CENTER FOR FUTURE WARFARE STUDIES
INSTITUTE OF INTERNATIONAL STUDIES
SEOUL NATIONAL UNIVERSITY

서울대학교 국제문제연구소
미래전 연구센터
08826 서울시 관악구 관악로 1
서울대학교 종합교육연구동 220동 517호

Tel. 02-880-6311
Fax. 02-871-4115

Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 워킹페이퍼 No.73(발간일: 2021.5.24.)

군사정보 · 데이터 안보의 미중경쟁과 한국

손한별 국방대학교 군사전략학과 부교수

Ⅰ. 머리말

'중국의 부상'이라는 주제가 새로운 것은 아니다. 중국의 잠재력에 비해 상대적으로 열세했던 군사 · 외교 · 경제력이 크게 성장하면서 부각되고 있을 뿐이다. 여기에 중국이 더욱 적극적으로 행동하고 나서면서, 이른바 "부상과 두려움(rise and fear)"이라는 세력전이론의 대명제가 설득력을 얻고 있다.(Graham Allison, 2017) 2012년 공산당 총서기에 오른 시진핑은 "중화민족의 위대한 부흥"을 꾀하면서 이른바 "중국몽(中国梦)"을 내세웠는데, 이를 실현하기 위해서는 해외시장의 확보, 에너지 자원의 안정적 확보, 우호적 금융경제질서의 구축 등 새로운 세계질서를 구축해나갈 필요가 있다. 2018년 신년사를 통해 "세계 평화의 건설자, 글로벌 발전의 기여자, 국제질서의 수호자가 될 것"이라고 밝히면서 중국 중심의 세계질서 구축 의지를 밝혔고,(人民网, 2017.12.31.) 이같은 의지는 60여개 국가를 포괄하는 인프라 구축을 목표로 하는 "일대일로(一带一路) 전략"과 중국 주도의 "역내포괄적경제동반자협정(RCEP)" 추진 등으로 나타나고 있다.

미국과 중국의 경쟁은 다양한 부문에서 진행 중이다. 먼저, 중국은 국방개혁을 통해 미국과의 국방과학기술 격차를 좁히면서, 엄격한 근무기풍과 기율로 단련된 군대를 양성하고 확고한 안보태세를 구축하는 "강군몽(强軍夢)"의 실현을 추구하고 있다. 미국도 중국을 견제 · 차단하던 것에서 탈피하여 군사력으로 압도하기 위한 "3차 상쇄전략"의 기술혁신, "글로벌 영역에서의 합동접근 및 기동(JAM-GC)", "다영역작전(MDO)" 등의 작전개념을 발전시키고 있다. 경제부문에서

의 경쟁 역시 첨예하게 진행 중이다. 중국은 미국의 압도적인 경제력을 차단하면서 자국 중심의 경제레짐을 구축하기 위해 "아시아인프라투자은행(AIIB)"과 "역내포괄적경제동반자협정"을 적극 추진하고 있고, 중국과 러시아를 중심으로 하는 "상하이협력기구(SCO)"를 적극적으로 활용하고 있다.

미중의 안보 및 경제 패권경쟁이 명시적이라면, 이른바 기술패권 경쟁은 보다 암묵적으로 진행 중이다. 특히 미국의 입장에서 중국 과학기술이 범세계적으로 확산되는 것을 전략적인 관점에서 바라보면, 기술의 유출과 지적재산권 침해, 민주주의에 대한 도전, 군사안보 및 기술패권 경쟁과 같은 주제와 연결된다.(Danielle Cave, et al., 2019) 역사적으로 기술경쟁은 패권국과 도전국의 운명을 결정해왔지만, "복합지정학"의 관점에서 바라본 미중의 기술경쟁은 보다 다양한 의미를 제시한다. 전통적 지정학의 관점에서 기술패권 경쟁을 바라볼 수도 있지만, 상호의존 질서에 주목하는 비(非)지정학, 주관적으로 공간구성을 바라보는 비판지정학, 사이버 공간과 같은 탈영토적 '흐름의 공간'에 주목하는 탈지정학을 동시에 고려해야 한다는 것이다.(김상배, 2019, 132-133) 다만 자국의 이익을 극대화하기 위한 표준과 규범을 관철하여 세계질서를 주도적으로 이끌고자 하는 미래 패권경쟁의 일환이라는 데에는 이견이 없을 것이다.[1)]

"기술패권" 경쟁이 장기적인 차원에서 미래 글로벌 패권을 다투는 강대국 간의 문제라면, 국가안보의 목적을 가지고 기술을 안보의 영역에서 활용하는 경우에는 보다 직접적이고 현재적인 문제가 된다. 기술발달은 "양질전화의 과정"을 거쳐 "이슈연계의 임계점"을 넘어서게 되고, 지정학적인 분쟁으로 발전할 가능성은 더욱 커진다.(김상배, 2018, 5) 정보기술의 혁명적 발전과 탈냉전기 전략전쟁을 두 축으로 하는 "전략적 정보전쟁(Strategic Information Warfare, SIW)"은 평시와 위기시의 구분을 무색하게 만들고 있는데,(Roger Molander, et al., 1998) 빅데이터, 인공지능, 자율화 무기체계 등 다양한 군사기술의 발전과 연계되면서 새로운 전쟁양상의 등장을 예고하고 있다. 결국 기술경쟁은 전통적 안보와도 직접적으로 연계되어 있다는 것을 의미한다.

최근 더욱 복잡해진 미중간의 기술경쟁을 안보적 관점에서 확인할 수 있는 대표적 사례는 중국 최대 통신회사인 "화웨이(华为) 사태"이다. 미래를 선도하기 위해 "기술표준"을 선점하기 위한 경쟁으로 보는 국제정치경제적 관점도 존재하지만, 제품에 숨겨진 "백도어"를 통해 데이터가 중국으로 이전될 수 있다는 우려를 가지고 '실재하는' 안보위협으로 보는 관점도 존재한다. 2012년 미 하원은 특별위원회를 통해 화웨이와 ZTE에 대한 안보관련성 조사를 실시했지만, 충분한 자료를 제출하지 않아 특기할만한 결론에 이르지 못한 바 있다.(U.S. House of Representatives, 2012.10.8.) 하지만 2018년 이후 미국의 정보기관들은 화웨이 제품의 위해성을 경고하고 나섰고, 국방수권법에 의해 정부조달에서 제외시켰으며, 우방국들에게 화웨이 제품

1) 미국의 경쟁자들은 비교우위에 입각한 군사적 여건조성 접근법을 활용할 수 있다. 미국에게 고도의 기술 개발 비용과 위험을 부담시킴으로써 후발주자의 이점을 취한다는 것이다. 과도한 비용이 발생하는 신기술 개발을 미국에 전가하면서, 기존 기술의 점진적 개선, 지식의 확산 및 경제 선진화를 통해 기술패권을 잠식해가는 것이다.(SSG Cohort IV, 2017, 62)

의 도입을 중단할 것을 요구하기에까지 이르렀다.

결국 미중 간의 기술경쟁은 경쟁 상대에 대한 정보우세를 추구하는 전통적인 관점의 "정보전(information warfare)"으로 귀결된다. 현재 디지털 기술이 발달하면서 변화하는 안보환경을 "디지털 안보"로 개념화할 수 있다면, 이러한 디지털 환경 속에서 행해지는 정보전은 "데이터 획득"과 "데이터 보안"으로 대별할 수 있는 "데이터 안보"로 명명할 수 있을 것이다. 이른바 '원자료(raw data)'가 별다른 의미를 갖지 않았던 과거와 달리, 빅데이터와 인공지능에 힘입어 데이터가 첩보(information) 또는 정보(intelligence)의 의미를 동시에 갖게 된 현실을 반영한다. 개인정보와 기업정보와 같은 비군사적인 데이터들도 통합, 축적되고 다른 데이터들과의 연계되면서 국가안보에 영향을 줄 수 있는 정보로 활용될 수 있다는 것이다.

이에 따르면 다음과 같은 연구질문이 도출된다. 첫째, "디지털 안보"의 시대에 있어 정보전의 의미는 어떻게 달라졌는가? 국가정보, 정보영역, 정보전 등의 개념은 어떻게 달라지고 있으며, 그에 따른 위협과 취약성은 어떻게 변화하는가? 둘째, 미중의 정보전은 어떻게 전개되고 있는가? 정보우세를 위한 양국의 노력은 어떤 것이 있으며, 각각의 정보영역에서 실제로 벌어지고 있는 정보전의 사례는 무엇인가? 셋째, 미중의 데이터 안보경쟁이 한국에 주는 함의는 무엇이 있는가? 강대국 경쟁 속에서 부각되고 있는 데이터 주권의 개념은 무엇이며, 데이터 안보를 위한 한국의 핵심전략과 정책이슈들에는 무엇이 있는가? 본 연구는 이러한 연구질문에 하나씩 답하는 방식으로 논의를 이어간다.

II. "디지털 안보" 시대의 정보전

"정보전(information warfare, IW)"이라는 개념은 쉽게 접할 수 있지만, 정보통신, 인터넷과 관련한 과학기술의 비약적인 발전으로 정보전의 방법과 수단을 단정해서 말하기 어렵다. 일반적으로 정보전은 "상대적인 정보우세를 달성하기 위한 공격과 방어행위, 또는 이를 위한 정보의 이용과 관리"를 의미한다.(Catherine Theohary, 2018, 1) 군사력 또는 기타 군사적 행동을 수반하지 않는다는 점에서 전쟁이나 전투라는 단어를 사용하는 것에 거부감은 있지만, 정치동맹, 경제수단, 비밀공작, 심리전, 전자전, 군사기만과 같은 수단을 적극적으로 활용하는 "정치전(political warfare)"(George Kenan, 1948)의 한 형태로서 자리잡고 있다.

정보전은 이제 새로운 환경에서 이루어진다. 그야말로 "디지털 데이터의 산사태(digital data avalanche)"를 만나게 된 것이다.(Fred Cate, 2015, 299-300) 인간의 모든 행동과 습관은 데이터로 저장되고, 이를 통해 예측이 가능한 수준에 이르렀다. 데이터의 폭발적 증가 뿐만 아니라, 학계와 산업계, 정부를 막론하고 이러한 데이터를 요구하고 나서면서 데이터에 접근, 수집, 공유, 사용할 수 있는 행위자도 크게 늘어났다. 여기에 데이터 기반체계가 크게 발전하면서 거의

모든 사물이 인터넷과 연결되고 있다. 데이터, 네트워크, 통제체계는 독립적이지 않다는 것이다. 결국 "데이터는 제4차 산업혁명을 이끄는 새로운 원유(new oil)"로서 역할한다. 아울러 큰 활용 가치로 인해 모두가 원하는 빅데이터는, 그만큼 공격과 탈취에 취약할 수밖에 없게 되었다.

1. 정보전의 세 영역

정보전에는 선전공작, 정치공작, 준군사공작, 역정보, 방첩과 같이 다양한 형태의 정보수단이 활용되지만, "정보환경(information environment)"의 영역 내에서 이루어진다. 정보환경은 정보요구-수집-처리-분석 및 생산-배포의 절차가 이루어지는 개인과 조직, 체계 등으로 구성된다. 일반적으로 정보전이 수행되는 정보환경은 "물리영역", "정보영역", "인지영역"의 세 가지 영역으로 구분해왔다.(JP 3-13) 영역 구분에 주목하는 이유는 각 영역에서 일어나는 활동이 다르기 때문인데, 영역별 특성과 활동을 개략적으로 살펴보면 다음과 같다.

첫째는 물리영역(physical layer)이다. 궁극적으로 얻고자 하는 효과를 위해 물리적 행동이나 자극이 행해지는 영역이다. 행위자들이 실질적인 영향을 미치려는 상황이 존재하는 장소로서, 지상, 해양, 공중, 우주와 같은 물리적 공간을 가진다. 여기에는 물리적 플랫폼과 지휘통제 체계, 부수적인 기반체계들이 존재한다. 이 영역의 요소들은 비교적 측정하기가 쉬운데 주로 치명성, 생존성과 같은 기준을 가지고 능력을 측정하게 된다.

물리영역의 활동들은 실행(act)으로 표현되는데, 인지영역에서 결심된 것으로부터 직접 전환된 것이기도 하고 정보영역을 통하여 전환된 것이 간접적으로 이루어지는 것이기도 하다. 그결과 물리영역에서는 전통적인 개념의 물리적 충돌이 발생한다. 기동과 화력, 방호, 군수와 같은 기능들로 대표되는데, 탱크, 항공기와 같은 기동 및 수송수단이나 포병, 미사일의 화력수단이 있다. 플랫폼 중심의 물리력이 직접 충돌하여 상대방을 파괴하고 살상하는데 목적을 둔다. 이같은 물리력의 움직임을 정확하게 파악하고 대응하는 것은, 아군의 피해를 최소화하고 상대의 피해를 강요하는데 있어 핵심적인 과업이 된다. 또한 양적으로 충분한 자원을 확보하고 적시에 지원하기 위한 활동도 중요하다.

둘째는 정보영역(informational layer)이다. 실제 정보가 위치하는 영역으로, 정보가 생산, 처리, 유통, 저장되는 네트워크 체계를 의미한다. 정보영역에 존재하는 정보는 물리영역의 실제적 진실을 반영할 수도 있지만, 정보 간의 상호작용에 의해 영향을 받기도 한다. 대부분의 경우 의사교환은 정보영역에서 이루어진다. 정보영역은 정보전의 주요한 전장이었지만, 현대에 이르러 국가 간 분쟁의 중요한 전장으로 부상하였다. 정보영역의 중요성이 더욱 부각됨에 따라 아측의 정보영역 보호와 방어, 상대방 정보영역에 대한 탐지와 침투 등은 필수적인 군사과업이 되었다.

