아태연구 제30권 제2호 (2023) https://doi.org/10.18107/japs.2023.30.2.003

# 영국의 사이버 안보 전략 지향성과 결정 요인:

## 화웨이 사태와 데이터 안보에 대한 대응을 중심으로

신승휴*

| 목 차 |



| 논문요약 |

이 글은 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응에서 일관되게 나타나는 전략적 지향성을 포착하여 사이버 안보 전략 기조와 그 결정 요인을 분석한다. 역할이론과 정보순환론의 논의를 복합적으로 원용하여 정책결정자의 위협인식과 국제적 역할구상 그리고 정보기관의 판단이 사이버 안보 이슈에 대한 영국의 대응을 결정하는 주요 요인으로 작용한 과정을 추적한 이 글은 영국의 사이버 안보 전략이 자유민주주의 연대 구축을 주도하려는 기조를 보이게 된 배경에 영국 정부의 대중국 위협인식과 국제적 역할구상 그리고 GCHQ의 사이버 안보 위험평가의 복합적 영향이 존재하였음을 주장한다. 이를 통해 국가 사이버 안보 전략은 외생적-구조적 요인 외에도 내생적-관념적 요인에도 영향을 받아 수립·추진되며, 아울러 이슈별 대응을 관통하는 전략적 지향성에 대한 분석이 선행되어야만 사이버 안보 전략의 성격과 방향성을 더욱 분명히 이해할 수 있음을 보이고자 한다.

▪ 주제어: 사이버 안보, 화웨이 사태, 데이터 안보, 영국, 정부통신본부

* 서울대학교 정치외교학부 박사과정

# Ⅰ. 머리말

2021년 12월 영국은『국가사이버전략 2022(National Cyber Strategy 2022)』을 발표함으로써 자국 사이버 안보 전략의 핵심이 국익 보호와 체제 수호를 위한 자체적인 역량 강화와 국제적 연대 구축에 있음을 천명하였다(HM Government 2021b). 특히 국제적 연대 구축을 위해 자유롭고 개방된 사이버 공간을 추구하고, 사이버 공간에서 자유민주적 국제규범을 형성하며, 자유민주주의 진영을 중심으로 하는 디지털 진지를 구축하는 데에 적극적으로 참여하겠다는 의지를 드러냈다. 그와 동시에 자국에 대한 사이버 공격의 주요 가해국이자 권위주의적 사이버 안보 거버넌스를 추구하는 경쟁국으로 중국, 러시아 등을 지목하기도 하였다. 이처럼 영국의 새로운 사이버 안보 전략은 사이버 공간을 이념과 체제의 경쟁이 전개되는 무대로 보는 인식과 그러한 경쟁에서 야기되는 도전 및 국제적 협력을 요구하는 문제들에 자유민주주의 동맹으로 대응한다는 동맹과 진영의 논리를 강하게 드러냈다.

사실『국가사이버전략 2022』에 담긴 이러한 인식과 논리는 2020년을 전후로 영국이 보인 사이버 안보 관련 이슈에 대한 대응 방식에서도 유사하게 나타났다. 특히 화웨이 사태와 데이터 안보 문제의 대응 과정에서 비슷한 인식과 논리가 적용된 듯 보였다. 2010년대 후반까지만 해도 화웨이 장비 사용을 허가하고 이를 자체적으로 관리하겠다는 뜻을 견지해온 영국은 2020년 6월 중국과의 관계 악화에 따른 막대한 경제적 손실 위험에도 불구하고 화웨이 장비를 완전히 퇴출하였다. 아울러 데이터 안보와 관련해서도 유럽의 데이터 주권론이 팽배한 상황에서 유럽연합의 반대를 무릅쓰고 미국과 데이터 공유 행정협정을 체결하는 모습을 보이기도 하였다.

이렇듯 2020년을 전후로 영국은 사이버 안보 분야에서 미국과 적극 발을 맞추고, 비유럽 차원의 협력을 모색하며, 중국과의 관계 악화에 따른 비용을 감수하는 등 기존의 정책 노선을 이탈하는 듯한 행보를 보이기 시작하였다. 또한 사이버 공간의 국제규범과 질서를 자유민주주의라는 가치와 연결 지어 추구하면서 언뜻 보기에 미국이 주도하는 반중(反中) 전선에 적극적으로 참여하는 듯하였다. 이러한 기류 속에서 사이버 안보를 단순히 사이버 공격에 대한 방어와 피해 관리의 문제로 보는 기존의 접근을 넘어 자유민주주의 연

대와 동맹으로 맞서야 하는 문제로 격상하기에 이르렀다.

최근 영국의 사이버 안보 전략을 주제로 한 연구는 주로 사이버 전략의 내용과 추진체계의 변화를 조명하거나(Prince & Sullivan 2019; 조은정 2022), 사이버 안보에 대한 정부와 민간의 협력 양상의 변화를 분석하는 데 초점을 맞추고 있다(Carr 2016; Carr & Tanczer 2018). 또는 전략의 변화를 사이버 위협에 대한 영국의 군사적 이해의 맥락에서 접근해 분석하는 시도도 있다(Sexton 2016; Thornton & Miron 2019). 그러나 2020년 전후를 기점으로 포착되는 영국의 사이버 안보 전략 기조와 사이버 안보 분야의 주요 쟁점 이슈들에 대한 대응 방식 간 상관성에 주목하여 그 전략적 지향성을 조명한 연구는 아직 제대로 이루어지지 못한 상황이다. 또한 외부 위협의 증가 같은 외생적 요인이 아닌 국가 내부 행위자들의 인식이나 판단 등 내생적 요인의 영향을 중심으로 영국의 사이버 안보 전략을 분석한 연구 역시 미진하다.

사이버 위협에 대한 영국의 인식은 이미 2000년대 후반부터 2010년대를 거치며 지속해서 강화되어왔다는 점을 고려할 때 2020년을 전후로 나타난 이 같은 전략적 지향성은 단순히 사이버 위협의 양적 증가만으로는 설명되지 않는다(HM Government 2009). 미국의 반중 전선에 대한 참여 압박이 영국의 전략 변화를 유도한 단일한 요인이었다고 보기도 어려운데, 이는 미국의 대중국 디지털 경제 봉쇄 전략과 이에 대한 동맹국의 참여 압박이 이미 2017년부터 이루어졌기 때문이다(신승휴 2022, 118-125). 즉 외부 환경의 변화 이외에도 추가적인 요인이 존재하였음을 의미한다. 이러한 문제의식을 바탕으로 이 글은 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응을 살펴보고, 이슈별 대응에서 일관되게 나타나는 전략적 지향성(strategic orientation)을 포착함으로써 영국의 사이버 안보 전략 기조와 그 결정 요인을 찾는 것을 목적으로 하였다.

이 글은 영국이 2020년을 전후로 자국의 사이버 안보 전략 기조를 자체적인 공격 방어와 위협 관리에서 자유민주주의 연대 구축과 이를 위한 주도적 역할 모색으로 전환하였으며, 이러한 전략적 지향성의 변화는 영국 정부의 대(對)중국 위협인식과 국제적 역할구상(role conception)이 주요 동인으로 작용하는 가운데 사이버 안보에 대한 국가정보기관 정부통신본부(Government

Communications Headquarters: 이하 GCHQ)[1]의 위험평가(risk assessments)가 정부의 결정에 영향을 미치게 되면서 나타난 결과라고 주장한다. 따라서 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응 역시 중국에 대한 정부의 위협인식, '민주주의 동맹을 통한 국제질서 보호'와 '글로벌 선도국으로서 자국의 국제적 영향력 확장'을 추구하는 정부의 역할구상, 그리고 사이버 안보에 대한 GCHQ의 위험평가와 밀접한 관련이 있는 것으로 볼 수 있다.

이러한 시각을 뒷받침하기 위해 이 글은 역할이론(role theory)과 정보순환론(intelligence cycle theory)의 논의를 복합적으로 원용함으로써 영국 정부의 대중국 위협인식과 국제적 역할구상이 GCHQ의 사이버 안보 위험평가와 결합하면서 사이버 안보 전략의 주요 결정 요인으로 작용하는 과정을 추적하고자 하였다. 역할이론과 정보순환론은 각각 외교정책연구와 국가정보연구에 적용되고 있지만, 이들 이론의 시각에서 국가 사이버 안보 전략을 분석한 연구는 미진한 상황이다. 국가 사이버 안보 전략 또는 사이버 안보 이슈에 대한 국가적 차원의 대응은 국가 간 갈등과 협력의 장으로 부상한 사이버 공간을 대상으로 하는 국가전략이며, 이를 수립하고 추진하는 과정에서 정책결정자와 정보기관의 상호작용이 중요하다는 점에서 역할이론과 정보순환론은 유용한 이론적 자원을 제공한다고 할 수 있다.

