이동을 유지하는 것이 국익에 부합하다고 판단하고 있고 또 유럽위원회의 적정성 결과 초안 역시 영국의 데이터 보호수준을 적정하다(adequate)고 평가한 만큼 앞으로도 양자 간 데이터 국외이전은 유지될 가능성이 크다.

영국의 데이터 안보전략에서 또 하나 눈여겨볼 점은 미국과 데이터 공유를 강화하려는 움직임이다. 미국의 <클라우드법>이 통과되고 약 1년 뒤인 2019년 2월 영국은 중대범죄수사청(Serious Fraud Office)이 협정체결국 내에 저장된 해외 데이터에 접근할 수 있도록 하는 <크라임법(Crime(Overseas Production Orders, COPOA))>을 통과시켰다. 그리고 그해 10월 3일 미국과 영국은 데이터 공유 행정협정을 체결함으로써 양국이 광범위한 데이터를 더 신속하게 상호 공유할 수 있게 되었다.

2. 호주: '화웨이 배제 결정'과 '데이터의 관리된 통제 모색'

일찍이 2011년부터 자국의 4G 네트워크에 화웨이 장비를 상당수 사용해왔던 호주는 2018년 8월 23일 외국 정부의 영향을 받을 가능성이 있는 통신장비업체의 5G 장비 도입을 금지할 것을 선언하였다. 이는 미국의 트럼프 대통령이 자국 공공기관의 화웨이 및 ZTE 장비 사용을 금지하는 내용이 포함된 국방수권법에 서명한 뒤 단 10일 만에 내려진 조치로서, 사실상 화웨이와 ZTE를 호주의 5G 네트워크 구축사업에서 전면 배제하는 것을 의미했다. 턴불(Malcolm Turnbull) 당시 호주 총리는 이러한 결정이 중국 통신기업이 중국 정부의 사이

---

20) 예로, 독일의 메르켈(Angela Merkel) 총리는 2019년 11월 독일 고용주협회컨퍼런스에서 "유럽연합(EU)이 독자적인 데이터 플랫폼을 개발해 구글, 마이크로소프트, 아마존 등 미국 대형 IT기업들의 클라우드 서비스에 대한 의존도를 낮춰야한다…너무 많은 기업이 자사의 모든 데이터를 미국 기업에 아웃소싱하고 있다…데이터에서 만들어지는 부가가치 상품들이 미국에 의존해 만들어지는 게 좋은지 확신할 수 없다"며 미국 기업으로부터 유럽 데이터 주권을 보호해야 한다고 주장한 바 있다. 프랑스 역시 2019년 10월 독일과 함께 유럽 내 데이터를 이용, 수집, 공유할 수 있는 클라우드컴퓨팅 인프라의 자체적 개발을 추진하는 '가이아-X' 프로젝트에 착수할 것을 발표하기도 하였다.; 진영화, "메르켈 '유럽, 실리콘 밸리에 데이터 주권 빼앗겨선 안돼'," 『매일경제』 2019년 11월 13일. https://www.mk.co.kr/news/world/view/2019/11/940146/ (검색일: 2021.5.6.)

21) UK Department of Digital, Culture, Media & Sport, "UK government welcomes the European Commission's draft data adequacy decisions," Government of the United Kingdom, February 19, 2021. https://www.gov.uk/government/news/uk-government-welcomes-the-european-commissions-draft-data-adequacy-decisions (검색일: 2021.5.8.)

버 공격 및 탈취 수단으로 이용될 위험이 크다는 자국 신호정보국(Australian Signals Directorate, ASD)의 조언을 바탕으로 한 것이라고 밝혔다. 실제로 2018년 초 호주 정부는 국가 5세대 통신망이 공격받을 시 발생할 수 있는 위협을 측정하기 위해 ASD 소속 전문 해커들과 함께 사이버 공간에서의 모의전(war game)을 시행하였는데, 모의전에 임했던 해커들은 자신들이 행한 비슷한 수준의 사이버 공격이 호주의 5G 네트워크에 가해질 경우, 모든 주요 기반시설이 마비되어 국가적 피해가 엄청날 것이라는 보고를 올렸다.[22]

이렇듯 국가안보상의 이유로 파이브 아이즈 국가 중 가장 먼저 전면적인 화웨이 퇴출을 선언한 호주는 나머지 정보동맹국들에게도 중국 통신장비업체의 5G 네트워크 장비 사용을 배제할 것을 강력히 요구하였다. 일례로 턴불 총리는 퇴임 이후인 2019년 3월 영국을 방문하여 가진 연설에서 "호주는 이러한 (화웨이 퇴출) 결정을 내린 첫 번째 국가이다. 우리가 이러한 결정을 내린 것은 우리 스스로 주권을 지키고 변화에 대비하기 위함이다…영국이 (화웨이에 대한) 결정에 앞서 여전히 고민 중인 것으로 아는데, 나는 영국 신호정보국이 (화웨이 장비의 보안문제와 관련해) 우리와 일치한 견해를 드러냈다는 사실에 놀라지 않았다" 면서 영국의 동참을 촉구하였다.[23] 또한, 그는 트럼프 대통령에게 "안전한 5G 공급업체가 최소한 한 곳이라도 미국이나 파이브 아이즈 동맹국들에 있어야 한다"면서 미국이 우방국들과 협력하여 5G 네트워크 기술 개발에 앞장서 줄 것을 요구하기도 하였다.[24]

화웨이 사태에 대한 대응에서와 마찬가지로 데이터 안보 문제에도 역시 호주는 위협차단과 동맹관계 강화를 최우선으로 하는 접근방식을 취해왔다. 먼저, 호주의 데이터 안보전략은 데이터에 대한 중앙정부의 접근권한을 강화하고, 국가적 차원에서 중요한 데이터의 국외이전을 철저하게 통제하는 것을 지향하는 방향으로 추진되어왔는데, 대표적인 예로 호주 정부는 데이터 접근권 강화를 위해 2018년 12월 정부 기관이 민간기업들에 사용자 메시지 데이터의 암호화 해제를 강제할 수 있도록 하는 <지원및접근법(Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018)>을 제정하였다. 이 법은 정보기관과 법 집행기관이 국가안보적 필요에 따라 통신 서비스 제공업체의 암호화된 통신 메시지에 언제든지 접근할 수 있도록 '암호화 백도어(encryption backdoor)' 설치를 강제하는 규정을 담고 있는데, 이는 통신의 암호화가 안전한 온라인 환경에 필수적이기도 하지만 동시에 사이버 공간에서 국가안보를 위협하는 외부 세력 및 범죄 조직의 수단으로 악용되기도 한다는 정부의 판단에서 비롯된 것이었다.[25]

한편, 호주 정부는 자국의 데이터 주권을 강화하기 위한 제도적 장치 마련에도 힘써왔는

---

22) Cassell Bryan-Low and Colin Packham, "How Australia led the US in its global war against Huawei," *The Sydney Morning Herald,* May 22, 2019. https://www.smh.com.au/world/asia/how-australia-led-the-us-in-its-global-war-against-huawei-20190522-p51pv8.html (검색일: 2019.5.30.)

23) Malcolm Turnbull, "Address to the Henry Jackson Society, London," The Hon Malcolm Turnbull's official website, March 5, 2019a. https://www.malcolmturnbull.com.au/media/address-to-the-henry-jackson-society-london (검색일: 2021.6.7.)

24) Malcolm Turnbull, "Malcolm Turnbull warns Brits about letting Huawei build 5G network," *The Sydney Morning Herald,* March 6, 2019b. https://www.smh.com.au/world/europe/malcolm-turnbull-warns-brits-about-letting-huawei-build-5g-network-20190306-p5120s.html (검색일: 2021.6.10.)

25) Australian Department of Home Affairs, "The Assistance and Access Act 2018," Commonwealth of Australia, September 16, 2019a. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption (검색일: 2019.11.11.); 암호화 백도어란, 모바일 기기, PC, 클라우드 서버 등에 저장된 사용자 데이터를 인위적으로 빼돌릴 수 있도록 하는 프로그램을 의미한다.

데, 2020년 7월 로버트(Stuart Robert) 정부서비스 장관은 호주 정부가 민감한 데이터의 국외 유출을 방지하고자 해당 데이터를 호주 영내 데이터 센터에만 보관하게끔 강제하는 새로운 데이터 주권 규칙을 발표하였다. 해당 규칙에 따르면, 보건·인구통계자료 등 민감한 데이터의 경우 외국에서 접근이 불가하도록 신호정보국(Australian Signals Directorate)이 인증한 클라우드 서버에 저장해야 하며, 물리적으로 데이터를 저장할 때는 호주 영내에 설치된 데이터 센터를 이용해야만 한다.[26] 이는 내각 차원에서 높은 수준의 보안을 요구하는 데이터만을 자국 영내 클라우드 서버에 저장·관리하도록 했던 기존의 조치에서 한 단계 더 강화된 조치라 할 수 있다.

그런데 호주와 미국 간 데이터 공유만은 빠른 속도로 강화되었는데, 2019년 10월 호주 정부는 미국과 데이터 공유 행정협정에 대한 공식 협상을 시작하였고, 2020년 5월 5일 행정협정 체결을 위한 통신법 개정안을 발표하였다. 일명 <IPO법안(International Production Orders Bill)>으로 알려진 이 개정 법안은 미국과의 행정협정을 체결하기 위한 선결 조건으로서 타국과의 통신 데이터 공유 조건을 완화하고, 전자통신서비스 사업자에 정부의 데이터 접근 등과 관련해서 기술적 지원 등을 의무화하기 위한 목적으로 추진되었다.[27] 호주는 <클라우드법> 행정협정 체결과 이를 위한 <IPO법안> 통과가 자국의 안보 증진과 미국과의 동맹관계 강화라는 두 마리 토끼를 모두 잡는 데에 유익하다고 판단하고 있는 것으로 보이는데, 일례로 행정협정 협상을 주도한 더튼(Peter Dutton) 호주 내무부(Department of Home Affairs) 장관은 첫 번째 협상이 이루어진 날 성명을 통해 <클라우드법>이 "동지국가들이 앞으로 나아가야 할 방향"이라고 말하며 궁극적으로 호주의 국익에 부합함을 강조하였다.[28]

3. 캐나다: '화웨이 배제 유보'와 '데이터의 관리된 유통 모색'

파이브 아이즈 국가 중 미국과 가장 지리적으로 가까운 위치에서 가장 밀접한 문화·경제적 관계를 맺고 있는 캐나다는 다중이해당사자주의에 입각한 사이버 안보 거버넌스 형성과 정보의 자유로운 흐름을 지향하는 등 큰 틀에서만큼은 미국과 발을 맞춰왔다. 그러나 화웨이를 둘러싼 문제에 있어서만큼은 중도적인 태도를 고수하며 미국의 화웨이 퇴출 요구를 선뜻 받아들이지 않는 모습을 보여왔다. 2018년 7월 화웨이 제재를 논의하기 위한 파이브 아이즈 동맹국 정보기관장 회동이 캐나다 북동부 노바스코샤주의 주도 핼리팩스에서 열리고 약 석 달이 지난 12월 1일, 캐나다 정부는 미국의 요청에 따라 멍완저우 화웨이 부회장을 체포하였다. 이 사건은 캐나다가 중국과의 갈등을 무릅쓰고 미국의 대화웨이 공조체제에 적극 참여하게 될 것이라는 전망을 낳았다. 하지만 캐나다 정부는 멍완저우 부회장 체포 이후에도 그 전과 마찬가지로 화웨이에 대한 직접적인 입장을 표명하지 않은 채 자국 5G 네트워크 구축 사업에 대한 화웨이의 참여 가능성을 열어두었다. 멍완저우 체포 사건 직후 중국이 캐나다 출신 전직 외교관과 대북 사업가를 국가안보법 위반 혐의로 체포하고, 2019년 1

---

[26] Tom Burton, "Sensitive data to remain in Australia," *Australian Financial Review.* July 6, 2020. https://www.afr.com/policy/foreign-affairs/sensitive-data-to-remain-in-australia-20200706-p559kn (검색일: 2021.2.27)

[27] 한국인터넷진흥원, "미-호주 간 클라우드법 행정협정 체결 이슈," 2020년 5월, p. 4.

[28] Australian Minister for Home Affairs, "Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton," Commonwealth of Australia, October 7, 2019b. https://minister.homeaffairs.gov.au/peterdutton/Pages/australian-negotiation-cloud-act.aspx (검색일: 2021.5.8.)

월 캐나다인에게 마약 밀매 혐의로 사형을 선고하는 등 보복을 가했음에도 화웨이 5G 장비에 대한 캐나다 정부의 뚜렷한 태도 변화는 나타나지 않았다.