정보영역에서 일어나는 활동으로는, 먼저 물리영역에 대한 간접적인 감지활동인 관찰이 있다. 물리영역에서 실재하는 객체와 현상은 정보영역을 거쳐 인식하게 된다. 다음으로는 정보활동

이 있는데, 물리영역에서 수집된 데이터의 처리와 유통을 의미한다. 개별적으로 관찰된 결과를 의미있는 환경에 집어넣는 것으로, 의사소통, 해석 등 처리에 적절한 방식이 사용된다. 마지막으로 인지영역에서 생성된 지식을 저장하는 것도 정보영역에서 이루어진다. 문서나 정보의 형태로 저장되어 있다가 추가적인 감지 및 인식의 과정에 활용되기도 한다.

셋째는 인지영역(cognitive layer)이다. 정보를 수용하고 결심, 대응하는 인간의 인식영역으로, 지각, 인식, 이해, 신념, 가치 등이 존재한다. 측정 자체가 어려운 요소들이지만 다양한 전쟁과 전투 사례에서 보듯이 실제 승패를 결정하는 핵심적인 요소들이라는 점에서 인지영역 선점이 가지는 의미는 매우 크다. 일부 연구에서는 인지영역을 개인차원의 협의로 해석하면서, 인식 및 이해의 공유가 일어나는 영역을 "사회적 영역"으로 분리해서 보기도 한다.(신동찬 등, 2013, 32-33)

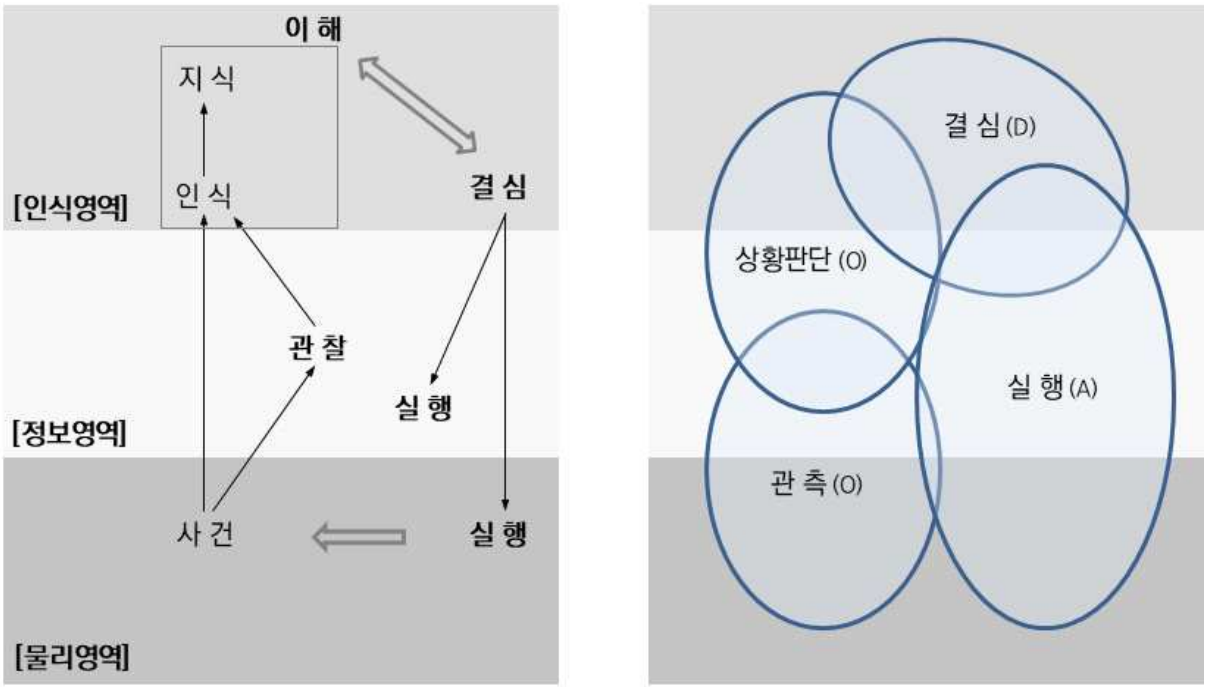
인지영역의 활동을 모두 개념화할 수는 없지만, 다른 영역과의 관계를 중심으로 살펴보면 다음의 몇가지 활동으로 정리할 수 있다. 먼저 물리적 객체와 현상에 대한 직접적인 감지가 있는데, 시각, 청각, 후각에 의한 직접적인 경험이 있다. 다음으로 지식의 생성이 인지영역에서 일어난다. 사전에 축적된 지식, 물리영역에서의 직접감지, 경험과 훈련, 타인과의 교류, 정보 등을 융합하여 지식화된다. 인식과 이해는 인지영역에서만 일어난다. 인식이 직접 또는 간접감지의 결과로 과거와 현재에 대한 것이라면, 이해는 이러한 인식과 지식을 통찰함으로써 미래를 예측하고 영향요인을 분석하는 종합적인 사고의 과정이다. 결심 역시 인지영역의 독특한 활동으로, 인지영역에서 다른 결심에 영향을 주든가, 물리영역에서 실행되거나 영향을 주고, 정보영역을 통해 전달 또는 실행된다.

위에서 살펴본 세 영역의 상호작용은 정보전에 있어 핵심적인 위치를 점한다. 먼저 정적인 관점에서 각 영역이 교차하는 영역이다. 첫 번째 물리영역과 정보영역이 중첩되는 영역에서는 정확성이 증강된 물리적 능력이 존재하는데, 아울러 속도와 접근성이 강화되는 효과를 가진다. 둘째는 정보영역과 인식영역이 중첩되는 곳에서는 인식의 공유와 전술적인 혁신이 이루어진다. 세 번째 물리영역과 인식영역이 교차하는 영역에서는 간명성, 자율성 등이 강화된 작전운용으로 작전적, 전략적 효과를 가져올 수 있다.(신동찬 등, 2013, 33) 세 영역의 역할과 중첩을 "복합체계(system of systems)"로 단순화하여, 전투공간식별, 첨단 C4I, 정밀타격체계로 제시하기도 한다.(William Owens, 1995, 37)

다음으로는 동적인 관점에서 영역을 넘어서는 활동도 있다. 각각의 영역에서 이루어지는 활동을 연결하는 과정에서 발생한다. "OODA 루프"는 개별 행위자의 결심과정을 토대로 하고 있어 정보행위를 지나치게 단순화하고 있다는 비판은 있지만, 각 영역을 연결하는 정보행동을 간명하게 보여준다. 관측(observe)은 물리영역으로부터 정보영역으로, 상황판단(orient)는 정보영역에서 인지영역으로, 결심(decide)는 인지영역 내에서, 실행(act)은 인지영역에서 정보영역을 거쳐 물리영역에 이른다.[2] 다른 한편으로는 둘 이상의 행위자가 상호작용을 하기도 하는데, 정보영역

에서의 정보공유, 인지영역에서의 지식공유, 인지-정보 영역에서의 공유된 인식과 협력, 인지-물리영역에서의 동기화 등과 같은 방식으로 나타난다. 이같은 활동들은 정보의 풍부함과 도달범위를 동시에 상승시키는 효과를 가져온다.(David Alberts, et al., 63-80)

〈그림1〉 정보전의 세 영역



출처 : Davis S. Alberts, et al., 『정보시대 전쟁의 이해』, 권태환 역 (서울: 국방대학교, 2004), pp.21-44의 그림을 종합 및 재구성

2. 정보전 양상의 변화

정보전의 세 가지 영역은 여전히 유효하다고 하더라도, 데이터 안보의 시대에 들어서면서 몇 가지 특징적인 변화가 일어나고 있다. 일반적으로는 안보행위자, 위협의 대상과 성격, 안보공간에서 변화가 확인된다.[3] 구체적으로는 낮은 진입비용으로 인한 행위자의 증가, 위협의 대상과 능력의 불확실성, 전술적 경고의 어려움, 공격자와 공격대상 파악 곤란, 피해평가의 어려움, 전통적 영역구분의 붕괴, 무기효과에 대한 불확실성, 사회기반구조의 취약성 증가 등을 들 수 있

2) 보이드 대령은 공대공 전투에서의 의사결정 순환과정 모델을, 관찰(observe)-상황판단(orient)-결심(decide)-실행(act)의 "OODA loop"로 설명하였다.(David Jordan, *et al.,* 2014, 287-289)

3) 미래전 양상에 대한 일반론적인 논의는 토플러 내외의 "정보문명시대 전쟁의 패러다임"에서 포괄적으로 다루어진바 있다. 정보와 지식이 전쟁의 승패를 결정하는 핵심요소로 등장하고, 디지털 전투원에 의한 정보마비전이 수행될 것이라고 전망했다.(Alvin Toffler and Heidi Toffler, 1995)

다.(Roger Molander, et al., 1998, 17-23) 몇 가지 특징적인 변화를 보다 자세히 살펴보면 다음과 같이 정리할 수 있다.

첫째, 여전히 "정보우세" 경쟁은 유효하며 오히려 그 중요성은 더욱 강화되고 있다. 정보를 통제하는 수준에 따라 정보패권(information supremacy), 정보지배(information dominance), 정보우세(information superiority)로 구분하는데, 사실 정보패권과 지배는 달성가능성이 높지 않다.(배달형, 2005, 51-53) 정보우세는 "정보가 중단되지 않도록 수집, 처리, 배포할 수 있고, 적의 능력을 이용하거나 거부할 수 있는 능력"을 의미하며, 지속적으로 유지될 수도 있지만 특정한 기능, 관점, 지역, 시기로 한정될 수 있다.(JP 3-13, 2014, GL-3) 이같은 정보우세는 정보체계, 피아 정보의 획득과 관리, 정보작전 등으로 구현된다. 특히 정보영역에서의 질량적인 변화를 가져온 정보혁명은 정보의 도달범위와 가치를 획기적으로 변화시켰고, 정보우세는 다른 기능들의 성패를 직접 이끌게 되었다.

미국은 이미 1996년 『합동비전(Joint Vision) 2010』에서 최초로 정보우세 달성의 의지를 천명한 바 있다. 정보우세와 기술혁신을 바탕으로, 우세한 기동, 정밀교전, 집중화된 군수, 전차원 방호를 통해 전영역에서 우위를 달성하겠다는 것이다.(US JCS, 1996, 50-51) 2000년 발간된 『합동비전 2020』에서는 "정보우세가 합동군 작전능력의 변환과 합동지휘통제를 위한 주요 촉진자(enabler)"라면서 핵심적인 지위를 부여하였다.(US JCS, 2000) 미국은 양적으로 비대칭적인 정보를 획득하고, 임무달성을 위한 정보요구 충족을 위한 수단을 확보하며, 정보이점을 활용하여 제한적인 전력우위를 상쇄하고자 노력하고 있다. 결국 정보의 질과 양을 동시에 증진시킴으로써 정보우세를 달성하게 될 것이다.

둘째, 빅데이터(Big Data)와 인공지능의 활용으로 인해 자료(data)-첩보(information)-정보(intelligence)의 단계 구분이 무의미해지고 있다. 수집된 원자료(raw data)는 이해될 수 있는 형태로 처리되면 첩보가 되고, 첩보는 다른 첩보와의 비교 및 통합을 통해 신뢰성있는 정보가 된다. 당연히 정보생산의 과정을 통해 신뢰성과 유용성은 높아지지만, 그만큼 시간과 노력이 들 수밖에 없다. 그러나 최근에는 자료가 한정적으로만 가지고 있던 용도에 대한 관심이 높아지고 있다. 데이터의 수집과 처리, 정보활동의 결심과 실행에 소요되는 시간과 노력이 크게 줄어들면서, 데이터 자체를 첩보 또는 정보로써 활용될 수 있게 된 것을 의미한다.(김상배, 2015, 10-11) 다른 한편으로 국가행위자들은 데이터 자체의 품질을 높이기 위한 다양한 노력을 병행하고 있다. 데이터 수준에서의 정보전이 활성화되면 공격과 방어, 방첩과 보안의 경계도 모호해질 수밖에 없을 것이다.

미 합동참모본부는 2017년 새롭게 펴낸 『합동군교리(Doctrine for the Armed Forces of the United States)』 에서 기존의 6개 합동기능에 "정보(Information)"를 추가하였다.(Joint Publication, JP-1, 2017) 합동기능으로 유지하고 있던 "군사정보(Intelligence)"가 군사첩보나 비밀에 대한 감시정찰 위주의 '군사활동'을 의미한다면, 새로운 정보기능은 보다 포괄적인 차원에

서 정치, 경제, 사회적 환경으로부터의 위협과 대응에 초점을 맞춘다는 점에서 차별성을 가진다.[4] 데이터 중심의 감시정찰, 결정속도의 증가, 치명성의 강화와 같은 환경 속에서,(The Joint Staff, 2016) 행위자의 인식, 행태, 행동과 무행동 등에 영향을 줄 수 있는 정보의 관리와 적용에 주목한다.[5]

셋째, 전투의 지향점이 선행단계로 이전하고 있다. 다니엘 애보트(Daniel Abbott, 2010)는 제5세대 전쟁의 특징을 설명하면서, 전쟁세대가 진화할수록 상대방의 영역으로 더욱 더 깊숙이 들어가게 될 것이라고 주장하였다. 전쟁의 영역이 위에서 살펴본 OODA 루프의 선행단계로 옮겨간다는 것인다. 병력에 의한 1세대 전쟁이 적의 결심(D)과 실행(A) 능력 무력화에 중점을 두었다면, 화력전투가 주를 이뤘던 2세대 전쟁은 판단(O) 및 결심(D) 능력 무력화, 기동전투의 3세대 전쟁은 상황판단(O)에 중점을 두었다는 것이다. 그 이후부터는 OODA 루프의 첫 단계인 관찰(O)을 지향하는데, 4세대 전쟁은 관찰 능력의 무력화를, 5세대 전쟁은 관찰의 조작을 추구하는 것이다. 잘 수행된 5세대 전쟁의 경우, 상대는 전쟁이 일어나고 있는지, 전략이익을 잠식당하고 있는지를 모를 수 있다.