이 글은 크게 세 부분으로 구성되었다. Ⅱ장에서는 사이버 안보 전략 결정 요인으로서 정책결정자의 위협인식과 국제적 역할구상 그리고 정보기관의 위험평가를 역할이론과 정보순환론을 복합적으로 원용한 시각에서 검토하고, Ⅲ장에서는 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응을 개괄적으로 살펴보았다. 마지막으로 Ⅳ장에서는 영국의 이슈별 대응이 동맹을 활용하여 자유민주주의 연대를 구축하고 이를 주도하려는 일관된 전략적 지향성을 보였음을 조명하고, 이를 바탕으로 영국의 사이버 안보 전략을 결정하는 요인으로서 정부의 대중국 위협인식과 국제적 역할구상 그리고 GCHQ의 위험평가를 추적하였다.

1) GCHQ는 국내외 통신과 전기 신호를 감시해 정보를 수집하고 외국 암호 체계를 해독·분석하는 것을 주요 업무로 하는 국가정보기관이며, 외교장관 직속 기구이지만 외무·영연방·개발부 소속은 아니다.

# Ⅱ. 사이버 안보 전략 결정 요인으로서 위협인식, 역할구상, 위험평가

## 1. 정책결정자의 위협인식과 역할구상

국가전략은 외부 환경이나 특정 이슈에 대한 국가의 대응이자 국익 증진을 위한 의사결정의 결과물을 의미한다. 마찬가지로 사이버 안보 전략 역시 사이버 공간이라는 특수한 환경과 거기에서 발생하는 다양한 안보 이슈들에 대한 국가의 판단을 토대로 내려지는 정책결정과 다름없다. 여기서 국가의 판단이란 결국 안보적 사안, 즉 위협에 관한 정책결정자의 판단으로서 위협인식이라는 개념으로 정의될 수 있다. 따라서 사이버 안보 전략에 내재한 정책결정자의 위협인식은 기본적으로 사이버 안보 환경과 이 분야에서 발생하는 특정 이슈에 대한 인식을 의미한다.

다만, 사이버 안보 전략이 사이버 공간에서 전개되는 국가 간 경쟁과 협력을 염두에 둔 국가전략이라는 점에서 정책결정자의 위협인식은 '사이버'에 대한 인식에만 국한되지 않는다. 사이버 안보는 복합지정학적(complex geopolitical) 성격을 지닌 영역이라는 점에서 이를 대상으로 한 국가전략에는 지정학적 맥락에서 이해되는 국제관계나 특정 국가에 대한 인식까지도 포함될 수밖에 없다. 이러한 관점에서 보자면, 특정 국가가 개입된 사이버 위협을 바라보는 정책결정자는 사이버 위협 자체에 대한 인식과 더불어 지정학적 맥락에서 갖게 되는 그 국가에 대한 인식을 동시에 가진다. 이 같은 위협인식은 정책결정자가 자국에 자의적으로 부과하는 국제적 지위, 역할, 기능 등과도 밀접한 연관성을 가진다는 점에서 중요하다고 볼 수 있다.

자국의 국제적 지위, 역할, 기능 등에 대한 정책결정자의 기대는 역할구상의 논의를 통해 설명될 수 있다. 역할이론의 논의에 의하면, 역할구상은 정책결정자가 국제체제에서 자국이 수행해야 하는 기능과 역할에 대한 정의와 신념을 포함하는 개념이다(유동원 2017, 8). 지도자나 정부 같은 국가 내 주도 세력의 신념이나 '자기구상(self-conception)' 등을 통해 발현되는 역할구상은 타국에 의해 부여되는 역할규정(role prescription)과 대비되는 개념으

로서 특정 국가가 타국과의 관계 속에서 자신의 지위(status)에 대해 가지는 인식으로 정의될 수 있다(Holsti 1970, 245-246).

이 글은 역할구상의 주체로서 정책결정자를 정부로 규정하였다. 국제적 환경 속에서 자국에 걸맞은 기능, 역할, 위신, 행동 등에 대한 신념이나 이미지는 지도자 개인이나 특정 정치 집단의 것으로 개념화될 수도 있지만, 그보다는 국가적 차원에서 공유되는 집단적 기대를 반영하는 개념에 가깝다. 이는 정부가 제시하는 국가의 국제적 역할구상이 대개 사회화와 국제화를 거쳐 국가의 행위를 선도하고 국가전략을 뒷받침하는 안정적인 인식구조이자 신념체계로 자리매김하기 때문이다(유동원 2017, 22-23). 달리 말해 정부의 역할구상은 이미 국내적 지지와 국제적 인정의 조건을 어느 정도 충족함을 의미한다. 따라서 국제체제에서 자국의 위신과 영향력 확보를 추구하는 주체로서 정부가 사실상 정책결정자를 대변하는 것으로 보고, 정부의 역할구상이 이미 국가 내외부적으로 당면하게 되는 여러 제약과 압력으로부터 영향을 받아 형성된 관념적 요인임을 가정하였다(Holsti 1970, 268-269, 294-295).

## 2. 정보기관의 위험평가

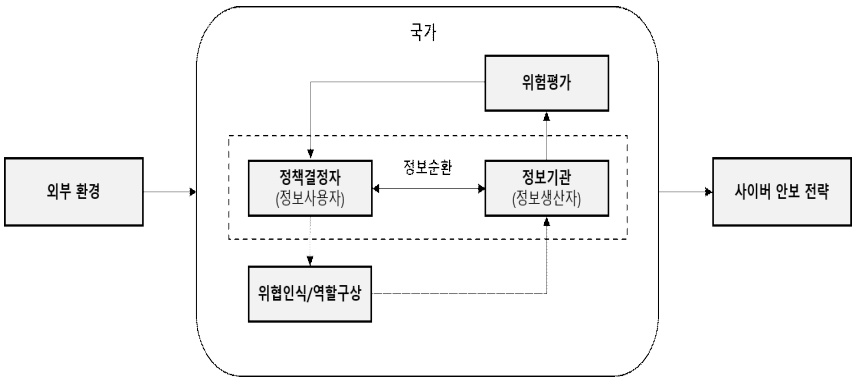
국가전략을 결정하는 또 다른 중요 변수로서 이 글은 정보기관의 위험평가에 주목하였다. 보통 정보기관은 국가지도자나 정부 등 정책결정자의 필요와 지시에 따라 관련 정보를 수집하고 보고하는 역할을 담당하는 조직으로 그려지며, 독립적인 행위자보다는 국가 내부의 수동적인 하위행위자로 취급되는 경우가 많다. 그로 인해 정보기관의 기능과 역할 역시 정보사용자로 구분되는 정책결정자의 정보요구사항(intelligence requirements)을 하달받아 그 필요에 맞춰 정보를 수집·분석·생산·배포하는 것에 한정하기 쉽다(염돈재 2002, 86-88). 하지만 정보화시대에 접어들면서 정보순환과정(intelligence cycle)에서 정보기관은 기존의 수직적이고 획일적인 구조를 벗어나 스스로 정보요구사항과 정보생산의 우선순위를 설정하는 행위자로 부상하였고, 정보분석에서의 기능 역시 크게 증대되고 있다(Marrin 2009, 131-133; 전웅 2015, 14-15).

이러한 현실을 반영하여 최근 정보순환론을 바탕으로 한 연구들은 정보

기관의 확장된 역할과 영향력에 주목하여 정책결정자와 정보기관 간 관계의 변환을 주장한다. 구체적으로, 정보기관의 판단이 정책결정을 위한 정보순환과정에 중요한 영향을 미치게 된다고 보거나(Lockheart 1987), 국가정보의 생산과 배포 과정에서 정보생산자로서 정보기관과 정보사용자로서 정책결정자 간 긴밀한 교류와 접촉을 인정하는 새로운 정보순환모델을 제시한다(Herman 1996, 293-296). 비슷한 맥락에서 정보화시대에 따라 정보순환과정이 정보 분석관과 정보사용자 간 직접적이고 빈번한 접촉이 이루어지는 방향으로 변화할 필요성을 강조하기도 한다(Berkowitz & Goodman 2000, 79).