2020년 7월 영국이 자국 5G 네트워크에서 화웨이 장비를 전면적으로 퇴출하기로 한 결정을 발표하자 캐나다의 유보적인 입장은 다시 한번 압박을 받게 되었다. 영국이 미국, 호주와 함께 반화웨이 전선에 서게 됨에 따라 캐나다가 파이브 아이즈 정보동맹 내부적으로 압박을 받게 될 것이며, 따라서 화웨이를 퇴출할 수밖에 없을 거라는 전망이 제기되었다.[29] 캐나다 내 반화웨이 정서가 증대하는 현상 역시 이러한 전망에 힘을 실었다.[30] 이처럼 화웨이가 캐나다 국민에게 5G 네트워크 공급업체로서 환영받지 못함이 분명한 상황에도 불구하고 캐나다 정부의 화웨이 퇴출 결정은 내려지지 않았다. 오히려 변화의 조짐은 캐나다 통신사들을 중심으로 발견되었다. 2020년 들어 캐나다 주요 통신사들은 자사 5G 장비 공급업체로 화웨이가 아닌 노키아나 에릭슨과 같은 유럽 업체를 선택하는 모습을 보였다. 2020년 6월에 발표된 바에 따르면, 캐나다 1위 통신사 벨캐나다(BCE)는 에릭슨을 5G 장비 공급업체로 선정하였고, 2위 업체인 텔러스(Telus Corp.)는 에릭슨과 노키아의 장비를 공급받아 5G 네트워크를 구축하기로 하였다. 이미 4G 네트워크에 화웨이 장비를 사용해왔던 이들 통신사는 화웨이의 5G 장비 도입을 배제함으로써 막대한 장비 교체 비용을 감당해야만 하는 상황이었고, 특히 텔러스는 2020년 2월까지만 해도 화웨이 장비를 사용하겠다는 뜻을 밝혀왔다는 점에서 주목할만한 변화였다.[31]

한편 화웨이 사태에 중도적인 태도로 일관해온 캐나다는 데이터 안보 문제에 있어서만큼은 미국과 함께 데이터의 자유로운 이동을 지향해왔다. 2020년 7월 캐나다는 기존의 북미자유무역협정을 대체하는 차원에서 미국, 멕시코와 USMCA 협정을 체결하였는데, 데이터 안보와 관련하여 주목할 점은 이 협정에 데이터 현지 저장 요건 부과를 금지하는 규정이 포함되었다는 점이다. 이는 중국과의 ICT분야 경쟁에서 우위를 장악하기 위해 데이터의 초국적 이동 자유화와 데이터 지역화 금지를 디지털 통상의 국제 표준으로 추진하려는 미국의 의도가 반영된 결과로서 캐나다 역시 데이터 현지화에 반대하는 미국 주도 진영에 서 있음을 보여주는 계기가 되었다.[32] 사실 캐나다는 USMCA 체결 이전에도 포괄적·점진적 환태평양경제동반자협정(CPTPP) 회원국으로서 CPTPP에 명기된 비슷한 데이터 현지화 금지 규정을 준수해왔는데, USMCA를 통해 데이터 현지화 금지를 더욱 강력히 강제하게 된 것으로 평가된다. 실제로 캐나다는 CPTPP의 데이터 현지화 제한 규정을 준수하면서도 정당한 공공정책 목표에 따라 예외적으로 이를 허용하는 정책적 유연성을 지켜왔지만, 이러한 유연성을 배제한 USMCA를 체결함으로써 철저하게 데이터 현지화를 금지하게 되었다는 분석이 존재한다.[33]

---

29) Ian Young, “Canada faces new pressure to block Huawei from 5G, after UK ban risks marooning Ottawa from Five Eyes intelligence allies,” *South China Morning Post,* Jul 15, 2020, https://www.scmp.com/news/china/diplomacy/article/3093198/canada-faces-new-pressure-block-huawei-5g-after-uk-ban-risks (검색일: 2021.5.6.)

30) 2020년 5월 캐나다 국민을 대상으로 시행된 한 설문조사 결과에 따르면, 1,518명의 응답자 중 78%가 화웨이를 퇴출해야 한다는 데 찬성했다. 이는 그 전년 11월 시행된 설문조사 결과보다 무려 9%나 더 오른 수치였다. 또 다른 기관이 실시한 조사에서도 비슷한 수치인 75%의 응답자가 화웨이 퇴출에 찬성한다는 뜻을 밝혔다.; Young, 2020.

31) 유인태, “파이브 아이즈 캐나다의 화웨이 사태 대응 전략: ‘결정 부재의 결정’,” 서울대학교 국제문제연구소 이슈브리핑, 122호, (2021.1.20.), p. 4.

32) KOTRA, “USMCA 발효에 따른 산업별 영향 및 시사점,” Global Market Report 20-012, 2020년 6월.

33) Michael Geist, “How Canada Surrendered Policy Flexibility for Data Localization Rules in the USMCA,” Personal website, October 10, 2018.

데이터 유통에 대한 캐나다의 지지는 국내적 차원의 제도를 마련하는 과정에서도 나타났다. 2020년 11월 17일 캐나다 하원에서는 <민간부문 개인정보보호 법제 개편을 위한 법안(Bill C-11)>이 제출되었는데, 개인정보보호에 관한 민간부문 법제에 해당하는 <소비자 개인정보보호법(CPPA)> 제정을 위한 이 법안 역시 데이터 이동권을 지지하는 방향으로 마련되었다. 해당 법안은 디지털 기술의 발전이 급격하게 이루어지는 환경에서 정보주체의 권익과 개인정보보호를 강화한다는 목적하에 '정보주체가 자신의 개인 데이터를 안전한 방식으로 한 조직에서 다른 조직으로 자유롭게 이동할 수 있도록 데이터 이동권'을 보장하는 내용을 담고 있다.[34]

물론 연방정부가 데이터의 자유로운 이동을 지향한다고 하여 민감한 데이터의 국외 유출을 우려하지 않은 것은 아니다. 2018년 발표된 「데이터 주권과 공공 클라우드」 백서에서 캐나다 정부는 공공부문의 업무혁신과 디지털 산업 부문 경쟁력 강화를 위해 클라우드 환경에 의존할 수밖에 없는 상황에서 민감한 정부 관련 데이터가 외국 정부에 유출될 가능성과 그에 따른 국익 손실이 발생할 수 있음을 명기하였다. 특히, 자국의 데이터 주권에 대한 위협으로 미국의 <국외정보감시법(Foreign Intelligence Surveillance Act)>과 정보 수집 능력 그리고 미국-캐나다 간 정보공유협약을 꼽으며, 미국이 캐나다 정부에 통보하지 않고도 자국 데이터에 접근할 수 있는 현실에 주목하였다.

그럼에도 캐나다 정부는 기본적으로 데이터 현지화가 경제적 이해관계에 부합하지 않다는 인식하에 이를 배제해야 한다는 입장을 고수하고 있는 것으로 보인다. 이는 테리엔(Daniel Therrien) 캐나다 개인정보보호위원회(Office of the Privacy Commissioner of Canada) 위원장의 발언에서 잘 드러난다. 2020년 6월 퀘벡주는 기업이 주외(州外)로 데이터를 이전할 시 사전에 주정부에 프라이버시 영향평가서를 제출하게끔 강제하는 법안('개인정보보호 법제의 현대화를 위한 개정안', 이하 'Bill 64')을 발표하였는데, 그해 9월 퀘벡주의회 제도위원회와 Bill 64 개정안을 주제로 가진 화상회의에서 테리엔 위원장은 다른 제도권 간 데이터 보호법의 상호 운용성이 중요하다고 역설하며 "캐나다와 퀘벡주는 유럽과 미국의 주요 경제 파트너이다. 우리가 파트너들과 대체로 공유하는 권리와 가치를 침해하지 않으면서 무역을 위한 데이터가 국경을 넘어 이동하는 것은 필수적"이라고 말하였다.[35]

4. 뉴질랜드: '화웨이 배제 유보'와 '데이터의 관리된 통제 모색'

화웨이 사태 초기에 뉴질랜드는 미국의 화웨이 퇴출 공조에 대한 자국의 참여를 부인하는 한편 화웨이 문제를 정부 차원에서 다루지 않으려는 모습을 보였다. 2018년 11월 리틀(Andrew Little) 뉴질랜드 정보기관 책임장관은 화웨이 문제에 대해 "뉴질랜드는 자체 계획을 수립할 것이며, 정부는 (뉴질랜드 내 주요 통신기업인) 스파크(Spark), 보다폰(Vodafone NZ), 2디그리스(2degrees)가 그들의 5세대 네트워크 기술 향상을 위한 기술제공업체를 선정

---

https://www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/ (검색일: 2021.5.9.).

34) 한국인터넷진흥원, "캐나다 소비자 개인정보보호법(CPPA) 제정 배경 및 주요 특징 분석," 『해외 개인정보보호 동향보고서』 2020년 11월, p. 4.

35) Office of the Privacy Commissioner of Canada, "Appearance before the Committee on Institutions of the National Assembly of Quebec regarding Bill 64, An Act to modernize legislative provisions as regards the protection of personal information," September 24, 2020. https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200924/ (검색일: 2021.5.10.)

하는 과정에 개입하지 않을 것"이라고 밝혔다.[36] 또한, 그는 기술제공업체 선정은 자국 내 기업들이 뉴질랜드의 <전자통신(감청 및 보안)법안 (Telecommunications (Interception Capability and Security) Act, TICSA>'을 준수하여 내릴 상업적 결정이라는 점을 분명히 하였다.[37]

그러나 뉴질랜드 정부는 2018년 말 자국 통신기업 스파크가 새로운 통신망에 화웨이 장비를 사용하려는 계획을 발표하자 국가안보상의 이유로 이를 불허하였는데, 이에 대해 당시 리틀 장관은 해당 장비에 대해 정부통신보안국이 조사를 진행한 결과 해당 장비가 국가안보에 심각한 위협이 될 수 있다고 여겨져 사용을 불허하게 되었다고 밝혔다. 그러면서도 그는 만약 스파크가 해당 장비 사용을 계속 원할 시 정부통신보안국과의 협력하에 위협을 완화하는 방법을 모색해나갈 수 있을 거라는 뜻을 전하기도 하였다.[38] 2019년 초 아던(Jacinda Ardern) 뉴질랜드 총리 역시 스파크가 정부통신보안국이 제기하는 안보적 우려를 불식할 수 있다면 화웨이 장비를 사용할 수 있을 거라는 뜻을 전하기도 하였다.

2020년 1월 영국이 자국 기업들의 화웨이 5G 장비 사용을 부분적으로 제한했을 때도 화웨이에 대한 뉴질랜드의 모호한 입장이 재차 대두되었다. 리틀 장관은 "그들(영국)은 그들만의 이유로 그러한 결정을 내렸다"고 말하며, 뉴질랜드가 영국의 결정을 따라가지는 않을 것이라는 입장을 밝혔다.[39] 같은 해 7월에 이르러 영국이 화웨이 5G 네트워크 장비 구매금지를 결정하자 이때도 역시 리틀 장관은 화웨이에 대한 정부의 결정은 철저히 뉴질랜드만의 평가를 바탕으로 하여 "기술적 역량과 국가안보에 대한 위협 여부에 따라 정해질 것이며… 현재 뉴질랜드는 그 어떤 통신기업도 배제하지 않는다"고 말하였다. 그러면서도 그는 "현재 로선 5G 네트워크와 관련하여 화웨이 장비를 사용하겠다고 알려온 기업은 없다"면서, "기업이 사용을 희망하는 특정 기술에 대한 평가는 개별적(case-by-case)으로 이루어져 왔고 또 앞으로도 그렇겠지만… 국가안보적 이해관계가 최우선시될 것"이라는 점을 강조함으로써 배제 결정을 유보하였다.[40]

한편 데이터 안보 문제에 있어서 뉴질랜드는 데이터 주권을 보호하는 차원에서 관리된 통제를 모색하는 경로를 추구해왔다. 2016년 들어 정부 차원의 공공 클라우드 서비스 추진의 가속화가 이루어지면서 데이터 주권 문제가 부각되자 2017년 뉴질랜드 정부는 공공 클라우드 서비스의 「관할권 위험(jurisdictional risks) 관리 대응법 안내서」를 발표하였는데, 이 안내서는 자국의 데이터가 특정 클라우드 서비스업체를 통해 저장·처리·이전되는 과정에서

---

36) 『중앙일보』, "캐나다에 이어 뉴질랜드도 화웨이 배제 안하기로", 『중앙일보』, 2018년 11월 26일. https://news.joins.com/article/23157264 (검색일: 2020.12.29.)

37) 2013년 발효된 전자통신(감청 및 보안)법안 (TICSA: Telecommunications (Interception Capability and Security) Act)의 핵심은 1) 감청기관이 효율적으로 합법적인 감청을 시행할 수 있게 하고, 2) 감청기관이 새로운 통신 기술의 도입을 막지 않도록 하며, 3) 통신 관련 기업 및 서비스 제공업체는 그들의 목적에 따라 자유롭게 시스템 디자인과 사양을 결정할 수 있게 하는 것이다.