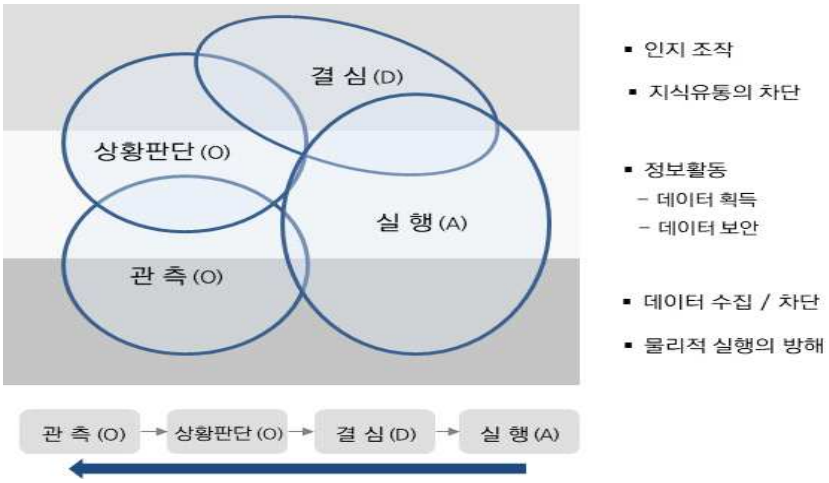
이같은 변화는 중첩영역이 확대되고, 각 활동의 구분이 모호해지는 것과 연계되어 있는데, 전통적으로 물리영역에서의 위협에서 머물던 것이, 정보영역과 인지영역으로 확대되었음을 의미한다. 인간정보(HUMINT)는 여전히 중요한 정보원이지만, 다양한 기술정보(TECHINT)가 확대되면서 비롯된 것이다. 기술정보는 상대적으로 정보활동의 위험부담이 적고, 보안조치에도 불구하고 획득이 용이하며, 획득가능한 범위와 내용이 크다는 장점이 있다. 아울러 데이터 시대에 이르러 단점으로 제기되어온 문제들이 극복되는 현상을 보이는데, 대단위의 첩보를 처리, 분석할 수 있게 되면서 예산과 시간을 절약할 수 있게 되었고, 정보활동이 인지영역으로 확대되면서 공격과 방어의 의미가 무색해졌다. 또 신속하게 많은 양의 자료를 확보할 수 있는 공개출처정보(OSINT)가 데이터화되면서 이른바 “완전정보(complete information)” 상태에서 경쟁하는 상황으로 발전하고 있는 것이다.

---

4) intelligence와 information은 구분없이 “정보”라는 명칭으로 사용된다. intelligence는 일반적으로 information보다 정제된 형태의 지식으로서 이해되지만, information이 intelligence를 포괄하는 개념으로 사용되기도 한다. 또는 자료-정보(information)-지식(understanding)으로 계서화하고, 정보활동(intelligence)은 활동 또는 과정을 의미하는 개념으로 이해하기도 한다. 학자들의 논의를 종합해보면, intelligence는 비밀성이 내포된 상대발에 대한 지식 또는 이를 수집하는 활동으로 정리할 수 있다.(전웅, 2015, 3-5)

5) Information 기능의 작전적 행동은 다음과 같다. 1)작전환경에서의 정보의 역할 이해, 2)행동에 영향을 주기 위한 정보의 활용: 대상 행위자에 대한 영향력, 국내외 청중에 대한 정보제공, 정보네트워크와 체계에 대한 공격과 활용, 3)인간 또는 자율결심체계 지원: 공유된 이해 제고, 정보보호 등이다.(JP 3-0, 2017, Ⅲ-17-27)

〈그림2〉 데이터 시대의 OODA Loop



결론적으로 여전히 정보우세를 차지하기 위한 경쟁은 유효하지만, 정보기술(information technology)이 태생적으로 가지고 있는 능력과 취약성은 더욱 급격한 변화를 경험하고 있다. 획득과 조작이 비교적 용이한 데이터의 취약성을 보완하고, 정보영역과 인지영역으로 확대된 위협에 대응해야 하는 것이다. 이같은 정보기술은 기능성, 상호운용성, 효율성, 편리성으로 인해 정보와 정보체계 뿐만 아니라 지휘통제, 기동, 지속지원과 같은 전통적인 기능과 통합되고 있다. 기술변수가 안보문제가 만나는 과정이 "이슈연계"의 메커니즘을 따라 더욱 복잡해지는 양상을 보이는 것이다. 따라서 정보기술에 대한 의존성이 커질수록 내재적인 취약성들도 확장되고, 적에 의한 위협도 동시에 커질 수밖에 없다. 이같은 변화는 미중 간의 경쟁에서도 그대로 드러난다.

Ⅲ. 미중의 "정보우세" 경쟁과 "데이터"

전통적인 정보전의 개념이 완전히 변화하고 있다. 전략목표를 달성하기 위한 정보전의 비중이 더욱 커졌는데, 특히 강대국간의 전략적 안정성, 핵터부(nuclear taboo), 경제적 상호의존성 등으로 인해 무력충돌의 가능성이 낮아지면서 강대국간의 정보우세를 위한 경쟁은 더욱 첨예화되고 있다. 미국은 2018년 『국방전략서(National Defense Strategy, NDS)』에서 "(미국의) 경쟁자들과 적들은 목적을 달성하기 위해 우리의 네트워크와 운용개념을 공격하기 위한 '최적화(optimize)'를 추구하고 있다"고 밝히기도 했다.(Department of Defense, 2018, 3)

그런 의미에서 미시적 안전문제에 머물러있던 기술의 문제가 "안보화"를 통해 양질전화의 임계점에 접근하는 단계나, 이미 지정학적 임계점에 다다른 안보영역에서의 정보전을 말하는 것은 아니다. 지금까지는 관계없는 것으로 보이던 각각의 이슈들이 연계되는 지점에서의 "정보우

세" 경쟁을 다루고자 한다. 이른바 "기술냉전"의 시대를 조망해보는 시도이다.(중앙일보, 2020.4.27.) 본 장에서는 정치, 외교, 통상, 산업, 시민사회와 같은 영역을 넘나들고 있는 상황을 미중 간의 데이터 경쟁을 통해서 살펴보려고 한다.

1. 미중의 정보우세(Information Superiority) 경쟁

중국은 전통적으로 피아의 정보를 활용하는 "책략(策略)"을 전승의 중요한 요소로 고려해 왔다. 중국의 책략은 상대 정보의 내용과 절차, 인식의 방향에 영향을 주고 오인과 오판을 일으킴으로써 중국의 미약한 군사력을 보완하는 중요한 기제로서 활용되었다. 특히 사이버 공간이 확대되면서 물리적 공간에서 벗어나 감시정찰, 정보탈취, 네트워크 침입, 정보왜곡 등을 더욱 용이하도록 만들고 있다. 중국은 전시 뿐만 아니라 평시에도 "무제한전(Unrestricted Warfare)"을 추구하면서, 이른바 심리전, 여론전, 법률전의 "삼전(三战)"을 정보전의 핵심개념으로 제시한 바 있다.(Wang Xiangsui and Liang Qiao, 2017) 특히 디지털 안보 시대에 있어 미중 간의 정보우세 경쟁은 더욱 복잡한 양상을 보이고 있다. 미국은 과학기술에 대한 의존성이 높기 때문에 태생적으로 취약성을 가지고 있고, 다양한 소스의 정보를 융합하는 과정에서도 맹점을 가질 수밖에 없다.

중국은 이를 상대적 기회로 활용하면서 다양한 형태의 데이터 공격과 방어를 통해 안보 및 경제적 이익을 추구해왔다. 아래에서 자세하게 살펴보겠지만, 2009년 중국은 록히드마틴(Lockheed Martin) 社로부터 방대한 양의 F-35 설계와 관련된 자료를 탈취한 것으로 알려지며,(Catherine A. Theohary, 2018, 11-12) 2014년에도 보잉 社의 C-17 수송기 데이터가 중국 측으로 넘어간 것으로 알려진다.(The New York Times, 2014.7.12.) 이러한 데이터의 유출은 단순히 기술의 모방이나 복제에 그치는 것이 아니라, 유사시 해당 플랫폼의 지휘통제 체계를 무력화하거나 침투할 수 있는 가능성 때문에 국가안보와 직결된다. 미 국방부는 2013년 처음으로 중국 정부와 군이 미국에 대한 사이버 공격을 해왔다고 밝히면서, 중국 정부가 직접 연결되어 있음을 공식화했다.(Washington Post, 2013.5.27.) 중국은 다른 한편으로는 자국의 "사이버 주권"을 내세우면서 정보의 유통을 강력하게 통제하는 "황금방화벽(Golden Firewall)" 프로그램을 가동하면서 보안을 강화하기도 했다.(Bloomberg, 2018.11.5.)

미국과 중국이 정보영역에서 직접적으로 공격과 방어를 수행하는 것만은 아니다. 학교와 연구소의 연구에서 중국의 부정적인 이미지를 벗기 위해 전문가들에게 물질적인 인센티브를 제공하기도 했고, 2018년 FBI의 크리스토퍼 레이(Christopher Wray) 국장은 상원 정보위에서 미국 내 대학교에 중국어 및 문화교육을 위해 설립된 "공자학원"이 첩보수집과 여론조작에 관여되어 있다고 밝히기도 했다.(KBS News, 2018.3.7.) 아울러 경제적, 문화적 이익을 얻기 위해 영화산업에도 영향력을 추구해온 것으로 알려진다. 국제사회에서 평화적이고 협력적인 이미지를 구축

하기 위한 외교전도 정보전의 일환으로 시행되었고, 정보무기(informationa weapons)에 대한 군비통제 제안을 내놓은 것도 적대국인 미국의 상대적 우세를 상쇄하기 위한 전략으로 이해된다.(Catherine Theohary, 2018, 11-12)

중국 위협론에 대한 평가는 다양하고, 그에 대한 대응전략 역시 다양하다.[6] 다만 "역사-행태적인 접근"을 통해 볼 때, 중국은 미국에 대한 정보우세를 달성하기 위해 보다 적극적인 행보를 취할 가능성이 커 보인다. 마오쩌둥의 "인민전쟁(人民戰爭)"은 군사동원을 위한 전사회적(whole-of-society) 접근과 군현대화에 기여하는 산업발전을 전제하고 있는데, 이른바 "민-군융합(Military-Civil Fusion)"의 관점은 정보우세 경쟁에서도 동일하게 작동할 것이기 때문이다.[7] 정보기술의 획기적 발전과 함께 크게 증가하고 있는 중국의 스파이(espionage) 행위가 늘어나는 추세에 있는데, CSIS는 2000년대 이후 137건이라는 통계치를 내놓았으며,[8] 274건에 이른다고 집계한 연구도 있다.(Nicholas Eftimiades, 2018a) 사실 미국은 경쟁자들의 "선진 정보전" 개념에 맞서 경쟁하고 승리하기 위한 관점에 익숙하지 못하다. 미국 국내법에 의해서 규정, 보호되는 산업스파이 사례는 제외하고 "데이터" 정보우세를 다투는 사례만을 몇 가지 유형으로 구분하여 살펴보자.

---

6) 화웨이 사태를 "안보화"의 관점에서 바라보면서, 중국의 기술패권 확대를 막기 위한 중국위협론의 확대된 담론으로 보는 견해도 있다. 이른바 기술패권예방전쟁, 기술민족주의, 디지털보호주의의 일환이며, 위협을 과장하고 과도한 대응책을 요구하는 "초안보화(hypersecuritization)"으로 개념화한다.(김지영, 2019)

7) 중국의 민-군통합(military-civil integration)이 국방분야의 재구성과 민간분야로부터의 지식유입(spin-on)에 중점을 두었다면, 민-군융합은 사회전반의 연구역량과 스타트업 생태계까지를 포괄하는 정도의 일체화를 이룬 현실을 반영한다. 예를 들어, AI와 슈퍼컴퓨터 분야 민군융합연구센터가 다수 설립되었고, Thousand Talents Program(海外高层次人才引进计划) 등을 통해 해외인재를 중국으로 불러들이고 있으며, 이중용도기술의 획득과 연구원, 학생의 해외파견도 크게 확대하였다.(USCC, 2019, 208-209)

8) CSIS는 137건 중 57%가 중국 정부 및 군에 의해서, 36%가 사기업, 7%는 비중국인에 의해서 자행되었으며, 36%는 군사기술, 46%는 상업기술인 것으로 평가했다. 특기할만한 사항은 2000년부터 2009년까지 27%였던 것이 2010년 이후에는 73%를 차지한 것이 크게 증가하고 있는 현실을 반영한다. "Survey of Chinese-linked Espionage in the United States Since 2000" (CSIS, 2019). https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000 (검색일: 2020.2.28.).