이러한 논의를 종합하자면, 정보순환과정은 국가안보와 이익에 관한 정책결정을 위한 것이며 정보순환과정에서 정보기관의 행위성(agency), 역할, 기능 등이 강화되었다는 것은 정책결정에 대한 정보기관의 영향력이 증대하였음을 의미한다(Marrin 2009, 133-134). 또한 외부 환경이나 특정 이슈에 대한 정보기관의 위험평가나 판단이 정책결정자에게 더욱 비중 있게 고려될 수밖에 없음을 시사하기도 한다. 특히 사이버 안보와 같이 고도의 전문성이 요구되는 분야에서 정보기관의 위험평가는 정책결정자가 사이버 안보와 관련한 문제상황을 이해하는 과정에 큰 영향을 미치는 변수로 작용한다고 볼 수 있다(문정인 2002, 115).

**<그림 1> 사이버 안보 전략의 변화 동인으로서 정책결정자의 위협인식 및 역할구상과 정보기관의 위험평가**




▪ 염돈재(2002, 86)의 연구에서 제시한 '첩보요구의 순환절차'를 참고하여 저자가 새롭게 구성

위의 논의를 종합해볼 때, 사이버 안보 전략은 정책결정자의 위협인식과 국제적 역할구상 그리고 정보기관의 위험평가에 복합적으로 영향을 받는 것으로 이해될 수 있다. 또한 <그림 1>에서 보는 바와 같이 정부의 위협인식과 국제적 역할구상은 정보기관의 위험평가와 상호구성적인 관계에서 서로 영향을 주고받는 것으로 볼 수 있다. 정책결정자는 특정 이슈와 관련하여 정보기관이 제공하는 위험평가나 판단을 참고해 해당 이슈에 대한 위협인식과 이에 대한 자국의 역할구상을 세우게 되며, 역으로 정보기관의 위험평가나 판단도 정책결정자의 정보요구사항에 담긴 위협인식과 역할구상에 따른 정책선호(policy preferences)를 어느 정도 반영할 수밖에 없기 때문이다(문정인 2002, 118; Herman 1996; Marrin 2009; Berkowitz & Goodman 2010).

# Ⅲ. 사이버 안보 분야 영국의 이슈별 대응

## 1. 화웨이 5G 통신장비 퇴출 결정

2010년대 초 영국의 정보통신 정책은 서비스업에 집중된 자국 산업 구조가 첨단 통신기술 장비 생산에 불리하다는 위기의식을 바탕으로 중국의 투자를 유도하는 데 집중되었다(National Cyber Security Centre 2017, 5; 한국인터넷진흥원 2019). 특히 5G 네트워크 기술과 관련하여 영국은 2010년대에 접어들면서 이미 경제성이 높은 화웨이의 5G 장비를 '필요악'으로 간주하고 이를 도입함으로써 화웨이가 자국 통신망 시장에서 주도적인 위치를 점하는 것을 사실상 용인하였다. 이 시기 영국 기업에 대한 외부의 사이버 공격이 꾸준히 증가하면서 정보보호를 강화할 필요성과 더불어 파이브 아이즈 정보동맹 차원의 공조와 협력의 중요성이 높아졌지만, 영국은 경제적 이해관계에 따라 화웨이를 배제할 수도 없는 처지에 놓여있었기에 화웨이에 대한 영국의 초기 입장은 경제적 이해관계와 외교안보적 이해관계 사이에서 균형을 모색하는 방향으로 설정되었다(전혜원 2021, 1-2).

2018년 7월에는 영국의 화웨이 사이버보안평가센터(Huawei Cyber Security Evaluation Centre: 이하 HCSEC)가 화웨이 장비의 보안 문제를 지적하는 보

고서를 발표하면서 국내적으로 화웨이에 대한 우려가 다시금 나타났지만, 그 이듬해인 2019년 2월 GCHQ 산하 국가사이버보안센터(National Cyber Security Centre: 이하 NCSC)가 5G 네트워크에 화웨이 장비를 사용하더라도 보안 위험을 완화하고 관리할 방법이 있다고 발표함으로써 화웨이에 대한 영국의 수용적 입장은 크게 바뀌지 않았다. 실제로 영국 정부는 2010년부터 NCSC와 HCSEC를 통해 화웨이를 집중적으로 감시하는 맞춤형 보안 전략을 실행함으로써 자체적으로 위험을 관리하는 노력을 전개해왔고, 이를 통해 자국의 주요 통신망과 정보동맹의 공조 체계에 대한 잠재적 위협을 예방하고자 하였다(House of Commons 2020, 4). 그런 이유로 2019년 미국의 화웨이 퇴출 캠페인이 쟁점화되었을 당시 마틴(Ciaran Martin) NCSC 센터장은 영국 공영방송 BBC와의 인터뷰를 통해 지난 10년 동안 파이브 아이즈 동맹국들이 화웨이와 그 외 다른 이슈들에 항상 같은 대응을 해온 것은 아니라며, 미국의 대응과 일치한 정책을 추진할 필요성을 부인하기도 하였다(*Reuters* 2019/04/24). 이렇듯 화웨이의 5G 네트워크 장비 도입이 자국 안보에 위협을 초래할 수 있음에도 불구하고 영국이 화웨이를 퇴출하지 않은 것은 자체적인 위험 관리를 통해 경제성 높은 화웨이 장비 사용을 지속하길 원하였기 때문이다.

그러나 사실 영국의 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(전혜원 2021, 4-5; *ThePrint* 2020/06/04). 이 조치는 화웨이 장비를 전면 배제하진 않더라도 네트워크를 핵심(core)과 비핵심(periphery) 영역으로 구분하고 후자에만 화웨이를 제한적(비핵심 영역 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(National Cyber Security Centre 2020). 나아가 같은 해 11월에는 자국의 비핵심 영역 네트워크에서 화웨이 장비의 점유율을 35%로 제한하는 시기를 2023년 1월까지 한정함으로써 퇴출을 가속화하는 한편, 5G 공급망에 대한 자체적인 투자와 다변화를 추진하기 시작하였다

(*Reuters* 2020/11/30). 이러한 조치는 사실상 일찍이 화웨이 퇴출을 선언한 미국, 호주의 행보와 맥을 같이 하는 것이었다.

실제로 2020년 7월 화웨이 전면 퇴출 결정이 발표되기 약 두 달 전인 5월 영국 정부는 이듬해 있을 G7 정상회의에 한국, 인도, 호주를 게스트 국가로 초청하는 계획을 미국과 논의하였고, 그해 12월 영국 정부는 기존 G7을 확장하는 방식으로 전 세계의 민주적이고 기술이 발전한 국가 간에 협력을 강화한다는 D10(Democracy 10, 또는 민주주의 10개국) 구상을 내놓았다. D10 구상은 화웨이를 대체할 수 있는 공급자를 모색하고 더 나아가 중국 기업을 배제한 5G 공급망을 구축하려는 노력으로 해석되었는데, 해당 구상이 발표된 시점에 다우든(Oliver Dowden) 당시 영국 디지털문화미디어체육부 장관은 자국 정부가 유사입장 국가들과 단일한 통신 전략(telecoms strategy) 수립을 위해 더욱 강력히 협력해나가고 있다고 발언하기도 하였다(*Financial Times* 2020/07/13).

화웨이에 대한 영국의 입장이 이처럼 급변하게 된 데에는 미국의 행정적 조치가 어느 정도 영향을 미쳤다는 점은 부인하기 어렵다. 2020년 5월 15일 내려진 미국의 화웨이 제재조치(Foreign-Produced Direct Product Rule Amendment)는 화웨이 장비에 대한 영국의 대응이 선회할 수밖에 없는 산업적·기술적 환경을 조성하였다는 지적이 있다(Dowden 2020).[2] 2019년 5월 16일 미국은 연방 수출관리규정(Export Administration Regulation: 이하 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(박영욱 2020). 그러나 화웨이 퇴출 결정으로 인

2) Prince, Conrad and James Sullivan (2020), "The UK's New Way on Huawei", https://rusi.org/commentary/uks-new-way-huawei. (accessed on April 24, 2023)

해 초래될 막대한 경제적 손해를 고려할 때(*Information Age* 2020/09/06), 미국의 행정적 조치가 영국의 갑작스러운 입장 변화를 유도한 단일한 요인이었다고 단정하긴 어렵다.