38) Radio New Zealand, "Reasons to block Spark's 5G rollout 'classified'," *Radio New Zealand*, November 28, 2018. https://www.rnz.co.nz/news/national/377014/reasons-to-block-spark-s-5g-rollout-classified (검색일: 2020.12.29.)

39) Radio New Zealand, "No UK approach to Huawei for NZ, but using it here not ruled out completely," *Radio New Zealand*, January 29, 2020a. https://www.rnz.co.nz/news/political/408379/no-uk-approach-to-huawei-for-nz-but-using-it-here-not-ruled-out-completely (검색일: 2021.1.1.)

40) Radio New Zealand, "Andrew Little says New Zealand won't follow UK's Huawei 5G ban," *Radio New Zealand,* July 15, 2020b. https://www.rnz.co.nz/news/political/421286/andrew-little-says-new-zealand-won-t-follow-uk-s-huawei-5g-ban (검색일: 2021.1.8.)

해당 서비스업체가 속한 국가의 법령 적용대상이 됨에 따라 발생하는 위험에 주목하고, 나아가 클라우드 대상 관할권(국가)과 서비스업체를 평가하는 프레임워크를 제시하는 목적에서 마련되었다.[41] 특히 주목할만한 특징은 관할권 평가 대상국으로 정부 기관들이 가장 선호하고 또 실제로 가장 많이 이용하고 있는 국가들이 선정되었는데, 여기에는 미국, 네덜란드, 독일, 싱가포르, 영국, 아일랜드, 호주, 캐나다 등 8개국이 포함되었다.

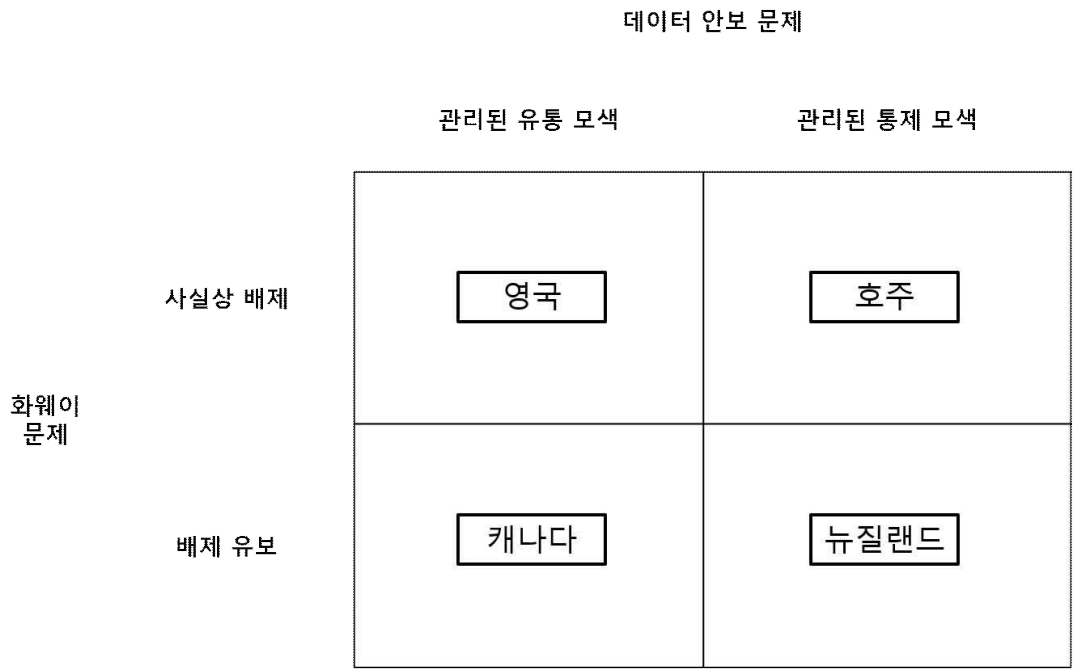
이처럼 뉴질랜드 정부는 클라우드 서비스 이용에 따른 데이터의 국외 저장·처리·이전이 해당 데이터에 대한 외국 정부의 합법적인 접근을 가능하게 한다는 위험에 주목하고, 이에 대한 대응책으로서 관할권 평가라는 제도적 장치를 마련하였다. 법제적 장치를 통해 자국민의 데이터를 보호하려는 노력은 2020년 12월 발효된 <개인정보보호법(Privacy Act 2020)>의 데이터 이동에 관한 규제 내용에서도 잘 나타나는데, 이 법은 외국 행위자(person or entity)가 뉴질랜드와 유사한 수준의 개인정보 보호 시스템을 준수해야 하는 요건을 충족할 시에만 데이터 개방(disclose)을 허용하며, 본사와 데이터를 공유하는 해외 법인 역시 본사와 유사한 수준의 개인정보 보호 시스템을 준수해야 하는 요건을 충족할 시 데이터를 해외 법인에 개방할 수 있도록 강제한다.[42]

그럼에도 이웃 국가인 호주와 비교할 때 뉴질랜드는 데이터 주권 문제에 상대적으로 더 유연한 입장을 취하고 있는 것으로 평가되는데, 뉴질랜드 정부는 정부 기관들이 앞서 명기된 8개 관할권 평가 대상국 외에 다른 국가의 클라우드 서비스업체를 선택하는 것을 용인하였다. 다만, 그 경우 선정된 관할권의 정부가 자신의 영내에 저장·처리·이전된 데이터에 접근하는 방식과 더불어 선정된 클라우드 서비스 업체가 외국 정부의 데이터 접근 요청에 대응하는 방식에 대한 구체적인 평가가 사전에 반드시 이루어져야 한다는 조건을 걸었다. 즉 뉴질랜드는 5G 장비 공급업체와 마찬가지로 클라우드 서비스업체 및 관할권 역시 개별적인 평가제도를 통해 선정하고, 특정 업체나 국가를 배제하지 않겠다는 입장을 취한 것이다.

---

41) New Zealand Government, *Managing Jurisdictional Risks for Public Cloud Services*, July, 2017.; 해당 안내서에서 뉴질랜드 정부는 데이터 주권 개념 대신 '관할권 위험'이라는 개념을 사용하였다.

42) New Zealand Legislation, "Privacy Act 2020," June 30, 2020. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html (검색일: 2021.4.17.)



[그림 1] 화웨이 사태와 데이터 안보에 대한 파이브 아이즈 국가의 대응

Ⅳ. 4개국 전략의 비교분석

이상에서 살펴본 바와 같이, 파이브 아이즈 4개국은 화웨이 사태와 데이터 안보 문제에 대응하는 과정에서 상이한 행태를 보였다. 먼저 화웨이 사태에 있어서 영국과 호주는 화웨이의 5G 네트워크 장비를 사실상 배제하는 결정을 내렸지만, 캐나다와 뉴질랜드는 미국의 동료 압박에서 불구하고 화웨이 배제 결정을 유보하는 모습을 보였다. 한편 데이터 안보 문제에 있어서 영국과 캐나다는 데이터의 관리된 유통을 지향하였고, 호주와 뉴질랜드는 데이터의 관리된 통제를 위한 전략을 수립하고 추진하는 모습을 보였다. 이러한 상이한 대응 경로는 대미·대중관계와 주변 안보 환경에서 이들 국가가 각기 다른 성격의 상황적 조건에 놓여있었고, 또 화웨이와의 관계와 데이터 유통에 관한 국제규범 논의 구조에서도 각기 다른 상황과 위치에 처해있었기 때문에 비롯된 결과로 볼 수 있다.

1. 대미·대중관계 및 안보 환경에서 각국의 위치

미중 디지털 패권경쟁 구조는 전체적인 차원에서 미국과 중국이 사이버·데이터 안보 문제를 중심으로 경합을 벌이는 갈등 구조이지만, 좀 더 세부적인 차원에서는 미중 양자택일의 압박을 받는 나머지 국가들이 사이버·데이터 안보 문제를 두고 각각 미국, 중국과 관계를 맺고 있는 구조이기도 하다. 중견국은 강대국에 비해 구조의 영향을 더 많이 받을 수밖에 없음을 고려할 때, 파이브 아이즈 4개국의 대응전략은 이들 국가가 미국, 중국과 맺고 있는 관계에 직접적인 영향을 받았다고 볼 수 있다. 따라서 이들 4개국의 대응전략을 분석하기

위해서는 이들 국가가 대미·대중관계에서 처해있는 구조적 상황과 위치를 파악할 필요가 있다. 다시 말해, 사이버·데이터 안보 분야에서 미중이 갈등하는 상황 가운데 이들 4개국과 미국·중국 간 '유동적 관계'의 이익구조와 상황적 제약은 어떠했는지, 또 그러한 관계 속에서 각국은 어떠한 위치를 차지하고 있었는지를 탐구해야 함을 의미한다.

파이브 아이즈 4개국은 미국과의 관계 그리고 중국과의 관계에서 각기 다른 상황과 위치에 놓여있었다. 물론 집합적 국력이나 자원 권력의 측면에서만 보자면, 파이브 아이즈 정보동맹의 위계적 구조에서 이들 4개국은 하위 동맹국의 위치에 놓여있기 때문에 상위 동맹국인 미국의 이해관계에 상충하는 행태를 보이거나 미국의 요구를 거부할 여지가 적다고 단정하기 쉽다. 그러나 구조적 위치론의 시각에서 보면, 이들 하위 동맹국과 미국 간의 비대칭적 관계는 구조적 상황의 조건에 따라 얼마든지 조율될 수 있다.[43] 중국과의 관계 역시 단순히 비대칭적 경제관계에 국한되기보다는 여러 상황적 조건의 영향을 받으며 형성된다고 볼 수 있다. 따라서 이들 4개국과 미국·중국 간 관계에서 발견되는 외교적·안보적·경제적 상황과 그 안에서 각국이 차지하는 위치는 이들 국가의 대응전략을 이해하는 실마리를 제공한다.

이러한 맥락에서 이들 4개국이 각기 다른 성격의 안보 환경에 놓여있는 국가라는 사실에도 주목할 필요가 있다. 이들 각국이 화웨이 사태와 데이터 안보에 대응하는 과정에서 전개해온 전략은 미중 디지털 패권경쟁의 구조나 사이버·데이터 안보 영역에서의 위협뿐만 아니라 전통적으로 이들이 당면해온 주변 안보 환경에도 많은 영향을 받았다. 중견국은 지정학적으로 결정된 안보 환경에 많은 영향을 받을 수밖에 없는데, 강대국에 둘러싸여 자신의 지역 내에서 유의미한 변화를 끌어내는 데 어려움을 가지는 중견국과, 상대적으로 지정학적 안보 위협에서 자유로운 환경에 놓인 중견국은 상이한 외교행태를 보일 가능성이 크다.[44] 미중 디지털 패권경쟁이 지정학적 경쟁의 성격을 강하게 보인다는 점과 더불어 화웨이 사태와 데이터 안보 문제 역시 지정학적 임계점을 통과한 신흥안보(emerging security) 위협이라는 점에서 파이브 아이즈 4개국이 각기 당면한 전통적 차원의 안보 환경은 이들 각국의 사이버·데이터 안보 전략에도 상당한 영향을 미쳤다고 볼 수 있다.

(1) 미국과의 관계

먼저 영국은 자국 정부와 기업에 대한 외부 세력의 사이버 공격 꾸준히 증가하는 상황에서 유럽 내 유일한 미국의 정보동맹국으로서 자신이 가지는 구조적 위치를 적극적으로 활용하는 모습을 보였다. 그에 따라 자국의 정보보호 산업을 강화하기 위해서는 화웨이를 배제할 수 없다는 기존 입장을 사실상 철회하고 미국을 비롯한 우방국들과의 안보협력을 증진하는 방향으로 정책을 수정하였다.[45] 그 과정에서 2020년 7월 화웨이 전면 퇴출 결정이 발표

---

43) 하위 동맹국이 상위 동맹국을 상대로 행사할 수 있는 위치 권력에 대한 논의 중에서는 롱(Tom Long)의 연구가 주는 시사점이 크다. 롱에 의하면, 소국 또는 하위 국가(hypo-power)가 행사할 수 있는 권력에는, 강대국과 동맹관계에 있는 소국이 강대국과의 구성적 관계에서 얻어낼 수 있는 파생 권력(derivative power); 소국이 다른 비강대국들과의 관계(연대)에서 끌어낼 수 있는 집단 권력(collective power); 그리고 소국이 인구, 영토, 지리적 위치, GDP, 군사력 등 다양한 본질적 권력 중 특정한 분야에서 상대적으로 우세한 위치를 활용하여 행사하는 특유(특정한 본질적) 권력(particular-intrinsic) 등이 있다(Long 2017).

