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.68(발간일: 2021.5.18.)

신흥기술과 디지털 안보의 세계정치:

이론적 분석틀의 모색

김상배 서울대학교 정치외교학부 교수

〈차 례〉

Ⅰ. 머리말

미래의 글로벌 패권을 놓고 벌이는 미국과 중국의 경쟁이 점점 더 복잡한 양상으로 전개되고 있다. 두 강대국의 경쟁은 다양한 분야에서 벌어지고 있지만, 그 중에서도 핵심은 첨단부문의 기술 패권경쟁이다. 이른바 4차 산업혁명으로 알려진 분야의 주도권을 둘러싼 두 나라의 힘겨루기가 한창이다. 첨단부문의 기술경쟁은 민간 부문에서 기업들이 벌이는 경쟁의 차원을 넘어선다. 양국의 정부, 경우에 따라서는 양국의 국민들이 참여하는 다차원적인 국력경쟁이다. 또한 좁은 의미의 기술과 산업을 넘어서 무역과 금융, 그리고 정책과 제도 등을 포괄하는 복합경쟁이다. 최근 미중 무역갈등이 다소 완화되는 경향을 보이고 있음에도, 오히려 양국의 기술경쟁은 더욱 가속화될 것으로 예견되는 것은 바로 이러한 이유 때문이다.

미중 기술경쟁에서 최근 두드러지는 나타나는 현상은 기술변수와 안보문제의 만남이다. 첨단기술 분야의 주도권을 놓고 벌이는 양국의 경쟁이 국가안보에 대한 위협이라는 구도에서 이해되고 있다. 4차 산업혁명으로 대변되는 신흥기술(emerging technology)의 변수가 미래 국력경쟁에서 차지하는 비중이 커지는 것만큼 기술경쟁력이라는 변수가 안보문제라는 프레임에 투영되어 해석되고 있다. 실제로 최근의 미중경쟁을 보면 기술변수가 경제와 산업의 경계를 넘어서 안보와 외교의 문제로서 자리매김하고 있으며, 이러한 과정에서 기술안보는 '지정학적 위기'를 야기하는 요인으로 부각되는 양상을 보이고 있다.

최근 기술변수가 안보문제와 만난 대표적인 사례는 사이버 안보였다(김상배, 2018a). 2010년대 들어 해킹 공격과 방어의 문제는 단순한 기술과 공학의 문제를 넘어서 급속히 군사와 외교, 그리고 국가안보의 쟁점이 되었다. 완벽한 방어가 어려울 뿐만 아니라 공격자를 밝히기조차 쉽지 않은 특성상 사이버 안보는 일찌감치 국가안보 이슈로 '안보화'되었다. 2020년대로 넘어오면서 기술안보의 화두는 드론과 같은 무인무기체계가 장식하고 있다. 기술발달은 군사혁신을 촉진할 뿐만 아니라 미래 전쟁의 승패를 가를 변수로 자리매김해 가고 있다. 그럼에도 기술변수가 야기하는 안보문제는 해킹 공격이나 드론 작전과 같은 좁은 의미의 군사안보에 머물지 않고 좀 더 포괄적인 의미의 안보문제를 야기하는 것으로 보아야 한다.

이 글은 넓은 의미의 기술안보를, 신흥기술로서 디지털 기술의 발달이 야기하는 안보, 즉 '디지털 안보'라는 개념으로 이해하였다. 디지털 안보의 세계정치를 극명하게 보여주는 사례들이 최근의 미중경쟁 과정에서 출현하고 있다. 초기 쟁점이 사이버 안보였다면, 이것이 양적으로 늘어나고 있을 뿐만 아니라 여타 다양한 이슈와도 연계되고 있다. 최근 미중경쟁의 불꽃이 무역을 넘어 관세, 환율, 자원, 그리고 군사안보와 동맹외교, 국제규범 등이 관련된 분야로 번져가고 있다. 이러한 과정에서 미중경쟁은 일부 분야에 국한된 이해갈등이 아니라, 미래 글로벌 패권경쟁을 거론할 정도로 양국의 사활을 건 국가안보의 문제로 진화하고 있는 모습이다.

이러한 신흥기술과 디지털 안보의 세계정치는 미시적 차원의 문제일지라도 그 수량이 늘어나고 여타 이슈들과 연계되면서 거시적 차원의 난제로 창발(創發)하는 '신흥안보'(emerging security)의 속성을 지닌다. 다시 말해, 디지털 안보는 초기에는 '개인안전'이나 '기관보안' 정도로만 이해되는 문제였을지라도 그 양이 늘어나면서 '국가안보'의 문제로 비화되는 성격을 지닌다. 또한 기술안보의 문제가 오프라인 공간의 무역이나 금융과 같은 경제안보 문제와 만나고 더 나아가 사이버 공간의 데이터 안보 문제 등과 만나면서 안보문제로서의 폭발력을 키워나간다. 결국 이러한 디지털 안보의 양적 · 질적 창발 과정이 군사나 외교와 같은 전통안보의 영역에 이르게 되면 기술안보의 문제는 지정학적 경쟁의 대상으로 자리매김하게 된다.

디지털 안보가 지정학적 문제가 되었다지만, 이것이 단순히 '전통 지정학'으로의 회귀를 의미하는 것은 아니다. 사실 디지털 안보는 사이버 공간을 매개로 이루어지는 탈(脫)지리적 공간의 안보 문제이다. 게다가 아무리 영토국가들의 이해갈등이 부각되더라도, 디지털 안보를 이해함에 있어서 첨단부문에서 초국적 자본이 추동하는 지구화의 추세를 무시할 수는 없다. 게다가 디지털 안보의 창발과정에서는 객관적으로 실재하는 위협의 존재만큼이나 그 위협을 주관적으로 구성해 내는 담론정치의 과정도 매우 중요한 부분을 차지한다. 이런 점에서 이 글은 지정학적 시각의 유용성을 인정하면서도 전통 지정학을 넘어서는 다양한 시각을 엮어낸다는 의미에서 개념화된 '복합지정학'(Complex Geopolitics)을 원용하고자 한다(김상배, 2015a).

복합지정학의 시각에서 이해한 미중 디지털 안보 경쟁은, 좁은 의미의 자원경쟁이나 기술경쟁을 넘어서 표준경쟁 또는 플랫폼 경쟁의 형태로 전개되고 있다. 이러한 경쟁에 관여하는 행위자들도 전통적 국가 행위자가 아니라 '국가-비국가의 복합 행위자'라는 시각에서 보아야 한다. 또한 경쟁의 결과로 발생하는 세계질서의 구조변동도 전통 지정학이 상정하는 '세력균형(Balance of Powers)의 전이'라기보다는 좀 더 복잡한 형태로 그려지는 '세력망(Network of Powers)의 재편'이다. 이러한 디지털 안보의 세계정치에 대응하는 한국의 전략적 선택은 미중 사이에 낀 중견국의 중요한 국가안보적 사안이 아닐 수 없다(김상배, 2014).

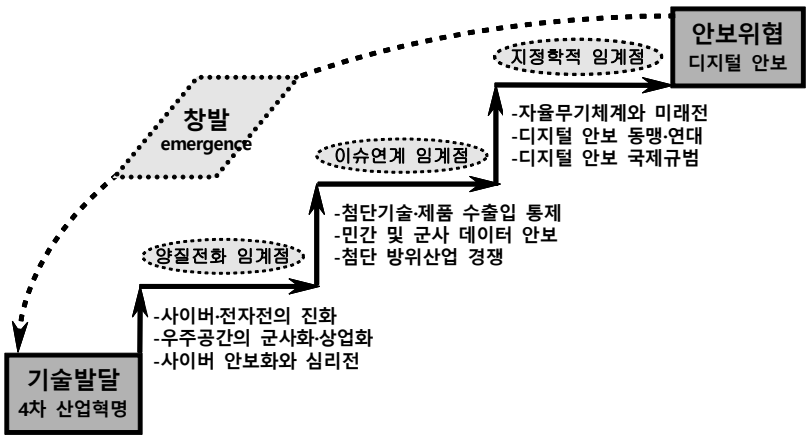
이 글은 신흥안보와 복합지정학의 시각에서 싱흥기술과 디지털 안보의 세계정치를 살펴보았다. 제2장은 신흥안보로서 디지털 안보를 이해하는 복합지정학의 분석틀을 제시하였다. 제3장은 '양질전화(量質轉化)'의 시각에서 사이버 · 전자전, 우주안보 · 산업, 사이버 심리전 등의 사례를 살펴보았다. 제4장은 '이슈연계'의 시각에서 첨단기술과 보안제품의 수출입 통제, 민간 및 군사 분야의 데이터 안보, 밀리테크와 첨단 방위산업 등의 사례를 살펴보았다. 제5장 '(복합)지정학'의 시각에서 자율무기체계 도입과 미래전의 창발, 디지털 안보의 동맹 및 연대외교, 디지털 안보 거버넌스와 국제규범 등의 사례를 살펴보았다. 끝으로, 맺음말은 이 글의 주장을 종합 · 요약하고, 신흥기술과 디지털 안보의 세계정치에 대응하는 한국이 고려할 미래전략의 방향을 간략히 짚어 보았다.

II. 신흥안보와 복합지정학의 분석틀

1. 신흥안보로서 디지털 안보

4차 산업혁명 시대의 기술안보는 기술 시스템 그 자체가 생성하는 위험의 문제인 동시에 이에 관여하는 인간 행위자들이 야기하는 위협의 문제이다. 특히 미래 국력경쟁에서 기술 변수가 차지하는 비중이 커지면서 국가 및 비국가 행위자들이 직간접적으로 개입하는 안보위협이 늘어나고 있다. 〈그림-1〉에서 보는 바와 같이, 다양한 분야에서 시작된 기술 관련 안보위협이 창발(創發, emergence)의 메커니즘을 따라서 양적 · 질적으로 진화하면서 국가 행위자들 간의 이해갈등과 물리적 충돌을 예견케 하는 지정학적 이슈로 발전하고 있다. 이런 점에서 디지털 안보는 미시적 안전(安全, safety)의 문제가 거시적 안보(安保, security) 문제가 되는 '신흥안보(新興安保, emerging security)'의 대표적 사례라고 할 수 있다.

〈그림-1〉 신흥안보로서 디지털 안보의 창발



출처: 김상배(2018b) p.5에서 응용

첫째, 디지털 안보 문제는 양적증대가 질적변화를 야기하는 '양질전화(量質轉化)'의 과정을 거쳐서 발생한다. 기술발달은 육 · 해 · 공을 넘어서 4차원의 우주공간과 5차원의 사이버 공간에서도 안보위협이 증대되는 환경을 조성하고 있다. 최근 사이버 공격의 건수는 매년 가파르게 증가하고 있으며, 그 목적도 국가 기간시설의 교란과 시스템 파괴에서부터 금전취득을 위한 해킹, 개인 · 기업 정보의 절취 등에 이르기까지 다변화되고 있다. 또한 그 공격수법도 디도스 공격에서부터 악성코드의 침투, 랜섬웨어의 유포 및 전자전 · 우주전과의 결합 등으로 진화하고 있다.

사이버 공격의 주체도 단순한 해커의 장난이나 테러리스트의 저항수단에서 국가지원 해킹으로 다양화되고 있다. 더 나아가 사이버 공격은 타국의 선거개입 등과 같은 사이버 정보 · 심리전과도 연계되면서 그 위험성이 증폭되고 있다.