## 2. 데이터 안보 정책의 탈유럽화와 대미 협력 강화

화웨이 사태와 함께 사이버 안보 분야에서 쟁점화된 또 한 가지 중요한 이슈는 민감한 데이터의 저장과 관리 그리고 공유를 둘러싼 데이터 안보 문제였다. 초기 데이터 안보 문제에 대한 영국의 대응은 큰 틀에서 유럽연합의 데이터 주권론에 발을 맞추는 방식으로 전개되었는데, 2018년 5월 유럽연합 차원에서 일반개인정보보호법(General Data Protection Regulation: 이하 GDPR)이 시행되자 영국은 자국의 데이터보호법(Data Protection Act 2018)[3]을 GDPR에 연동하는 방식을 채택하였다. GDPR은 유럽연합 회원국 간 개인정보의 자유로운 이동을 보장하고 정보주체인 개인의 개인정보보호 권리를 강화하는 한편 자국민 데이터의 해외서버 이전은 엄격히 제한하고자 제정된 통합 규정으로서 유럽의 데이터 주권 보호를 위한 조치이다. GDPR은 데이터의 국외이전을 유럽연합 회원국 또는 적정성 평가를 통과한 제3국에게만 허용하는 등 유럽 시민의 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.

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 의

3) 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. 자세한 내용은 한국인터넷진흥원(2019)을 참고할 것.

존해 만들어지는 게 좋은지 확신할 수 없다"며 미국 기업으로부터 유럽 데이터 주권을 보호해야 한다고 주장한 바 있다(『매일경제』 2019/11/13). 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.

이렇듯 데이터 안보에 대한 유럽 차원의 접근이 주권 보호론으로 기우는 상황에서 2020년 1월 31일 공식적으로 유럽연합을 탈퇴한 영국은 데이터 안보와 관련해서는 브렉시트(Brexit) 이후에도 자국의 데이터보호법에 GDPR을 흡수하겠다는 뜻을 밝혔다. 그에 따라 GDPR을 자국 버전으로 개정한 UK GDPR 마련을 통해 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.[4] 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 데이터 안보 문제에 대한 영국의 접근은 유럽 GDPR의 적극적인 수용으로 이어질 것으로 전망되었다.

그런데 2022년 3월 영국 정부는 새로운 데이터 개혁 법안을 도입할 계획을 발표하였는데, 해당 법안은 자국 정보보호위원회(ICO)에게 데이터 규정 위반 사업체에 대한 강력한 제재를 취할 수 있는 권한을 부여하고, 영국의 과학기술력 제고를 위해 연구 목적의 개인정보 활용에 대한 규제를 완화하는 등을 목적으로 하는 것으로 알려졌다(*National Law Review* 2022/05/13). 그리고 같은 해 10월 도넬란(Michelle Donelan) 영국 신임 디지털문화미디어체육부 장관은 보수당(Conservative Party) 전당대회 연설에서 정부가

4) Government of the United Kingdom (2021), "UK government welcomes the European Commission's draft data adequacy decisions", https://www.gov.uk/government/news/uk-government-welcomes-the-european-commissions-draft-data-adequacy-decisions. (accessed on March 26, 2023)

UK GDPR을 새로운 “영국식 데이터 보호 체계(British data protection system)”로 교체할 계획에 있음을 밝혔다. 그녀는 현재 UK GDPR을 포함한 자국의 데이터 보호법이 기업, 특히 중소규모 기업들의 활동을 제약하는 불필요한 관료제적 형식주의로 작용하고 있음을 지적했다(*National Law Review* 2022/10/17). 이는 곧바로 유럽의회(European Parliament)의 반발을 초래했는데, 델보스-코필드(Gwendoline Delbos-Corfield) 유럽의회 의원은 영국 정부의 데이터 보호법 개혁 계획이 인권을 전혀 고려하지 않은 채 성장과 혁신에만 집중된 잘못된 결정이며, 해당 조치로 인해 유럽이 “기만 당했다(taken for a fool)”라며 날 선 비판을 가했다(*Politico* 2022/11/07).

한편 영국은 GDPR 수용 결정에 앞서 미국과 데이터 공유를 강화하는 움직임을 보이기도 했다. 2018년 3월 미국은 사법기관이 자국의 IT기업에 미국 또는 해외에 위치한 서버에 저장된 데이터를 합법적으로 요구할 수 있도록 하는 CLOUD법(Clarifying Lawful Overseas Use of Data Act)을 통과시켰는데, 약 1년 뒤인 2019년 2월 영국 역시 중대비리조사청(Serious Fraud Office)이 협정이 체결된 국가에 있는 해외 데이터에 접근할 수 있도록 하는 COPOA(Crime Overseas Production Orders)법을 통과시켰다. 그리고 그해 10월 3일 미국과 영국이 데이터 공유 행정협정을 체결함으로써 양국은 상대국에 위치한 서버에 저장된 데이터에 더 신속하게 접근할 수 있게 되었다(UK Government 2019b).[5)]

영국이 GDPR 수용을 통해 유럽의 데이터 주권 보호에 지속적인 참여를 결정한 상황에서 미국과 데이터 공유 행정협정을 체결하자 일각에서는 이러한 결정이 영국과 유럽연합 간 데이터 공유에 부정적인 영향을 미칠 수 있다는 우려를 제기하였다. 실제로 유럽개인정보보호이사회(EDPB)는 2020년 6월 미국-영국 간 행정협정 체결이 갖는 문제점, 특히 미영 행정협정과 미국의 CLOUD법 간 갈등이 발생할 경우 전자보다 후자가 우선시될 가능성, 영국에서 제3국으로의 데이터 국외이전 문제, 영국의 GDPR 적정성 평가에 대한 영향 등을 우려하는 서안을 유럽의회에 보내기도 하였다(Jelinek 2020). 이렇듯 유럽연합과의 결별과 무관하게 GDPR 수용론을 유지해오던 영국이

5) 해당 협약의 정식 명칭은 ‘Access to Electronic Data for the Purpose of Countering Serious Crime’이며, 2020년 2월 28일 정식 발효되었다.

유럽연합과의 마찰을 감수하며 대미 데이터 공유 협정 체결을 강행한 일련의 행보는 단순히 브렉시트만으로는 충분히 설명되지 않는다.

# Ⅳ. 영국의 사이버 안보 전략 지향성과 결정 요인

## 1. 민주주의 동맹 기반의 사이버 안보 국제협력 지향

화웨이 사태와 데이터 안보 문제에 대한 영국의 대응은 세 가지 유사한 특징을 보였는데, 이는 첫째, 집단적 대응 기제로서 자유민주주의 연대를 통해 해당 문제들에 맞서야 한다는 구상과 그러한 연대 구축을 자국이 주도해야 한다는 전략적 사고가 강하게 나타났으며, 둘째, 자유민주주의 연대 구축과 이를 주도하는 과정에서 양자 또는 다자 동맹을 적극적으로 활용하는 움직임을 보였고, 마지막으로, 특정 국가와의 관계 약화 현상이 나타났다는 것이다. 이는 달리 말해 영국의 대응에서 특정한 전략적 이해관계나 사고를 바탕으로 한 중개(brokerage)와 연대(collective) 외교가 전개되었음을 의미한다.

영국은 화웨이 사태에 대응하는 과정에서 미국, 호주 등 일찍이 화웨이를 퇴출한 자유민주주의 국가들과의 관계를 강화한 반면에 중국 정부와 화웨이의 강한 비난과 우려에도 불구하고 화웨이의 5G 통신장비를 퇴출함으로써 기존의 중국 중시 노선에서 이탈하는 움직임을 보였다. 데이터 안보 문제와 관련해서도 역시 유럽연합이 유럽 시민의 데이터 주권 보호를 위해 GDPR을 시행하고 가이아-X 프로젝트를 추진하며 데이터 안보에 대한 유럽 차원의 접근을 하나로 결집하려는 상황에서 영국은 유럽연합과의 갈등과 마찰을 감수하면서까지 GDPR 수용 노선에서 벗어나는 한편 미국과의 데이터 공유 행정협정을 체결하기도 하였다. 즉 미국과의 관계를 강화한 반면에 유럽연합과는 상대적으로 멀어지는 선택을 한 것이다.