44) 최종현, "중견국 공적개발원조 정책의 결정요인: 스웨덴과 호주의 비교를 중심으로," 김상배, 이승주, 전재성 엮. 『중견국 외교의 세계정치: 글로벌-지역-국내 삼중구조 속의 대응전략』 사회평론아카데미, 2020, pp.130-133.

45) National Cyber Security Centre, *The cyber threat to UK business: 2016/2017 Report,* 2017. p. 5.; 한국인터넷진흥원, "2019 글로벌 정보보호 산업시장 동향조사 보고서(30개국)," 2019년 12월 13일.

되기 약 두 달 전인 5월 영국 정부는 이듬해 있을 G7 정상회의에 한국, 인도, 호주를 게스트 국가로 초청하는 계획을 미국과 논의하고 있다는 소식이 전해졌고, 그해 12월 D10 계획을 정식으로 발표함으로써 기존 G7을 확장하려 한 미국의 전략에 발을 맞췄다.[46] 데이터 안보 문제에 있어서도 역시 영국은 자신의 구조적 위치를 활용하여 미국과 유럽을 잇는 데이터 유통 허브로서 자리매김하기 위해 노력해왔다. 이를 위해 유럽연합의 데이터 주권론을 옹호하면서도 동시에 미국과의 데이터 공유를 강화하려는 노력을 전개해왔다.[47]

호주의 화웨이 퇴출과 데이터 주권 강화는 미국과의 동맹관계에서 자신이 차지하는 위치에 대한 위기의식에 많은 영향을 받았다. 그간 호주는 군사 인공위성 등 '정보·감시·정찰(ISR)' 자산에 대한 막대한 투자 없이도 미국과의 정보동맹 관계를 통해 최고급 군사·전략 정보를 취해왔다. 그런데 최근 미국과 호주가 공동 운영하는 호주 영내 정보 수집 시설의 중요성이 향후 경감될 수 있다는 우려가 대두되면서 파이브 아이즈 내 호주의 위상이나 미국과의 동맹에서 호주의 전략적 가치가 상대적으로 감소할 수 있다는 우려가 대두되었다.[48] 따라서 호주는 화웨이 사태에서 미국과 발을 맞춤으로써 동맹국으로서의 신뢰와 입지를 강화하길 원하였다고 볼 수 있다. 더욱이 파이브 아이즈 정보동맹의 경우 미국과 나머지 주니어 파트너 국가 간 정보·첩보 교환(intelligence exchange)이 비대칭적 관계 속에서 이루어지기 때문에 호주로서는 미국과 견고한 신뢰관계를 유지함으로써 동맹 내부적으로 자국의 입지를 강화하여 미국으로부터 더 많은 정보를 지원받길 원하였을 가능성이 크다.[49] 호주는 2016년 국방백서에서도 "파이브 아이즈 정보공동체가 제공하는 정보우세(information superiority)와 첩보협력은 호주 방위 계획에 필수적"이라고 명기한 바 있는데,[50] 이는 자국을 겨냥한 중국의 사이버 공격과 내정간섭 위협이 증가하는 상황에서 호주가 정보동맹을 통한 미국의 협력을 더욱 필요로 하게 되었음을 방증한다. 마찬가지로 호주 정부가 더 강화된 데이터 지역화를 추진하게 된 데에도 역시 미국과의 데이터 공유 강화에 대한 국내적 우려를 불식시키는 동시에 이를 정당화하려는 의도가 더 크게 작용했다고 볼 수 있다.

한편 캐나다는 대표적인 중견국으로서 기본적으로 국제 분쟁에 대응함에 있어 규범과 원칙에 근거한 다자주의적 해법을 지향해왔는데, 특히 친미(親美)노선을 분명히 해온 보수당에 비해 현 정부를 구성하는 자유당은 기본적으로 자국이 외교안보적으로 미국에 경도되는 것을 경계하면서 적대와 배제를 위한 연합보다 다자주의에 근거한 연루(engagement) 정책을 선호해왔다. 이러한 외교 기조가 화웨이 사태에 대한 캐나다의 인식에 직접적인 영향을 미쳤다고 확언할 수는 없지만, 지금까지 화웨이 문제와 관련해서 중국과의 마찰을 자제해온 캐나다 정부가 최근 들어 인권 문제에 있어서만큼은 중국을 강도 높게 규탄해왔다는 사실을 고려하면 충분히 주목할만한 요인이라 할 수 있다. 예로, 2020년 10월 자유당 정부를 이끄는 트뤼도(Justin Trudeau) 총리는 중국과의 수교 50주년을 맞아 가진 언론 인터뷰에서 중국의

---

46) Yusuke Nakajima, "UK calls on South Korea, India and Australia to attend G-7 summit," *Nikkei Asia*, December 16, 2020. https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/UK-calls-on-South-Korea-India-and-Australia-to-attend-G-7-summit (검색일: 2021.5.5.)

47) Arcadis. 2021. The Arcadis Data Center Location Index 2021. https://datacenters.arcadis.com/locationindex/p/1 (검색일: 2021.4.27.)

48) 박재적, "호주의 화웨이 배제: 주요 동인, 프레임 짜기, 연대 외교," 서울대학교 국제문제연구소 이슈브리핑, 123호, (2021.1.20.), pp. 4-5.

49) Andrew O'Neil, "Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance." *Australian Journal of International Affairs,* Vol. 71, No. 5. 2017. pp. 529- 543.

50) Australian Department of Defence. *2016 Defence White Paper.* Commonwealth of Australia. 2016. p. 122.

캐나다 국민 구금과 홍콩 국가보안법 시행, 중국 내 이슬람 소수민족인 위구르족 탄압 정책 등을 “생산적이지 못한 행로”라고 비판하고, 나아가 “중국의 강압적 외교 방식은 중국에 성공적인 전략이 되지 못할 것이라는 점을 부각하기 위해 우방과 협력하는 데 빈틈없이 할 것”이라고 말하였다.[51] 그보다 앞선 5월에는 미국, 영국, 호주와 함께 홍콩 국가보안법을 비난하는 공동성명을 발표하였고, 7월에는 홍콩과의 범죄인 인도조약 파기를 선언하기도 하였다. 이렇듯 국제규범과 원칙에 부합하는 다자주의 연대에는 적극적으로 참여해온 캐나다 정부가 화웨이 사태와 관련해서는 그러한 태도를 보이지 않는 것은 결국 자국이 미국에 지나치게 경도되는 것을 경계하는 한편 미국 주도의 대화웨이 공조를 적대와 배제를 위한 연합으로 인식하기 때문으로 볼 수 있다.

마지막으로 뉴질랜드는 초국적 범죄 예방과 인권보호의 프레임에 기초한 사이버·데이터 안보전략을 추진함으로써 디지털 공간에서 발생하는 안보 이슈를 강대국 간 전략적 갈등구조에서 분리하여 자국의 정책이 미국의 이해관계에 끌려가는 것을 방지하고자 하였다. 구체적으로, 사이버·데이터 안보전략을 수립하고 추진하는 과정에서 사이버 범죄의 초국적 위협을 글로벌 차원의 협력을 통해 해결해야 한다는 인식을 바탕으로 사이버 공간에 대한 국제법 적용과 국제협력을 통한 제도 수립에 초점을 맞춘 ‘제도적 협력’을 강조해왔다.[52] 이렇듯 뉴질랜드가 화웨이 사태와 데이터 안보 문제를 규범의 관점에서 접근해 온 것은 해당 문제를 가능한 한 탈안보화하려는 의도에서 비롯된 것으로서, 결국 디지털 공간에서 발생하는 안보 이슈를 강대국 간 전략적 갈등구조에서 분리하여 자국의 정책이 미국의 이해관계에 끌려가는 것을 방지하고자 한 것으로 해석된다. 이러한 의도는 틱톡 둘러싼 갈등국면에서 뉴질랜드 총리가 보인 입장에서도 잘 드러난다. 2020년 8월 미국이 데이터 안보화 논리를 앞세워 틱톡 금지령을 발포하자 곧바로 뉴질랜드에서도 틱톡에 대한 안보적 우려가 제기되었지만, 아던 총리는 “총리로서 애플리케이션 사용이나 소통의 형식과 관련한 안보문제를 언제나 유념하고 있다”고 말하며 틱톡 문제가 지나치게 안보화되는 것을 경계하는 모습을 보였다.[53] 이는 1984년 ANZUS 위기를 계기로 국제적 차원의 비핵지대 운동을 주도하는 중견국으로 인정받게 된 뉴질랜드가 자국이 내세우는 가치와 원칙 그리고 이익을 위해서라면 강대국의 안보 정책과 이익에 반하는 한이 있더라도 독자적인 목소리를 낼 수 있어야 한다는 기조를 가져온 것과도 무관하지 않다.[54] 사이버 안보 분야에서도 역시 이러한 기조를 따르

---

51) 조재용, “‘중국과 수교 50주년’ 캐나다총리 강압 외교에 우방과 협력대처,” 『연합뉴스』, 2020년 10월 14일, https://www.yna.co.kr/view/AKR20201014075500009 (검색일: 2021.5.4.)

52) 그러한 맥락에서 뉴질랜드 정부는 2019년 「사이버안보전략」에서 자국이 규칙기반 국제질서와 다중이해당사자주의적 인터넷(multi-stakeholder Internet) 환경을 옹호한다는 점을 분명히 하였으며, 2011년 「사이버안보전략」과 2015년 「사이버 범죄 대응을 위한 국가계획」 그리고 2019년 「사이버안보전략」에서 사이버 범죄와 테러조직의 인터넷 악용에 선제적이고 협력적으로 대응하기 위해 유럽평의회의 부다페스트 사이버범죄방지협약(Council of Europe’s Budapest Convention on Cybercrime, 이하 ‘부다페스트 협약’) 가입을 적극적으로 추진해나갈 것을 공표하였다. 또한, 온라인상의 테러행위 및 폭력적 극단주의 관련 콘텐츠 제거를 위해 2019년 5월 뉴질랜드가 프랑스와 함께 주도하여 도출해낸 ‘크라이스트처치 콜(Christchurch Call)’ 선언을 강조하며, 자국이 자유롭고 개방적이며 안전한 인터넷 환경 유지와 사이버 공간에 대한 국제인권법 적용에 앞장서겠다는 뜻을 밝혔다. 2020년 12월 뉴질랜드 정부가 발표한 ‘사이버 공간에서의 국가행위에 대한 국제법 적용’ 성명 역시 이러한 의도에서 비롯된 것으로 볼 수 있다.; New Zealand Ministry of Foreign Affairs and Trade, “The Application of International Law to State Activity in Cyberspace,” December 1, 2020. https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/ (검색일: 2020.12.28.)

53) NZ Herald, “New Zealand MPs told to delete TikTok over security concerns,” *NZ Herald*, August 4, 2018. https://www.nzherald.co.nz/nz/new-zealand-mps-told-to-delete-tiktok-over-security-concerns/BQU5VV2YFBAO2AAHXMOBBLJLMY/ (검색일: 2021.6.2.)

고 있는 것으로 볼 수 있다.

(2) 중국과의 관계

영국의 화웨이 퇴출 결정과 미국과의 데이터 공유 강화는 영국과 중국의 관계 악화에도 큰 영향을 받았다. 영국은 화웨이 장비가 중국발 사이버 공격 및 침탈 위협의 수단으로 악용될 위험성을 어느 정도 인지하고 있었지만, 2017년 중국이 <국가정보법(National Intelligence Law)>을 도입하면서 이전부터 제기되었던 화웨이와 중국 공산당 간 관계의 위험성을 우려하는 목소리가 다시금 커지게 되었다.[55] 또한, 2020년 7월 중국이 <홍콩국가보안법>을 시행하자 1984년 홍콩반환협정(또는 중영공동선언)의 당사국으로서 홍콩 사태에 관여할 정당성을 가지고 있다고 여겨온 영국은 해당 법 제정이 홍콩반환협정과 '일국양제(一國兩制)'원칙을 위반하는 행위이자 홍콩 시민들에 대한 억압이라고 규탄하며 강한 우려와 불만을 표하였다.[56] 즉 중국의 제도적 환경의 변화가 영중 관계 악화로 이어졌고, 그러한 관계 악화가 화웨이 사태와 데이터 안보에 대한 영국의 전략에 영향을 미쳤다고 볼 수 있다.