둘째, 디지털 안보 문제는 미시적인 안전의 문제로 시작하지만 다양한 '이슈연계'의 메커니즘을 따라서 복잡화되는 성격을 갖는다. 최근 사이버 안보는 국가기밀을 담은 데이터의 유출과 경제적 가치가 높은 지적재산의 절취와 연계되어 통상마찰을 야기하는 문제로 인식되고 있다. 최근 미국과 중국, 그리고 러시아 등 강대국들이 사이버 안보와 관련된 IT보안제품의 수출입 문제를 연계시키면서 이 분야의 다국적 기업들에 대한 규제를 강화하는 시도도 벌이고 있다. 게다가 이러한 사이버 안보 관련 통상문제는 민간 분야 빅데이터의 국경 간 이동 문제나 군사 분야의 첩보 등과도 연계되는 양상을 보이고 있다. 더 나아가 민군겸용기술의 함의가 큰 첨단 방위산업의 국가 간 경쟁도 유발하고 있다. 이러한 과정에서 기술안보는 오프라인과 온라인의 통상과 산업의 문제와 연계되며 포괄적인 디지털 안보의 문제로 상승한다.

끝으로, 기술안보와 경제안보에서 시작되어 양적으로 늘어나고 질적으로 변화의 과정을 밟은 디지털 안보 문제는 군사나 외교 분야의 경계를 넘어서 지정학적 분쟁으로 발전할 가능성을 늘려 놓았다. 사이버 공격은 재래식 전쟁과 연계되어 수행되고 있으며, 인공지능과 같은 4차 산업혁명 분야의 기술과도 연동되고 있다. 최근에는 드론을 활용한 군사작전이 수행되면서 논란이 벌어지기도 했다. 이러한 맥락에서 강대국들은 군사전략 추진의 일환으로 자율무기체계의 도입 경쟁을 벌이고 있으며, 이와 병행하여 신흥기술 및 디지털 안보 분야의 동맹 및 연대외교의 움직임도 활발히 진행되고 있다. 또한 이러한 변화가 근대 전쟁과는 구별되는 새로운 전쟁 양식의 출현을 예견케 하는 가운데 디지털 안보 관련 기술의 미래를 규제하려는 국제규범을 마련하는 시도도 진행되고 있다.

이러한 관점에서 보면 신흥안보로서 디지털 안보는 전통안보의 지정학적 문제들로 귀결되는 속성을 내포하고 있다. 그러나 디지털 안보를 단순히 전통적인 지정학의 시각에서만 규정하기는 어렵다. 사실 4차 산업혁명 시대의 디지털 안보 문제는 기본적으로 영토국가의 경계를 넘어서는 과정에서 발생하는 성격을 지닌다. 그러나 좁은 의미의 지정학을 넘어서려는 시도를 강조하려는 것이 자칫 기존의 (고전)지정학의 시각을 폐기하는 데로 기울어서는 안 된다. 오히려 디지털 안보의 세계정치를 제대로 이해하기 위해 필요한 것은 기존의 지정학을 포괄하면서도 새로운 시각을 품어내는 좀 더 복합적인 분석틀의 개발이다.

2. 디지털 안보의 복합지정학

기본적으로 디지털 안보가 창발하는 과정은 우리가 알고 있던 지정학의 시각을 넘어선다. 무엇보다도 안보위협의 기반이 되는 신흥기술 변수, 즉 인터넷과 악성코드, 인공지능이나 로봇

등과 같은 첨단기술은 기본적으로 지리적 공간을 초월하는 사이버 공간을 배경으로 작동한다. 이러한 사이버 공간은 정보통신과 인터넷의 복합 네트워크가 만들어내는 '흐름으로서의 공간(space as flows)' 또는 탈(脫)지정학적 공간이다(Castells, 2000). 이러한 탈지정학적 사이버 공간을 배경으로 발생하는 디지털 안보의 세계정치에는, 〈그림-1〉에서 제시한, 세 가지 차원의 임계점을 넘는 '복합지정학'(complex geopolitics)의 메커니즘이 작동한다.

첫째, 디지털 안보의 위협이 '양질전화 임계점'의 문턱에 접근하는 과정에서 '안보화'(securitization) 담론 생성의 '비판지정학'이 작동한다. 비판지정학은 특정한 발언이나 재현을 통해 영향력을 갖게 되는 담론적 실천이 지정학적 현실을 구성 및 재구성하는 과정에 주목한다. 지정학적 지식이 어떤 특정 정치집단에 의해 이용되고 생산되고 왜곡되는지와 관련된 권력과정의 분석이 주관심사이다(Ó Tuathail, 1996). 이런 점에서 비판지정학은 구성주의 국제정치이론과 맥이 닿는다. 사실 디지털 안보는 객관적으로 '실재하는 위험'만큼이나 위험을 주관적으로 '구성하는 과정,' 즉 국제안보 연구의 코펜하겐 학파에서 말하는 '안보화'가 중요한 게임이다(Hansen and Nissenbaum, 2009).

둘째, 디지털 안보의 세계정치는 글로벌 차원에서 발생하는 갈등을 영토의 발상을 넘어서는 협력으로 풀어야 하는 비(非)지정학적 문제이기도 하다. 이러한 시각은 국가영토의 경계를 넘어서는 흐름의 증대에 주목하는 '상호의존'과 글로벌 거버넌스의 논의와 일맥상통하며, 국제협력과 규범형성을 강조하는 자유주의 국제정치이론의 시각과 맥이 닿는다(Ikenberry, 2014). 디지털 안보는 지정학적 공간에 고착된 일국적 시각을 넘어서 글로벌 차원에서 이해당사자들의 긴밀한 협력을 통해서 초국적 해법을 모색해야 하는 문제이다. 최근 디지털 안보 문제가 통상, 데이터, 산업, 외교 등과 같은 다양한 차원에서 '이슈연계 임계점'을 넘나들고 있는 상황은 이러한 인식을 뒷받침한다.

끝으로, '지정학적 임계점'의 문턱에까지 다다른 디지털 안보의 위협은 영토적 발상을 기반으로 하는 고전지정학적 사안으로 이해할 수밖에 없다. 고전지정학은 권력의 원천을 자원의 분포와 접근성이라는 물질적 또는 지리적 요소로 이해하고 이를 확보하기 위한 경쟁이라는 차원에서 국가전략에 접근한다(지상현 · 플린트, 2009; Mead, 2014). 이는 물질적 권력의 지표를 활용하여 국가 행위자 간의 패권경쟁과 세력전이를 설명하는 현실주의 국제정치이론의 인식과 통한다(Gilpin, 1981; Organski and Kugler, 1980). 고전지정학의 시각에서 본 디지털 안보 게임의 핵심은 기술과 인력의 역량개발을 통해서 영토와 자원 확보의 경쟁, 그리고 기술패권경쟁에서 우위를 점하는 것이다.

요컨대, 신흥기술과 디지털 안보의 세계정치는 전통안보 분야의 (고전)지정학적 시각뿐만 아니라 여타 다양한 시각을 원용해서 이해해야 하는 복합지정학의 게임이다. 탈지정학적 공간으로서 사이버 공간의 부상은 비국가 행위자들에 의해 도발될 '비대칭 안보위협'의 효과성을 크게 높여 놓았다. 이러한 과정에서 보이지 않는 디지털 안보위협을 경고하는 안보화의 세계정치도 출

현하고 있다. 또한 이들 기술이 살상무기로 활용되는 과정은 국제질서의 안정성 확보를 위한 국제협력의 거버넌스와 국제규범의 형성을 거론케 한다. 이 글에서 주요 연구대상으로 삼은 미중 디지털 안보 경쟁은 이상에서 설명한 신흥안보의 복합지정학을 극명하게 보여주는 대표적인 사례라고 할 수 있다.

Ⅲ. 디지털 안보의 양질전화 과정

1. 사이버전과 전자전의 진화

지난 수년 동안 양적인 차원에서 사이버 공격의 건수는 꾸준히 증가하고 있으며, 그 공격의 패턴도 질적으로 변화하고 있다. 사이버 공격의 양상을 보면, 국가 기간시설의 교란과 시스템 파괴에서부터 금전탈취와 정보절취 등에 이르기까지 다변화되고 있다. 사이버 공격에 동원되는 수법이라는 측면에서도 디도스(DDoS) 및 봇넷 공격, 악성코드 침투, 가상화폐를 노린 해킹과 랜섬웨어 유포, 인공지능(AI)을 활용한 사이버 공격의 자동화 등으로 다양화되고 있다. 특히 최근 가장 많은 양을 차지하는 금전탈취나 정보절취의 경우, 그 수법도 다양하게 진화하여 기관사칭 공격, 취약기관 연계침투, 정치외교적 사건을 전후한 국가안보 관련 정보절취 등이 크게 늘어나고 있다.

공격 주체 면에서도 초창기에는 해커나 테러리스트와 같은 비국가 행위자들이 나섰다면 최근에는 국가 지원 해킹이 두드러지고 있으며 오프라인 작전에 사이버 작전을 병행하여 그 효과를 극대화하고 있다. 2007년 에스토니아와 2008년 조지아에 대한 러시아의 사이버 공격, 2010년과 2012년 미국 · 이스라엘과 이란 간에 오고 간 사이버 공방, 2013년 이후 부쩍 논란이 된 미국과 중국 간의 사이버 공방 등이 대표적인 사례이다. 이렇듯 국가 행위자가 지원하여 수행되는 사이버전이 독자적인 작전의 형태를 띠면서 물리적 군사력과 통합된 '사이버-물리전'(Cyber-Kinetic Warfare)의 도래가 점쳐지고 있다. '다영역 작전'(multi domain operation) 또는 '5차원 전쟁'의 개념의 출현은 사이버 공간이 육 · 해 · 공 · 우주 작전 운용의 필수적인 변수가 되었다는 인식을 반영한다(김상배, 2019a).

사이버 위협이 증가함에 따라 세계 주요국들은 자국 환경에 맞는 사이버 안보 정책을 다차원에서 마련하려는 노력을 경주하고 있다. 특히 미국과 서방 진영 국가들의 경우, 러시아, 중국, 이란, 북한 등으로부터 가해지는 사이버 공격에 능동적으로 대응하는 조치를 취해왔다. 미국은 국내 사법체계를 활용하여 해커를 공개 수배하기도 했으며, 이스라엘은 무장 테러조직인 하마스 그룹의 해킹거점을 공습 파괴하는 무력대응의 방법을 동원하기도 했다. 또한 미국은 북한의 3대 해킹그룹을 정조준하여 국제제재의 칼날을 뽑아 들기도 했다. 아울러 미국은 자국의 사이버

안보 관련 조직 정비에 적극 나서고 있으며, 영국도 2016년 브렉시트 이후 사이버 안보에 적극적이고 능동적인 방어 전략을 추진하고 있다.

이러한 사이버전에 대한 논의는 EMP(Electro Magnetic Pulse)나 HPM(High Power Microwave) 등을 사용하는 전자전의 전개와도 연결된다. 미국은 2013년 2월 북한의 미사일 발사를 무력화시키는 목적으로 '발사의 왼편'(Left of Launch)이라는 사이버 · 전자전을 감행한 것으로 알려져 있다. 최근 개발되는 민간 또는 군사 부문의 기술과 서비스들은 사이버 · 우주공간의 복합성을 전제로 하고 있다. GPS와 드론 등을 활용한 지상무기체계의 무인화와 위성기술을 활용한 스마트화 등을 통해서 사이버 · 우주공간을 연결하는 복합시스템이 등장하고 있다. GPS 신호를 방해하는 전자전 수단인 GPS 재밍(Jamming)은 바로 이러한 환경을 배경으로 출현한 비대칭 위협 중의 하나이다(김상배, 2019a).