이처럼 영국의 대응에서 발견되는 일관된 특징은 자유민주주의 연대 구

축을 위해 전통적인 동맹국이나 우방국과의 관계를 강화하고 그 과정에서 특정 국가와의 관계는 희생하는 전략이 전개되었다는 것이다. 영국은 일반적으로 미국을 비롯한 자유민주주의 동맹국 내지는 우방국들과의 양자적 또는 다자적 협력관계를 강화하였는데, 이들 협력 대상국은 미국 주도의 소다자 안보협력을 구성하는 자유민주주의 국가들인가 동시에 주로 중국과 갈등관계에 있는 국가들이기도 했다. 따라서 이러한 관계 강화 노력은 『국가사이버전략 2022』 등에 담긴 전략 기조, 즉 자유롭고 개방된 사이버 공간을 지향하며 자유민주주의 연대를 통한 사이버 안보 질서 확립을 추구한다는 이해관계와 맞물리면서 앞서 조명한 두 가지 이슈를 관통하는 일관된 정책적 지향성으로 나타났다.

한편 영국의 전략에서는 이슈에 따라 중국이나 유럽연합 등을 상대로 한 관계의 약화 현상이 나타나기도 했다. 이러한 현상이 이슈에 따라 각기 상이한 행위자를 대상으로 전개되었다는 사실은 관계의 단절이나 의도적 약화가 자유민주주의 연대를 강화하려는 과정에서 이루어진 보완적 행위이자 불가피한 조치였음을 시사한다. 이는 화웨이와 데이터 안보에 영국이 대응하는 과정에서 유럽연합과의 관계를 어떻게 설정하였는가를 살펴볼 때 더욱 분명히 나타난다. 데이터 안보 문제와 관련하여 영국은 미국과의 데이터 공유 강화를 위해 유럽연합과의 관계를 상대적으로 포기하는 행태를 보였지만, 화웨이에 대한 전면적인 퇴출을 선언하기 전까지만 해도 유럽 주요 국가들과 유사한 방식으로 화웨이 문제에 접근하였다.

데이터 안보 이슈와 관련하여 영미 간 데이터 공유 행정협정 체결은 양자 차원에서 이루어진 협력이라는 점에서 자유민주주의 연대 구축을 위한 영국의 노력으로 보는 것이 다소 무리일 수 있다. 그러나 미국과의 데이터 공유 행정협정은 영국뿐만 아니라 또 다른 파이브 아이즈 국가인 호주에서도 이루어졌으며, 동맹국 간 데이터 공유를 강화하려는 이와 같은 움직임은 정부의 데이터 통제력 강화와 초국적 범죄 예방을 추구하는 파이브 아이즈 차원의 노력과 비슷한 시기에 병행되었다. 이를 고려할 때, 데이터 안보에 대한 영국의 대응 역시 자유민주주의 연대를 구축하고자 하는 전략적 지향성에 따른 행보로 볼 수 있다.

그렇다면 여기서 제기되는 질문은 영국이 각각의 이슈에 대응하는 과정

에서 유사한 전략적 지향성을 보이게 된 이유가 무엇인가 하는 것이다. 달리 표현하자면, 영국이 2020년 전후를 기점으로 사이버 공간을 이념과 체제의 경쟁이 전개되는 무대로 보는 인식을 드러내고, 또 사이버 공간에서 발생하는 도전들에 자유민주주의 연대 내지는 동맹으로 대응한다는 논리를 내세우게 된 이유는 무엇인가? 이는 사이버 위협의 증대라는 외생적 요인만으론 충분히 설명되질 않는다.

사이버 안보 분야에서 영국이 자의적으로 설정한 역할구상과 특정 이슈에 대한 위협인식을 이해하기 위해선 영국의 대외정책 기조에서 발견되는 국제적 역할과 지위가 무엇이었으며, 외부 환경의 변화에 대한 인식이나 사이버 안보 전반 혹은 상술한 관련 이슈들에 대한 이해와 판단이 어떠하였는가를 살펴보는 것이 중요하다. 앞서 Ⅱ장에서 살펴본 바와 같이 정책결정자의 위협인식과 역할구상 그리고 이에 직간접적으로 영향을 미치는 정보기관의 판단은 국가 사이버 안보 전략의 주된 변화 동인으로 작용한다. 이러한 시각에서 보자면, 영국의 사이버 안보 전략의 변화 역시 이 같은 요인들의 영향을 복합적으로 받으며 나타난 결과로 볼 수 있다. 이 같은 맥락에서 사이버 안보 분야 영국의 이슈별 대응에서 나타난 일관된 전략적 지향성은 중국에 대한 영국 정부의 위협인식과 국제적 역할구상 그리고 정보기관 GCHQ의 위험평가를 종합적으로 검토하지 않고선 충분히 설명되기 어렵다.

## 2. 정부의 대중국 위협인식 및 국제적 역할구상과 GCHQ의 위험평가

### (1) 정부의 대중국 위협인식

영국의 사이버 안보 전략에 영향을 미친 첫 번째 요인으로 중국에 대한 영국 정부의 위협인식을 꼽을 수 있다. 2021년 3월 영국 정부는『경쟁적 시대의 글로벌 영국(Global Britain in a Competitive Age: the Integrated Reviews of Security, Defense Development and Foreign Policy)』전략서를 발간하였는데, 동 전략서는 영국이 인도-태평양 지역에 대한 관여를 증대하고 중국의 부상을 견제하는 쪽으로 대외정책의 방향성을 수정하였음을 가장

잘 보여주는 문서이다. 동 전략서는 영국의 대외정책이 인도-태평양 지역으로 그 초점을 옮기게 된 이유가 중국의 부상으로 야기된 국제질서의 변화에 대응하기 위함임을 밝히며, 중국을 '체제적 경쟁자(systemic competitor)'로 묘사함과 동시에 중국과의 갈등이 단순히 특정 사안에 국한된 것이 아니라 구조적인 문제임을 분명히 하였다(전혜원 2022).

이러한 대중국 위협인식은 영국의 AUKUS 삼각 안보협정 참여 과정에서도 발견된다(전혜원 2022, 18-19). 2021년 9월 15일 영국은 미국, 호주와 핵심 기술의 도입과 운영 가속화를 통해 군사력 강화를 추진한다는 목적 아래 삼자 안보협정을 체결함으로써 공식적으로 AUKUS를 출범시켰다. 동 협정의 주요 골자는 인도-태평양 지역의 안정과 번영을 위해 삼국이 외교·안보·군사 영역에서 합동역량과 상호 운용성을 강화하고, 이를 위해 사이버 역량, 인공지능, 양자 기술, 수중 군사력 등의 분야에서 상호 기술 및 정보 공유를 강화한다는 것이다(Shoebridge 2021; *ISAS Insights* 2022/04/01; *The Strategist* 2022/09/16). AUKUS를 통해 호주에 대한 미국과 영국의 핵잠수함 기술 및 핵연료 이전과 미중 경쟁의 주 무대로 여겨지는 핵심 기술 분야에서 삼국 간 역량 강화를 위한 혁신적 협력이 약속되면서 중국의 강한 반발이 이어졌다(*The China Project* 2021/11/29).

2010년대 중반까지 대중국 경제협력 강화 노선을 걸어온 영국이 중국과의 대립을 불사하면서 AUKUS를 출범시킨 배경에는 해양 군사화, 해군력 증대, 일대일로 정책 등을 통해 기존 국제질서를 위협하는 중국을 견제하려는 의도가 존재하였다(Hemmings 2018). 특히 사이버, 인공지능, 양자 기술, 수중 군사력 등 첨단기술 분야에서 빠르게 부상하는 중국을 견제하기 위해 미국, 호주와 협력하여 좁게는 인도-태평양 지역과 넓게는 글로벌 차원의 안정을 유지하고자 한 것이다(전혜원 2022).

중국에 대한 이 같은 위협인식의 증가는 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응에도 상당한 영향을 미친 것으로 볼 수 있다. 민주주의 연대를 통해 자유민주주의 국제질서를 보호하는 것에 앞장선다는 영국의 전략 목표는 중국에 대한 영국 정부의 부정적 인식이 강화한 현상과 무관하지 않으며, 이러한 인식의 증가는 화웨이 퇴출 결정에 큰 영향을 미쳤다. 앞서 논한 바와 같이, 영국은 일찍이 화웨이 장비가 중국발 사이버 공격 및 침탈

위협의 수단으로 악용될 가능성을 어느 정도 인지하고 있었지만, 2017년 중국이 국가정보법(National Intelligence Law)을 도입하면서 이전부터 GCHQ가 제기한 화웨이의 보안 문제를 중국 공산당의 내정간섭과 연결된 체제적, 이념적 위협으로 여기기 시작하였다(House of Commons 2020, 34-35). 설상가상으로 2020년 7월 중국이 홍콩 국가보안법을 시행하자 영국 정부는 중국의 권위주의적 행보가 민주주의, 인권, 자유 등 서구의 이념 및 가치와 상충하며 앞으로도 그럴 것으로 판단하게 되었고, 결국 화웨이에 대한 제재의 수준을 대폭 높이다가 결국 퇴출해버리는 결정에 다다르게 된 것이다.