호주의 화웨이 퇴출 결정과 데이터 주권에 대한 의지는 중국과의 외교관계 악화와 밀접한 연관이 있다. 2016년 전후로 호주를 겨냥한 중국발 사이버 공격행위가 증가하면서 양국 관계는 빠르게 악화되었는데, 호주는 자신을 겨냥한 중국발 사이버 공격이 단순히 사이버 공간에만 국한된 위협이 아닌 정치적 안보(political security)[57]를 위협하는 내정간섭, 간첩행위 등과 밀접하게 연관되어있다고 보고 이를 더욱 심각한 사안으로 인식해왔다.[58] 이러한 부정적 인식은 2019년 10월 더튼(Peter Dutton) 호주 내무부(Department of Home Affairs) 장관이 호주를 겨냥한 중국의 사이버 공격과 내정간섭 행위를 비난했던 데서 잘 드러난다. 더튼 장관은 "호주는 중국과 매우 중요한 무역 관계를 맺고 있다. 그러나 우린 우리 대학생들이 부당하게 영향을 받는 것을 용납하지 않을 것이며, 지적재산 침탈과 정부 및 비정부기관을 겨냥한 해킹을 용납하지 않을 것"이라고 발언함으로써 중국 정부에 대한 비난 수위를 높였다.[59]

한편 캐나다가 화웨이에 대한 국민적 반감과 파이브 아이즈 정보동맹국의 공조 압박 그리고 자국 통신기업들의 연이은 화웨이 배제 결정에도 불구하고 화웨이 문제에 중도적인 태도를 보여온 것은 현 정부를 구성하는 자유당의 전통적인 외교 기조가 작용한 결과로 볼 수

---

54) 1984년의 'ANZUS 위기(ANZUS Crisis)'는 미국의 핵 함정 기항을 불허하는 것을 공약으로 내세웠던 뉴질랜드 노동당이 총선에서 승리하면서 빚어진 뉴질랜드-미국 간 외교적 갈등을 뜻한다. 1987년 뉴질랜드 정부가 '뉴질랜드 비핵지대 및 군축법(New Zealand Nuclear Free Zone, Disarmament and Arms Control Act)'을 통과시키자 미국은 뉴질랜드를 ANZUS 동맹에서 퇴출시켰다.

55) House of Commons, 2020, pp. 34-35.

56) 표나리, "2020년 홍콩 국가보안법 통과의 의미와 시사점," IFANS 주요국제문제분석 2020-25. 국립외교원 외교안보연구소. 2020년 8월 19일.

57) 코펜하겐 학파가 이야기하는 정치적 안보는 정치적 구성단위(political units)의 조직적 안정성(organisational stability)에 관한 것으로서 그 핵심에는 국가 주권에 대한 위협을 두고 있다(Buzan, Wæver and Wilde 1998: 141).

58) Australian Security Intelligence Organisation, *ASIO Report to Parliament 2008-09,* (Commonwealth of Australia, 2009), p. 12.

59) Ben Doherty and Melissa Davey, "Peter Dutton: China accuses home affairs minister of 'shocking' and 'malicious' slur," *The Guardian,* October 12, 2019. https://www.theguardian.com/australia-news/2019/oct/12/peter-dutton-accuses-china-of-stealing-intellectual-property-and-silencing-free-speech (검색일:2019.11.2.)

있다. 캐나다 자유당은 전통적으로 자국이 미국으로 지나치게 경도되는 것을 경계하는 한편 중국과의 경제적 관계를 중시해왔다. 이러한 기조는 트뤼도 총리의 행보에서도 잘 드러난다. 2016년 8월 총리 취임 후 처음으로 중국을 방문한 트뤼도 총리는 리커창(李克强) 국무원 총리를 만난 자리에서 캐나다 새 정부가 대중(對中) 우호적 전통을 계승해 양국관계의 전방위적인 실질협력을 심화시키길 희망한다고 전하며 중국과의 관계 개선에 열의를 보였고, 미국이 환태평양경제동반자협정(TPP) 탈퇴를 결정하고 북미자유무역협정(NAFTA) 재협상이 교착상태에 빠졌던 2017년 말의 상황에서도 그는 중국과의 교역 확대를 위한 방중을 추진하였다. 이러한 외교 기조가 화웨이에 대한 대응에도 일정 수준 영향을 미쳤다고 추측해볼 수 있다.[60]

마지막으로 뉴질랜드 역시 중국과의 경제적 관계가 급격히 악화되는 것을 피하려는 의도에서 화웨이 퇴출 결정을 유보하는 한편 데이터 안보 문제에서도 중립적인 입장을 유지하였다고 볼 수 있다. 뉴질랜드는 2001년 12월 서방 국가 중 처음으로 중국의 WTO 가입 지지를 표명하였고, 2008년 4월엔 OECD 회원국 가운데 가장 먼저 중국과 FTA를 체결하는 등 전통적으로 경제적 관계에 있어서만큼은 친중(親中)노선을 지켜왔다.[61] 2020년 기준 중국은 뉴질랜드 전체 수출액의 30%를 차지하는 최대 무역국으로 자리매김하였고, 미중 간 갈등의 골이 깊어져 가는 가운데 2021년 1월에는 뉴질랜드와 중국 간 개정된 FTA가 체결되었다. 이를 체결하는 자리에서 아던 총리는 “중국은 우리에게 가장 중요한 관계국 가운데 하나이며…코로나19 대유행 속에 양국간 FTA 개정의 의미는 상당히 크고 중요하다”고 말하며 중국과의 관계가 갖는 중요성을 강조하였다.[62] 즉 뉴질랜드는 중국을 최대 무역국으로 삼고 있는 처지에서 화웨이 배제 결정이 그 자체만으로 중국의 경제적 보복을 불러일으킬 수 있으며, 그러한 조치가 미국의 대중국 봉쇄전략에 대한 참여로 확대해석되어 자신과 중국의 관계 단절로 이어질 수 있음을 우려하였다고 볼 수 있다. 한편, 데이터 안보 문제에 대한 대응 역시 중국과의 관계를 고려한 조치로 해석된다. 뉴질랜드 정부가 제시한 관할권 위험 평가 프레임워크는 사실상 강력한 데이터 통제권을 행사하는 중국 내 클라우드 서비스업체 이용을 제한하는 제도적 장치가 될 수 있지만, 동시에 최근 중앙정부의 데이터 통제권 강화에 주력하고 있는 미국이나 호주의 서비스업체에도 장애가 될 수 있다는 점에서 제도를 통해 미중 사이에서 균형을 모색하려는 의도가 반영된 것이라 할 수 있다.[63]

(3) 주변 안보 환경

영국은 오랜 기간 이슬람계 테러 조직과 극우집단의 표적이 되어왔는데, 최근에는 이러한 안보위협이 사이버 테러리즘이나 핵티비즘(Hacktivism) 등의 형태로 나타나기 시작하였다.[64] 이러한 위기에 대응하고자 영국은 GDPR 수용을 통해 유럽의 데이터 주권 보호에 지

---

60) 조창원, 이정은, “미국 동맹국 잇단 이탈…친중행보 가세,” 『파이낸셜뉴스』, 2017년 12월 4일, https://www.fnnews.com/news/201712041555233715 (검색일: 2021.5.7.)

61) Bo Zhiyue, “Is New Zealand moving away from its traditional pro-China policy?,” *South China Morning Post,* May 7, 2021. https://www.scmp.com/week-asia/opinion/article/3132468/new-zealand-moving-away-its-traditional-pro-china-policy (검색일: 2021.5.8.)

62) 이슬기, “[줌인] 濠 때리고 뉴질랜드와 무역 강화...'反中 동맹' 와해 노리는 中,” 『조선일보』, https://biz.chosun.com/site/data/html_dir/2021/01/27/2021012702280.html (검색일: 2021.5.8.)

63) Richard MacManus, “Australia’s encryption law threatens NZ cloud data,” *Newsroom,* December 18, 2018. https://www.newsroom.co.nz/australias-new-encryption-law-threatens-nz-cloud-data (검색일: 2021.5.11.)

속적인 참여를 결정한 상황에도 불구하고 미국과 데이터 공유 행정협정을 체결하였다고 볼 수 있다. 실제로 유럽개인정보보호이사회(EDPB)가 2020년 6월 미국-영국 간 행정협정 체결이 갖는 문제점을 지적하는 서안을 유럽의회에 보내기도 하는 등 강한 우려를 제기하였음에도 불구하고 영국은 주변 안보 환경을 고려하여 미국과의 데이터 공유를 그대로 추진하였다.[65] 화웨이 퇴출 결정 역시 비슷한 위협인식에서 비롯된 것이라 할 수 있다. 영국은 증대하는 글로벌 테러 위협에 대응하기 위해서는 자체적인 국방력과 더불어 미국과의 안보협력을 통한 정보력을 강화해야 한다고 인식해왔고, 그에 따라 화웨이 사태에서 미국과 적극적으로 공조하는 모습을 보여왔다.

한편 인도-태평양 지역 내 미국의 핵심 동맹국인 호주는 최근 남태평양 지역에서의 중국의 군사적 압박과 내정간섭 그리고 사이버 공격과 탈취 등 심각한 안보위협에 직면해왔다. 2018년 다국적 정보기술 보안업체 CISCO가 발표한 보고서에서 호주는 아시아-태평양 지역에서 가장 많은 사이버 공격을 받는 국가로 지목된 바 있다.[66] 2016년 호주 연방정부가 발표한 「국가사이버안보전략」에 따르면, 호주는 악의적 사이버 공격으로 인해 매년 약 170억 호주달러의 경제적 손해를 입어왔고, 정부 기관이나 정당 또는 주요 대학 등을 겨냥한 사이버 공격의 표적이 되어왔다. 특히 중국발 사이버 공격이 큰 위협이 되었는데, 일례로 2017년 말 턴불 총리는 자국에 대한 외국의 내정간섭을 방지하기 위한 <외국영향투명성제도법안(Foreign Influence Transparency Scheme Act 2018)>을 제안하는 과정에서 정보기관의 보고서를 인용하여 지난 10년간 호주에 대한 중국 정부의 지속적인 내정간섭 및 간첩행위가 있었다고 주장하였다.[67] 이러한 안보 환경은 호주가 화웨이 사태와 데이터 안보 문제를 국가안보적 차원에서 접근할 수밖에 없게끔 만들었다고 볼 수 있다.

캐나다는 글로벌 사이버 테러의 표적이 되어온 영국이나 중국발 사이버 공격과 내정간섭 위협을 받아온 호주에 비해 상대적으로 안보 위협에 덜 노출되어 있었다고 볼 수 있다. 따라서 당장 화웨이를 배제함으로써 미국과의 안보협력 관계를 더욱 강화할 필요도, 데이터 주권을 앞세워 중요 데이터의 유출을 막아야 할 필요도 이들 국가보다 상대적으로 덜 느껴왔을 가능성이 크다. 지정학적 측면에서 볼 때, 캐나다는 미국의 세력권인 북아메리카 지역에서 상대적으로 덜 위협적인 안보 환경에 놓여있다. 이는 중국의 세력 팽창의 주 무대가 되는 인도-태평양 지역에 덩그러니 놓여있는 호주의 안보 환경과 비교할 때 더욱 두드러진다.

뉴질랜드 역시 캐나다와 비슷하게 비교적 덜 위협적인 안보 환경에 놓여있었기 때문에 화웨이 사태와 데이터 안보 문제에 호주나 영국보다 좀 더 여유로운 대응이 가능했다고 볼 수 있다. 뉴질랜드는 1951년 미국, 호주와 ANZUS 삼각군사동맹을 체결하였지만, 1984년 미국

---

64) 한국인터넷진흥원, 2019. p. 99.

65) EDPB는 해당 서안에서 구체적으로 미영 행정협정과 미국의 <클라우드법> 간 갈등이 발생할 경우 전자보다 후자가 우선시될 가능성, 영국에서 제3국으로의 데이터 국외이전 문제, 영국의 GDPR 적정성 평가에 대한 영향 등에 대한 우려를 제기하였다.; Andrea Jelinek, “Letter to the European Parliament members,” European Data Protection Board, June 15, 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf (검색일: 2021.5.8.)

66) Cisco, *Cisco 2018 Asia Pacific Security Capabilities Benchmark Study,* Cisco, 2018.

67) Christopher Knaus and Tom Phillips, “Turnbull says Australia will ‘stand up’ to China as foreign influence row heats up,” *The Guardian,* December 9, 2017. https://www.theguardian.com/australia-news/2017/dec/09/china-says-turnbulls-remarks-have-poisoned-the-atmosphere-of-relations (검색일: 2019.11.7.)

의 핵 함정 기항 문제로 미국과 갈등을 빚게 되면서 결국 1987년 동맹국의 지위를 잃게 되었다. ANZUS 위기 이후 뉴질랜드와 미국의 관계는 꾸준한 회복세를 보여왔고, 2013년 미국 오바마 행정부가 아시아 회귀정책을 추진하는 과정에서 뉴질랜드 함정의 진주만 기항을 허락하는 결정을 발표하면서 양국 간 군사협력이 대폭 강화되었다. 그러나 여전히 양국 간 군사동맹은 체결되지 않은 상태에 머물러있다. 그럼에도 불구하고 뉴질랜드는 호주를 매개로 하여 미국과 긴밀한 군사적 협력관계를 유지하고 있으며, 호주와의 양자동맹을 통해 지정학적 차원에서 안보를 보장받고 있다. 당장 남태평양 지역에 대한 중국의 세력팽창에 뉴질랜드가 호주보다 덜 민감하게 반응해온 것 역시 호주의 세력권 내에서 자신의 안보를 상당 수준 보장받을 수 있기 때문이다. 이러한 안보 환경으로 인해 뉴질랜드는 미국과의 안보협력 관계를 위해 화웨이 배제나 데이터 유통 또는 미국과의 데이터 공유를 강행할 필요를 덜 느꼈다고 볼 수 있다.

