Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.12.(발간일: 2025.2.3.)

데이터 안보의 복합지정학:

새로운 이론적 시각의 모색

김상배 서울대학교 정치외교학부 교수/ 미래전연구센터장

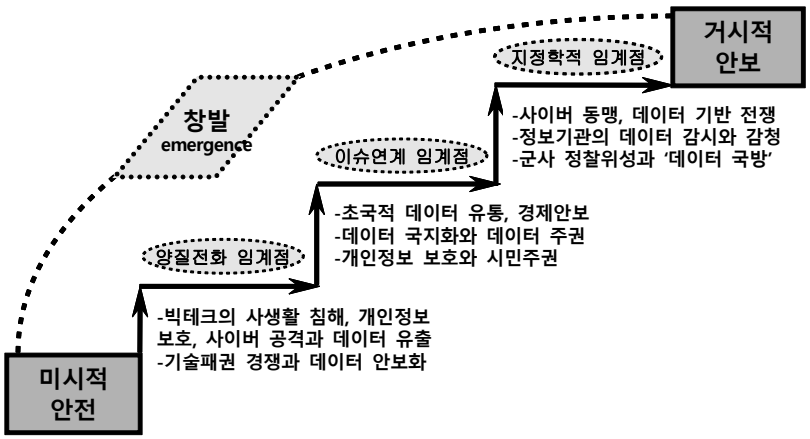
Ⅰ. 머리말

데이터의 국외 이전에 대한 논점이 이동하고 있다. 정치경제 관점에서 본 '데이터 주권'이 여태까지의 쟁점이었다면, 최근에는 국가안보 관점에서 본 '데이터 안보'가 관건으로 부상했다. 이러한 과정에서 두 가지 주장이 경합한다. 그 하나는 데이터가 중요하고 이는 국가안보 문제인데, 현재는 '데이터 안보불감증'이 만연해서 그 인식을 높여야 한다는 주장이다. 다른 하나는 국가안보를 거론하는 접근은 자칫 모든 걸 '안보 문제'로 환원할 우려가 있고, 이는 데이터 경제의 활성화를 저해한다는 논리다. 오늘날 안보 이슈가 확장되었고 데이터가 안보의 핵심 논제가 된 건 맞다. 그런데 모든 걸 다 국가안보의 렌즈로 보는 것 또한 문제다. 지금 거론하는 안보 문제는 전통적인 군사안보의 문제만은 아니기 때문이다. 데이터 경제뿐만 아니라 데이터 국방도 넘어서 데이터 안보를 보는 새로운 이론적 시각이 필요하다 (김상배, 2020).

오늘날 데이터 안보는 새로운 안보이론, 즉 '신흥안보(emerging security)'의 시각으로 봐야 하는 논제다(김상배, 2016). 신흥안보는 복잡계 이론에서 말하는 '창발(emergence)'의 개념에 기반을 둔다. '안보'와 합성어를 만들면서, '창발'보다는 좀 더 자연스러운 '신흥(新興)'으로 'emergence'를 번역했다. '창발/신흥'이란 미시적 안전의 문제가 양적으로 늘어나고 다양한 이슈가 연계되면서 임계점을 넘어서 거시적 안보의 문제가 되는 현

상을 개념화하기 위한 시도다. 자연계에서 발견되는 거대한 개미탑의 건축이나 새 떼의 군무 등과 같은 현상을 사회현상, 그중에서도 국제정치의 안보현상에 적용했다. 신흥안보로서 데이터 안보는 '양질전화(量質轉化)'와 '이슈연계(issue linkage)', 그리고 '지정학(geopolitics)'의 3단계 임계점을 넘어서 창발한다(〈그림 1-1〉 참조).

〈그림 1-1〉 신흥안보로서 데이터 안보의 창발



첫째, '양질전화'의 시각에서 보는 데이터 안보의 창발이다. 데이터 관련 이슈가 양적으로 늘어나면서 안보를 거론케 하는 질적 전화가 발생한다는 것이다. 미시적 차원에서는 개인의 '안전(安全)' 정도로 이해되던 데이터의 문제가 양적으로 증가하면서 집단의 '보안(保安)'과 관련된 성격을 띠게 되고, 더 나아가 거시적 차원에서 국가의 '안보(安保)'를 거론케 할 정도로 창발한다는 것이다. 실제로 개인정보의 유출 정도로 이해되던 데이터 안전 문제가, 그 양이 많아지고 대상이 다양화되면서 특정 조직의 데이터 보안 문제가 되고, 더 나아가 국가안보를 내세워 데이터의 국경 간 이동을 통제하는 문제가 되기도 한다. 게다가 이러한 데이터 안보의 양질전화 과정은 어느 순간에 돌발적으로 발생하는 '극단적 사건(X-이벤트)'의 형태로 나타나는 경우가 많아서 예측하기가 어렵다. 따라서 아직 발생하지 않은 안보위협을 주관적으로 구성하는 안보화(securitization)의 과정이 논란을 일으키기도 한다.