〈표1〉 미중 데이터 경쟁의 주요사건

시 기		내 용
2003		중국 해커, 미 해군항공무기센터에서 핵무기 실험·설계 데이터, 스텔스기 데이터 탈취
2003	4	FBI, Katrina Leung을 비밀정보를 중국에 넘긴 죄로 구속, 10년형 구형
2004	2	전 DIA 분석관 Ronald Montaperto, Ⅰ, Ⅱ급 정보를 중국무관에게 전달 발각
2005	6	Noshir Gowadia, 03-05년 사이 6차례 중국을 방문하여 순항미사일의 스텔스 배기가스노즐 기술지원 및 대가로 11만 달러 수령
2005	10	Chi Mak 등 중국 정보원, 미 해군의 현용 및 미래 전함기술 획득 및 중국 전달 시도
2005	11	미 우주항공회사 대표로 대만서 10년간 근무한 Moo Ko-Suen, 중국 정보원으로 활동 및 F-16 제트엔진 및 순항미사일 정밀부품 구매 시도
2005		중국 해커, "Titan Rain" 작전을 통해 미 국방부 네트워크 침입하여 방위산업체, 육군정보체계사령부, 국방정보체계청, 해군대양체계센터 등 접근
2005	4	중국 해커, Lockheed Martin, Boeing이 관리하는 NASA 네트워크 침투, 우주왕복선 Discovery 프로그램 정보탈취
2006	7	중국 해커, 미 국무부 일반 네트워크에 침입하여 민간정보 및 비밀번호 탈취
2006	8	중국 해커, 미 국방부 NIPRNet(일반)에 침입하여 10-20테라바이트 정보 획득
2006	12	중국 해커, 미 해군대학에 침입
2007		중국 해커, 국방부 JSF 프로젝트에 침입하여 F-35 관련 데이터 탈취
2007	9	해커들, 계약자를 통해 국토안보부 네트워크에 침입하여 일반정보 탈취
2007	10	중국 국가안전부(MSS), 해커의 42%는 대만, 25%는 미국인이며, 핵심정보 탈취시도 공개, 2006년의 경우 CASIC의 보안부서와 고위급의 컴퓨터에서 스파이웨어 발견
2007	12	중국 해커, Oak Ridge 및 Los Alamos 국가연구소, 에너지부 핵안보실 정보 탈취
2008	2	전 보잉사 기술자 Dongfan Chung, 1979년 이후 중국 정보원으로 활동하면서, 우주왕복선, C-17 수송기, Delta IV 로켓에 대한 정보를 중국에 제공
2008	2	Tai Shen Kuo, 펜타곤 무기정책분석관 Gregg Bergersen로부터 비밀정보를 중국에 전달
2008	11	중국 해커, 오바마와 맥케인 대선캠프 네트워크에 침입하여 미래정책 어젠다 탈취
2008	11	중국 해커, 백악관 네트워크에 침입하여 정부 고위관료들의 이메일 탈취
2009	3	중국 스파이 네트워크가 최소 103개 국가의 정치, 경제, 사회기관에 침입한 사실 확인
2009	3	중국 해커, Ball Nelson 상원의원 정보 탈취
2010	1	중국이 2009년 초부터 구글, 야후 등의 기업들에 대한 사이버공격을 통해 무역정보 획득
2010		중국군이 민간예비군비행대(CRAF)에 침입하여 항공기록, 자료, 보안메일 등 탈취
2011	4	중국 해커, Oak Ridge 국가연구소에서 1기가바이트의 정보 탈취
2011	8	중국 해커, 미국 정부 네트워크를 포함 72개 기관에 대한 사이버 공격 시도
2011	111	중국 해커, 미국 위성 시스템에 침입하여 민감정보 탈취
2012	2	중국 해커가 F-35 관련 비밀기술정보 탈취했다고 보도
2012	3	NASA 감사국, 2011년 13차례 사이버 공격을 받았고 150개의 사용자 접속정보 탈취

2012	3	Trend Micro, 중국이 사이버공격 "Luckycat"을 통해 미국 내 인도와 일본 군사연구, 티벳 활동자 등을 겨냥했다고 밝힘
2012	6	중국군 61398부대, digital Bond, SCADA 보안회사 등을 스피어피싱 공격
2012	8	전 CIA 요원 Jerry Lee, 중국내 CIA활동 관련 비밀정보를 중국에 전달
2013	1	국방과학위원회, 중국 해커들이 무기체계 정보를 탈취했다고 보고 * PAC-3, THAAD, 이지스, F/A-18, V-22 오스프리, 빌랙호크, 연안전투함 등
2013	1	뉴욕타임스, 월스트리트저널 등 다수의 언론사가 중국발로 의심되는 지속된 사이버공격 사실 보도
2013	2	중국군 61398부대, 2006년 이후 115차례 미국 해킹
2013	3	중국 해커, 2012년부터 남중국해에서의 민간 및 군사작전에 대한 해킹 시도
2013	6	중국군 해커, 미국 수송사령부 네트워크에 침입하여 민간군사정보 탈취
2013	6	스노든, 미국이 중국을 대상으로 다양한 사이버 스파이 행위를 행해왔다고 폭로
2013	9	중국 해커, "Sykipot" 멀웨어를 통해 통신, 컴퓨터, 항공 등 방산기업에 침입
2014	9	화웨이, T-mobile로부터 로보틱스 설계 정보에 대한 탈취 시도
2014	11	중국 해커, 미 우편국 네트워크 침입하여 8십만명의 직원정보 탈취
2015	1	Fujie Wang, 건강보험회사 Anthem Inc.에 침입하여 7,880만명 정보 탈튀
2015	11	네덜란드 보안회사 Fox-IT, "Mofang" 등의 중국 해커가 미 정부, 군사, 기업 사이버공격 공개
2016	3	FBI 직원 Kun Shan Chun, FBI 감시방법, 내부기관, 특수요원의 해외활동 패턴 등을 포함한 민감정보를 중국 정부에 제공하여 24개월 형
2016	4	미 원자력공학기술자 Szuhsiung Ho, DOE 승인없이 중국 CGNPC의 핵물질 및 원자로 개발에 정보 및 기술자 제공
2017	3	위키리크스, CIA가 개발한 수억 개의 코드를 통해 2013부터 2016까지 CIA의 해킹툴이 사용되었다고 폭로
2017	4	중국, THAAD를 한국에 배치하기로 결정했다는 발표 이후에 한국군, 정부, 방산 네트워크에 대한 침입 시도가 크게 증가
2018	1	중국 해커, 미 수중전투센터 계약회사에 침임하여 624 기가바이트 가량의 초음속 대함미사일, 암호체계와 전자전장비 관련 무선실 정보를 탈취
2018	1	중국, 아프리카연합(AU)에 공급한 컴퓨터 네트워크가 AU의 비밀정보에 접근하고, 도청하며, 중국으로 정보를 전송한다는 의구심을 부인
2018	10	국토안보부, 미 중간선거에 앞서 선거 인프라에 대한 다수의 사이버 활동을 식별했다고 공개
2018	11	중국관영통신, 2018년에 외국의 해커로부터 다수의 비밀메일, 디자인, 군부대 목록 등을 탈취당하는 피해를 받았다고 공개
2018	12	중국 해커, 45개 기술회사와 미국 정부로부터 수백 기가바이트의 정보를 탈취
2018	12	중국 해커, 수년간 EU의 통신체계에 침입하여 민감외교전문에 대한 접속 유지
2018	12	미국, 호주, 캐나다, 영국, 뉴질랜드는 중국 해커 2명을 기소하면서, 중국이 12년 동안 12개국 이상에 대한 IP정보와 무역정보 등을 탈취해왔다고 공개
2019	3	중국 해커, 미군과 연계된 이스라엘 방산업체에 대한 침입 시도
2019	3	미국의 최소 27개 대학이 중국 해커로부터 해군기술연구 관련 정보 해킹 피해
2019	5	중국정보기관, 2016년부터 NSA 해킹툴을 활용하여 해킹 지속
2019	6	중국정보기관, 향후 정보원으로 활용하기 위한 대상자 물색을 위해 호주대학 해킹 시도

2019	7	중국 해커, 동아시아 국가의 기술정보, 대외관례, 경제개발 관련 정부기관 해킹 시도
2019	7	Capital One, 1억명의 신용카드 정보(사회보장번호, 계좌번호) 해킹사실 발표
2019	8	화웨이 기술자, 두개의 아프리카 국가 정부관료가 야당 및 보안통신에 접근하도록 지원
2019	9	화웨이, 미 정부의 인트라넷과 내부정보시스템 해킹시도에 대한 혐의
2019	10	1억명 이상이 사용 중이며 중국 정부가 지원하는 선전용 어플에 위치정보, 메시지, 사진, 접속기록, 원격녹음 등이 가능한 백도어 프로그램이 발견,
2019	10	중국 해커, 독일, 몽골, 미얀마, 파키스탄, 베트남 및 유엔안보리의 ISIS 관련 결의안 관련자, 아시아 종교 및 문화단체 등에 대한 해킹 시도

참고 : CSIS, ""Survey of Chinese-linked Espionage in the United States Since 2000";
"Significant Cyber Incidents since 2006" (CSIS, 2019) 중 미중 간의 일부 사건을 정리.

2. "데이터" 정보우세 경쟁 사례

"데이터"와 관련된 정보우세 경쟁 역시 상대적인 개념이다. 특히 정보우세는 물리영역에서의 시간과 공간적 제약을 초월하고, 정보영역과 인지영역을 넘나든다는 점에서 "상대적 정보 이점(relative information advantage)"의 연속체로서 의미를 가진다. 따라서 미중 간의 정보우세 경쟁은 시간적, 공간적으로 한정되지 않는다. 지리적으로는 양국의 영토 범위를 벗어나 지구적 차원에서, 시간적으로는 한시적일 수도 있고 지속될 수도 있다. 또 가공되지 않은 데이터로부터 정보를 선점함으로써 상대적인 이점을 확보하려는 시도는 계속된다. 아래는 데이터 안보의 시대에 더욱 첨예화되고 있는 미중 간 정보우세 경쟁의 대표적 사례를 제시한 것이다.

1) 물리영역에서의 기반체계 교란

물리영역에서는 전통적인 정보활동이 지속된다. 먼저 물리현상을 관측하고, 데이터를 획득한다. 여기에는 상대의 관측을 차단하고 교란하며, 데이터 수집을 방해하는 다양한 활동도 포함된다. 다음으로는 결심된 사항이 실행되는 것을 차단하기 위해 물리적인 무기체계가 표적이 될 수 있다. 항공기, 함정, 포병, 정밀 유도무기, 방공무기 등의 플랫폼도 있고, C4I, 군수, 작전과 같은 군사 기반구조와 통신, 수송, 에너지, 금융 등의 민간 기반시설 등을 목표로 할 수 있다. 물리영역에서의 미중 데이터 경쟁 사례는 다음과 같다.

• 2001년 "정찰기 충돌사건"은 물리 영역에서 벌어진 미 · 중 간 정보우세 경쟁이 수면 위로 드러난 사건이다. 4월 1일 미국 카데나 공군기지의 EP-3 정찰기가 정찰 업무 수행 중에 이를 제지하던 중국 공군의 F-8기와 충돌하였다. 중국 공군기는 추락하고 미국 정찰기는 중국 해남도 공항에 비상 착륙하였다. 사건의 근본 요인은 미 · 중 모두에게 전략적 요충지인 남중국해에서 늘

어나는 중국의 군사활동과 정찰활동, 이를 견제하기 위한 미국의 전략적 이해관계가 충돌하였기 때문이다.(강준영, 2001, 170) 2017년 7월 23일에는 서해에서 미해군 EP-3 정찰기와 중국의 J-10 전투기가 100미터까지 근접하는 충돌 위기 상황이 벌어졌다.(TV조선 뉴스, 2017.7.25.) 이러한 사건은 '정보우세'를 둘러싼 정찰기-요격기간 물리적 마찰이 현재 진행형임을 보여준다.

• 2007년 1월 11일 중국은 DF-21로 추정되는 탄도미사일로 고도 약 850km에 위치한 자국의 노후위성(FY-1C)을 요격하였다. 이로써 중국은 미국과 러시아에 이은 세 번째 위성요격용무기(ASAT: Anti SATellite Weapons) 보유국가가 되면서, 정보수집 분야에서 위성에 크게 의존하는 미국의 약점을 노릴 수 있게 되었다.[9] 최근 중국은 2018년 2월에 3만km 상공의 군사위성을 타격할 수 있는 신형 ASAT인 'DN-3'의 발사시험 성공을 발표하였고, 일부 매체에 따르면 이는 중국이 보유한 비대칭 전쟁 무기들 가운데 가장 강력한 것 중 하나로 평가된다.(연합뉴스, 2018.4.3.)