2. 화웨이와의 관계에서 각국의 위치

화웨이 사태에 대한 파이브 아이즈 4개국의 대응전략은 화웨이와의 관계, 즉 각국이 화웨이와 협력 또는 갈등을 벌여온 상황에도 일정 수준 영향을 받았다고 볼 수 있다. 4차 산업혁명 시대에 국력 강화의 수단으로 정보통신기술 발전이 모색되는 가운데 그 기반 인프라로서 5G 네트워크 기술의 필요성이 증대하는 상황에서 화웨이는 경제성 높은 네트워크 장비를 앞세워 주요 국가들의 통신시장에 빠르게 진출해왔다. 본 논문이 주목한 4개국 역시 화웨이 사태 발발 이전까지만 해도 모두 자국 통신시장에 화웨이의 접근을 용인해왔는데, 그 과정에서 이들 각국과 화웨이 간 관계는 협력과 갈등의 정도에서 차이를 보였다.

중국과 높은 수준의 무역관계를 맺어온 영국은 일찍이 2005년 자국 통신시장에 대한 화웨이의 진출을 허용함으로써 사실상 화웨이가 글로벌 시장에 진출할 수 있는 발판을 마련해주었다. 2005년 4월 화웨이는 영국의 통신 네트워크 구축사업을 주도했던 브리시티텔레콤(British Telecommunications, 이하 'BT')와 장비 공급 계약을 체결하였는데, 이 계약은 화웨이가 중국을 벗어나 최초로 맺은 계약이었다. 당시 국제 계약으로는 홍콩의 투자지주회사인 허치슨왐포아(Hutchison Whampoa)와 체결한 협약이 유일했던 화웨이는 영국 BT와의 협업을 계기로 유럽 시장에 빠르게 진출할 수 있었고, 이는 결국 화웨이가 글로벌 기업으로 성장하는 데 교두보가 되었다.[68] 이후로 영국은 화웨이의 국제 사업 기지로 자리 잡게 되면서 화웨이에 대한 영국의 기술 의존도 역시 자연스럽게 높아졌다. 그 결과 2020년을 기준으로 영국 통신 관련 기업의 1/3이 화웨이 무선장비를 사용하기에 이르렀고, 대표적인 예로 주요 이동통신 기업 중 하나인 보다폰(Vodafone)은 라디오 접근 네트워크용 베이스 스테이션의 32%를 화웨이에 의존하는 것으로 알려졌다.[69] 그런데 기술 의존도의 급격한 상승은 역으로 화웨이 장비에 대한 영국 정보기관과 정책결정자들의 우려를 꾸준히 증가시켰는데, 일례로 영국 하원 정보보안위원회(ISC)는 2013년 발간한 보고서에서 2005년 BT와 화웨이 간 협약이 체결 직후에야 관련부처 장관들에게 보고되었음을 지적하면서 화웨이에 대한 정

---

68) Nic Fildes, "How Huawei used the UK to become a global gaint," *Financial Times*, December 8, 2018, https://www.ft.com/content/16381afa-f986-11e8-8b7c-6fa24bd5409c (검색일: 2021.6.25.)

69) Paul Sandle, "Vodafone says complete UK ban on Huawei would cost it millions of pounds," *Reuters,* March 7, 2019. https://www.reuters.com/article/us-britain-vodafone-huawei/vodafone-says-complete-uk-ban-on-huawei-would-cost-it-millions-of-pounds-idUSKCN1QO1LZ(검색일: 2021. 6. 25).

부 차원의 경계를 늦추지 않을 것을 주문하기도 하였다.[70]

파이브 아이즈 동맹국 중 중국에 대한 무역 의존도가 가장 높은 호주 역시 일찍이 2004년부터 자국 통신시장에 대한 화웨이의 진출을 허용하였다. 화웨이는 자사 장비의 높은 경제성을 무기로 호주 통신시장에 꾸준히 접근한 덕에 호주 주요 통신사 모두가 5G 이전 단계에서 화웨이와 공동으로 사업을 진행할 만큼 기술 의존도를 높일 수 있었다. 대표적인 예로, 2010년 말 주요 통신사인 보다폰(Vodafone Hutchison Australia)이 화웨이를 자사 2G 및 3G 네트워크 장비 공급업체로 선정하였고, 2012년에는 또 다른 거대 통신사인 옵터스(Optus)가 최초로 4G 네트워크에 화웨이 장비를 도입하였다. 그러나 2012년 호주 정부가 안보정보국(ASIO)의 조언에 따라 자국 국가광대역통신망(NBN) 사업에서 화웨이를 배제하면서 호주와 화웨이 간 관계의 균열이 나타나기 시작하였다.[71] 이후로 호주는 지속해서 화웨이에 대한 지나친 의존을 경계해왔고, 2017년에는 화웨이가 남태평양 도서국을 대상으로 시장을 키워가는 상황에서 호주가 파푸아뉴기니와의 해저 케이블을 직접 관리하겠다고 나서면서 다시 한번 호주 정부와 화웨이 간 갈등이 불거지기도 하였다. 그리고 2018년 8월 호주 정부가 자국 5G 네트워크 구축사업에서 공식적으로 화웨이를 배제할 때까지 화웨이에 대한 기술 의존은 관리되는 수준에서만 허용되어왔다.

한편, 파이브 아이즈 국가 중 가장 낮은 대중국 경제 의존도를 보이는 캐나다에서 2008년부터 활동을 이어온 화웨이는 영국이나 호주에서와 달리 상대적으로 낮은 시장 점유율을 보여왔지만, 최근 들어 캐나다 5G 네트워크 사업 진출에 주력하면서 빠른 속도로 입지를 키워왔다. 그 과정에서 2018년 캐나다 일간지 글로브앤메일이 화웨이가 캐나다 5G 네트워크 사업 참여에 필요한 지적재산 수집을 위해 캐나다 대학들과 방대한 관계망을 구축해 이를 활용해왔다고 보도하면서 안보 우려가 제기되었고, 여기에 미국의 압박이 더해지면서 화웨이를 포함한 외국 통신장비 공급업체의 보안 위협에 대한 정부 차원의 조사가 이루어졌다.[72] 그러나 이는 캐나다 정부와 화웨이 간 관계 균열로 이어지진 않았는데, 그해 9월 존스(Scott Jones) 사이버안보센터장은 자국 정보기관이 외국 통신장비 공급업체의 보안 문제를 관리할 수 있는 역량을 갖추고 있다면서 당장 화웨이 장비를 퇴출할 필요가 없다고 주장하였고, 트뤼도 총리 역시 화웨이의 자국 5G 사업 참여문제가 정치화되는 것을 반대한다는 의사를 표명하였다. 물론 그해 11월 구데일(Ralph Goodale) 공공안전부장관이 자국 5G 네트워크 구축사업에서 화웨이를 배제할 가능성이 여전히 남아있다고 밝힘으로써 정부의 입장이 화웨이를 수용하는 쪽은 아니라는 점을 분명히 하였지만, 그 이후로 화웨이와의 관계에서 눈에 띄는 균열은 나타나지 않았다.[73]

뉴질랜드 역시 캐나다와 마찬가지로 화웨이와의 관계에 있어 갈등의 수위를 가능한 한 조

---

70) Fildes, 2018.

71) Jennifer Duke, “Huawei’s history with Australia,” *The Sydney Morning Herald*, December 8, 2018. https://www.smh.com.au/business/companies/huawei-s-history-with-australia-20181207-p50kyj.html (검색일: 2021.6.26.)

72) Robert Fife and Steven Chase, “Ottawa launches probe of cyber security,” *The Globe and Mail,* September 18, 2018a. https://www.theglobeandmail.com/politics/article-ottawa-launches-probe-of-cyber-security/ (검색일: 2021.6.24.)

73) Robert Fife and Steven Chase, “Ottawa not ruling out blocking Huawei from 5G supply contracts,” *The Globe and Mail,* November 1, 2018b. https://www.theglobeandmail.com/politics/article-ottawa-not-ruling-out-blocking-huawei-from-5g-supply-contracts/ (검색일: 2021.6.23.)

정하려는 모습을 보여왔다. 제조업 기반의 2차, 3차 산업이 발달하지 못한 뉴질랜드는 4차 산업혁명 시대를 맞이하여 정보통신기술을 통한 경제 발전에 높은 관심을 보여왔고, 그 근간이 되는 5G 네트워크 상용화에 주력해왔다. 2005년 처음 오클랜드 사무소를 개소한 이후로 지난 15년간 화웨이는 뉴질랜드 통신 인프라 구축에 핵심적인 역할을 수행하면서 스파크, 2디그리스, 보다폰 등 주요 뉴질랜드 이동통신사들의 화웨이 의존도 역시 빠르게 상승하였다. 특히 스파크와 화웨이 간 4G 네트워크 구축 협업은 뉴질랜드가 4G 상용화를 신속히 이뤄내는 데 결정적으로 이바지했다.[74] 주요 통신사들이 화웨이 통신장비를 도입하면서 통신망 중단 사고가 현저히 줄어들자 화웨이에 대한 긍정적인 평가와 인식 역시 빠르게 확산되었다. 그러나 2018년 뉴질랜드 정부가 스파크의 화웨이 5G 장비 도입을 사실상 불허하고, 이후 미국, 영국, 호주 등이 화웨이를 전면 퇴출하게 되면서 사실상 뉴질랜드와 화웨이 간 관계는 더 나빠지지도 좋아지지도 않는 상태에 놓이게 되었다. 애초에 화웨이와 5G 네트워크 공급계약을 체결하길 희망했던 스파크는 2019년 말 5G 전략을 멀티 벤더(다중 공급사 채택) 전략으로 수정하여 삼성, 노키아, 화웨이를 우선협상 대상으로 지정하였고, 결국 2020년 3월 삼성과 공급계약을 체결하였다.[75] 보다폰 역시 글로벌 전략에 따라 당분간 핵심 네트워크에 화웨이 장비 사용을 중단하겠다고 밝혔다. 그럼에도 멀티 벤더 전략에 따라 이들 통신사가 화웨이를 공급업체로 택할 가능성이 여전히 남아있다는 점에서 뉴질랜드와 화웨이 관계는 교착상태에 머물러있다.

3. 데이터 유통에 관한 국제규범 논의 구조에서 각국의 위치

앞서 본 바와 같이, 영국, 호주, 캐나다, 뉴질랜드는 대미관계, 대중관계, 주변 안보 환경에서 각기 당면한 상황적 조건에 따라 데이터 주권론과 데이터 유통론 사이에서 나름대로 위치를 설정해왔다. 그런데 자세히 살펴보면, 이들 4개국은 데이터 주권-유통의 스펙트럼에서 양극단 중 어느 한쪽만을 지향하기보다 각자의 구조적 상황에 따라 데이터 유통과 데이터 주권의 비중을 적절히 조절해 수용하는 방향으로 데이터 안보전략을 모색해왔다. 그 결과 영국과 캐나다는 데이터의 '관리된 유통'을, 호주와 뉴질랜드는 데이터의 '관리된 통제'를 지향하게 되었다. 여기서 한가지 짚고 넘어갈 점은 이들 4개국 모두가 데이터 유통에 관한 국제협약에 회원국으로 참여하거나 참여를 희망해왔다는 사실이다. 이것이 의미하는 바는, 이들 4개국이 정도의 차이는 있지만 모두 데이터의 초국적 이동을 위한 국제규범 모색에 동참해왔다는 것이다. 따라서 파이브 아이즈 4개국의 데이터 안보전략은 대미관계, 대중관계, 주변 안보 환경의 상황적 조건 이외에도 데이터 유통에 관한 국제규범 논의 구조에서 각국이 차지하는 위치, 즉 데이터 유통을 지지하는 국제 협약에 각국이 참여해온 상황에도 영향을 받았다고 볼 수 있다. 이 점에서 데이터 무역에 관한 대표적인 협약인 CPTPP, USMCA 등에 각국이 동참해온 양상에도 주목할 필요가 있다.

영국은 브렉시트 이후에도 유럽연합과의 자유로운 데이터 이동이 국익에 부합하다는 판단에서 자국 <데이터보호법>에 GDPR을 흡수하기로 함으로써 유럽연합의 데이터 주권 보호

---

74) Bill Bennett, "Huawei's role in NZ runs way deeper than 5G," *NZ Herald*, April 3, 2019. https://www.nzherald.co.nz/business/huaweis-role-in-nz-runs-way-deeper-than-5g/S5AWQLQXMAOMEXLN2LRV5URLUU/ (검색일: 2021.6.25.)