### (2) 정부의 국제적 역할구상

영국의 사이버 안보 전략에는 정부의 국제적 역할구상 역시 중요한 요인으로 작용하였는데, 이는 『국가사이버전략 2022』를 통해 설정된 사이버 안보에 대한 구체적인 전략 목표와 연결된다. 사이버 안보 분야에서 영국이 추구하는 전략 목표는 『국가사이버전략 2022』에 다섯 가지 전략 축으로 명기되어 있는데, 이는 '영국의 사이버 생태계를 강화하고', '회복력 있고 번영하는 디지털 영국을 구축하며', '사이버 파워(cyber power)에 필수적인 기술 개발을 선도하고', '영국의 글로벌 리더십과 영향력을 향상하며', '위협이 되는 적들을 탐지, 방해 및 저지'하는 것이다(HM Government 2021b, 14-15).

아울러 『국가사이버전략 2022』는 영국의 비전에서 가장 중요한 것이 "사이버 공간을 더 자유롭고 개방적이며 평화롭고 안전하게 만드는 것"이며, 이를 위해 "사이버 파워에 책임감 있고 민주적으로 접근하면서 개방성과 민주주의라는 공동의 가치를 증진하기 위해 동류국가들과 협력할 것"임을 밝히고 있다(HM Government 2021b, 33). 동 전략서에서 영국의 역할이 '책임감 있고 민주적인 사이버 강국(leading responsible and democratic cyber power)'으로 묘사되고 있다는 점과 더불어 '민주주의' 또는 '민주적'이라는 단어가 총 18번이나 언급된다는 점 역시 눈여겨볼 대목이다(HM Government 2021b, 32). 즉 영국 정부는 자국에 대한 사이버 위협을 차단하는 것만큼이나 민주주의와 개방성에 기초한 사이버 공간의 질서 보호에 자국이 앞장서야 함을 핵심적인 목표이자 국제적 역할로 추구하였음을 알 수 있다.

여기서 짚고 넘어갈 점은 이와 같은 전략 목표가 영국의 대외정책 전반에 깔린 기조를 통해 나타나는 역할구상과 맞물려 있다는 사실이다. 브렉시트 이후 영국의 대외정책은 크게 두 가지 전략적 이해관계를 바탕으로 하여 수립·추진되어오고 있는데, 이는 첫째, '민주주의 연대를 통해 자유민주주의 국제질서를 보호'하는 것이며, 둘째, '글로벌 선도국으로서 자국의 국제적 영향력을 확장'하는 것이다. 이와 같은 역할구상은 2021년에 나온 『경쟁적 시대의 글로벌 영국』 전략서에 명기된 목표를 통해 더욱 명확히 드러난다. 동 전략서는 2030년까지 영국이 첨단기술 분야에서 선도국이 되는 것을 목표로 하며, 서구형 민주주의 발전 등을 통해 자유주의 국제질서를 공고히 하고, 유럽연합에 치중하던 글로벌 안보 기여 범위를 '인도-태평양 지역으로 돌리며(Indo-Pacific tilt)', 자유민주주의 국제질서를 위협하는 행위를 저지하는 데 앞장설 것임을 밝히고 있다(HM Government 2021a; 한국군사문제연구원 2021).

이 같은 역할구상은 새로운 5G 공급망 구축을 주도하고자 하는 영국의 노력으로 발현되었고, 그 과정에서 화웨이 퇴출 결정에 중요한 영향을 미쳤다. 영국은 5G 기술이 다양한 부문의 디지털 전환과 그에 따른 상당한 경제적 이익 창출에 필수적인 조건이라고 인식해왔고, 이러한 기술·경제적 고려에서 상대적으로 경제성이 높은 화웨이 장비를 도입하여 국내 5G 네트워크 인프라 건설과 디지털 환경 조성에 주력하였다. 그러나 화웨이를 전격 퇴출하게 되면서 중국을 배제한 채로 자국의 5G 경쟁력을 키울 수 있는 대안적 공급망을 마련할 필요를 느끼게 되었다. 이는 영국이 D10 연대 구축을 주도하는 노력으로 이어졌는데, 화웨이 전면 퇴출 결정이 이루어진 시점에 영국 정부는 D10 계획을 정식으로 발표함으로써 기존 G7을 확장하는 방식으로 전 세계의 민주적이고 기술이 발전한 국가 간에 협력을 강화하겠다는 야심을 드러냈다(*Nikkei Asia* 2020/12/16). 이러한 행보는 영국 정부의 화웨이 전면 퇴출 발표와 비슷한 시점에 나타났다는 점에서 D10 연대 결성을 주도하여 중국을 배제한 5G 공급망을 구축하려는 영국의 역할구상에서 비롯된 결과로 볼 수 있다.

한편 유럽의 데이터 주권론과의 마찰 가능성에도 불구하고 영국이 미국과 데이터 공유 행정협정을 체결하는 과정에서도 정부의 역할구상은 중요한

변수로 작용하였다. 2020년 9월 발표된『국가데이터전략』에서 영국 정부는 디지털 경제 강화를 위해 "경제 전반에서 데이터의 가치 실현, 신뢰할 수 있는 데이터 제도 보장, 정부의 데이터 활용을 통한 효율성 제고와 공공 서비스 개선, 데이터 인프라의 보안 및 복원력 보장, 국제적 데이터 유통 선도"를 5대 과제로 설정할 만큼 데이터 기반 디지털 경제 발전에 강한 의지를 보여왔다(정용찬 2020). 이는 영국 정부가 자국이 세계 최고 수준의 디지털 경제국으로 도약하기 위해서는 유럽연합과 미국 양쪽 모두와의 자유로운 데이터 흐름이 필수적이라고 판단하였음을 방증한다.

국가 데이터 경쟁력을 평가한 한 지표에 따르면, 영국은 전 세계에서 데이터 센터 설립에 가장 선호되는 국가로서 북아메리카와 유럽을 잇는 데이터 유통 허브의 위치를 차지하고 있는 것으로 평가된다.[6] 이러한 결과는 영국이 사이버 안보, 데이터 보호, 개인정보보호 규칙 등 여러 측면에서 우수한 국가로 평가되기 때문이기도 하지만(Carr & Tanczer 2018), 유럽 내 미국의 유일한 정보동맹국으로서 나름대로 영향력을 확장하고자 하는 목표를 꾸준히 추구해왔기 때문에 가능한 것으로 해석될 여지가 있다.

### (3) GCHQ의 사이버 안보 위험평가

GCHQ는 영국이 사이버 안보 분야에서 특정 국가들과의 협력관계를 강화하거나 거리를 두게 되는 과정에서 정부가 내리는 정책결정의 당위성을 뒷받침하는 핵심적인 행위자로 등장하였다. 먼저, 화웨이 사태와 관련하여, 화웨이 장비의 보안 위험성에 대한 우려는 2010년대 후반에 접어들면서 GCHQ를 통해 꾸준히 제기되었는데, 이는 GCHQ의 참여를 통해 HCSEC 감독 위원회가 국가안보보좌관에게 제출한 2018, 2019, 2020년도 연례보고서를 통해 잘 나타난다. 2018년도 보고서에는 화웨이의 소프트웨어 개발에 대한 접근 방식이 영국 사업자에게 위협 증가를 초래할 수 있는 "걱정스러운 문제들을 내포하고 있다"는 위험평가가 담겼으며, 2019년도 보고서 역시 "화웨이의 엔지니어링 프로세스에서 영국의 네트워크에 새로운 위협을 가

6) Arcadis (2021), "The Arcadis Data Center Location Index 2021", https://datacenters.arcadis.com/locationindex/p/1. (accessed on April 22, 2023)

할 수 있는 중요한 기술적 문제가 발견되었고, 이러한 보안 문제들을 개선하기 위한 화웨이의 진전이 충분히 이루어지지 못하였음"을 지적하였다. 2020년도 보고서에서도 화웨이 장비에 대한 같은 동일한 평가와 보안 우려가 재확인되는 한편 "화웨이가 장기적으로 영국의 네트워크에 대한 위험을 충분히 완화할 역량이 있는지 장담하기 어렵다"는 견해가 담겼다(UK Government 2018; UK Government 2019a; UK Government 2020).