• 중국의 산업스파이 행위는 미국의 기술적 우위를 잠식하면서 중국에 경제적 이익뿐만 아니라 군사적, 안보적 이익을 가져온다. 중국은 2009년 방산업체 록히드마틴의 컴퓨터에서 F-35 Joint Strike Fighter의 설계 데이터를 대량으로 빼돌린 혐의를 받고 있는데, 2012년에는 F-35의 중국 버전으로 의심되는 J-31이 등장하였다. 또 2014년에는 한 중국인이 보잉사의 C-17 군용 수송기의 관련 자료를 훔친 혐의로 기소되었다. 이와 같은 최신예 군용기에 대한 정보 탈취는 중국이 복제를 통해 최신 기술을 가진다는 점 뿐만 아니라, 유사시 군용기의 지휘통제시스템을 해킹하여 불능화시키는 능력을 가질 수 있다는 점에서 직접적인 위협이다.(Catherine A. Theohary, 2018, 11-12)

• 스노든의 폭로에 따르면 미 정보기관은 2011년에만 231건의 공격작전을 실행했는데, 중국 2곳을 포함하여 전세계에 "Load Stations"를 운용하면서 컴퓨터 시스템을 차단하고, 멀웨어 또는 부품을 부착했다. 또 NSA의 "Tailored Access Operations(TAO)" 그룹은 정교한 멀웨어를 수만 대의 컴퓨터, 라우터, 방화벽에 접근시키는 "은밀경로"를 개척했는데, 이로써 시간당 2페타바이트(petabytes)의 자료에 접근할 수 있었던 것으로 알려진다.(Fred Cate, 2015, 303-305) 또 다른 자료는 코드명 "Turbine"을 다루고 있는데, 수백만 개의 이식체를 통해 첩보입수 뿐만 아니라 시스템을 교란, 침해, 파괴할 수 있었다. 대상 컴퓨터를 통해 녹음 뿐만 아니라 모든 접속기록을 추적할 수 있다.(Fred Cate, 2015, 303-305)

• 워싱턴포스트는 2차 세계대전 이후 전세계 정부를 상대로 수십년간 암호 장비를 팔아온 스위스 회사 '크립토AG'가 사실 미국 중앙정보국(CIA)의 소유였고, 서독의 정보기관과 함께 정보를 빼내왔음을 폭로하였다. 이 회사의 고객은 120개국이 넘으며 한국과 일본, 인도와 파키스탄 및 이란과 사우디아라비아도 리스트에 포함되었다. 이 장비로 CIA는 1979년 이란에서의 미국인 인

9) 이미 미국과 소련의 우주에서의 정보우세 경쟁이 존재하였는데, 1960년대 미국의 정찰위성에 대응하기 위해 소련은 궤도 폭격 시스템(Orbital Bombardment System)을 개발했고 미국은 1985년 약 555km 상공의 노후위성 파괴시험에 성공한 바 있다.(공현철 등, 2007, 2,030-2,035)

질 사태 당시 이란의 이슬람율법학자들을 모니터링할 수 있었으며, 포클랜드 전쟁 시엔 아르헨티나군의 정보를 영국에 손쉽게 넘겨줘 영국의 승리에 기여하기도 하였다. 한편, 미국의 주요 타겟이었던 구소련과 중국은 이 장비가 서방과 연계되어 있음을 의심하여 이용하지 않았다. 하지만 CIA는 다른 나라들이 구소련 등과 연락하는 과정을 추적함으로써 구소련으로부터 상당량의 정보를 취득할 수 있었다고 알려진다.(연합뉴스, 2020.2.12.)

• 2019년 창설된 미국 우주군은 2020년 3월 13일에 첫 우주 공격용 무기체계의 전력화를 발표하였다. 2004년에 적대국들의 '위성요격무기' 운용에 대항하는 것을 목적으로 배치된 '지상기반 이동형 우주무기(Counter Communications System, CCS)'는 적들의 위성통신을 쌍방향으로 교란할 수 있는 능력을 갖는다. 전문가들은 향후 미 우주군이 지상 배치 위성교란 체계를 직접 타격하는 우주무기들을 실전배치하게 될 것이라고 분석하였다.(VOA KOREA, 2020.3.17.)

2) 정보영역에서의 공격과 방어

정보영역에서는 전통적인 정보활동이 일어나는데, 우선은 정보처리과정을 통해 데이터를 첩보화하거나, 상대의 정보처리를 방해하는 활동이 있다. 다음으로는 정보의 수집, 유통, 저장이라는 정보활동의 공격과 방어이다. 특히 빅데이터와 AI 활용을 통해 데이터 자체가 정보로서의 가치를 가지게 되면서, 데이터 획득과 방호가 핵심적인 활동으로 자리잡게 되었다. 상대의 데이터를 적극적으로 획득, 처리, 저장함으로써 정보우세를 달성할 수 있다는 점에서, 미중 정보전의 핵심적인 지위를 차지한다.

• 중국은 2017년 6월 '사이버 보안법'을 도입하여, 기업들이 중국에서 수집한 각종 데이터를 국가안보라는 이유를 들어 중국 내에만 저장하도록 규정하였다. 이는 해외에 서버를 둔 기업들의 사업 자체를 방해하는 조치로 평가된다. 또 중국 정부는 2019년 '정보보안등급보호규정(MLPS) 2.0'를 발표하였는데, 중국 정부부처, 기관 기업 및 외국기업의 전산망들에 대한 점검을 실시하고 5단계의 보안등급을 부여하였다. 낮은 등급인 3-5등급은 연 1회이상 중국 공안의 감사를 받아야하고, 2등급은 정부 요청시 관련자료를 보고해야할 의무가 생긴다. 1등급을 제외하고는 사실상 중국 정부가 보안을 빌미로 기업들의 전산망을 자유롭게 모니터링할 수 있게 됨을 의미한다.(한국일보, 2019.11.12.)

• 미국은 2018년 3월 "해외 데이터의 투명한 이용에 관한 법(Clarifying Lawful Overseas Use of Data, CLOUD)"을 공포했다.(H.R.4943) 명목상으로는 강력범죄 수사를 위해 미국 기업의 해외서버를 압수수색하도록 하는 것이지만, 적극적으로는 미국 IT기업들을 활용하는 외국인들의 각종 데이터를 미국 사법당국이 확인할 수 있다. 미국이 합법적으로 외국의 데이터를 확보하는 수단을 늘리게 된 것이다.

• 2019년 5월 트럼프 대통령은 미국 기술을 향한 해외세력의 위협에 대해서 국가비상사태를

선포했다. '정보통신 기술 및 서비스 공급망 확보(Securing the Information and Communications Technology and Services Supply Chain)'로 명명된 위의 행정조치는 국가안보에 위협이 되는 기업의 통신장비를 사용하지 못하도록 하는 내용을 골자로 한다. 비록 이러한 행정조치는 화웨이를 콕 집어 언급한 것은 아니지만 트럼프 행정부는 줄곧 화웨이가 자사의 장비에 백도어를 심는 방식을 통해 중국 정부의 스파이 활동을 지원할 수 있을 것으로 의심해 왔으며, 미국의 동맹국들로 하여금 화웨이의 5G 네트워크를 사용하지 않도록 촉구해온 것을 근거로, 워싱턴 포스트를 비롯한 미국의 주요 언론들은 이번 조치가 중국과의 무역전쟁, 특히, 화웨이발 위협을 봉쇄하는 조치라 설명했다.(Washington Post, 2019.5.16.)

• 2020년 초, 미국 하버드 대학교의 교수가 중국으로부터 비밀리에 금품을 받은 혐의로 체포되었다. 하버드대 화학학과장 찰스 리버(Charles Lieber) 교수는 지난 2012년부터 2017년까지 5년간 중국 허베이성 우한에 위치한 우한이공대학으로부터 매년 15만 달러의 생활비와 매달 5만달러의 월급을 받고 이를 하버드대 및 국방부, 미국 국립보건원에 숨긴 혐의를 받는다. 이같은 중국의 지원은 해외 우수인력 유치를 위한 '천인계획(Thousand Talents Plan)'의 일환으로 밝혀졌으나, 미국은 중국이 이 계획을 통해 산업스파이를 양성한다고 의심하며, 중국이 해커, 과학자, 유령회사와 같은 비전통적 방법을 통해 정보를 수집하고 있다고 비난하였다.(뉴스1, 2020. 1. 29.)

• 미국 상무부는 2019년 6월 21일 슈퍼컴퓨터와 관련된 5개의 중국 기업 및 국영연구소를 거래제한 명단에 올렸다. 슈퍼컴퓨터 제조업체 중커수광(Sugon), 하이곤(Higon), 우시 장난 컴퓨터 테크놀로지 연구소(Wuxi Jiangnan Institute of computing Technology) 등이 이 블랙리스트에 포함되었으며, 미국 상무부는 이들 기업이 미국의 국가안보와 외교적 이익에 반하는 활동에 관여할 위험이 있다고 밝혔다. 특히, '중커수광'은 고성능 컴퓨터를 이용하여 다양한 군사적 정보를 수집하고 있고, '우시 장난 컴퓨터 테크놀로지 연구소'는 중국 인민해방군 총참모부의 '제56 리서치 연구소' 소유로 중국군의 현대화 지원임무를 맡고 있다고 설명하였다.(한국일보, 2019. 6. 22.)

3) 인지영역에서의 메타공격(meta-attack)

인지영역에서의 정보우세 경쟁은 그 의도와 실체를 파악하기가 더욱 어렵다. 먼저 OODA 루프 속에서 결심지점으로의 연결을 차단하는 활동이 있을 수 있다. 다음으로는 지식의 생성, 인식과 이해 등을 중간에 차단하는 활동도 있으며, 축적된 지식과의 연결을 차단하거나 정보가 지식화되는 것을 방해하는 다양한 활동이 수반된다. 마지막으로 리더십을 표적으로 하여 이들의 인식과 결심을 물리적으로 공격하는 것도 포함되는데, 정치, 군사, 사회, 문화적 리더십을 망라한다. 정보전은 설득, 영향행사 등 결국 상대의 인식을 핵심표적으로 삼는다는 점에서 인지영역에

서의 활동은 더욱 중요하다. 몇가지 사례를 제시하면 다음과 같다.

• 2011년 출범하여 중국의 지배적 소셜네트워크으로 성장한 위챗(WeChat)은 자유민주주의 국가 내 중국의 디아스포라(diaspora)에 대한 선전유포의 통로로써 활용된다. 중국 교포들은 해당 국가의 정치인과의 의사소통에 위챗을 사용하는데, 기본적으로 중국 공산당의 검열을 받는다는 것을 의미한다. 2017년에 캐나다 국회의원 제니 콴(Jenny Kwan)이 위챗에 2014년 홍콩의 민주화 운동을 지지하는 글을 올렸는데, 위챗의 검열을 받아 삭제된 적이 있었다.(Danielle Cave, et al., 2019, 11-12) 또 위챗은 정보의 검열뿐만 아니라 감시에도 활용되는데 중국 당국은 공개적으로 삭제된 위챗 메시지를 수집할 수 있음을 인정하기도 했다.(Vision Times, 2019.11.17.)

• 스노든이 폭로한 바와 같이 미국은 중국 통신회사, 광섬유 네트워크 소유주, 베이징대학교 등에 대한 해킹행위를 해 왔다.(Newsweek, 2013.11.1.) 특히 NSA가 화웨이 네트워크에 백도어를 심어놓은 것은 단지 중국의 정보를 획득하기 위한 것뿐만 아니라, 화웨이를 사용하는 다른 국가를 감시하고 사이버 공격작전을 취하려고 했던 것으로 분석된다.(The New York Times, 2014.3.22.)

• 중국의 기술회사들은 일부 비민주 국가의 정부와 관계 발전을 통해 타국의 정치와 정책에 관여한다. 일대일로(一帶一路) 구상에 벨라루스가 참여하게 되고 그들 간의 외교 경제적 유대 관계가 심화되면서, 벨라루스와 중국 기술회사들 간의 협업이 급속도로 확대되었다. 화웨이는 이 과정에서 벨라루스에 대해 정치적, 정책적 영향력을 행사하였는데, 2014년 현지 자회사를 통해 '지적 원격감시 시스템'을 위한 연구실을 발족했고, 벨라루스 국민의 중국 유학에 대해 협약을 맺었으며, 벨라루스 주립 통신대학과 공동의 훈련센터를 위한 협약을 체결하는 등 교육 분야에까지 정치적 영향력을 확장하였다.(Danielle Cave, et al., 2019, 14)

• 중국의 데이터 안보 기술은 특히 독재정권의 독재력 강화에도 이용된다. 화웨이는 짐바브웨의 국영 이동통신 기업인 NetOne과 수백만 달러의 계약을 얻어냈으며, ZTE 또한 2015년 짐바브웨 최대의 이동통신 회사 Econet과 5억 달러의 계약을 맺었다. 짐바브웨 정부는 2016년부터 국민들로 하여금 소셜미디어를 사용하지 못하도록 제한하는 법을 통과시켰다. 또 중국을 롤모델로 삼아 안면인식 기술을 통한 '정교한 감시 시스템'의 구축을 도모하고 있는데, 경찰과 교통통제 시스템에 하이크비전사(社)의 감시카메라를 공급받고 있다.(Danielle Cave, et al., 2019, 11-12)

• 미 의회는 회계감사원(Government Accountability Office, GAO)으로 하여금 미국 내 중국 연구자와 학생들에 의한 불법행위를 조사하도록 지시하였는데, 수학, 과학, 공학 분야의 관련 중국인 숫자, 소속, 연구분야와 체류기간, 연구자금의 출처, 비자 프로그램 등 총체적인 분석을 요구하였다. 공자학원(Confucius Institutes)을 중심으로 미국 대학교 내에서 광범위하게 벌어지고 있는 스파이 행위에 대한 예방조치로 평가된다.(GAO-10-401T, 2019)

• 인공지능(AI) 기술을 이용하여 사람의 이미지와 음성 · 영상을 합성 및 변형하여 허위 콘텐츠를 만드는 딥페이크(Deep Fake)에 대한 우려가 커지고 있다. 정치권에서는 진위를 파악하기 어려울 정도로 정교하게 발전된 이 기술이 가짜뉴스에 악용된다는 점에서 큰 위협으로 인식하고 있다. 실제 2018년 멕시코 대선 당시 야당 후보였던 현 대통령 로페스 오브라도르(López Obrador)를 음해하는 가짜 녹취파일이 등장하였다. 인도에서는 정부 측 지지자들이 정부에 비판적이었던 여성 언론인의 얼굴로 만든 음란영상이 유포하는 사건이 있었다. 2020년 대선을 앞둔 미국은 2018년 12월 딥페이크 규제 법안을 제출하는 등 가짜뉴스 방지를 위한 적극적인 대응을 실시하고 있다.(아시아경제, 2019.12.19.)