75) 장주영, "삼성 5G 영토확장, 화웨이 4G 쓰던 뉴질랜드 뺏었다," 『중앙일보』 2020년 3월 6일, https://news.joins.com/article/23723404 (검색일: 2021.6.23.)

에 대한 지속적인 참여를 약속하였다. 그러나 데이터 주권론에 대한 영국의 지지는 어디까지나 유럽 차원에만 국한된 것으로서, 국제적 차원에서는 데이터의 초국적 유통규범을 모색하는 협약에 적극적으로 참여해왔다. 2020년 9월 영국은 브렉시트 이후 처음으로 일본과 자유무역협정을 체결함으로써 데이터 지역화 금지에 합의하였는데, 이에 대해 영국 정부는 해당 협정이 CPTPP로 나아가기 위한 초석이라 밝혔다.[76] CPTPP가 기본적으로 데이터의 초국적 이동을 지지하는 국제 협약이라는 점을 고려할 때, 데이터 유통에 관한 국제규범 논의 구조에서 영국이 차지하는 위치는 데이터의 관리된 유통을 모색하는 대응전략에 어느 정도 영향을 미쳤다고 볼 수 있다.

국가안보를 앞세워 데이터 주권 강화를 모색해온 호주 역시 CPTPP 회원국이라는 점에서 데이터 유통을 둘러싼 국제규범 논의에 사실상 참여해왔다. 앞서 본 것처럼, 호주는 국가안보상의 이유로 데이터 주권 행보를 보여왔지만, 기본적으로 자국 기업들의 성장에 자유로운 데이터 이동이 필요하다는 인식에서 CPTPP를 통한 데이터의 초국적 유통을 지지해왔다. 근래 중국발 사이버 위협이 급증하면서 데이터 주권 강화를 위한 법제 마련에 주력하면서도 CPTPP에 따라 원칙적으로 데이터 지역화 강제조치에 반대한다는 뜻을 고수해온 것이다. 이러한 입장은 최근 미국과 디지털 협정을 주도해온 시노디노스(Arthur Sinodinos) 주미 호주대사의 발언에서도 잘 나타나는데, 그는 미국과의 협정이 호주 중소기업(SME)의 디지털 무역을 촉진하기 위한 장벽 제거 및 규범·표준 설정에 집중될 것이라고 밝히기도 하였다.[77]

한편 CPTPP뿐만 아니라 USMCA에도 참여하고 있는 캐나다는 데이터 유통에 관한 국제규범 논의 구조에서 미국과 가장 근접한 위치에 놓여있는 국가라 할 수 있다. 물론 국내적 차원에서 데이터 유통론에 대한 합의가 완벽히 이루어졌다고 보긴 어려운데, 캐나다와 미국의 프라이버시 및 데이터 보호 관련 규제 체계 사이에 많은 차이점이 존재하는 상황에서 USMCA 체결을 통해 데이터 현지화가 철저하게 금지되면서 캐나다 사회 일각에서는 향후 정보의 흐름이 자국의 경제, 사회, 국가안보 등에 더 큰 영향을 미치게 되는 시점에 정부가 USMCA로 인해 자체적인 데이터 안보 관련 규제나 정책을 시행하는 데 어려움을 겪게 될 수 있다는 우려가 제기되었다.[78] 더욱이 캐나다 주정부(provincial government) 중 브리티시 콜럼비아, 노바스코샤 주(州) 등 일부가 데이터의 이동을 제한하거나 데이터 현지화를 따르고 있기에 미국으로의 데이터 이동 문제를 두고 연방정부와 주정부 간 충돌이 불가피하다는 전망 역시 존재한다.[79] 한편 데이터의 국외 이전에 대한 국민적 우려도 높게 나타났는데, 한 설문조사 결과에 따르면, 브리티시컬럼비아주에 거주하는 캐나다 국민의 75%가 개인정보의 국외 이전을 우려하는 것으로 나타났다.[80] 이렇듯 데이터 유통론에 대한 국민적 합의 및 연방·주정부 간 법제적 호환이 제대로 마련되지 못하였지만, 캐나다는 오랜 기간 미국과 함께

---

76) UK Department for International Trade, “Press release: UK and Japan agree historic free trade agreement,” Government of the United Kingdom, September 11, 2020. https://www.gov.uk/government/news/uk-and-japan-agree-historic-free-trade-agreement (검색일: 2021.6.27.)

77) James Riley, “Australia-US in talks on digital trade pact,” *InnovationAus*, June 7, 2021. https://www.innovationaus.com/australia-us-in-talks-on-digital-trade-pact/ (검색일: 2021.6.28.)

78) Max Jarvie, “Canada: Cross-border transfers and data localisation after the USMCA,” OneTrust DataGuidance, June, 2020. https://www.dataguidance.com/opinion/canada-cross-border-transfers-and-data-localisation (검색일: 2021.5.9.)

79) Chetan Phull, *Big Data Law in Canada*, Smartblock Law Professional Corporation, 2019, pp. 68-70.

80) FIPA, “British Columbians want action on privacy protection: Polling results,” June 4, 2020. https://fipa.bc.ca/2020-privacy-poll/ (검색일: 2021.5.10.)

데이터 유통에 관한 국제규범 모색에 앞장서왔기에 데이터의 초국적 이동을 지지하는 입장이 확고히 유지될 수 있었다.

호주와 마찬가지로 데이터의 관리된 통제를 지향해온 뉴질랜드 역시 CPTPP 원칙에 근거하여 데이터의 초국적 이동을 지지해왔다. 최근 정부 차원의 클라우드 서비스 도입이 가속화되면서 데이터 유출 문제가 부각되자 뉴질랜드는 데이터의 국외 저장·처리·이전을 효과적으로 관리하는 제도적 장치를 마련하게 되었지만, 나머지 정보동맹국들과 마찬가지로 데이터 현지화를 지양하며 데이터 유통에 관한 국제규범 모색에 동참해왔다. 일례로, 2018년 말 호주가 지원및접근법을 제정함에 따라 호주 영내에 보관된 뉴질랜드 정부와 국민의 데이터가 위협받을 수 있다는 우려가 제기되면서 데이터 현지화에 대한 요구가 국내적으로 증가하였는데, 이에 대해 뉴질랜드 내무부(Department of Internal Affairs)는 기존의 클라우드 서비스 관할권 위험 관리 대응법을 수정하지 않고도 충분히 위험을 관리할 수 있다는 입장을 밝힘으로써 데이터 주권 행보가 데이터 현지화로 이어지는 것을 경계하는 모습을 보였다.[81]

Ⅴ. 결론

미중 디지털 패권경쟁의 구조 속에서 미국의 화웨이 퇴출 및 데이터 공유 압박을 받아온 영국, 호주, 캐나다, 뉴질랜드는 미국의 정보동맹국으로서 이들이 갖는 공통된 위치나 서방 자유민주주의 국가로서 갖는 비슷한 속성에도 불구하고 화웨이 사태와 데이터 안보 문제에 상이한 방식으로 접근해왔다. 이러한 상이한 대응전략은 강대국과의 동맹관계에 초점을 둔 현실주의에 입각한 위계적 구조론이나 특정 국가군의 행태, 기질 등에 주목하는 속성론, 또는 경제적 상호의존에 입각한 자유주의 등 전통적인 국제정치이론의 시각에선 충분히 설명되지 않는다. 이러한 문제의식을 바탕으로 본 논문은 구조와 행위자를 복합적으로 엮어서 보는 구조적 위치론의 시각에서 이들 4개국의 대응전략을 비교분석하였다.

이들 4개국은 미중 디지털 패권경쟁 속에서 공통적으로 미국의 동료 압박과 미중 양자택일의 압박을 받아왔지만, 좀 더 자세히 살펴보면 대미·대중관계, 주변 안보 환경, 화웨이와의 관계, 그리고 데이터 유통에 관한 국제규범 논의 구조에서 각기 다른 상황과 위치에 놓여있었다. 이러한 상이한 구조적 상황과 위치로 인해 이들 국가는 서로 대비되는 대응의 경로를 추구하며 미국의 화웨이 배제와 데이터 유통 압박을 수용하는 정도에서 차이를 드러냈다.

파이브 아이즈 4개국은 미국의 동맹국이면서 동시에 중견국이라는 점을 고려할 때, 본 논문은 이들 국가와 비슷한 처지에 있는 또 다른 중견국 한국에도 시사하는 바가 크다. 미국과 중국의 디지털 패권경쟁이 심화하는 상황은 미국을 동맹국으로, 중국을 최대 무역국으로 두고 있는 한국에게 심각한 위기가 되고 있다. 이러한 상황 가운데 트럼프 행정부 집권 시기 한국은 화웨이 배제 결정을 유보하는 등 전략적 모호성을 유지하며 미중 양자택일의 압박을 회피하고자 노력해왔다. 2020년 말 미국 의회가 화웨이의 5G 장비를 도입한 국가들에 미군과 미국의 전략무기 배치를 불허 또는 철회하는 조항을 마련하면서 화웨이 사태가 다시 한번 쟁점화되었을 때에도 한국은 화웨이를 배제하지 않았다. 현재까지도 한국은 화웨이 문

81) Richard MacManus, “Australia’s encryption law threatens NZ cloud data,” *Newsroom,* December 18, 2018. https://www.newsroom.co.nz/australias-new-encryption-law-threatens-nz-cloud-data (검색일: 2021.5.11.)

제가 민간 차원에서 다뤄질 문제라는 초기 입장을 그대로 유지해오고 있다.

바이든 행정부 출범 이후로도 미중 디지털 패권경쟁은 그대로 유지되고 있으며, 어떤 측면에서는 우방국에 대한 미국의 반중 연대 압박이 이전보다 더 강해지기도 하였다. 따라서 '제2의 화웨이 사태'나 새로운 '데이터 안보 사태'가 한국을 비롯한 중견국들에게 다시 한번 심각한 도전이 될 가능성은 여전히 크게 남아있다. 본 논문이 조명한 파이브 아이즈 4개국의 대응 사례에서 드러나는 바와 같이, 한국의 사이버·데이터 안보전략 역시 한국이 당면한 구조적 상황과 그 안에서의 위치를 고려하여 마련되어야 할 것이다.

참고문헌

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

_____. 2016. “제3세대 중견국 외교론의 모색: 네트워크 이론의 시각.” 손열, 김상배, 이승주 편. 『한국의 중견국 외교: 역사, 이론, 실제』 명인문화사. pp. 29-63.

_____. 2017. “세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각.” 『국제지역연구』 26권 3호, pp.67-108.

_____. 2019a. “사이버 안보와 미중 기술패권 경쟁: 그 진화의 복합지정학.” EAI 특별기획논평 시리즈: 미중 경쟁과 세계 정치 경제 질서의 변환 - 기술편.

_____. 2019b. “미중 데이터 규범경쟁과 한국: 유럽연합의 ‘데이터 주권론’이 주는 함의.” EAI 특별기획논평 시리즈, 동아시아연구원. 2019년 10월 28일.

박영욱. 2020. “화웨이 제재를 위한 미국의 법적 조치.” KISA Report vol. 9, 한국인터넷진흥원. 2020/9.

박재적. 2021. “호주의 화웨이 배제: 주요 동인, 프레임 짜기, 연대 외교.” 서울대학교 국제문제연구소 이슈브리핑 123호.

송영진. 2018. “미국의 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점.” 『형사정책연구』29권 2호. pp.149-172.

유인태. 2021. 2021. “파이브 아이즈 캐나다의 화웨이 사태 대응 전략: '결정 부재의 결정'.” 서울대학교 국제문제연구소 이슈브리핑 122호.

유재동, 이건혁. 2020. “美의회 ‘미군 해외배치때 화웨이 사용여부 고려’.” 『동아일보』 2020년 12월 7일. https://www.donga.com/news/Inter/article/all/20201207/104314856/1

이슬기. 2021. “[줌인] 濠 때리고 뉴질랜드와 무역 강화...'反中 동맹' 와해 노리는 中.” 『조선일보』, 2021년 1월 27일. https://biz.chosun.com/site/data/html_dir/2021/01/27/2021012702280.html

이응용. 2020. “미국과 중국의 5G 사이버보안 최신 정책 동향.” *KISA Report* vol.9, 한국인터넷진흥원, 2020년 9월.

장주영. 2020. “삼성 5G 영토확장, 화웨이 4G 쓰던 뉴질랜드 뺏었다.” 『중앙일보』 2020년 3월 6일. https://news.joins.com/article/23723404

전재성. 2014. “네트워크 이론의 관점에서 본 북핵 문제와 6자 회담.” 『국가안보와 전략』14권 2호, pp.57-93.

전혜원. 2021. “영국의 화웨이 정책: 관리에서 퇴출까지.” 서울대학교 국제문제연구소 이슈브리핑 121호.