4차 산업혁명 시대의 기술발달과 관련하여 사이버 공격과 방어에 인공지능(AI)을 활용하는 문제가 관건이다. 사이버전이 독자적인 군사작전으로 부상하는 가운데 인공지능을 활용하여 무차별적으로 악성코드를 전파하는 사이버 공격을 가하거나, 혹은 반대로 알고리즘 기반 예측과 위협정보 분석, 이상징후 감지 등이 사이버 방어에 활용되고 있다. 지속적으로 악성코드를 바꾸어서 진화하는 사이버 공격에 대해서 과거 수행된 공격 패턴을 파악하는 식의 통상적인 방어책은 점점 더 그 효과를 상실하고 있다. 게다가 자동화된 방식으로 사이버 공격이 이루어지고 있는 상황에서 인간 행위자가 이를 모니터링 한다는 것은 거의 불가능하다. 이런 맥락에서 인공지능을 사용하여 기존의 취약점을 확인하고 보완 · 수선하는 자율방식이 모색되고 있다(김상배, 2019a).

이른바 5G 이동통신 시대의 도래는 사이버전이나 전자전의 수행에도 큰 영향을 미칠 것으로 예견된다. 사실 사이버 안보와 미래전 환경은 5G에 의해 근본적으로 바뀔 수 있다. 5G 환경에서는 인터넷에 연결된 사물이 기하급수적으로 늘기 때문에 파급력도 기하급수적으로 확장될 것으로 예상된다. 예를 들어, 4G에서는 1㎢당 2천 개의 사물을 연결할 수 있었다면, 5G는 100만 개의 사물을 연결할 수 있으며 여기에는 군용 장비도 포함된다. 5G 기술이 상상했던 것보다 더 많은 대역폭을 제공하게 되면서 사물인터넷(IoT)을 일상의 현실로 만들기에 충분하다는 전망을 낳고 있다. 이런 맥락에서 최근 미국은 5G 분야에서의 중국 기업, 화웨이의 약진을 견제하고 나섰다.

2. 우주공간의 군사화와 상업화

최근 우주공간의 군사화와 상업화 문제가 새로이 조명을 받고 있다. 4차 산업혁명 시대의 기술 · 정보 · 데이터 환경을 배경으로 우주공간의 상업적 활용에 대한 논의가 활성화된 것이 계기이다. 아울러 인공위성 및 GPS 장치를 이용한 사이버 · 우주전의 가능성에 대한 우려도 커지고 있다. 예를 들어, 위성을 활용한 정찰, GPS를 이용한 유도제어, 군 작전 수행 등 민간 및 군

사 분야에서 우주자산이 큰 관심을 끌고 있다. 이러한 시각에서 볼 때, 우주공간은 육 · 해 · 공 · 사이버 공간의 연속선상에서 나열되는 또 하나의 별개 공간이 아니라 전통적인 공간과 복합적으로 연동되면서 미래 인류공간을 입체화시키는 '확장된 신(新) 복합공간'의 일부로서 이해되어야 한다. 군사안보의 관점에서 볼 때, 우주복합공간의 등장은 미래전의 일환으로서, 앞서 언급한, 다영역 작전의 출현과 맥이 닿는다(김상배, 2021a).

고도의 과학기술과 자본이 필요한 분야라는 특성 때문에 과거 우주개발은 참여국의 숫자가 극히 제한되어 있었다. 우주진입 초기에는 미국과 구소련 간의 양자 경쟁이 진행되었으며, 최근에는 중국의 진입으로 경쟁구도가 확장되었다. 이들 우주강국들은 우주공간에서 전쟁 수행능력을 확보하기 위한 경쟁을 벌여왔다. 특히 최근 중국의 위성역량 증대는 미국에게 새로운 위협으로 인식되었다. 또한 중국이 2019년 1월 인류 최초로 달의 뒷면에 탐사선 '창어(嫦娥) 4호'를 착륙시키자, 미국은 우주군 창설을 공포하는 등의 반응을 보이기도 했다. 2000년대 이후에는 기존 우주강국뿐만 아니라 독일, 일본, 인도, 한국 등도 우주개발에 본격적으로 참여하면서 우주경쟁이 가속화되고 있다. 오늘날 전세계적으로 단독 혹은 국제협력을 통해 우주개발에 참여하고 있는 국가는 50개국이 넘으며, 이중에서 15개국 정도는 독자적인 우주군사 프로그램을 수행 중인 것으로 알려져 있다.

오늘날 우주경쟁은 인공위성, 우주과학 및 우주탐사 등 우주시스템 등의 연구개발 경쟁을 근간으로 한다. 우주개발 경쟁이 본격화되면서 상업적 목적의 우주산업이 차지하는 비중이 급격히 증가하고 있다. 그런데 이러한 추세는 역설적으로 우주공간과 관련된 새로운 안보위협의 요인으로 작용하기도 한다. 우주공간에서의 상업적 활동은 사실상 군사적 활동을 전제하거나 또는 수반하는 측면이 강하기 때문이다. 이러한 점에서 우주산업 관련 민군겸용기술(dual-use technology)에 특히 주목할 필요가 있다. 최근 모든 국가의 군과 정부는 상업적 우주산업에 대한 의존도가 날로 증대되고 있다(유준구, 2016). 이러한 변화는 과거 정부 주도의 '올드 스페이스 모델'로부터 민간 업체들이 신규 시장을 개척하는 '뉴 스페이스' 모델로의 패러다임 전환을 바탕에 깔고 있다(한국항공우주연구원, 2019).

4차 산업혁명 시대를 맞이하여 특히 주목을 받는 우주 관련 기술은 글로벌 위성항법시스템(Global Navigation Satellite System, GNSS)이다. 위성항법시스템은 4차 산업혁명 시대의 사회 기간시설을 지원하고, 개인의 편익을 증진하는 국가의 주요 인프라로 부상하고 있다. 또한 위성항법시스템은 항법, 측지, 긴급구조 등 공공부문뿐만 아니라 스마트폰 등과 같은 국민 개개인의 생활 속까지 그 활용 영역을 급속히 확대하고 있다. 게다가 최근 현대전이 인공위성의 위성항법장치를 이용한 우주전의 형태를 띠고 있다는 점에서 그 디지털 안보적 함의가 크다. 이러한 추세에 부응하여 미국과 유럽 국가들뿐만 아니라 러시아, 중국, 일본 및 인도 등의 국가도 독자적인 위성항법시스템을 구축했거나 또는 구축하기 위한 준비를 펼치고 있다(주정민, 2019).

이밖에 급속한 개발에 따른 우주공간의 체증현상 발생, 우주 쓰레기의 위험, 전자간섭 문

제 등도 우주공간이 제기하는 안보문제이다. 사실 최근 인공위성과 우주활동국의 수가 증가하면서 우주환경이 피폐화 및 과밀화되는 문제가 발생하고 있다. 다만, 사이버 안보 분야와는 달리 우주의 경우 아직까지는 우주 물체의 제조, 발사, 항행 등이 정부에 의해서 통제 가능하다. 기본적으로 우주공간은 일국의 주권적 영유가 인정되지 않는 '국제공역(international commons)'으로서 사용자의 자유로운 접근을 위해 국제사회가 효율적 규범을 마련해야 할 공간이다. 실제로 국제사회는 우주활동의 목적, 즉 상업적 활동 또는 군사적 활동의 여부를 불문하고 지속가능한 우주환경 조성과 우주에서의 군비경쟁 방지를 위하여 정책적·규범적 방안을 동시에 모색하고 있다.

3. 사이버 안보화와 사이버 심리전

신흥안보, 그 중에서도 특히 사이버 안보는 그 특성상 안보화의 과정이 매우 중요한 변수가 된다(Hansen and Nissenbaum, 2009). 특히 2010년대로 넘어오면서 양적으로 늘어난 사이버 공격은 미국 오바마 행정부로 하여금 적극적인 안보화의 과정을 통해서 대응하는 카드를 꺼내들게 했다. 특히 중국발 사이버 공격이 논란거리였으며, 이른바 '중국해커위협론'은 2010년대 초중반 미중관계를 달구었던 뜨거운 현안 중의 하나였다. 이때에 즈음하여 오바마 행정부는 국가기간시설에 대한 해킹을 국가안보 문제로 안보화하고 때로는 미사일을 발사해서라도 대응하겠다는 '군사화'의 논리를 내세우며 사이버 안보를 국가 안보전략의 핵심 항목으로 격상시켰다. 급기야 사이버 안보 문제는 2013년 6월 미중 정상회담의 공식의제로 채택되는 상황에까지 이르렀다(김상배, 2015b).

2017년 트럼프 행정부 출범 이후 미중 사이버 갈등은 좀 더 복합적인 양상으로 전개되었다. 예상과는 달리 미중 사이버 공방은 군사적 충돌로 비화되기보다는 오히려 산업과 통상 문제와 긴밀히 연계되는 양상을 보였다. 트럼프 행정부는 이른바 '중국산 IT보안제품 위협'이라는 안보화 담론을 내세워 중국 기업들의 IT보안제품에 대한 규제를 강화했다. 특히 5G 이동통신 분야와 같은 4차 산업혁명 분야에서 기술경쟁력을 쌓고 있는 중국 기업들에 대한 미국의 견제가 가해졌다. 실제로 화웨이, ZTE, 차이나모바일, DJI, 하이크비전, 푸젠진화 등과 같은 중국 IT기업들이 미국 시장에 진출하는 과정에서 다양한 문제들이 빌미가 되었다. 기술경쟁과 통상마찰의 외양을 한 이들 문제는 사이버 안보나 데이터 주권 등의 쟁점과 연계되면서 그 복잡성이 더해갔다

이 중에서도 제일 문제가 된 기업은 5G 분야의 선두주자인 화웨이였다. 화웨이의 장비를 쓰는 것이 위험하다는 안보화 담론의 근거는, 백도어라는 것이 지금은 아니더라도 언제든지 심어 넣을 수 있는 미래의 위협이기 때문이다. 특히 5G 시스템은 공급업체가 제공하는 소프트웨어 갱신에 크게 의존하기 때문에 언제든지 악성코드를 심는 것이 가능하다는 것이었다. 게다가 화웨이라는 기업의 성장배경이나 성격을 보면, 이러한 미국 정부의 주장은 나름대로의 '합리적 의심'이었다. 특히 미국은 화웨이라는 기업의 뒤에 중국 정부가 있다는 사실을 의심했다. 이러한 상황에

서 화웨이가 5G 이동통신망을 장악할 경우 이는 미국의 핵심적인 국가정보를 모두 중국 정부에게 내주는 꼴이 될 것이라는 우려가 제기되었다(김상배, 2019b).

이러한 '안보화 정치'와 동전의 양면과도 같은 관계에 있는 것이 사이버 루머와 가짜뉴스(fake news)이다. 최근 미국이나 서방 진영 국가들의 선거과정에서 수행된 러시아발 가짜뉴스 공격은 인터넷과 소셜 미디어 상에서 여론을 왜곡하고 사회분열을 부추기며 서구 민주주의 체제의 정상적인 작동을 방해하는 효과를 빚어냈다(Walker and Ludwig, 2017). 러시아 정부가 수행한 전술은 고도화된 설득전략을 바탕으로 정교하게 구사되었을 뿐만 아니라, 인공지능을 활용한 다양한 정보확산의 기술을 사용하고 있는 것으로 알려져 있다. 아울러 최근 인공지능과 가상현실(VR) 등을 사용해 만든 '딥페이크(deep fake)'도 최근 쟁점으로 떠올랐다. 2020년 코로나19 사태와 미국 대선 등을 거치면서 사이버 공간에서 유포되는 허위정보와 가짜뉴스를 디지털 안보의 관점에서 보아야 한다는 인식이 확산되었다(김상배, 2020a).