2019년 턴불(Malcolm Turnbull) 당시 호주 총리가 영국을 방문해 가진 한 연설에서 영국의 화웨이 퇴출을 촉구하며 "GCHQ가 (화웨이 장비의 보안 문제와 관련해) 호주와 일치한 견해를 드러냈다는 사실에 놀라지 않았다"라고 발언한 것 역시 화웨이에 대한 GCHQ의 판단이 호주의 그것과 다르지 않았음을 간접적으로 보여준다.[7] 호주의 화웨이 퇴출 결정은 호주신호정보국(Australian Signals Directorate: 이하 ASD)이 실시한 5G 네트워크 공격 모의전 결과 및 위협 분석에 상당한 영향을 받은 것으로 알려졌는데(*The Sydney Morning Herald* 2021/05/21), 턴불 총리의 그와 같은 발언은 화웨이 문제에 대한 GCHQ의 위험평가가 ASD와 유사한 수준이었다는 점과 더불어 호주 정부의 퇴출 결정에 ASD의 판단이 미친 영향만큼이나 영국의 결정에도 GCHQ의 판단이 강하게 작용하였을 가능성이 크다는 점을 시사한다.

영국이 유럽연합의 데이터 주권론을 수용하면서도 다른 한편으론 미국과의 데이터 공유를 강화한 데에도 GCHQ의 위험평가, 즉 사이버 위협 관리에 미국과의 공조가 필수적이라는 GCHQ의 판단과 제언이 중요한 요인으로 작용하였다. 2016년 발표된 『국가사이버안보전략(National Cyber Security Strategy 2016 to 2021)』에 따르면, 영국은 국가 행위자에 의한 사이버 공격, 사이버 테러리즘, 핵티비즘(Hacktivism) 등 다양한 사이버 위협에 노출되어 왔고, 특히 최근에는 이슬람계 테러 조직과 극우집단의 사이버 공격을 지속해서 받아왔다. 이러한 위협을 관리하기 위해 2016년 10월 정부, 산업, 공공분야의 사이버 위협 대응 및 관리를 총괄하는 기관으로서 NCSC가 GCHQ 산하에 설치됨으로써 영국의 사이버 안보 전략 수립에 있어 GCHQ의 위상과 영향력은 더욱 강화되었다. 이 가운데 영국 정부는 사이버 안보 분야에

7) Turnbull, Malcolm (2019), "Address to the Henry Jackson Society, London", https://www.malcolmturnbull.com.au/media/address-to-the-henry-jackson-society-london. (accessed on April 20, 2023)

19억 파운드(약 2조 7천억원)를 투자하는 등 위협 대응을 위한 지원을 확대하였고(한국인터넷진흥원 2019, 99), 미국과의 데이터 공유 행정협정 체결 역시 사이버 공간을 매개로 발생하는 초국적 위협에 대응하기 위해 동맹국과의 데이터 공유를 강화하려는 노력에서 이루어진 결과였다.

파이브 아이즈 정보동맹 네트워크에서 영국을 대표하는 정보기관인 GCHQ는 영미 간 데이터 공유 강화를 증대하는 사이버 위협에 대응하는 과정에서 필수적으로 이루어져야 할 동맹 차원의 안보협력으로 판단하였다고 볼 수 있다. 영국을 포함한 파이브 아이즈 국가들이 사이버 위협을 포함한 초국가적 조직 범죄 해결을 위한 대응 기제로서 해당 정보동맹 네트워크를 기반으로 하는 협력의 필요성을 강조해왔다는 사실은 미국의 CLOUD법과 그에 맞춰 통과된 영국의 COPOA법이 단순히 범죄 수사를 위한 사법당국의 해외 데이터 접근성을 높이는 용도로만 사용되기보다 정보동맹의 기능을 보완하는 데 활용될 여지가 있음을 시사한다(*The Guardian* 2022/06/08). 무엇보다 2018년 8월 플레밍(Jeremy Fleming) GCHQ 국장이 영국 언론에 기고한 글을 통해 "우리의 적들이 국경의 제약을 받지 않는 것처럼 우리는 우리의 입법 및 기술 준비가 보조를 맞출 수 있도록 해야 한다. 영국처럼 개인정보 보호가 강력한 국가들이 심각한 범죄 및 테러 위협을 근거로 미국 통신회사가 보유한 사용자 데이터를 요청할 수 있는 능력 - 즉 CLOUD법 - 은 실현가능한 훌륭한 예"라고 주장한 사례는 영미 간 데이터 공유 행정협정과 GCHQ의 판단이 밀접한 연관이 있음을 방증한다.[8]

## Ⅴ. 맺음말

이 글은 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응에서 공통적으로 나타나는 전략적 지향성을 포착하여 영국의 사이버 안보 전략 기조를 이해하고, 이를 결정하는 주요 요인을 추적해보는 것을 목적으로 하였다.

8) GCHQ (2018), "Director GCHQ writes about the importance of securing the next generation of technology", https://www.gchq.gov.uk/news/jeremy-fleming-securing-next-generation-technology. (accessed on April 17, 2023)

2020년 전후를 기점으로 영국의 사이버 안보 전략은 사이버 공간을 배경으로 쟁점화된 문제들에 자유민주주의 연대로 대응한다는 동맹과 진영의 논리를 강하게 드러내기 시작했다. 이와 같은 인식과 논리는 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응에서도 일관되게 발견되었다.

역할이론과 정보순환론의 논의를 복합적으로 원용함으로써 정책결정자의 위협인식과 국제적 역할구상 그리고 정보기관의 판단이 영국의 사이버 안보 전략을 결정하는 주요 요인으로 작용하는 과정을 추적한 이 글은 영국의 전략이 자유민주주의 연대 구축을 주도하려는 기조를 보이게 된 배경에 영국 정부의 대중국 위협인식과 국제적 역할구상 그리고 사이버 안보 이슈에 대한 GCHQ의 위험평가의 복합적 영향이 존재하였음을 주장하였다. 이를 통해 화웨이 사태와 데이터 안보 문제에 대한 영국의 대응 방식에서 공통적으로 발견되는 전략적 지향성 역시 이 세 가지 요인과 밀접한 연관이 있음을 밝혔다.

이 글이 주목한 영국의 사례는 크게 두 가지 시사점을 제시한다. 첫째, 국가 사이버 안보 전략은 단순히 위협의 양적 증가나 외부의 압박과 같은 외생적이고 구조적인 변수 외에도 정책결정자의 위협인식과 국제적 역할구상 등 내생적이고 관념적인 요인에도 영향을 받아 수립·추진된다는 것이다. 아울러 사이버 안보 전략을 결정하는 주체로서 정부 외에도 정보기관과 같은 국가 하위행위자의 역할과 기능을 간과할 수 없음을 보여준다. 따라서 정부 차원의 전략서를 통해 선언되는 위협인식과 전략 목표뿐만 아니라 사이버 안보 분야에서 중요한 기능을 수행하는 하위행위자의 판단 역시 종합적으로 검토해야 할 필요성을 강조한다.

둘째, 사이버 안보 분야에서 발생하는 이슈에 대한 국가의 대응은 각 이슈의 특수한 정치적·기술적 배경과 전개 상황으로 인해 서로 분리된 것으로 보이기 쉬우나 실상은 이슈별 대응을 관통하는 전략적 지향성이 존재한다는 것이다. 그리고 이러한 전략적 지향성은 정부 차원에서 마련되는 국가 사이버 안보 전략의 기조와 밀접한 연관이 있다. 이 점에서 사이버 안보 분야 이슈별 대응의 전략적 지향성을 포착하고 나아가 국가 사이버 안보 전략 기조와의 상관성을 분석하는 시도는 국가 사이버 안보 전략에 관한 연구가 이슈의 특수성에 매몰되는 것을 피하는 데 유용할 것이다.

## | 참고문헌 |

### 1. 논문 및 단행본


문정인 (2002). “정보분석론.” 문정인(편).『국가정보론』. 박영사, pp. 114-151.

신승휴 (2022). “미국의 사이버 안보 국제협력 정책의 진화: 네트워크 이론과 구성적 제도주의의 시각.”『국제정치논총』. 제62집. 제2호, pp. 107-151.

염돈재 (2002). “첩보수집론.” 문정인(편).『국가정보론』. 박영사, pp. 82-113.