조재용. 2020. “‘중국과 수교 50주년’ 캐나다총리 강압 외교에 우방과 협력대처.” 『연합뉴스』, 2020년 10월 14일. https://www.yna.co.kr/view/AKR20201014075500009

조창원, 이정은. 2017. “미국 동맹국 잇단 이탈…친중행보 가세.” 『파이낸셜뉴스』, 2017년 12월 4일. https://www.fnnews.com/news/201712041555233715

『중앙일보』. 2018. “캐나다에 이어 뉴질랜드도 화웨이 배제 안하기로.” 『중앙일보』, 2018년 11월 26일. https://news.joins.com/article/23157264

진영화. 2019. “메르켈 ‘유럽, 실리콘 밸리에 데이터 주권 빼앗겨선 안돼’.” 『매일경제』 2019년 11월 13일. https://www.mk.co.kr/news/world/view/2019/11/940146/

최종현. 2020. “중견국 공적개발원조 정책의 결정요인: 스웨덴과 호주의 비교를 중심으로.” 김상배, 이승주, 전재성 엮. 『중견국 외교의 세계정치: 글로벌-지역-국내 삼중구조 속의 대응전략』 사회평론아카데미. pp.123-153.

표나리. 2020. “2020년 홍콩 국가보안법 통과의 의미와 시사점.” IFANS 주요국제문제분석 2020-25. 국립외교원 외교안보연구소. 2020년 8월 19일.

한국인터넷진흥원. 2019. “2019 글로벌 정보보호 산업시장 동향조사 보고서(30개국).” 2019년 12월 13일.

_____. 2020a. “미-호주 간 클라우드법 행정협정 체결 이슈,” 2020년 5월.

_____. 2020b. “캐나다 소비자 개인정보보호법(CPPA) 제정 배경 및 주요 특징 분석.” 『해외 개인정보보호 동향보고서』 2020년 11월.

Arcadis. 2021. The Arcadis Data Center Location Index 2021. https://datacenters.arcadis.com/locationindex/p/1

Australian Department of Defence. 2016. *2016 Defence White Paper*. Commonwealth of Australia, Canberra.

Australian Department of Home Affairs. 2019a. “The Assistance and Access Act 2018.” Commonwealth of Australia. September 16, 2019. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

Australian Minister for Home Affairs. 2019b “Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton.” Commonwealth of Australia. October 7, 2019. https://minister.homeaffairs.gov.au/peterdutton/Pages/australian-negotiation-cloud-act.aspx

Australian Security Intelligence Organisation. 2009. *ASIO Report to Parliament 2008-09.* Commonwealth of Australia, Canberra.

_____. 2016. *ASIO Report to Parliament 2015-16.* Commonwealth of Australia, Canberra.

Bennett, Bill. 2019. “Huawei's role in NZ runs way deeper than 5G.” *NZ Herald.* April 3, 2019. https://www.nzherald.co.nz/business/huaweis-role-in-nz-runs-way-deeper-than-5g/S5AWQLQXMAOMEXLN2LRV5URLUU/

Burt, Ronald S. 1992. *Structural Holes: The Social Structure of Competition.* Cambridge, MA: Harvard University Press.

Burton, Tom. 2020.“Sensitive data to remain in Australia,” *Australian Financial Review.* July 6, 2020.

https://www.afr.com/policy/foreign-affairs/sensitive-data-to-remain-in-australia-20200706-p559kn

Buzan, Barry, Wæver, Ole, and Wilde, Jaap de, 1998. *Security: A New Framework for Analysis.* Boulder, Colorado: Lynne Rienner Publisher.

Bryan-Low, Cassell, and Packham, Colin. 2019. "How Australia led the US in its global war against Huawei." *The Sydney Morning Herald.* May 22, 2019. https://www.smh.com.au/world/asia/how-australia-led-the-us-in-its-global-war-against-huawei-20190522-p51pv8.html

Cisco. Cisco 2018 Asia Pacific Security Capabilities Benchmark Study. 2018.

Coyne, John, Shoebridge, Michael and Zhang, Albert. 2020. "National security agencies and the cloud: An urgent capability issue for Australia." *ASPI Special Report.* Australian Strategic Policy Institute.

Doherty, Ben and Davey, Melissa. 2019. "Peter Dutton: China accuses home affairs minister of 'shocking' and 'malicious' slur." *The Guardian.* October 12, 2019. https://www.theguardian.com/australia-news/2019/oct/12/peter-dutton-accuses-china-of-stealing-intellectual-property-and-silencing-free-speech

Duke, Jennifer. 2018. "Huawei's history with Australia." *The Sydney Morning Herald.* December 8, 2018. https://www.smh.com.au/business/companies/huawei-s-history-with-australia-20181207-p50kyj.html

Fife, Robert, and Chase, Steven. 2018a. "Ottawa launches probe of cyber security." *The Globe and Mail.* September 18, 2018. https://www.theglobeandmail.com/politics/article-ottawa-launches-probe-of-cyber-security/

_____. 2018b. "Ottawa not ruling out blocking Huawei from 5G supply contracts." *The Globe and Mail.* November 1, 2018. https://www.theglobeandmail.com/politics/article-ottawa-not-ruling-out-blocking-huawei-from-5g-supply-contracts/

Fildes, Nic. 2018. "How Huawei used the UK to become a global gaint." *Financial Times.* December 8, 2018. https://www.ft.com/content/16381afa-f986-11e8-8b7c-6fa24bd5409c (검색일: 2021.6.25.)

FIPA. 2020. "British Columbians want action on privacy protection: Polling results." June 4, 2020. https://fipa.bc.ca/2020-privacy-poll/

Geist, Michael. 2018. "How Canada Surrendered Policy Flexibility for Data Localization Rules in the USMCA." Personal website. October 10, 2018. https://www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/

House of Commons. 2020. 'The Security of 5G', Defence Committee, Second Report of

Session 2019-21, HC 201, House of Commons. 8 October 2020. https://committees.parliament.uk/publications/2877/documents/27899/default/

Jarvie, Max. 2020. "Canada: Cross-border transfers and data localisation after the USMCA." OneTrust DataGuidance. June, 2020. https://www.dataguidance.com/opinion/canada-cross-border-transfers-and-data-localisation

Jelinek, Andrea. 2020. "Letter to the European Parliament members." European Data Protection Board. June 15, 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf

Kassam, Natasha. 2019. *Lowy Institute Poll 2019.* Lowy Institute, Sydney.

Knaus, Christopher. and Phillips, Tom. 2017. "Turnbull says Australia will 'stand up' to China as foreign influence row heats up." *The Guardian.* December 9, 2017. https://www.theguardian.com/australia-news/2017/dec/09/china-says-turnbulls-remarks-have-poisoned-the-atmosphere-of-relations

KOTRA. 2020. "USMCA 발효에 따른 산업별 영향 및 시사점." Global Market Report 20-012. 2020년 6월.

Long, Tom. 2017. "Small States, Great Power? Gaining Influence Through Intrinsic, Derivative, and Collective Power." *International Studies Review,* 19. pp.185-205.

MacManus, Richard. 2018. "Australia's encryption law threatens NZ cloud data." *Newsroom.* December 18, 2018. https://www.newsroom.co.nz/australias-new-encryption-law-threatens-nz-cloud-data

Nakajima, Yusuke. 2020. "UK calls on South Korea, India and Australia to attend G-7 summit." *Nikkei Asia.* December 16, 2020. https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/UK-calls-on-South-Korea-India-and-Australia-to-attend-G-7-summit

National Cyber Security Centre. 2017. *The cyber threat to UK business: 2016/2017 Report.*

_____. 2020. *Summary of the NCSC analysis of May 2020 US sanction.* December 14, 2020. https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction

New Zealand Department of Prime Minister and Cabinet. 2019. *New Zealand's Cyber Security Strategy.*

New Zealand Government. 2017. *Managing Jurisdictional Risks for Public Cloud Services.* 2017/7. https://snapshot.ict.govt.nz/resources/digital-ict-archive/static/localhost_8000/guidance-and-resources/using-cloud-services/assess-the-risks-of-cloud-services/jurisdictio

nal-risks/index.html

_____. 2020. Privacy Act 2020. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

New Zealand Legislation. 2020. "Privacy Act 2020," June 30, 2020. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

New Zealand Ministry of Foreign Affairs and Trade. 2020. "The Application of International Law to State Activity in Cyberspace." December 1, 2020. https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il/

NZ Herald. 2018. "New Zealand MPs told to delete TikTok over security concerns." *NZ Herald.* August 4, 2018. https://www.nzherald.co.nz/nz/new-zealand-mps-told-to-delete-tiktok-over-security-concerns/BQU5VV2YFBAO2AAHXMOBBLJLMY/

Office of the Privacy Commissioner of Canada. 2020. "Appearance before the Committee on Institutions of the National Assembly of Quebec regarding Bill 64, An Act to modernize legislative provisions as regards the protection of personal information." September 24, 2020. https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200924/

O'Neil, Andrew. 2017. "Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance," *Australian Journal of International Affairs* Vol. 71, No. 5, pp.529- 543.

Packham, Colin. 2019. "Exclusive: Australia concluded China was behind hack on parliament, political parties - sources." *Reuters.* September 16, 2019. https://www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VF

Parliamentary Counsel Office. 2013. Telecommunications (Interception Capability and Security) Act 2013. 2013/11/11. https://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.html

Phull, Chetan. 2019. *Big Data Law in Canada.* Smartbloc Law Professional Corporation. 2019.

Radio New Zealand. 2018. "Reasons to block Spark's 5G rollout 'classified'." *Radio New Zealand.* 28 November 2018. https://www.rnz.co.nz/news/national/377014/reasons-to-block-spark-s-5g-rollout-classified

_____. 2020a. "No UK approach to Huawei for NZ, but using it here not ruled out completely," *Radio New Zealand.* 29 January 2020. https://www.rnz.co.nz/news/political/408379/no-uk-approach-to-huawei-for-nz-but-using-it-here-not-ruled-out-completely

_____. 2020b. “Andrew Little says New Zealand won't follow UK's Huawei 5G ban.” *Radio New Zealand.* 15 July 2020. https://www.rnz.co.nz/news/political/421286/andrew-little-says-new-zealandwon-t-follow-uk-s-huawei-5g-ban

Richardson, Jeffrey T., and Ball, Desmond. 1990. *The ties that bind: Intelligence Cooperation between the UKUSA Countries-the United Kingdom, the United States of America, Canada, Australia and New Zealand.* Sydney: Allan & Unwin.

Riley, James. 2021. “Australia-US in talks on digital trade pact.” *InnovationAus.* June 7, 2021. https://www.innovationaus.com/australia-us-in-talks-on-digital-trade-pact/

Sandle, Paul. 2019. “Vodafone says complete UK ban on Huawei would cost it millions of pounds,” *Reuters,* March 7, 2019. https://www.reuters.com/article/us-britain-vodafone-huawei/vodafone-says-complete-uk-ban-on-huawei-would-cost-it-millions-of-pounds-idUSKCN1QO1LZ

Tillett, Andrew. “Chinese spies suspected in cyber attack on major parties.” *The Australian Financial Review.* February 18, 2019. https://www.afr.com/politics/cyber-attack-on-major-parties-computer-systems-scott-morrison-reveals-20190218-h1bdzm

Turnbull, Malcolm. 2019a. “Address to the Henry Jackson Society, London.” The Hon Malcolm Turnbull's official website. March 5, 2019. https://www.malcolmturnbull.com.au/media/address-to-the-henry-jackson-society-london

_____. 2019b. “Malcolm Turnbull warns Brits about letting Huawei build 5G network.” *The Sydney Morning Herald.* March 6, 2019. https://www.smh.com.au/world/europe/malcolm-turnbull-warns-brits-about-letting-huawei-build-5g-network-20190306-p5120s.html

UK Department for Digital, Culture, Media & Sport. 2019. UK Telecoms Supply Chain Review Report, CP 158. Government of the United Kingdom. July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

_____. 2021. “UK government welcomes the European Commission's draft data adequacy decisions,” Government of the United Kingdom. February 19, 2021. https://www.gov.uk/government/news/uk-government-welcomes-the-european-commissions-draft-data-adequacy-decisions

UK Department for International Trade. 2020. “Press release: UK and Japan agree historic free trade agreement.” Government of the United Kingdom.. September 11, 2020. https://www.gov.uk/government/news/uk-and-japan-agree-historic-free-trade-agreement

Young, Ian. “Canada faces new pressure to block Huawei from 5G, after UK ban risks marooning Ottawa from Five Eyes intelligence allies.” *South China Morning Post.* Jul 15, 2020. https://www.scmp.com/news/china/diplomacy/article/3093198/canada-faces-new-pressure-block-huawei-5g-after-uk-ban-risks

Zhiyue, Bo. 2021. “Is New Zealand moving away from its traditional pro-China policy?.” *South China Morning Post.* May 7, 2021. https://www.scmp.com/week-asia/opinion/article/3132468/new-zealand-moving-away-its-traditional-pro-china-policy