3. 미중 경쟁의 전망

현재까지의 양상은 미국의 정보우세 상황에 중국이 도전하는 모양새이다. 중국의 도전이 미국에 위협이 되고 있느냐의 문제와는 별개로, 그동안 중국의 시도가 성공적이었는가에 대해서는 의견이 나뉜다. 중국 국내정치의 불안정성 때문에 정보기관의 임무수행이 효과적이지 못했으며, 수집된 데이터가 전달되는 과정이 경직되어 합리적인 정책결정을 지원하지 못했다는 분석이 있다. 또 현재까지의 상황은 전통적인 군사정보 수집활동이 사이버 영역으로 확대된 것에 불과하며, 오히려 미국에 과도한 경각심을 일으켜 불필요한 갈등을 양산해냈다는 분석도 있다.(Peter Mattis, 2015) 그러나 현재까지의 중국의 시도가 효과를 가져오지 못했다고 할지라도, 현재까지 축적된 데이터만으로도 향후 미중의 정보우세 경쟁에서 유리한 위치를 점할 수 있는 조건이 될 것이다.

지금까지 확인된 몇가지 사례를 통해 볼 때, 향후 미중의 데이터 정보우세 경쟁은 다음과 같은 양상으로 전개될 것으로 전망된다. 첫째는 과거 현상의 지속 및 확대로서 양질전화이다. 우선은 경제영역에서의 정보 탈취행위가 지속될 것이다. 물론 미중의 “지적재산권(intellectual property, IP)” 분쟁이 하루 이틀의 일이 아니고, 미중 간의 문제만도 아니다. 1980년대에는 프랑스, 1990년대에는 일본의 경제스파이 행위가 크게 대두된 바 있으며, 2015년에는 한국의 코오롱이 듀퐁(DuPont)으로부터 방탄섬유인 아라미드(Aramid) 기술을 탈취했다는 판결이 보도된 바 있다. 그러나 중국은 다른 어느 나라보다도 적극적으로 활동하고 있는 것으로 평가된다. 2017년 미국 무역대표부(USTR)는 중국의 지재권 탈취로 인한 경제적 피해가 연간 최소 2,250억 달러에서 최대 6,000억 달러라고 밝힌 바 있다.(USTR, 2017)

현재까지는 중국이 가치있다고 판단하는 첩보와 정보가 주요한 타겟이었다면, 정보기술이 적용되면서 데이터 자체의 축적과 정보의 추출이 더욱 확대될 것이라고 전망할 수 있다. 특히 시진핑 주석의 “중국몽”과 “Made in China 2025”(State Council, 2015)는 해외로부터의 투자 확대, 선진기술의 이전, 정부의 적극적인 지원, 전문기술인력의 해외 양성과 복귀 등을 요구하고 있

다. 2017년 이후에는 클라우드 컴퓨팅, 인공지능, 사물인터넷, 생명공학, 로보틱스, 농업기계와 기술, 첨단의료기기 등이 중국 정부의 주요한 타겟이었다고 분석된다.(Peter Harrell, 2018) 물론 양적으로도 엄청난 증가가 있을 것이지만, 디지털 포렌식 기술이 발전하면서 숨겨있던 사실들이 드러날 것도 예상할 수 있다.[10)]

둘째는 현재의 이슈연계가 얼마나 확장될 수 있는가의 관점이다. 지금까지 미국은 경제적 이득을 취하기 위한 중국의 경제스파이 행위와 민감정보를 얻기 위한 정부, 군사 분야에 대한 전통적 스파이 행위를 명확하게 구분해왔다. 그러나 미국의 경제와 국가안보의 구분을 넘어, 미국의 정치적 제도와 거버넌스에도 영향을 미치기 시작했다.(Nicholas Eftimiades, 2018) 나아가서 동맹과 우호국으로부터 시작된 침해행위는 제3세계 국가들로 확대되면서 지구적인 영향력 경쟁으로 확대되었다. 결국 경제 및 군사정보와 다른 이슈들과의 연계성은 더욱 높아질 것이며, 중국은 미국의 기술, 경제, 군사, 정치적 우위와 통제력을 침해하면서 미국의 패권에 도전하는 요인이 될 것이다.

이슈연계의 핵심은 데이터의 수집 및 축적에 있다. 이슈영역의 분리는 관찰과 인식이라는 정보처리과정을 거쳐 이루어지며, 가치중립적인 데이터 차원에서는 이슈영역이 연계될 수밖에 없기 때문이다. 결국 데이터의 격차는 비대칭적인 정보요구, 상대적으로 더 빠르고 양호한 의사결정에서의 우위, 물리영역에서 실행으로의 전환 속도에 영향을 주어 결국 승리에 기여하는 정보이점을 제공한다. 때문에 미중 간의 데이터 경쟁은 정부부처로부터 대학과 연구소로 이전하고 있다. 대학과 연구소에서 만들어진 기술은 산업현장에서 생산되기도 하고, 군사적으로 활용된다는 점에서 경제적, 군사적 이익에 직결되기도 하지만, 국제적 교류활동을 통해서 정보경쟁의 상대적 취약성을 드러내기도 한다는 문제가 있다. 또 학계에 대한 침투는 정보영역에서 뿐만 아니라 인식영역에도 영향을 준다는 특징을 가진다.

셋째는 언제 전통지정학의 경쟁으로 발전할 것인가이다. 미중 간의 경쟁은 물리영역을 넘어 우주와 사이버 영역에서 가시화되고 있다. 다만 정보경쟁은 다른 분야와 달리 가시화되지 않았는데, 정보환경과 기술의 변화 속에서 경쟁은 잘 보이지 않게 된 까닭이다. 다만 데이터 자체가 가지고 있는 이슈연계적 특성을 가지고 있고, 각 이슈영역에서 경쟁의 결과가 드러나게 된다면 언제든지 전통지정학의 경쟁으로 발전하게 된다. 아울러 기술표준을 둘러싼 국가들의 줄서기, 국가 네트워크의 약한 고리에 대한 공격이 이어지면 경쟁의 양상은 더욱 뚜렷하게 나타날 것이다. 과거부터 지정학적으로 불편한 구조 속에 위치한 한국의 입장에서는 양국의 정보우세 경쟁이 어떻게 진행될 것인지 각별한 관심을 가질 수밖에 없다.

사실 트럼프-시진핑의 시대에 들어서 이미 양국의 정부가 상대국가의 기업에 대한 제한조치를 발동하면서 정보우세 경쟁은 이미 전통지정학의 영역으로 들어선 모양새이다. 2019년 6월

10) CISCO 사의 CEO였던 존 챔버스는 "세상에는 두 종류의 기업이 있다. 해킹을 당한 기업과 해킹을 당하고도 당했는지조차 모르는 기업이다"라고 말한 바 있다. 전문가들은 「포춘」 선정 500대 기업 중 97%는 이미 해킹을 당했다고 추정한다. (콘돌리자 라이스, 에이미 제가트, 2019)

G20 정상회의에서 미중 정상이 만나면서 갈등으로 치닫던 것이 다소 해결되는 듯 보였지만, 여전히 수출제한리스트(Entity List)에 상대국 기업의 이름을 거듭하여 올리고 있다. 미국 상무부의 조치에 대응해 중국 상무부도 "불신임 리스트"를 발간하면서 미국의 기업들을 다수 포함시켰고, 미국 수입량의 80%에 달하는 중국 희토류의 수출제한 가능성을 언급하면서 미국을 압박한 바 있다.(USCC, 2019, 48-49) 그러나 아직 미중 간의 경쟁은 수면 아래에 있다. 전환의 시점은 중국의 국가정보기관이 전통적인 정보활동의 영역을 넘어서 "새로운" 영역에서도 정보활동을 주도할 것인가, 또는 언제 그것이 미국 정부에 의해서 공식화되고 통합된 대응이 시작될 것인가의 문제로 귀결될 것이다.[11)]

Ⅳ. 한국의 "데이터 안보"

1. 국가간 "데이터 주권(Data Sovereignty)" 경쟁 구도

데이터 안보경쟁이 미중 간에만 발생가능한 것은 아니다. 미중 간의 첨예한 경쟁이 기술의 '패권' 경쟁으로 비치는 것은 다른 국가들의 데이터 주권에 대한 인식이 낮기 때문이다. RAND 연구진들은 이같은 구도를 "전략정보전의 엘리트 클럽(Club of SIW Elite)"에 의해 지배된다고 규정했는데, 핵무기의 등장 이후 핵보유국들이 국제체제의 구조를 결정했던 냉전기의 상황과 비교될 수 있다.(Roger Molander, et al., 1998) 현재는 국가별로 데이터 안보에 대한 능력과 인식의 격차가 큰데, 특히 소수의 국가만이 공격능력을 가지고 있어 능력을 갖춘 국가들은 서로 취약성을 갖고 있지만 다른 국가들로부터는 안전하다. 따라서 이러한 능력을 갖고 있는 국가들이 특수한 형태의 협력체 또는 협력의 기제를 추구하는 상황이다. 이러한 구도 속에서 능력을 갖추지 못한 국가는 상대적 이익의 불균형을 강요받게 된다.

따라서 한국과 같은 국가들은 데이터 주권을 확보하고, "방어우세의 국제 거버넌스"을 구축하도록 노력해야 한다. 크게는 국가안보 목적에서 국가가 주도적으로 데이터 능력의 군비경쟁으로 돌입하는 것을 차단하는 것을 의미하며, 위협평가와 취약성 보완을 위한 다자간 협력을 증진하는 것을 의미한다. 국경을 넘어 지구적으로 발생하는 문제행위에 대해 국가정부로부터 국제레짐으로 책임이 이양되는 단계적인 조치를 취하는 형태이다. 데이터가 일부 국가의 이익을 위해 비대칭적으로 활용되는 것을 차단한다는 것인데, 데이터를 활용한 범죄행위에 대한 국제 공동대응과 국내 법집행(law-enforcement)을 중심으로 접근한다. 따라서 강대국의 동맹관계 수립, 확장억제와 보증공약, 보복의 위협, 제한된 연구개발 협력 등의 전통적인 경쟁·협력 관계는 배제된다.

11) 2015년 중국은 국방개혁 조치를 단행하면서 군사정보의 담당조직에도 변혁을 꾀한 바 있다. 중국의 정보기관 및 능력에 대한 분석은 다양하다.(USCC, 2016)

방어우세의 국제체제를 구축하기 위해서는, 첫째, 국가가 "데이터 안보"를 위한 능력을 구비하는 것이 선행되어야 한다. 2차 핵시대에 와서 핵보유국의 '횡포'가 작동하지 않는 것은 핵무기 또는 핵무기 개발능력이 보편화되었기 때문이다. 최소한 주권이 미치는 범위 내에서 데이터의 흐름을 통제할 수 없다면 스스로 취약성을 그대로 드러내면서 피해를 강요받을 수밖에 없을 것이다. 둘째, 중앙집권적인 권위체가 필요하다. 정부 부처 내에서 분산된 권한을 집중할 수 있는 컨트롤타워는 필수적이며, 사적영역과의 협력 또는 통제 권한에 대한 분명한 합의도 요구된다. 또한 국제레짐과의 협력을 추진하는 지점으로서 국가행위자는 여전히 중요한 위치를 차지한다. 결국 데이터 안보를 위한 능력을 개발하고, 위협을 억제하고 대응하는 역할의 핵심은 국가 정부일 수 밖에 없다.

데이터 안보를 위해서는 일반적으로 세 가지의 노력선이 제기된다. 자체 방호력 증가를 위한 물리/비물리적 조치, 불법행위에 대한 처벌 강화, 불법행위에 대한 비용증가 등이다.(Peter Harrell, 2018) 기존의 억제이론이 제시해온 방호, 보복억제, 거부억제의 세가지 노력선과 맥을 같이 한다. 강력한 제재를 통해 분명한 비용이 있다는 것을 보여줄 필요도 있고, 의심행위을 법적으로, 물리적으로 차단할 필요도 있다. 여기에 유인책(inducement)으로 정부와 개인, 기업이 자발적으로 국제규범을 준수할 것을 유도할 수 있는 다양한 인센티브도 필요하다.

그러나 이같은 수동적인 방법만으로 완전한 해결은 불가능하다. 특히 최신 정보기술을 적용함으로써 방호력을 높이려는 노력은 새로운 기술에 의한 공격에 맞서서 곧 실패하고 말 것이기 때문이다. 오히려 유인책으로서 법적, 경제적 인센티브가 명확해야 한다는 것이다. 때로 개인과 기업의 방호를 위한 비용은 누구도 신경쓰지 않는 상황이 더욱 지배적이기 때문이다. 방호를 위한 비용은 막대하기 때문에, 사전에 억제하고 차단하는데 초점을 두어야 한다는 것이다. 효과에 대한 논쟁은 끊이지 않겠지만, 국제적으로 데이터 투명성을 확보하기 위한 다양한 노력이 요구된다.