이러한 가짜뉴스를 디지털 안보의 시각에서 봐야 하는 이유는, 소셜 미디어나 인공지능과 같은 기술이 사이버 심리전과 연계되는 양상을 보여주기 때문이다. 이러한 비군사적 교란행위는 단순히 경쟁국이나 적국의 사회혼란을 야기하는 여론전만을 목표로 하지 않는다. 다시 말해, 소셜 미디어의 전략적 효과를 노리고 언론매체에 빈번한 역정보 또는 허위정보를 유포하는 행위는 미래전의 한 양식을 보여준다. 현실공간의 무력분쟁과 연계되면서 이른바 하이브리드전(hybrid warfare)으로 비화될 가능성을 보여준다. 하이브리드전은 고도로 통합된 구상 속에서 노골적이거나 은밀한 형태로 군사 · 준군사 또는 민간 수단들이 광범위하게 운용되는 전쟁의 양상을 의미한다. 최근 하이브리드전은 전투원과 민간인이 구분되지 않는 구도에서 상대국의 군사적 대응을 촉발하기 직전에 멈추도록 교묘하고 신중하게 감행되고 있다.

예를 들어, 2014년 우크라이나에 대해서 사이버 공격과 병행하여 감행된 러시아의 하이브리드전은 새로운 분쟁 양식의 등장이라는 점에서 학계의 주목을 끌었다. 또한 2018년 나토가 시리아 정부의 화학무기 사용에 대해서 인도주의적 명분을 내세워 시리아에 대한 공습을 감행했을 때, 러시아가 취한 대응도 하이브리드전의 맥락에서 이해된다. 당시 러시아가 취한 반격은 군사적 대응이 아니라 사이버 공간에서 정보 · 심리전을 수행하는 활동이었다. 구체적으로 말해, 러시아는 서구 국가들의 인터넷과 소셜 미디어를 목표로 하여 트롤군(Troll Army)의 활동을 증대시켰다. 러시아의 이러한 행동은 향후 사이버 심리전을 겸비한 하이브리드전이 미래전의 한 양식으로 자리 잡을 가능성을 보여 주었다(송태은, 2019).

Ⅳ. 디지털 안보의 이슈연계 메커니즘

1. 첨단기술 및 보안제품의 수출입 통제

앞서 언급한 사이버 안보화의 문제가 이슈연계된 대표적인 영역은 수출입 통제를 둘러싼 통상 문제이다. 특히 미국은 중국 기업 특히 화웨이에 대해서 수입규제의 카드를 꺼내들었다. 사실 미국과 화웨이(또는 ZTE) 간의 갈등의 역사는 꽤 길다. 2003년 미국 기업 시스코는 자사의 네트워크 장비 관련 기술을 부당하게 유출했다는 의혹을 제기하면서 화웨이를 고소했다. 2012년 미 하원 정보위원회는 화웨이 통신장비들이 백도어를 통해서 정보를 유출하고 랜섬웨어 공격을 가한다며 안보위협의 주범으로 지적했다. 2013년 미국 정부도 나서 중국산 네트워크 장비 도입이 보안에 위협이 될 수 있음을 인정했는데, 2014년에는 화웨이와 ZTE 설비의 구매를 금지한다는 발표가 있었다. 2016년에는 미국 내 화웨이 스마트폰에서 백도어가 발견되는 사건이 발생하기도 했다.

이러한 분위기는 2018년 들어 급속히 악화되었다. 2018년 1월 미국 업체인 AT&T가 화웨이의 스마트폰을 판매하려던 계획을 전격 취소했다. 2월에는 CIA, FBI, NSA 등 미국의 정보기관들이 일제히 화웨이와 ZTE의 제품을 사용하지 말라고 경고했다. 3월에 FCC는 화웨이 등 중국 업체들에 대해 '적극적 조치'를 취하겠다고 발표했다. 4월에는 ZTE가 대(對)이란 제재 조치를 위반했다는 혐의로 미국 기업들과 향후 7년간 거래 금지라는 초강력 제재를 받았다가 6월에 구사일생했다. 7월에는 차이나모바일의 미국 시장 진입이 불허됐다. 8월에는 미국 정부는 '2019년 국방수권법'을 통과시키며 화웨이와 ZTE 등 5개 중국 기업의 제품을 정부 조달품목에서 원천 배제하기로 했다. 12월에는 화웨이 부회장 겸 최고재무책임자(CFO)인 멍완저우가 대(對)이란 제재 위반 혐의로 체포됐다. 2019년 2월 마이크 펜스 미국 부통령은 뮌헨안보회의에서 미국의 동맹국들이 화웨이 제품을 사용하지 말 것을 촉구했다(김상배, 2019b).

이러한 수입규제 행보는 수출규제 조치로 이어졌다. 2019년 5월 트럼프 대통령의 행정명령은 주요 IT기업들에게 거래 중지를 요구했다. 따라서 구글, MS, 인텔, 퀄컴, 브로드컴, 마이크론, ARM 등이 화웨이와 제품 공급계약을 중지하고 기술계약을 해지했다. 이러한 조치는 화웨이 제품의 수입중단 조치와는 질적으로 다른 파장을 낳았다. 글로벌 공급망에 크게 의존하고 있는 상황에서 부품 공급차질에 따라 장비와 소프트웨어의 업데이트 등이 막힌다면, 화웨이는 미국의 의도대로 5G 이동통신 시장에서 완전히 축출될 가능성도 배제할 수 없기 때문이다(송경재, 2019). 게다가 2019년 6월에는 중국에서 설계 · 제작되는 5G 장비를 미국 내에서 사용 금지하는 방안의 검토가 보도되었는데, 이러한 방안이 현실화된다면 미국의 통신장비 공급망이 완전히 새롭게 짜이는 것을 의미한다는 점에서 파장이 컸다(김치연, 2019).

한편, 2019년 5월 미국의 화웨이 제재가 정점으로 치닫던 시기, 중국 국가인터넷정보판

공실은 미국의 수출입 규제 조치에 맞불을 놓는 성격의 새로운 규제 방안을 발표했다. 그 내용은, 중국 정부가 자국 내 정보통신 인프라 사업자가 인터넷 관련 부품과 소프트웨어를 조달할 때 국가안보에 위해를 초래할 위험 여부를 점검하여 문제가 있다고 판단되면 거래를 금지할 수 있다는 것이었다. 이는 미국 첨단기술 제품의 중국 수출을 막을 수 있다는 신호를 보낸 것이었다(차대운, 2019). 또한 2019년 12월 초 중국 정부는 모든 정부 부처와 공공기관에 3년 안에 외국산 컴퓨터와 소프트웨어를 자국산으로 교체하도록 지시하였다. 델과 HP의 PC와 MS의 윈도 운영체제 등 미국 기업 제품을 겨냥하였다. 미국이 국가안보를 이유로 중국 통신장비 업체 화웨이와 ZTE 등을 제재하자 비슷한 방법으로 대응한 것이었다.

군사적 유용의 가능성이 있는 첨단기술의 수출통제는 냉전 시대부터 있어 왔던 이슈이다. 코콤이 해체되고 난 후 1996년 7월에 출범한 바세나르 협정은 재래식 무기와 민군겸용기술의 투명성을 제고하고 책임성을 강화하기 위한 조치였다. 특히 국가안보를 위협하는 재래식 무기의 과잉축적을 방지하고 이러한 물자들에 책임을 부여함으로써 안정성을 확보하는 것을 목적으로 했다. 그 이후 미국과 유럽연합은 수출통제 레짐에 대한 논의와 규범 형성을 주도하고 있는데, 특히 중국의 부상으로 인해 이 분야에서 비서구적 규범과 표준이 대두될 가능성을 경계했다. 트럼프 행정부가 신흥기술의 대두와 미중 기술경쟁의 가속화라는 빠른 환경변화를 반영한 수출통제 레짐의 개혁 필요성을 절감하고, 2018년 8월 수출통제개혁법(Export Control Reform Act, ECRA)을 발표한 것도 바로 이러한 맥락에서 이해될 수 있다. 이러한 행보의 바탕에는 신흥기술의 수출통제가 기술경쟁력의 보호 차원을 넘어서 국가안보의 문제로 인식되는 광범위한 합의가 깔려 있었다.

2. 민간 및 군사 분야의 데이터 안보

사이버 안보화에서 시작되어 수출입 통제 문제로 비화된 미중갈등의 불똥은 최근 데이터 안보 분야로 옮겨붙고 있다(김상배, 2020b). 화웨이 다음으로 표적이 된 것은 민간 드론 시장을 석권한 중국 업체 DJI였다. 미국 국토안보부(DHS) 사이버안보 · 기간시설 안보국(CISA)은 2019년 5월 중국의 드론이 민감한 항공 정보를 중국 본국으로 보내고, 중국 정부가 이를 들여다본다고 폭로하였다. 이를 두고 CISA는 국가기관의 정보에 대한 '잠재적 위협'이라고 경고하였다. CISA가 특정 드론을 거론한 것은 아니었지만, 사실상 중국의 DJI를 염두에 둔 발표였다. 이와 관련해서 DJI는 즉각 '우리 기술은 안전하다'고 반박했으나, CISA는 자국 소비자들에게 중국산 드론을 구입할 경우 신중해야 하며 인터넷 장비를 분리해야 한다는 방침까지 내놨다. 화웨이에 대해서 제기되었던 기술안보 공방을 연상케 하는 조치였다.

또한 미국 정부는 2017년부터 하이크비전, 다후아 등과 같은 CCTV업체들이 수집하는 데이터가 중국 정부로 유출될 수 있다는 의혹을 제기하고 있다. 특히 하이크비전은 CCTV 제작기

술에서 세계적으로 앞서갈 뿐만 아니라 안면 인식이나 사람들의 버릇과 신체 특성 등을 고려해 특정 인물을 식별하는 기술로 유명하다. 중국 정부는 이러한 기술을 감시도구로 활용해서 소수민족이나 반체제 세력을 통제하는 데 적극 활용하고 있다. CCTV의 하이크비전에 대한 압박은 미국이 중국의 기술굴기를 견제하고 중국 정부와 IT기업의 유착을 질타하는 차원을 넘어서, 천안문 사태 30주년을 맞이한 중국의 인권 문제를 겨냥했다는 해석을 낳았으며, 이는 당시 뜨거운 쟁점이 되었던 홍콩 시위 사태와도 무관치 않다.

2019년 말에 새로이 미국의 경계대상 목록에 등장한 중국의 인터넷 관련 서비스는 15초짜리 짧은 동영상을 공유하는 앱인 틱톡이다. 중국의 스타트업인 바이트댄스의 틱톡은 전세계 5억 명 이상이 사용자를 자랑하며, 미국에서만도 가입자가 2천 5백만 명에 달한다. 미국 정부는 2019년 2월 틱톡에 대해 아동 개인정보 불법 수집혐의로 과징금을 부과한 바 있고, 최근에는 미국 상원의원들이 틱톡의 국가안보 위험여부를 조사해달라고 공식 요청하였으며, 미국해외투자위원회(CFIUS)는 바이트댄스가 미국의 뮤직앱, 뮤지컬.리(musical.ly)를 인수한 데 대한 조사하고 있는 것으로 알려졌다. 미 육군과 해군도 사이버 안보에 위협이 될 수 있다며 소속 장병들에게 정부가 지급한 휴대폰에서 틱톡의 사용을 금지하고, 앱 자체도 삭제하라고 지시했다(정명섭, 2020).