유동원 (2017). “역할이론의 발전과 국제관계: 주요 개념과 구성주의.”『국제정치논총』. 제57집. 제3호, pp. 7-49.

전웅 (2015).『현대 국가정보학』. 박영사.

Berkowitz, Bruce and Allen Goodman (2000). *Best Truth: Intelligence in the Information Age.* New Heaven: Yale University Press.

Carr, Madeline (2016). “Public-private partnerships in national cyber-security strategies.” *International Affairs.* Vol. 92. No. 1, pp. 43-62.

Carr, Madeline and Leonie M. Tanczer (2018). “UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions.” *Journal of Cyber Policy.* Vol. 3. No. 3, pp. 430-444.

Herman, Michael (1996). *Intelligence Power in Peace and War.* New York: Cambridge University Press.

Holsti, K. J. (1970). “National Role Conceptions in the Study of Foreign Policy.” *International Studies Quarterly.* Vol. 14. No. 3, pp. 233-309.

Lockheart, John (1987). “Intelligence: A British View.” Robertson, K. G. (ed.). *British and American Approaches to Intelligence.* London: Palgrave Macmillan London, pp. 37-52.

Marrin, Stephen (2009). “Intelligence analysis and decision-making: Methodological challenges.” Gill, Peter, Stephen Marrin and Mark Phythian (eds.). *Intelligence Theory: Key questions and debates.* Abingdon, Oxon: Roudledge, pp. 131-150.

Sexton, Mark (2016). “U.K. cybersecurity strategy and active cyber defence - issues and risks.” *Journal of Cyber Policy.* Vol. 1. No. 2, pp. 222-242.

## 2. 기타

박영욱 (2020). “화웨이 제재를 위한 미국의 법적 조치.” KISA Report. Vol. 9. 한국인터넷진흥원.

전혜원 (2021). “영국의 화웨이 정책: 관리에서 퇴출까지.” SNU IIS 이슈브리핑. 제121호. 서울대학교 국제문제연구소.

_____ (2022). “글로벌 브리튼과 영국의 대(對)중국 정책.” 국립외교원 외교안보연구소 정책연구시리즈.

정용찬 (2020). “포스트 코로나19 시대의 데이터 주권과 데이터 거버넌스.” KISDI Premium Report. 20-10. 정보통신정책연구원.

조은정 (2022). “영국 「국가사이버전략 2022」의 특징과 시사점.” INSS 전략보고. 제174호. 국가안보전략연구원.

한국군사문제연구원 (2021). “영국의 『글로벌 국가안보전략서』 주요 내용.” KIMA 뉴스레터. 제960호. 한국군사문제연구원.

한국인터넷진흥원 (2019). “2019 글로벌 정보보호 산업시장 동향조사 보고서(30개국).”

Dowden, Oliver (2020). “Oral statement to Parliament: Digital, Culture, Media and Sport Secretary’s statement on telecoms.”

Hemmings, John (2018). “Global Britain in the Indo-Pacific.” Henry Jackson Society, Asia Studies Centre Policy Paper 2.

HM Government (2009). *Cyber Security Strategy of the United Kingdom: satefy, security and resilience in cyber space, Cm 7642.*

_____ (2021a). *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy. CP 403.*

_____ (2021b). *National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK.*

House of Commons (2020). “‘The Security of 5G’, Defence Committee, Second Report of Session 2019-21, HC 201.” House of Commons.

Jelinek, Andrea (2020). “Letter to the European Parliament members.” European Data Protection Board.

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.”

Prince, Conrad and James Sullivan (2019). “The UK Cyber Strategy Challenges for the Next Phase.” RUSI Briefing Paper.

Shoebridge, Michael (2021). “What is AUKUS and what is it not?: How does it connect to the Quad, the Sydney Dialogue, ASEAN and Indo-Pacific security?” Strategic Insight, Australian Strategic Policy Institute.

UK Government (2018). *HCSEC Oversight Board Annual Report 2018.*

_____ (2019a). *HCSEC Oversight Board Annual Report 2019.*

_____ (2019b). *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, CP178.*

_____ (2020). *HCSEC Oversight Board Annual Report 2020.*

“메르켈 ‘유럽, 실리콘 밸리에 데이터 주권 빼앗겨선 안돼’.”『매일경제』. 2019년 11월 13일.

“Britain bans new Huawei 5G kit installation from September 2021.” *Reuters.* November 30, 2020.

“UK cyber boss says Five Eyes have taken different approach to Huawei before.” *Reuters.* April 24, 2019.

Crawford, Alan. “UK set on collision course with China over Hong Kong and Huawei.” *ThePrint.* June 4, 2020.

Gering, Tuvia. “Why China is genuinely worried about AUKUS.” *The China Project.* November 29, 2021.

Hartcher, Peter. “Huawei? No way! Why Australia banned the world’s biggest telecoms firm.” *The Sydney Morning Herald.* May 21, 2021.

Hunton Andrews Kurth’s Privacy and Cybersecurity. “UK Announces Data Reform Bill.” *National Law Review.* May 13, 2022.

Hurst, Daniel. “Five Eyes must ramp up fight against rising organised crime, AFP commissioner warns.” *The Guardian.* June 8, 2022.

Ismail, Nick. “Huawei ban could cost UK economy £18.2 billion due to 5G roll-out delay.” *Information Age.* September 9, 2020.

Kang, Jocelinn. “Enhancing cyber capabilities through AUKUS.” *The Strategist.* September 16, 2022.

Manancourt, Vincent. “‘We were taken for fools’: MEPs fume at UK data protection snub.” *Politico.* November 7, 2022.

Maude, Jonathan, Rachel Easton and Daniel Stander. “The End of UK GDPR?” *National Law Review.* October 17, 2022.

Nakajima, Yusuke. “UK calls on South Korea, India and Australia to attend G-7 summit.” *Nikkei Asia*. December 16, 2020.

Warrell, Helen, Alan Beattie and Demetri Sevastopulo. “UK turns to ‘Five Eyes’ to help find alternatives to Huawei.” *Financial Times*. July 13, 2020.

Wilkins, Thomas. “Is AUKUS really an ‘Alliance’?” *ISAS Insights*. April 1, 2022.

Arcadis (2021). “The Arcadis Data Center Location Index 2021.” https://datacenters.arcadis.com/locationindex/p/1. (accessed on April 22, 2023)

GCHQ (2018). “Director GCHQ writes about the importance of securing the next generation of technology.” https://www.gchq.gov.uk/news/jeremy-fleming-securing-next-generation-technology. (accessed on April 17, 2023)

Government of the United Kingdom (2021). “UK government welcomes the European Commission’s draft data adequacy decisions.” https://www.gov.uk/government/news/uk-government-welcomes-the-european-commissions-draft-data-adequacy-decisions. (accessed on March 26, 2023)

Prince, Conrad and James Sullivan (2020). “The UK’s New Way on Huawei.” https://rusi.org/commentary/uks-new-way-huawei. (accessed on April 24, 2023)

Turnbull, Malcolm (2019). “Address to the Henry Jackson Society, London.” https://www.malcolmturnbull.com.au/media/address-to-the-henry-jackson-society-london. (accessed on April 20, 2023)

| **논문투고일** : 2023년 05월 01일 |
| **논문심사일** : 2023년 06월 07일 |
| **게재확정일** : 2023년 06월 12일 |

| ABSTRACT |

# The Orientation and Determinants of UK Cyber Security Strategy:
## Focusing on its Response to Huawei Crisis and Data Security

Seung Hugh Shin
(Dept. of Political Science and International Relations,
Seoul National University)

This paper examines the UK's cyber security strategy and identifies the determinants of strategy by looking at the strategic orientation that is commonly associated with the country's response to the Huawei crisis and data security issue. Using the discussions of role theory and intelligence cycle theory, the paper traces how the decision-maker's threat perceptions and role conception, along with the risk assessments of the intelligence agency, have acted as major factors in determining the country's response to cyber security. It is argued that the British government's threat perception towards China, its role conception, and the GCHQ's cyber security risk assessments have determined the strategic orientation of the country's cyber security strategy, seeking out a leadership role in building international cyber security cooperation based on a democratic alliance. Based on its analysis, the paper aims to demonstrate two things. First, the national cyber security strategy is not only influenced by exogenous and structural factors but also endogenous and ideological factors, and second, the nature and direction of cyber security strategy can be clearly understood only when the common strategic orientation associated with issue-specific responses is analysed in advance.

▪ Key words: Cyber Security, Huawei Crisis, Data Security, UK, GCHQ