2. 핵심전략 및 정책이슈

1) 책임의 주체: 국가 통제권의 범위는 어디까지인가?

과연 국가가 정보통제권을 가질 수 있을 것인지, 어느 정도의 통제권을 허용해야 할지에 대한 사회적 합의를 이루는 것은 어려운 주제이지만, 이에 대한 분명한 합의가 있어야만 그 다음 단계의 문제를 해결할 수 있다. 정부의 어떤 부처가 데이터와 관련한 책임을 갖게 되는 것인지, 국제사회와의 협력은 어떤 부처를 중심으로 진행될 것인가의 질문에 답해야 한다. RAND의 연구진들은 목적과 주체의 두 가지 기준을 가지고 다섯 가지 대안을 제시한 바 있다. 즉, 국가안보에 초점을 두고 중앙정부가 책임을 가지거나, 법집행을 중심으로 한 중앙정부가 리더십을 발휘하거

나, 국가안보를 중심으로 국가간 협력이나 법집행 중심의 국가간 협력, 국가정부의 지원을 받는 국가간 산업차원의 협력 등이다.(Roger Molander, et al., 1998) 사실 어떠한 대안을 선택하든 간에 정부는 학계와의 정기적인 회합을 통해서 민감기술의 발전과 안보목적의 이용 가능성의 추세를 명확하게 이해할 필요가 있다. 책임주체 문제는 정당성, 개인정보보호, 국제협력과 같은 이슈들과 연결되는데, 결국 예산과 행정력이 투입되는 우선순위의 결정은 정치적 행위이기 때문이다.

2) 위험평가의 방법론: 누가, 어떻게 위험을 평가할 것인가?

위협의 대상이 확대되면서 이에 대한 평가방법도 달라져야 한다. 정보 및 데이터 분야의 위협인식과 경보, 분석 및 평가, 긴급대응을 포괄하는 위험평가의 방법론에는 몇가지 모델이 제시된다.(Roger Molander, et al., 1998) 국가안보를 추구하는 전통적인 정부주도 모델(NICON model)이 있고, 정부주도로 법집행에 중심을 둔 "대테러리즘" 모델(counter-terrorism model)도 있다. 질병통제대응센터(CDC)처럼 특정한 위협에 대해서만 예방과 대응을 주도하는 "CDC model"이나, 국가안보수준으로 격상되지 않은 문제에 대해서는 개별 기관이나 업체가 개별적으로 위험을 평가하는 방법도 있다. 이같은 모델들은 선택의 문제라기 보다는 위험의 크기에 따라서 단계적으로 적용되어야 한다. 이를 위해서는 국가중심적인 사고를 탈피하여 데이터와 관련된 발생가능한 다양한 위험을 평가하고 대응하기 위한 조직구조와 운영체계가 상비되어야 한다. 또한정된 자원을 가지고 국가정보 목표를 효과적으로 달성하기 위한 필수적인 작업으로 "국가정보 목표우선순위(PNIO)"의 재조정 과정은 필수적이다.(Sherman Kent, 1966, 38)

3) 취약성 분석: 어떻게 취약성을 최소화할 것인가?

정보영역이 광역화되고, 사전예측이 불가능해졌으며, 피해규모가 대형화되는 등 위험을 사전에 파악하기가 어려워지면서, 주체의 취약성을 분석하는 것이 더욱 중요한 과업으로 부각되었다. 자연스럽게 어떻게 취약성을 최소화할 것인지, 얼마만큼의 취약성을 감수할 것인지에 대한 "충분성"에 대한 고민이 수반된다. 국가중심적인 방법을 취할 것인지, 아니면 동맹 및 협력국 중심의 파트너십, 자유주의적 다자주의를 통해 취약성을 분석할 것인지의 문제는 여전히 남아있다. 다만 최근 미국 『국가정보전략(National Intelligence Strategy)』의 변화는 주목할 만하다. 해당 보고서는 정보공동체 내부자에 의한 기밀유출, 적대국의 대미 첩보활동 강화, 파편화되고 고립된 정보기관들의 비효율성을 취약점으로 분석하고, 이러한 취약성을 극복하기 위한 혁신통합, 파트너십, 투명성의 핵심가치를 제시하였다.(The Office of the Director of National Intelligence, 2019) 2014년에 발간된 『정보전략』이 스노든 사건 이후 중요해진 '투명성'을 강조했다면, 2019

년에는 중국과 러시아와 같은 잠재적 적대국의 기술 우위를 사전에 저지하고 미국의 기술 경쟁력을 강화하기 위한 "혁신"과 "통합"을 강조하였다.(조은정, 오일석, 2019, 03)

4) 선언정책의 마련: 상대를 어떻게 억제할 것인가?

데이터 보안은 위협에 대한 가장 기본적인 대응방법이지만, 방어적이고 소극적인 방법으로 한정한다면 위협에 온전히 대응할 수 없다. 위에서 본 바와 같이 위협의 대상, 시기, 범위 등을 특정하기 어렵기 때문에 상대의 취약점을 파고들어 적극적으로 공격해야만 정보우세와 억제를 달성할 수 있다. 따라서 방어적 차원의 보안과 함께 적극적으로 적대세력의 위협을 탐지, 파괴, 무력화, 역이용하는 등의 공격적인 활동이 병행되어야 한다. 미국 역시 9.11 이후 "선제적 방첩 전략(preemptive counterintelligence strategy)"을 선언하고 적대세력 내부에 침투하여 관련 정보를 수집하고, 상대의 정보활동을 무력화, 조종하는 적극적 활동을 추구하고 있다.(NCIX-2010-002) 다만 이러한 정책을 선언하는 것이 상대를 억제하는데 직접적으로 기여할 수 있다고 하더라도, 수단과 활용범위, 공개대상 등의 선언정책을 마련하는 것에는 신중하게 접근할 필요가 있다. 오히려 상대방의 경계심을 유발하여 이미 달성되었던 정보우위가 약화될 수도 있고, 발견되지 않았던 취약점이 발견되거나 새롭게 발생하기도 한다. 따라서 상대를 효과적으로 억제하기 위한 "맞춤형" 선언정책이 요구된다.

5) 국제 정보공유와 협력의 범위: 누구와, 어느 정도로 협력할 것인가?

역사-행태적인 입장에서 적대국과의 협력은 여전히 어렵지만, 데이터 경쟁의 특성상 국가 및 정부의 의도와 관계없이 언제든지 위협으로 발전할 수 있다는 점에서 전통적인 동맹국과의 협력도 쉽지 않다. 그러나 협력의 가능성을 미리 차단할 필요는 없을 것이며, "신뢰하라. 그러나 검증하라(Trust, but verify)"는 격언은 여전히 유효하다. 사실 데이터 위협의 특성상 국제협력 없이 취약성을 보완하고 위협에 대응하기는 불가능하다는 점에서 모든 국가와 협력해야 할 필요가 있다. 다만 어느 정도로 협력할 것인가의 문제가 있다. 방어기술, 국제범죄 대응, 제한적 참여 등으로 협력의 정도를 단계화하는 방안을 고려할 수 있다. 신뢰성이 담보된 국가들과의 국방 R&D는 공동대응과 상호운용성의 효과를 같이 가져올 수 있다는 점에서 확대될 필요가 있다. 또 학계를 중심으로 한 협력은 지구적 문제를 함께 풀어가기 위한 이론화 및 후속세대 양성, 공동연구, 산업적인 측면에서도 긴요하다. 물론 협력 속에서도 일부 불법적인 행위에 대해서는 정밀한 잣대를 적용할 수 있을 것이다.

6) 정보의 처리: 투명성과 효율성의 딜레마

국내적으로 투명성와 효율성이 딜레마 관계에 있다. 투명성은 공개성과 책임성을 요구하지만, 효율성은 비밀과 보안을 통해서 획득되기 때문이다. 이는 정보활동의 윤리성 문제를 다루는 것인데, 과연 정부의 정보활동을 어느 정도로 인정할 것인지, 국회는 예산으로 얼마나 지원할 수 있을 것인지 하는 것들이다. 최근의 데이터 3법 개정과 관련된 논쟁도 이와 연결된다. 데이터산업의 활성화를 위한 방향으로 이해되지만 보안실무자들은 정보의 유출을 이유로 강력하게 반대해왔다. EU의 "개인정보보호법(General Data Protection Regulation, GDPR)"은 이같은 딜레마를 극복하려는 노력의 일환으로 이해된다.(정일영 등, 2018) 결국 정보기관 자체의 확장성이 아니라, 기술혁신을 주도하고 있는 민간과의 협력 및 정보에 대한 비교 우위를 가지고 있는 국외정보기관과의 교류와 공조를 통해 딜레마는 완화될 수 있다. 다른 한편 정보기관은 투명성을 강화하기 위한 제도적 장치와 각종 활동을 실현함으로써 국민적 이해와 신뢰를 받아야 한다.(조은정, 오일석, 2019, 5)[12)]

Ⅴ. 맺음말

디지털 안보환경 속에서 미국과 중국의 데이터 경쟁은 진행 중이다. 산업분야에서 지적재산권과 기술 탈취로부터 시작되어 군사분야의 정보작전으로 이어져왔고, 위협과 취약성의 변화 속에서 더욱 첨예화되고 있다. 정보우세를 달성하기 위한 전략경쟁의 중요성은 지속되며, 더 많은 데이터를 더 빨리 선점하고, 선행 단계로 지향점을 옮겨가려는 노력도 계속된다. 물리영역에서는 관찰과 인식을 차단하고 실행을 방해하며, 정보영역에서는 데이터 확보와 데이터 보안의 공격, 방어가 일어난다. 인식영역에서는 보다 적극적으로 인지조작과 지식유통에 영향을 미치려는 활동이 빈번히 발생한다. 미중간의 경쟁은 양질전화, 이슈연계를 넘어 전통지정학의 영역으로 이행해가고 있다.

그러나 데이터 경쟁은 미국과 중국만의 일이 아니며, 각국이 참여하게 되면서 더욱 심화될 것이다. 4차 산업혁명은 데이터를 통해서 진행된다. 사물인터넷(IoT)는 데이터의 수집과 공유를 기반으로 작동한다. 시장을 통해 종합·분해·복제·탐색·판매되는 데이터는 한해 2천억 달러 규모로 추산된다.(World Economic Forum, 2020, 63) 데이터 의존도가 높아지면 위협과 취약성은 커지고, 정보의 불균형도 심화된다. 결국 데이터 정보우세를 달성하는 경우 얻을 수 있는 것이, 잃을

12) 데이터 안보와 관련하여 개인의 정보보호를 위해서는 국내법적 기반을 잘 마련하고, 이를 준수하는 것이 무엇보다 중요한 과제이다. 케이트는 미국의 헌법, 전자통신개인정보법(ECPA), 해외정보감시법(FISA), 기타 개인정보 관련 법을 자세히 설명하고 있다.(Fred Cate, 2015, 317-322)

것보다 많다면 새로운 형태의 군비경쟁은 지속될 것이다. 방어우세의 국제체제는 이익을 추구하는 행위자에 의해서 손쉽게 붕괴될 수 있다.[13] 그렇다고 해서 고립정책이 결코 안전하거나 유효한 대응방안이 아니다. 국제레짐의 선의에 편승할 수도 없고, 특별한 조치없이 방관하는 것은 더욱 위험하다.

한국에 있어서도 데이터 안보는 사활적 이익이다. 한국은 2010년부터 유엔이 평가하는 전자정부 순위에서 3회 연속 1위를 차지했고, 2016년과 2018년에는 3위에 자리했다. 온라인 정보제공과 정책참여, 정보통신 인프라 구축 등을 종합하는 지수로 정부 업무가 이미 고도로 전산화, 자동화되어 있다는 것을 의미한다. 중요한 것은 이에 합당한 데이터 보호 능력을 갖추었느냐에 있을 것이다. 한국의 "사이버 안보지수(Global Cyber Security Index, GCI)"는 2018년을 기준으로 아태지역 5위, 세계 15위 수준으로 상위권에 있지만,(ITU, 2019) 핵심 데이터를 보호하기 위한 능력의 필요성은 아무리 강조해도 지나치지 않다.

우선 한국은 미중 정보우세 경쟁관계 속에서 한국의 위치를 정립할 필요가 있다. 한국은 미국과 중국이라는 사이버, 정보영역의 강대국 사이에 있는 국가이다. 그러나 미중보다도 더 좋은 IT환경을 보유하고 있음을 고려한다면, 지정학적으로는 불리한 구조 속에 있음에도 불구하고 오히려 정보의 허브로서 미중 사이에서의 정보전에서도 우위 달성이 가능할 것이다. 둘째, 한국의 데이터 안보를 위한 노력이 필요한데, 한국 스스로 정보요구를 충족할 수 있는 자강력을 키울 필요가 있다. 기술적 차원의 데이터 안보 뿐만 아니라 데이터를 통한 이슈간의 연계와 차단을 자유로이 할 수 있어야 한다. 셋째, 국제 정보공유는 쉽지 않은 문제임에는 분명하지만, 지속적으로 강조되어야 한다. 특히 약소국들의 입장에서 국가간 협력과 사이버 공격 금지 등을 제안하지만, 대부분 제안에 머물거나 선언적인 협약에 머무른다.[14] 이같은 불균형을 극복하기 위한 다각적인 노력이 요구된다.

13) 최근 타이완 국가안보국 후무위안(Hu Mu-yuan) 부국장은 중국 공산당이 데이터 및 기술 확보를 위한 불법 캠페인을 통해 공정 무역을 훼손하고, 타이완, 일본, 한국 등을 위협하고 있다고 밝힌 바 있다.(*Reuters,* 2021.3.31.).