안보와 무관해 보이는 데이터 문제에 대해서 국가안보를 논하게 되는 배경에는 데이터 안보가 지니는 특성, 즉 개인정보의 보호 문제가 양질전화와 이슈연계 임계점을 넘어서 조직보안과 국가안보의 문제로 창발하는 신흥안보로서의 성격이 있다(김상배, 2021b). 이는 스몰데이터 환경에서 야기되는 안보문제가 아니라 빅데이터에서 발생하는 안보문제로서, 국가안보 또는 군사안보와 무관하게 보이는 데이터라도 그 양이 늘어나고 이슈가 복잡하게 연계되면, 새로이 국가안보의 함의를 지닌 패턴이 드러나는 신흥안보의 문제이다. 이런 시각에서 보면 다국적 기업들이 수집하는 비군사적이고 경제적인 데이터일지라도, 때에 따라서는 매우 중요한 군사안보의 논란을 일으킬 수도 있다. 실제로 이와 관련하여 최근 일국 단위에서 데이터 주권을 어떻게 수호할 것이냐의 논쟁이 일고 있다. 4차 산업혁명 시대를 맞이하여 민간의 데이터 안보 문제가 군사 분야의 정보 · 데이터 안보 문제와 연계될 가능성이 커졌기 때문이다.

군사 분야에서 정찰위성이나 정찰기 등의 기술을 활용한 군사 정보 · 데이터의 수집은 전략적 우위와 전쟁의 승패를 가를 중요한 능력으로 이해되어 왔다. 예를 들어, 미군은 정찰 위성이나 무인정찰기 및 드론 등을 활용하여 북한의 ICBM 이동발사 차량을 정확하게 추적 · 파악하고는 것으로 알려져 있다(Lieber and Press, 2017). 최근 논란이 되었던 지소미아(GSOMIA)에 의거하여, 일본은 북핵 · 미사일 기술 관련 정보를 제공해 왔는데, 일본의 위성은 하루에 3-4차례 한반도 상공을 지나가는 미국의 첩보위성이 커버하지 못하는 사각 시간은 일부 보완했다고 한다. 2019년 12월에는 미국이 북한의 추가 시험과 도발 동향 징후를 파악하기 위해서 한반도 상공에서 운용하는 특수정찰기가 하루 동안 3대나, 그것도 위치발신장치를 켠 상태로 비행하며

대북 감시 활동을 벌인 것으로 드러나 논란이 되기도 했다(최평천, 2019).

4차 산업혁명의 진전으로 인하여 좀 더 포괄적인 의미에서 본 데이터의 중요성이 군사 분야에서 점점 더 커지고 있다. 인공지능 기술의 발달로 인해 더 강력해진 (빅)데이터 처리 능력은 점점 더 군사안보를 위해 필요한 핵심능력으로 자리 잡을 것이다. 이러한 과정에서 전장 센서로부터 데이터를 수집하고, 더 많은 처리능력으로 보강한 알고리즘으로 데이터를 처리하고, 결과적으로 적보다 빠르게 침투하는 것이 핵심이다. 모든 전장정보를 데이터화시켜 클라우드 서버에 저장·분석하여 필요 부대에 정보를 제공하는 '지능형 데이터 통합체계'를 구축 활용하여 각종 정보와 데이터를 분석하고, 실시간으로 인간 지휘관의 지휘결심체계를 지원할 것으로 기대되고 있다. 이러한 과정에서 인공지능이 전장 빅데이터를 바탕으로 워게임과 모의실험 등 지휘결심 과정을 거쳐 최적의 대안을 제시한다는 것이다.

3. 밀리테크와 첨단 방위산업 경쟁

4차 산업혁명 시대의 도래라는 맥락에서 민군겸용기술(dual-use technology)과 첨단 방위산업 분야의 경쟁도 가속화되고 있다(Kurç and Neuman, 2017; 장원준 외, 2017). 냉전기에는 주로 군사 분야의 수요에 부응하여 기술발달이 이루어졌다면, 오늘날에는 역으로 민간 분야의 기술혁신이 방위산업에 영향을 미치고 있다. 좀 더 엄밀히 말하면, 4차 산업혁명 시대에는 군사기술과 민간기술을 구분하는 것이 불가능할 정도로 양자가 밀접히 결합되어 있다. 현재 민수와 군수 분야에서 주목하는 기술들도 상당 부분이 겹치는데, 군사 분야에서 주목하는 기술이 민간 분야에서도 혁신을 추동하고 있다. 예를 들어, 안면인식, 가상현실, 인공지능, 로봇, 자율주행차 등과 관련된 기술들은 상업적으로는 물론 군사적 목적으로도 활용되는, 이른바 밀리테크(militech)의 사례들이다(매일경제 국민보고대회팀, 2019).

이렇게 군사기술과 민간기술의 경계를 허문 일종의 하이브리드형 기술로서 밀리테크의 역량을 구비하는 것은 미래전과 4차 산업혁명을 동시에 준비하는 지름길로 인식된다. 오늘날의 밀리테크를 확보하는 나라가 미래전에서 승리하게 될 것이며 경제성장을 누리고, 더 나아가 글로벌 패권까지 장악할 수 있다는 의미이다. 특히 군사안보의 측면에서 볼 때, 일종의 '게임 체인저'로서 거론되는 첨단 무기체계의 개발능력을 보유하는 것은, 국방력 강화를 통한 선진군대의 육성을 의미한다. 또한 이러한 능력의 보유는 실제 전쟁의 수행이라는 군사적 차원을 넘어서 무기판매, 기술이전 등과 같은 경제·산업적 차원의 경쟁에서도 앞서가는 것을 의미한다. 요컨대, 첨단 방위산업의 기술력 보유는 기술을 바탕으로 한 군사력 경쟁의 의미를 넘어서 종합적인 의미에서 본 디지털 부국강병의 달성을 의미한다(김상배, 2020c).

미국, 중국 등 주요국들은 첨단 방위산업이 새로운 국력의 원천이라는 점을 인식하고, 이 분야에 대한 투자를 늘리고 있으며 이를 통해서 4차 산업혁명 분야의 기술을 활용한 첨단무기

개발에 나서고 있다. 다시 말해, 민간기술을 군사 분야에 도입하고, 국방기술을 상업화하는 등의 행보를 적극적으로 펼치고 있다. 특히 첨단화하는 군사기술 트렌드에 대응하기 위해서 민간 분야의 4차 산업혁명 관련 기술성과를 적극 원용하는 데 앞장서고 있다. 사이버 안보, 인공지능, 로보틱스, 양자 컴퓨팅, 5G 네트워스, 나노소재 등과 같이 기술이 대표적인 사례이다. 이러한 기술에 대한 투자는 국방 분야를 첨단 4차 산업혁명 기술의 테스트베드로 삼아 첨단 민간기술의 군사적 활용을 도모하는 것을 의미한다.

좀 더 넓은 의미에서 볼 때, 밀리테크 경쟁은 미래 무기체계의 표준 또는 플랫폼을 장악하기 위한 경쟁이다. 실제로 세계 최대 무기수출국인 미국의 행보를 보면, 단순히 첨단무기만 파는 것이 아니라 그 '운영체계'를 함께 판다. 다시 말해, '제품 수출'을 넘어서 '표준 전파'와 '플랫폼 구축'을 지향한다. 특히 4차 산업혁명 관련 기술을 탑재한 무기체계의 작동 과정에서 플랫폼의 장악은 매우 중요하다. 사실 방위산업은 승자독식의 논리가 통하는 분야이다. 우선 '전쟁에서 이기는 무기'를 구입하려 하고, 한번 구입한 무기는 호환성 유지 등의 이유로 계속 사용할 수밖에 없게 된다. 미국이 글로벌 방위산업을 주도하는 근간에는 이렇듯 무기와 표준을 동시에 제공함으로서 플랫폼을 구축하려는 전략, 그리고 더 나아가 전쟁 수행방식의 원리와 개념 및 담론까지도 장악하려는 전략이 자리 잡고 있다(김상배, 2020c).

최근 이러한 양상을 보여주는 사례 중의 하나가 드론 산업이다. 드론 기술은 민군겸용기술의 대표적인 사례인데, 단순한 무기기술만을 의미하는 것이 아니라 다양한 분야에 활용되는 민간기술들이 만나는 접점에서 발전해 왔다. 또한 드론 경쟁은 단순히 드론을 제조하는 기술경쟁의 의미를 넘어서 드론을 운용하는 데 필요한 소프트웨어와 서비스의 표준을 장악하는 경쟁이다. 사실 드론의 개발과 운용 과정을 보면 제품-표준-플랫폼-서비스 등을 연동시키는 것이 중요하다. 군사적인 관점에서 볼 때 이러한 드론 표준이 내포하고 있는 것은 미래무기의 표준인 동시에 미래 전쟁의 표준이다. 실제로 드론을 중심으로 미래전의 무기체계와 작전 운용방식이 변화하고 전쟁을 수행하는 주체와 전쟁의 개념 자체도 변화할 조짐을 보이고 있다.

한편 첨단 방위산업 경쟁의 이면에 밀리테크의 개발과 확산을 둘러싼 제도모델의 변화가 자리 잡고 있음을 놓치지 말아야 한다. 이는 기술혁신의 주체라는 점에서 4차 산업혁명이 주로 민간 행위자들에 의해서 주도된다는 특징에서 비롯된다. 오늘날 인공지능, 빅데이터, 로봇 등의 기술혁신은 지정학적 경계를 넘어서 민간 부문을 중심으로 초국적으로 이루어지고, 이후에 군사부문에 적용되는 '스핀온'(spin-on)의 양상을 보인다. 좀 더 엄밀하게 말하면, 4차 산업혁명 시대의 기술은 그 복잡성과 애매모호성으로 인해서 민군의 용도를 구분하는 것 자체가 쉽지 않다. 이러한 양상은 20세기 후반 냉전기의 주요 기술혁신이 주로 군사적 목적에서 이루어지고, 그 이후 민간 부문으로 확산되었던 '스핀오프'(spin-off) 모델과 대비된다(김상배, 2020c).

Ⅴ. 디지털 안보의 (복합)지정학적 차원

1. 자율무기체계의 도입과 미래전의 창발

이상에서 살펴본 디지털 안보의 창발은 지정학적 임계점을 넘어서 물리적 전쟁으로 비화될 가능성을 안고 있다. 예를 들어, 실제로 사이버 공격이 재래식 전쟁과 연계되는 사건이 발생하였는데, 2007년 에스토니아, 2008년 조지아, 2014년 우크라이나 등에 대한 러시아의 사이버 공격, 그리고 2010-12년 미국/이스라엘과 이란의 사이버 공방을 사례로 들 수 있다. 이렇게 지정학적 갈등을 내포한 사이버 공격에 대응하기 위해서 주요국들은 사이버 군대를 신설하거나 확대 및 격상하는 조치들을 취하고 있다. 역으로 이러한 전개 양상은 사이버 안보 문제가 전통 군사안보 전반에 연계될 가능성을 높이고 있다. 이러한 과정에서 인공지능을 탑재하여 자율기능을 확보한 첨단 무기체계가 해킹 공격을 당할 사태 등이 우려되고 있다.

세계 산업분야 전반의 자동화와 무인화 추세가 꾸준히 늘어나고 있어 결국 멀지 않은 장래에 무인무기체계가 실제 작전에도 배치될 것으로 예견된다. 인공지능, 빅데이터, 가상현실(VR), 드론, 사물인터넷(IoT), 3D 프린팅 등과 같은 4차 산업혁명의 거대한 물결이 사회 전반을 덮치고 있는 상황을 염두에 둘 때 군사 분야도 예외는 아닐 것이다. 그중에서도 미래전의 혁신적 변화를 야기할 기술로 인공지능이 손꼽힌다. 인공지능 기술은 위험지역에서의 폭발물 제거, 군수물자 수송 등과 같이 인간의 생명을 보호하고 군사적 비용을 낮추는 방향으로 활용될 것이 기대된다. 이처럼 군사기술의 급속한 발달은 전장 지형의 큰 변화를 예고한다.

특히 드론 기술의 적용이 논란거리이다. 장난감 같았던 드론이 치명적인 살상무기로 진화하여 전통적인 전쟁의 공식들을 뒤흔드는 상황이 벌어지고 있다. 2020년 9월 예멘 반군의 소행으로 추정되는 드론 공격이 사우디 국영회사 아람코의 석유시설과 유전에 대해 가해지면서 그 위협에 대한 우려가 커졌다. 2020년 1월에는 이란 혁명수비대의 솔레이마니 사령관이 미군의 공습으로 사망하는 사건이 발생했다. 미군의 공습에는 2001년 첫 비행을 한 기종의 드론인 MQ-9 리퍼가 동원된 것으로 알려졌는데, 미국이 한창 개발 중인 드론은 이미 리퍼를 뛰어넘는 성능을 갖추었으며, 게다가 군집기술과 인공지능을 접목해 그 기능이 큰 폭으로 강화되었다는 사실이 알려지면서 드론 공격에 대한 공포가 더욱 커지고 있다(이철재, 2020).

사정이 이렇다 보니 드론을 포함한 자율무기체계를 도입하려는 강대국들의 경쟁이 치열하게 벌어지고 있다. 미국은 중국과 러시아의 추격으로 군사력 격차가 좁아지는 상황에 대처하기 위해서 이른바 '3차 상쇄전략'을 추진하는 차원에서 일찍이 무인무기체계의 중요성을 인식하고 연구개발을 추진해 왔으며 다양한 무인무기를 개발해 실전 배치하고 있다. 예를 들어, 전 세계 군용 무인항공기의 60%를 미군이 보유하고 있다. 한편, 중국군도 4차 산업혁명이 제공하는 첨단 기술을 활용한 군 현대화를 적극적으로 추진하고 있다. 후발주자인 중국은 미국을 모방한 최신형

무인기를 생산 · 공개하고, 저가의 군용 · 민간용 무인기 수출을 확대하는 등 기술적 측면에서 미국의 뒤를 바짝 쫓고 있다. 향후 자율무기체계 개발경쟁은 미국과 중국이 벌이는 글로벌 패권경쟁과 연계되어 더욱 가속화될 것으로 예견된다.

4차 산업혁명 시대의 기술발달은 군사혁신을 유발하고 더 나아가 전쟁 수행방식의 진화를 야기할 것으로 전망된다. 실제로 최근의 변화를 보면, 기술발달을 바탕으로 한 자율무기체계의 도입은 단순한 무기체계 변환의 차원을 넘어서 군사안보 분야의 작전운용과 전투공간, 그리고 전쟁양식에 대한 개념까지도 변화시키고 있다. 2000년대 이래로 제기되었던 네트워크중심전(NCW), 스워밍(swaming), 모자이크전, 다영역 작전(MDO), 5차원 전쟁, 하이브리드전 등의 개념은 바로 이러한 맥락에서 이해할 수 있는 사례들이다. 1990년대와 2000년대의 초기 정보화(또는 3차 산업혁명)가 인간의 정보능력을 확장시켜 네트워크 지휘통제를 가능케 하는 작전 개념을 이끌어냈다면, 최근의 4차 산업혁명은 새로운 데이터 환경에서 인공지능과 로봇을 활용한, 이른바 '사이버-물리전'(cyber-kinetic warfare)의 출현을 예견케 한다.

4차 산업혁명 분야의 기술발달이 근대 전쟁의 기본적인 전제와 공식을 완전히 바꿔놓을 가능성도 없지 않다. 예를 들어, 자율무기체계의 도입은 클라우제비츠(Carl von Clausewitz)가 말하는 전쟁의 세 가지 속성, 즉 폭력성과 정치성, 불확실성을 재고케 한다. 기술발달 그 자체가 폭력행사의 절대능력을 증대시키는 방향으로 영향을 미칠 것이다. 자율무기체계에 의지하는 전쟁이 무력사용의 범위를 결정하는 인간의 정치적 의지 안에 머무른다는 보장도 없다. 기술발달의 복잡성이 증대되는 상황에서 자율무기체계를 활용한 미래전의 불확실성은 더 커졌다고 할 수 있다. 이와 더불어 자율무기체계의 도입은 군사조직과 제도의 혁신을 유발하고, 더 나아가 미래 세계정치의 주체와 구조, 그리고 그 작동방식과 구성원리까지도 변화시킬 가능성도 없지 않다(김상배, 2019a).

4차 산업혁명의 진전은 인간이 아닌 행위자들이 벌이는 전쟁의 가능성도 거론케 한다. 이러한 과정에서 인간 중심의 지평을 넘어서는 '포스트 휴먼'(post-human) 세계정치의 부상이 거론된다. '먼 미래' 전망의 관점에서 볼 때, 비인간 행위자로서 인공지능 기반의 자율로봇은 인류의 물질적 조건을 변화시킬 뿐만 아니라 인간을 중심으로 편제되었던 군사작전의 기본개념을 바꾸고 근대 국제정치의 기본 전제들에 의문을 제기하고 있다. 이러한 과정에서 자율무기체계로 대변되는 기술 변수는 단순한 환경이나 도구 변수가 아니라 주체 변수로서, 미래전의 형식과 내용을 결정하고 더 나아가 미래 세계정치의 조건을 규정할 가능성이 있다(김상배, 2019a).

2. 디지털 안보의 동맹 및 연대 외교

화웨이 사태는 사이버 안보를 둘러싼 동맹 및 연대외교의 동학을 부각시켰다. 2018년 말 트럼프 행정부는 '파이브 아이즈(Five Eyes)'로 대변되는 미국의 주요 정보동맹국들에게 화웨이

보이콧에 동참할 것을 촉구하며 화웨이 장비가 발붙일 곳을 아예 없애려는 듯 강경행보를 보였다. 영국은 대형 통신업체인 BT그룹이 화웨이와 ZTE 제품을 5G 사업에서 배제하려는 움직임을 보였다. 캐나다는 중국과의 무역마찰을 무릅쓰고 미국의 요청에 따라 화웨이의 부회장인 멍완저우를 체포했다. 호주와 뉴질랜드는 5G 이동통신 사업에 중국 업체가 참가하지 못하도록 하는 방침을 내렸다. 여기에 일본까지 가세해서, 정부 차원의 통신장비 입찰에서 중국 화웨이와 ZTE를 배제하기로 결정했으며, 일본의 3대 이동통신사도 기지국 등의 통신설비에서 화웨이와 ZTE 제품을 배제하기로 했다. 이러한 행보를 보고 일본, 독일, 프랑스 등 3개국이 합류한 '파이브 아이즈+3'의 출현이 거론되기도 했다(김상배, 2019b).

그런데 2019년 2월말을 넘어서면서 영국과 뉴질랜드 등이 '사이버 동맹전선'에서 이탈하는 조짐을 보였다. 영국 국가사이버보안센터(NCSC)는 화웨이 장비의 위험을 관리할 수 있어 그 사용을 전면 금지할 필요는 없다는 잠정 결론을 내렸다. 미국의 요청에 따라 화웨이를 배제했던 뉴질랜드도 저신다 아던 총리가 직접 나서 화웨이를 완전히 배제하지 않았다는 점을 분명히 했다. 이밖에도 독일 역시 특정 업체를 직접 배제하는 것은 법적으로 가능하지 않다는 점을 밝혔고, 프랑스도 특정 기업에 대한 보이콧은 하지 않겠다는 입장을 내놨으며, 이탈리아도 화웨이를 5G 네트워크 구축 사업에서 배제하지 않겠다는 보도를 부인했다. 또한 일찍이 화웨이 장비의 배제 입장을 내놓았던 일본 역시 그러한 제한은 정부기관과 공공부문 조달에만 해당되며, 5G 네트워크 구축에는 포함되지 않는다고 한발 빼기도 했다(김상배, 2019b).

이러한 전개는 한미관계에도 영향을 미쳤다. 실제로 화웨이 사태는 단순한 기술 선택의 문제가 아닌 동맹외교의 문제로 한국에 다가왔다. 2019년 6월 주한 미국대사가 직접 나서 한국이 화웨이에 대한 제재에 동참할 것을 공개적으로 요구하기도 했다. 이와 마찬가지로 데이터의 초국적 이동 문제도 향후 한미관계를 긴장시킬 가능성이 제기되었다. 2016년 한국 정부는 국가안보를 이유로, 구글이 요청한 1:5000 축적의 국내 지도 데이터의 해외 반출 요청을 거부하기도 했다. 2018년 10월에는 국회에서 구글 · 아마존 등 미국 IT기업들에게 국내에 데이터센터용 서버를 설치할 의무를 지우는 법안이 발의되자, 주한 미국대사가 "클라우드의 장점을 가로막는 데이터 현지화 조치를 피해줄 것"을 요구하기도 했다.

사이버 안보를 내세운 미국의 동맹결속 전략은 인도 · 태평양 전략에서도 나타났다. 2019년 4월에는 미국을 위협하는 북한과 중국의 사이버 공격에 대응하기 위한 국제협력체 신설을 골자로 하는 '인도 · 태평양 국가 사이버 리그(CLIPS)' 법안이 상원에서 발의됐다. 클립스(CLIPS)에는 인도 · 태평양 지역의 미국 동맹국과 파트너 국가들이 참여한다(이조은, 2019). 한편 미 국방부는 2019년 6월 공개한 '인도 · 태평양 전략보고서'에서 중국의 일대일로 구상에 맞서 인도 · 태평양 전략을 강화하였으며, 화웨이 사태를 정치, 경제 등 비군사적 요소와 사이버전, 심리전 등을 포함한 '하이브리드 전쟁'의 개념을 빌어 이해하는 모습을 보였다.

미국의 화웨이 견제에도 불구하고 중국은 일대일로 구상의 추진 차원에서 해외 통신 인프

라 확충을 가속화하고 있다. 2018년 4월 시진핑 중국 국가주석은 일대일로 건설을 계기로 관련 국가들, 특히 개도국에 인터넷 기반시설을 건설하고 디지털 경제와 사이버 보안 등 다방면에서 협력을 강화하여 '21세기 디지털 실크로드'를 건설해야 한다고 강조한 바 있다. 이러한 맥락에서 보면 동남아 국가들이 화웨이를 선호하는 조치를 취한 행보를 이해할 수 있다. 태국은 2019년 2월 8일 5G 실증 테스트를 시작하면서 화웨이의 참여를 허용했으며, 말레이시아, 싱가포르, 인도 등도 화웨이 장비로 5G 테스트를 진행할 계획을 밝혔다.