14) 2019년 서울안보대화(SDD)에서 베트남은 동남아시아와 동아시아의 주변국을 상대로 사이버 공격 금지를 제안했으며, 사이버 정보공유를 하자는 제안을 내놓은 바 있다.

[참고문헌]

가. 단행본 및 논문

강준영, "미국 부시행정부 출범 이후의 중,미 관계: 정찰기 충돌 사건을 중심으로," 『국제지역연구』, 제5권 제2호 (2001).

공현철, 송병철, 서윤경, "중국 위성요격실험의 의의와 영향에 따른 우주자산 보호방안 연구," 『대한기계학회 춘계학술대회 강연 및 논문 초록집』 (2007).

김상배, "빅데이터의 국가전략: 21세기 신흥권력 경쟁의 개념적 성찰," 『국가전략』, 제21권 3호 (2015).

_____, "트럼프 행정부의 사이버 안보 전략: 국가지원 해킹에 대한 복합지정학적 대응," 『국제지역연구』, 제27권 4호 (2018).

_____, "화웨이 사태와 미중 기술패권 경쟁," 『국제지역연구』, 제28권 3호 (2019).

김지영, "미중 사이버 패권경쟁의 담론과 실제-화웨이 5G 사태를 중심으로," 『국방연구』, 제62권 4호 (2019).

배달형, 『미래전의 요체 정보작전』, 서울: 한국국방연구원, 2005.

신동찬, 이희범, 두석주, 김도현, 김중희, 김숙영, 노수정, 『미래정보전: 미래 디지털 전쟁의 귀염둥이』. 서울: 황금소나무, 2013.

앨버트 데이비스, 존 가스트카, 리첸 헤이스, 데이비드 시그노리, 『정보시대 전쟁의 이해』, 권태환 역, 서울: 국방대학교, 2004.

전웅, 『현대 국가정보학』, 서울: 박영사, 2015.

정일영, 이명화, 김지연, 김가은, 김석관, "유럽 개인정보보호법(GDPR)과 국내 데이터 제도 개선방안," 『STEPI Insight』, Vol.227 (2018).

조은정, 오일석, "미 국가정보전략(2019) 발간의 의미와 한국에 대한 함의," 『이슈브리프』, 제104호 (2019.2.1.).

데이비드 조던, 제임스 키라스, 데이비드 론스데일, 이안 스펠러, 크리스토퍼 턱, 데일 윌턴, 『현대전의 이해』. 강창부 역, 파주: 한울, 2014.

콘돌리자 라이스, 에이미 제가트, 『정치가 던지는 위험(Political Risk)』, 김용남 역, 서울: 21세기 북스, 2019.

Chief of Staff of the Army's Strategic Studies Group Cohort IV (2015-2016), 『2030-2050년의 전쟁양상: 기술변화, 국제체제 그리고 국가』, 김철우 등 역. 서울: 한국국방연구원, 2019.

Abbott, Daniel, The Handbook of Fifth-Generation Warfare (5GW), Ann Arbor: Nimble Books LLC, 2010.

Allison, Graham, Destined for War: Can America and China Escape Thucydides's Trap?, Houghton Mifflin Harcourt, 2017.

Cate, Fred H., "China and Information Security Treats: Policy Responses in the United States," in Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron eds., China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, New York: Oxfrod University Press, 2015.

Cave, Danielle, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, "Mapping China's Tech Giants." ASPI (18 April 2019).

Department of Defense, National Defense Strategy. Washington, DC: Department of Defense, 2018.

GAO Testimony. 2019. "CHINA: Observations on Confucius Institutes in the United States and U.S. Universities in China," GAO-10-401T, Feb. 28, 2019. https://www.gao.gov/assets/gao-19-401t.pdf (검색일: 2021.3.23.)

Grynkewich, Alexus G., "Introducing Information as a Joint Function," Joint Force Quarterly, No.89 (2nd Quarter, 2018).

Harrell, Peter E., "Testimony before the Senate Judiciary Committee-China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses," (12 Dec 2018).

Holcomb, James, "Managing Strategic Risk," in J. Boone Bartholomees, Jr. ed. Theory of War and Strategy, Carlisle: U.S. Army War College, 2010.

International Telecommunication Union (ITU), Global Cybersecurity Index(GCI) 2018 (Dec. 2018), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (검색일: 2021.3.25.).

Kennan, George F., "The Inauguration of Organized Political Warfare", (30 April 1948), https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c (검색일: 2021.3.22.).

Kent, Sherman, Strategic Intelligence for American World Policy, Princeton: Princeton University Press, 1966.

Molander, Roger C., Peter A. Wilson, David A. Mussington, and Richard F. Mesic, Strategic Information Warfare Rising. Santa Monica: RAND, 1998.

Nicholas Eftimiades, "The Impact of Chinese Espionage on the United States: What is the cumulative impact of China's espionage activities for the United States' economy, security, and politics?," The Diplomat (4 Dec. 2018),

https://thediplomat.com/2018/12/the-impact-of-chinese-espionage-on-the-united-states/ (검색일: 2021.2.20.).

_____, "Uncovering Chinese Espionage in the US: A detailed look into how, why, and where Chinese spies are active in the United States," The Diplomat (28 Nov. 2018), https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/ (검색일: 2021.2.13.)

Office of the National Counterintelligence Executive. 2009. National Counterintelligence Strategy of the United States of America (NCIX-2010-002). http://www.ncix.gov/publications/policy/NatlCIStrategy2009.pdf (검색일: 2021.2.13.).

Office of the United Sates Trade Representative, "2017 Special 301 Report" (2017), https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF (검색일: 2021.2.12.)

Owens, William A., "The Emerging System of Systems," U.S. Naval Institute Proceedings, Vol.121, No.5 (1995).

State Council, "Made in China 2025(中国制造 2025)," (7 Jul 2015), http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf (검색일: 2021.2.11.).

The Joint Staff, Doctrine for the Armed Forces of the United States (Joint Publication 1), Washington, DC: The Joint Staff, 2017.

_____, Information Operations (Joint Publication 3-13), Washington, DC: The Joint Staff, 2016.

_____, Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World. Washington, DC: The Joint Staff, 2016.

_____, Joint Operations (Joint Publication 3-0), Washington, DC: The Joint Staff, 2017.

_____, Joint Vision 2010. Washington, DC: The Joint Staff, 1996.

_____, Joint Vision 2020. Washington, DC: The Joint Staff, 2000.

Theohary, Catherine A., "Information warfare: issues for Congress," Congressional Research Service Report #R45142 (5 March 2018).

Toffler, Alvin and Heidi A. Toffler, War and Anti-War: Making Sense of Today's Global Chaos, Grand Central Publishing, 1995.

U.S. House of Representatives, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," 112th

Congress (8 Oct. 2012).

U.S. Senate Armed Services Committee, Subcommittee on Cybersecurity, "Testimony of Rand Waltzman, The Weaponization of Information: The Need for Cognitive Security," Santa Monica: RAND, 27 Apr. 2017.

U.S.-China Economic and Security Review Commission(USCC), "Report to Congress" (Dec. 2016), https://www.uscc.gov/sites/default/files/2016-12/2016_Annual_Report_to_Congress.pdf (검색일: 2021.1.10.).

_____, "Report to Congress" (Dec. 2019), https://www.uscc.gov/sites/default/files/2019-12/2019_Annual_Report_to_Congress.pdf (검색일: 2021.1.10.).

Wang Xiangsui and Qiao Liang, Unrestricted Warfare: China's Master Plan to Destroy America. Brattleboro: Echo Point Books & Media, 2015.

World Economic Forum, The Global Risks Report 2020. Cologny: World Economic Forum, 2020.

나. 신문 및 인터넷 자료

강영두, "트럼프, '美정보통신 보호' 국가비상사태 선포...中 겨냥," 『연합뉴스』, 2019.5.16., https://www.yna.co.kr/view/AKR20190516010651071?input=1195m (검색일: 2021.3.19.).

김동현, "미 우주군 첫 공격용 무기 배치 '적 위성 통신 교란 목적'," 『VOA KOREA』, 2020.3.17., https://www.voakorea.com/korea/korea-politics/space-weapon (검색일: 2021.3.19.).

김선한, "러 · 중, 군사위성 요격미사일 발사시험 잇단 성공," 『연합뉴스』, 2018.4.3., https://www.yna.co.kr/view/AKR20180403079800009?input=1195m (검색일: 2021.3.19.).

박병진, "미국 '중국 스파이'라며 하버드대 교수 전격 체포," 『뉴스1』, 2020.1.29., https://www.news1.kr/articles/?3827285 (검색일: 2021.3.24.).

백나리, "수십년간 120개국 암호장비 댄 회사 배후는 CIA...한국도 고객," 『연합뉴스』, 2020.2.12., https://www.yna.co.kr/view/AKR20200212003600071?input=1195m (검색일: 2021.3.24.).

송지욱, "美 정찰기-中 전투기 서해 인근에서 충돌할 뻔," 『TV조선 뉴스』, 2017.7.25., http://news.tvchosun.com/site/data/html_dir/2017/07/25/2017072590101.html (검색일: 2021.3.19.).

연규선, "중국어 교육기관 공자학원은 첩보기관?…中 유학생도 감시 비난," 『KBS NEWS』,

2018.3.7., https://news.kbs.co.kr/news/view.do?ncd=3614958 (검색일: 2021.3.23.)

이관주, "내년 4·15 총선은 '딥페이크' 가짜뉴스와의 전쟁," 『아시아경제』, 2019.12.19., https://view.asiae.co.kr/article/2019121911494768016 (검색일: 2021.3.23.).

이주한, "中 공안, 인터넷 '댓글부대' 단속 강화," 『KBS NEWS』, 2018.12.9., http://news.kbs.co.kr/news/view.do?ncd=4091169&ref=A (검색일: 2020.12.3.)

인민망 한국어판 (2017.12.31.), http://kr.people.com.cn/n3/2017/1231/c203278-9310128.html (검색일: 2020.12.11.).

인민망 한국어판 (2019.1.1.), http://kr.people.com.cn/n3/2019/0101/c203278-9533545.html (검색일: 2021.12.11.).

최나실, "무역담판 앞둔 미국, '슈퍼컴퓨터' 中기업 5개도 블랙리스트 지정," 『한국일보』, 2019.6.22., https://www.hankookilbo.com/News/Read/201906221312061856?did=NA&dtype=&dtypecode=&prnewsid= (검색일: 2021.3.24.).

최연진, "미·중 데이터 패권 경쟁...'국가 안보' 이유로 해마다 장벽 강화," 『한국일보』, 2019.11.12., https://www.hankookilbo.com/News/Read/201911111500716467?did=NA&dtype=&dtypecode=&prnewsid= (검색일: 2021.3.24.).

홍성주, "기술 냉전시대가 온다," 『중앙일보』, 2020.4.27., https://news.joins.com/article/23763539 (검색일: 2021.3.23.).

"The Great Firewall of China," Bloomberg News. 5 Nov. 2018, https://www.bloomberg.com/quicktake/great-firewall-of-china (검색일: 2021.3.22.).

"U.S. trade war pushing China to steal tech, talent, Taiwan says," Reuters, 31 Mar, 2021, https://www.reuters.com/world/china/us-trade-war-pushing-china-steal-tech-talent-taiwan-says-2021-03-31/ (검색일: 2021.4.16.).

"WeChat: A Tool of Authoritarian Control?" Vision Times, 17 November 2019, https://www.visiontimes.com/2019/11/19/wechat-a-tool-of-authoritarian-control.html.

Apuzzo. Matt, "Chinese Businessman Is Charged in Plot to Steal U.S. Military Data," The New York Times, 12 Jul. 2014, https://www.nytimes.com/2014/07/12/business/chinese-businessman-is-charged-in-plot

-to-steal-us-military-data.html (검색일: 2021.3.23.).

CSIS. 2019. "Survey of Chinese-linked Espionage in the United States Since 2000," https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000 (검색일: 2021.3.20.).

CSIS. 2020. "Significant Cyber Incidents since 2006" https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (검색일: 2021.3.20.).

Eichenwald, Kurt, "How Edward Snowden Escalated Cyber War," Newsweek, 1 Nov. 2013, https://www.newsweek.com/2013/11/01/how-edward-snowden-escalated-cyber-war-243886.html (검색일: 2021.2.23.)..

Mattis, Peter, "China's New INtelligence War against the United States," War on the Rocks, 22 Jul. 2015, https://warontherocks.com/2015/07/chinas-new-intelligence-war-against-the-united-states/ (검색일: 2021.3.25.).

Nakashima, Ellen. "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," The Washington Post, 27 May 2013, https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html (검색일: 2021.3.17.).

Paletta, Damian, Ellen Nakashima and David J. Lynch, "Trump administration cracks down on giant Chinese tech firm, escalating clash with Beijing," The Washington Post, 17 May 2019, https://www.washingtonpost.com/world/national-security/trump-signs-order-to-protect-us-networks-from-foreign-espionage-a-move-that-appears-to-target-china/2019/05/15/d982ec50-7727-11e9-bd25-c989555e7766_story.html (검색일: 2021.2.13.).

Pellerin, Cheryl, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End" (21 Jul. 2017), www.defense.gov/News/Article/Article/1254719/project-maven-to-deploycomputer-algorithms-to-war-zone-by-yearsend/ (검색일: 2021.2.19.).

Sanger, David E. and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," The New York Times, 22 Mar. 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-a

s-spy-peril.html (검색일: 2021.2.18.).