이러한 사태의 전개는 2020년 후반기에 들어서면서 미중 간의 디지털 안보동맹 및 연대 외교의 경쟁으로 비화되었다. 특히 2020년 8월 폼페이오 미 국무장관은 중국으로부터 중요한 데이터와 네트워크를 수호하기 위한 클린 네트워크(Clean Network) 구상을 발표했다. 클린 네트워크 프로그램은 이동 통신사와 모바일 앱, 클라우드 서버를 넘어서 해저 케이블에 이르기까지 중국의 모든 IT 제품을 사실상 전면 금지하는 내용을 담고 있다. 미국민의 개인정보 보호 등을 위해 사실상 전 세계 인터넷 비즈니스와 글로벌 통신업계에서 중국 기업들을 몰아내겠다는 뜻이다(김상배, 2021b).

이에 대해 중국은 '글로벌 데이터 안보 이니셔티브'로 맞대응했다. 2020년 9월 왕이 중국 외교부장은 다자주의, 안전과 발전, 공정과 정의를 3대 원칙으로 강조했다. 데이터 안보에 대한 위협에 맞서 각국이 참여하고 이익을 존중하는 글로벌 규칙을 만들어야 한다는 것이었다. 이 구상은 데이터 안보와 관련해서 다자주의를 견지하면서 각국의 이익을 존중하는 글로벌 데이터 보안 규칙이 각국의 참여로 이뤄져야 한다고 주장했다. 아울러 일부 국가가 일방주의와 안전을 핑계로 선두기업을 공격하는 것은 노골적인 횡포로 반대해야 한다며 미국을 겨냥했다(김상배, 2021b).

이러한 과정에서 미국은 '클린(clean)'이라는 말에 담긴 것처럼 '배제의 논리'로 중국을 고립시키는 프레임을 짜려 하고, 중국은 새로운 국제규범을 통해 동조 세력을 규합해 미국 일방주의의 덫에서 벗어나려 하고 있다. 향후 바이든 행정부에서는 그러한 경쟁의 양상은 지속되는 가운데, 기술보다 가치를 강조하고 안보보다 규범을 강조할 것으로 예상된다. 실제로 바이든 행정부는 인권과 민주주의를 명분으로 동맹 전선을 고도화하여 국제적 역할과 리더의 지위를 회복하고 다자주의를 강조하고 있다. 개인정보를 보호하고 국가 기반시설 수호를 위해 다른 국가와 협력을 표명하며, '하이테크 권위주의'에 대한 대응의 차원에서 '사이버 민주주의 동맹'을 추진할 가능성이 크다. 이러한 미국의 공세에 대응하여 중국도 보편성과 신뢰성, 인권규범의 문턱을 넘어서야 한다. 보편 규범과 가치의 플랫폼 경쟁이 본격적으로 벌어지게 되는 것이다(김상배, 2021b).

3. 디지털 안보 거버넌스와 국제규범

디지털 안보 문제가 세계정치의 현안으로 부상하면서 다자외교의 장에서 국제규범을 마련하기 위한 논의도 한창이다. 1990년대 후반 이후 디지털 안보 분야의 규범형성 문제는 독립적 어젠다로 다루어졌다기보다는, 포괄적 맥락에서 본 글로벌 인터넷 거버넌스의 일부로서 취급되었다. 그러다가 2010년대에 들어서면서 사이버 안보의 전략적 중요성이 크게 부각되면서 국가행위자들이 나서 국제규범을 모색하는 양상이 나타났다. 이와 병행하여 우주안보, 자율무기체계 등과 같은 여타 디지털 안보 국제규범을 다루는 국제기구 차원의 논의도 진행되었다. 그럼에도 아직까지 디지털 안보의 규범에 대한 국제적 합의는 마련되지 않았으며, 오히려 최근에는 좀 더 복잡해지는 양상마저 드러내고 있다.

사이버 안보 국제규범은 국제기구나 국제법 차원의 논의뿐만 아니라 정부간 협의체나 지역협력체, 민간 행위자들이 참여하는 글로벌 거버넌스의 장을 빌어서 모색되었다(김상배, 2018a, 제9장). 최근 주목을 받는 것은, 2013년 이후 국제기구의 프레임을 빌어 사이버 안보의 국제규범을 마련하려는 시도였다. 이 중에서도 특히 제3차 유엔 정부자문가그룹(GGE)의 합의가 주목을 받았으나, 그 이후 2018년에 마무리된 제5차 GGE 회의에서는 합의문조차 도출하지 못했으며, 이러한 상황은 2019년 12월에 개최된 제6차 GGE에서도 지속되었다. 유엔 GGE의 틀을 빌어서 초국적이고 탈영토적인 사이버 위협에 대응하는 규범적 해법을 찾으려는 시도는 향후 당분간 그 활로를 찾기가 쉽지 않아 보인다.

유엔 GGE 활동이외에도, 2010년대에 들어서 서방 진영 국가들이 주도한 사이버공간총회나 유럽사이버범죄협약과 같은 정부간협의체 모델, 그리고 비서방 진영 국가들이 공을 들이고 있는 상하이협력기구와 같은 지역협력기구 모델이 사이버 안보 국제규범 논의의 전면으로 나선 바 있다. 이밖에도 서방 진영 국가들을 중심으로 이른바 사이버 안보 분야의 유사입장국(like-minded group) 회의가 지속적으로 열리고 있다. 좀 더 넓은 시각에서 본 글로벌 인터넷 거버넌스 분야의 규범 형성 노력도 간과해서는 안 된다. ICANN가 주도해 온 글로벌 인터넷 거버넌스 체제의 변환과 ITU의 새로운 관할권 주장의 과정에서도 사이버 안보의 국제규범을 모색하기 위한 움직임들이 진행되고 있기 때문이다(김상배, 2017).

현재 우주분야 규범화 논의는 사이버 안보의 경우와는 사정이 좀 다른데, 주로 유엔에서 우주개발 역량이 있는 선진국들을 중심으로 국제규범에 대한 논의가 진행됐다. 이 과정에서 아래로부터의 국제규범 형성 작업과 위로부터의 국제조약 창설 모색의 두 가지 트랙이 병행해서 진행되고 있다. 유엔 총회 산하에 우주 문제를 논의할 수 있는 위원회는 유엔 우주의 평화적 이용 위원회(COPUOS, Committee on the Peaceful Uses of Outer Space)와 유엔 군축회의(CD, Conference on Disarmament)가 있다. COPUOS는 지속가능한 우주환경 조성에 관한 방안을, 군축회의(CD)는 우주에서의 군비경쟁 방지를 위한 방안을 논의하고 있다. 이 과정에서 유엔의

여러 다자협의체에서 미국과 유럽의 서방 진영과 중 · 러 등의 비서방 진영 간의 이해대립이 첨예하게 벌어지고 있다(유준구, 2016).

COPUOS는 국제조약 채택을 주도하기보다는 국가 간 공동의 합의를 유도하는 방향으로 최근 선회하였으며, 이는 아래로부터의 공동합의를 통한 국제규범 형성을 모색하려는 서방 진영, 특히 미국의 사실상(de facto) 접근과 맥이 닿는다. 군축회의(CD)에서의 우주에 대한 논의는 일종의 위로부터의 국제조약 또는 국제우주법 모색의 논의로서 이해되며, 이는 중국과 러시아 등 비서방 진영이 주도하는 법률상(de jure) 접근과 맥이 닿는다. 이밖에 현재 우주 관련 국제규범의 형성 및 창설과 관련된 쟁점으로 논의되는 사항은 우주의 군사화·무기화, 자위권의 적용, 우주파편의 경감 등 위험요소 제거, 투명성 및 신뢰구축 등이 있으며, 각 쟁점들에서 각국은 자국의 이익을 반영하기 위해서 서로 다른 입장을 드러내고 있다(유준구, 2016).

자율무기체계의 전략적 함의가 커지면서 이 분야를 장악하기 위한 경쟁이 치열해질 뿐만 아니라 다른 한편으로는 자율살상무기, 이른바 킬러로봇에 대한 규범적 통제에 대한 논의도 출현하고 있다. 이러한 우려를 바탕으로 기존의 국제법을 원용하여 킬러로봇의 사용을 규제하는 문제가 논의되어 왔다. 예를 들어, 킬러로봇이 군사적 공격을 감행할 경우, 유엔헌장 제51조에 명기된 '자기방어'(self-defense)의 논리가 성립하는지, 좀 더 넓게는 킬러로봇을 내세운 전쟁이 '정당한 전쟁'인지 등의 문제가 논의되었다. 좀 더 근본적으로 제기되는 쟁점은 전장에서 삶과 죽음에 관한 결정을 기계에게 맡길 수 있느냐는 윤리적 문제였다(김상배, 2019a).

이러한 문제의식을 바탕으로 킬러로봇의 금지를 촉구하는 글로벌 시민사회 운동이 진행되고 있다. 예를 들어, 2009년에 로봇 군비통제 국제위원회(ICRAC, International Committee for Robot Arms Control)가 출범했다. 2012년 말에는 휴먼라이트와치(HRW)가 완전자율무기의 개발을 반대하는 보고서를 냈다. 2013년 4월에는 국제 NGO인 킬러로봇중단운동(CSRK, Campaign to Stop Killer Robots)이 발족되어, 자율살상무기의 금지를 촉구하는 서명운동을 진행했는데 2016년 12월까지 2천여 명이 참여했다. 이는 대인지뢰금지운동이나 집속탄금지운동에 비견되는 행보라고 할 수 있는데, 아직 완전자율무기가 도입되지 않은 상황임에도 운동이 진행되고 있음에 주목할 필요가 있다(김상배, 2019a).

이러한 운동은 결실을 거두어 2013년에는 23차 유엔총회 인권이사회에서 보고서를 발표했고, 유엔 차원에서 자율무기의 개발과 배치에 대한 토의가 시작되었다. 자율무기의 금지 문제를 심의한 유엔 내 기구는 특정재래식무기금지협약(Convention on Certain Conventional Weapons, CCW)이었다. 2013년 11월 완전자율살상무기에 대해 전문가 회합을 개최하기로 한 이후, 2014년 5월부터 2016년 12월까지 여러 차례 회합이 개최되었으며, 그 결과로 자율살상무기에 대한 유엔 GGE이 출범되었다. 한편, 2017년 8월에는 자율자동차로 유명한 엘론 머스크와 알파고를 개발한 무스타파 슬레이먼 등이 주도하여, 글로벌 ICT분야 전문가 116명(26개국)이 유엔에 공개서한을 보내 킬러로봇을 금지할 것을 촉구하기도 했다(김상배, 2019a).

Ⅵ. 맺음말

2019년 1월 다보스 포럼은 4차 산업혁명으로 인한 기술발달 문제를 '지정학적 위기'의 관점에서 볼 것을 제안한 바 있다. 오늘날 기술발달이 불균등 성장과 사회적 불평등을 심화시키고, 더 나아가 정치적 갈등과 지정학적 위기를 증폭시킬 수 있다는 문제제기였다. 실제로 4차 산업혁명 분야에서 벌어지는 선진국들의 경쟁은 이러한 불평등과 갈등 및 위기를 더욱 조장하는 방향으로 치닫고 있다. 특히 최근 벌어지고 있는 미중 패권경쟁의 양상은 기술 변수가 국가안보의 프레임으로 착색되면서 지정학적 위기를 낳을 조짐을 여실히 보여주었다. 이러한 문제의식을 바탕으로 이 글은 신흥안보와 복합지정학의 시각을 원용하여 4차 산업혁명 시대의 신흥기술 변수가 야기하는 안보 문제, 즉 디지털 안보의 세계정치를 살펴보았다.

지정학적 위기를 야기하는 디지털 안보의 이슈는 전통안보와는 다른 성격을 지닌다. 디지털 안보는 기본적으로 양질전화의 과정과 이슈연계의 메커니즘을 따라서 지정학의 임계점을 넘어서 창발하는 신흥안보의 이슈이다. 양적으로 늘어나고 있는 사이버 공격은 최근 전자전과 우주전, 사이버 심리전 등과 연계되면서 패턴변화를 보이고 있다. 최근에는 첨단기술과 보안제품의 수출입 통제, 민간 및 군사 분야의 데이터 안보, 민군겸용기술과 첨단 방위산업 분야의 경쟁 등도 상호 연계되어 발생하고 있다. 이러한 디지털 안보의 문제는 장차 군사안보 분야로 확대되어 실제 전쟁을 수행하는 문제로 촉발될 가능성이 있으며, 이러한 문제를 둘러싼 강대국들의 동맹과 연대외교 등과 관련된 지정학적 갈등의 대상이 될 가능성이 크다.

이러한 양상은 이미 미국과 중국이 첨단부문에서 벌이는 패권경쟁의 과정에서 나타나고 있다. 이 글은 이러한 미중경쟁의 양상을 전통적인 (고전)지정학의 시각뿐만 아니라 여타 다양한 국제정치이론, 특히 복합지정학의 시각을 원용하여 담아내기 위한 시도를 펼쳤다. 복합지정학으로 본 미중경쟁은 전통적인 자원권력론의 맥락에서 이해된 기술경쟁의 차원을 넘어서 디지털 안보 분야의 표준과 플랫폼을 장악하기 위해서 경쟁으로 발전하고 있다. 이러한 경쟁에 관여하는 주체도 전통적인 국가 행위자가 아닌 국가-비국가의 복합 행위자의 성격이 강하다. 이러한 경쟁의 결과로 출현할 세계질서의 모습도 전통 지정학이 상정하는 세력전이의 모습이라기보다는 좀 더 복합적인 공존의 질서일 가능성이 크다.

신흥기술과 디지털 안보 분야에서 벌어지는 미국과 중국의 복합지정학적 패권경쟁에 대응하여 한국은 앞으로 어떠한 전략을 펼쳐 나가야 할까? 우선, 양질전화의 과정을 통해서 창발하는 디지털 안보의 특성을 고려할 때, 각 분야별로 이에 대처하는 양적 · 질적 역량을 개발하는 과제가 제기된다. 넓은 의미에서 본 사이버 안보의 역량은 미래전뿐만 아니라 미래 국력경쟁 전반에서 중요한 의미를 갖는다. 강대국의 몫으로만 간주되었던 우주개발도 4차 산업혁명 시대를 맞

이하여 중견국으로서 한국이 역점을 두어야 할 분야가 되었다. 이들 디지털 안보 분야에서 선진 역량을 갖추기 위해서 기술개발, 인력양성, 제도개혁 등의 노력을 벌여야 할 것이다. 이러한 과정에서 한 가지 더 염두에 둘 것이 있다면, 디지털 안보의 양적 증대가 질적 위기로 치닫지 않도록 예방하는 신흥안보 거버넌스의 메커니즘을 갖추는 일이다.

둘째, 복잡한 이슈연계가 발생하는 디지털 안보의 특성을 고려할 때, 필요에 따라 다양한 이슈들을 '맺고 끊기'하는 포괄적이고 유연한 접근이 필요하다. 최근 기술과 안보의 문제는 통상과 데이터 및 산업의 이슈와 연계되고 더 나아가 군사와 외교 및 정치의 이슈와도 연계되는 양상을 보이고 있다. 디지털 안보 전략의 관점에서 볼 때, 이들 이슈를 적절히 연계하는 전략을 구사할 수도 있으며, 각 이슈들의 연계를 차단하는 전략이 필요할 수도 있다. 이러한 '연계'와 '차단'의 전략을 효과적으로 추진하기 위해서는 정부와 군, 그리고 민간의 다양한 행위자들이 협업하는 시스템을 설계하는 것이 중요하다. 이러한 맥락에서 오늘날 디지털 안보의 혁신모델이 종전의 '스핀오프'에서 '스핀온' 모델로 이행하고 있음을 명심할 필요가 있다.

끝으로, 향후 디지털 안보의 창발 과정이 지정학적 임계점을 넘어설 가능성을 인식하고 이에 대비하는 대응책을 마련해야 할 것이다. 무엇보다도 자율무기체계의 도입이 야기할 지정학적 지평의 변화를 정확히 이해해야 한다. 그러나 (고전)지정학적 측면에만 경도되지 말고, 다양한 변수들이 관여하는 복합지정학적 차원을 놓치지 말아야 할 것이다. 특히 최근 디지털 안보를 중심으로 발생하고 있는 동맹구도의 변화와 국제규범의 형성을 정확히 이해하고 이에 적극 참여하는 외교적 역량을 갖추어야 할 것이다. 더 나아가 디지털 안보 분야의 경쟁이 결과적으로 기존 국제질서의 전제가 되었던 관념과 정체성 및 윤리마저도 변화할 조짐을 보이고 있음을 알아야 한다(김상배, 2019c).

향후 디지털 안보의 미래전략을 추진함에 있어서 강대국들의 군사 · 안보 담론과 표준을 그대로 따라가지 않고 한반도의 안보환경에 맞는 담론과 표준을 개발하는 고민도 필요하다. 사실 4차 산업혁명이나 사이버 안보 분야에서 나름대로의 성과를 거둔 한국의 입장에서 볼 때, 이 글에서 살펴본 디지털 안보 분야는 다른 어느 분야에 비해서 나름대로 승산이 있는 분야라고 할 수 있다. 예전처럼 강대국이 주도하는 안보 패러다임을 수용하는 관행에서 벗어나 온전히 중견국의 입장에서 새로운 안보의 청사진을 그려봐야 한다는 문제제기에 힘이 실리는 것은 바로 이러한 이유 때문이다.

〈참고문헌〉

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

김상배. 2015a. "사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계."『국제 · 지역연구』, 24(3), pp.1-40.

김상배. 2015b. "사이버 안보의 미중관계: 안보화 이론의 시각."『한국정치학회보』49(1), pp.71-97.

김상배. 2018a.『버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국』한울.

김상배. 2018b. "트럼프 행정부의 사이버 안보 전략: 국가지원 해킹에 대한 복합지정학적 대응."『국제 · 지역연구』27(4), pp.1-35.

김상배. 2019a. "미래전의 진화와 국제정치의 변환: 자율무기체계의 복합지정학."『국방연구』, 62(3), pp.93-118.

김상배. 2019b. "화웨이 사태와 미중 기술패권 경쟁: 선도부문과 사이버 안보의 복합지정학."『국제 · 지역연구』28(3), pp.125-156.

김상배. 2019c. "사이버 안보와 중견국 규범외교: 네 가지 모델의 국제정치학적 성찰."『국제정치논총』, 59(2), pp.51-90.

김상배. 2020a. "코로나19와 신흥안보의 복합지정학: 팬데믹의 창발과 세계정치의 변환,"『한국정치학회보』54(4), pp.53-81.

김상배. 2020b. "데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각."『국가전략』26(2), pp.5-34.

김상배. 2020c. "4차 산업혁명과 첨단 방위산업 경쟁: 신흥권력론으로 본 세계정치의 변환."『국제정치논총』60(2), pp.87-131.

김상배. 2021a. "우주공간의 복합지정학: 전략 · 산업 · 규범의 3차원 경쟁." 김상배 편.『우주경쟁의 세계정치: 복합지정학의 시각』한울, pp.6-35.

김상배. 2021b. "디지털 플랫폼 경쟁의 국제정치경제: 미중 기술패권 경쟁의 진화,"『국제 · 지역연구』30(1), (2021), pp.41-76.

김치연. 2019. "미국, 중국에서 만든 5G장비 미국 내 사용금지 검토."『연합뉴스』, 6월 24일.

매일경제 국민보고대회팀. 2019.『밀리테크4.0: 기술전쟁시대, 첨단 군사과학기술을 통한 경제혁신의 전략』매일경제신문사.

송경재. 2019. "화웨이 규제 보복땐 中이 더 타격… 부품 막히면 퇴출될 수도."『파이낸셜뉴스』, 5월 17일.

송태은. 2019. "사이버 심리전의 프로퍼갠더 전술과 권위주의 레짐의 샤프파워: 러시아의 심리전과 서구 민주주의의 대응."『국제정치논총』59(2), (2019), pp.161-203.

유준구. 2016. "최근 우주안보 국제규범 형성 논의의 현안과 시사점."『주요국제문제분석』국립외교원 외교안보연구소. 1월 20일.

이조은. 2019. "미 상원, 인도태평양 사이버 연합체 '클립스' 설립 법안 발의…'북한 범죄 지속 가능성'." Voice of America, 4월 9일.

이철재. 2020. "전세계 경악시킨 이란 사령관 '드론 참수' · · · 이젠 떼로 공격한다."『중앙일보』. 1월 6일.

장원준 외. 2017. "4차 산업혁명에 대응한 방위산업의 경쟁력 강화 전략", 한국산업연구원, 12월.

정명섭. 2020. "美 육군, 중국 15초 동영상앱 '틱톡' 사용 금지... '사이버 위협 우려'."『아주경제』. 1월 2일.

주정민. 2019. "위성항법시스템과 국제협력." 우주복합공간의 미래전략 1차 간담회, 서울대학교 국제문제연구소. 9월 4일.

지상현, 콜린 플린트. 2009. "지정학의 재발견과 비판적 재구성."『공간과 사회』통권 1호, pp.160-199.

차대운, 2019. "中, IT인프라 부품 도입때 '국가안보위해' 심사 예고…美에 맞불."『연합뉴스』, 5월 25일.

최평천, 2019. "'첩보 위성급' 美글로벌호크 한반도 비행…15㎞ 상공서 감시."『연합뉴스』. 12월 11일.

한국항공우주연구원. 2019. "국내외 우주 산업 · 기술 동행과 정책 대안." 김세연 의원실.『이제 대한민국도 우주시대를 열자』11월 19일.

Castells, Manuel. 2000. The Rise of the Network Society. 2nd edition. Oxford: Blackwell.

Gilpin, Robert. 1981. War and Change in World Politics. Cambridge: Cambridge University Press.

Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." International Studies Quarterly, 53(4), pp.1155-1175.

Ikenberry, G John. 2014. "The Illusion of Geopolitics: The Enduring Power of the Liberal Order." Foreign Affairs, 93(3), pp.80-90.

Kurç, Çağlar and Stephanie G. Neuman. 2017. "Defence Industries in the 21st Century: A Comparative Analysis," Defence Studies, 17(3), pp.219-227.

Lieber, Keir A. and Daryl G. Press. 2017. "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence." International Security, 41(4),

pp.9-49.

Mead, Walter Russell. 2014. "The Return of Geopolitics: The Revenge of the Revisionist Powers." Foreign Affairs, 93(3), pp.69-79.

Ó Tuathail, Gearóid. 1996. Critical Geopolitics. Minneapolis, MN: University of Minnesota Press.

Organski, A.F.K. and Jack Kugler. 1980. The War Ledger. Chicago: University of Chicago Press.

Walker, Christopher and Jessica Ludwig. 2017. "The Meaning of Sharp Power: How Authoritarian States Project Influence" Foreign Affairs, November 16, pp.8-25.