둘째, '이슈연계'의 시각에서 보는 데이터 안보의 창발이다. 데이터 관련 이슈가 다양한 여타 이슈들과 복잡하게 연계되면서 안보 이슈가 된다는 것이다. 단순한 양적 증가의 논의를 넘어서 이슈 간의 질적 연계가 본격화되는 넥서스(nexus)의 형성이 쟁점이다. 실제로 최근 데이터 안보 이슈는 공급망 안보와 같은 경제안보 이슈와 연계되고, 사이버 공간의 플랫폼 안보 이슈와도 밀접히 연계되고 있다. 데이터의 초국적 유통을 다루는 디지털 통상규

범의 형성 과정에서도 데이터 안보가 쟁점이다. 또한 데이터 안보는 사이버 안보의 핵심 관심사이며, 인공지능(AI)과 같은 첨단기술 안보 이슈와도 연계된다. AI를 활용한 인지전(cognitive warfare)의 부상에서도 핵심은 데이터 안보다. 이러한 이슈연계 메커니즘에 주목해야 하는 이유는, 이를 통해서 안보위협의 구조가 질적으로 변화하고, 그 결과로 위기 발생의 임계점이 하락하는, 그래서 안보위협이 더 쉽게 창발하는 현상을 낳기 때문이다.

끝으로, '지정학'의 시각에서 보는 데이터 안보의 창발이다. 최근 데이터 안보 이슈가 전통적인 국가안보로 대변되는 지정학적 임계점을 넘고 있다는 것이다. 오늘날 데이터 안보는 국가 간 동맹의 이슈가 되었고, 민주주의와 인권 등 이념과 가치를 둘러싼 진영 간 대립의 대상이 됐으며, 국제규범의 형성을 놓고 벌이는 경쟁의 이슈가 되었다. 또한 데이터 이슈는 국가 정보기관이 벌이는 디지털 첩보활동의 주요 사안이 되었으며, 군사안보와 관련된 지정학적 이슈의 경계 안으로 편입되고 있다. 예를 들어, 군사 정찰위성의 데이터 수집이나 국방 데이터 시스템의 구축 등에 대한 관심이 증대되었으며, 데이터 기반 미래전(戰)의 부상도 세간의 화두가 되고 있다. 이러한 '데이터 지정학'의 현상은 데이터 안보의 창발 과정에 역으로 영향을 미쳐서 잠재해 있던 위기의 발생을 촉진하기도 한다. 최근 발생한 우크라이나 전쟁이나 미중 패권경쟁의 가속화는 이러한 양상을 보여주는 대표적 사례이다.

이상에서 살펴본 데이터 안보의 복합지정학이 초래하는 변화에 제대로 대응하기 위해서는 무엇보다도 데이터 안보를 보는 시각을 새롭게 정비해야 한다. 다시 강조컨대, 안보를 논하지만, 전통안보와는 다른 속성을 지닌 신흥안보의 시각에서 문제를 볼 필요가 있다. 이러한 문제의식을 바탕으로 이 글은 크게 세 부분으로 나누어 데이터 안보의 복합지정학적 논점들을 정리하고, 동시에 이 책에 담긴 각 장의 내용을 요약 · 소개하였다. 특히 이 글은 민간 데이터 보호로부터 공공 데이터 보안으로, 그리고 국방 데이터 안보로 창발하는 복합지정학의 동학을 핵심 사례를 통해서 살펴보았다. 각 국면에서 제기되는 이론적 논제로서 '데이터 주권'과 '데이터 보안(또는 안보)', 그리고 '데이터 국방'에 주목하였다. 끝으로, 맺음말에서는 국가적 차원에서 제기되는 데이터 안보 전략의 과제를 간략히 짚어 보았다.

II. 민간 데이터 보호

1. 데이터 경제와 데이터 권력

플랫폼 경제의 시대를 맞이하여 기술 경쟁력 못지않게 데이터 경쟁력이 중요시되고

있다. 데이터 경쟁력은 단지 많은 '양(mass)'의 데이터를 갖는 것만이 아니라, 큰 '규모(scale)'의 제대로 처리된 데이터를 갖는 데서 비롯된다. '데이터는 산업의 원유'라는 비유에 빗대어 보면, '원유를 가진다는 것'과 '이를 정제해서 쓴다는 것'의 차이를 떠올릴 수 있다. 특히 플랫폼 시대의 데이터 경쟁력은 자발적인 참여자들이 지속해서 제공하는 데이터를 바탕으로 생성된다. 이 과정에서 해당 플랫폼이 보유한 데이터의 '네트워크 효과'가 발생한다.

국제정치학의 시각에서 볼 때, 이렇게 축적되는 데이터는 미래 국력의 원천이고 '네트워크 권력' 또는 '플랫폼 권력'을 구성하는 핵심이기도 하다. 이러한 데이터 권력은 일차적으로 GAFA로 대변되는 미국 빅테크 기업들이 행사하며 논란을 초래하고 있다. 특히 빅테크의 사적(私的) 권력으로서 데이터 권력은 사생활 침해 논란을 유발했다. 여태까지 구글(G)은 개인정보 무단 수집 논란. 아마존(A)은 고객 정보 무단 공유 논란. 페이스북(F)/메타는 2016년 케임브리지 애널리티카(CA) 페북 이용자의 정보를 트럼프 대선캠프에 지원했던 논란, 애플(A)은 위치정보 수집 논란 등의 중심에 섰다.

데이터는 미중 디지털 패권 경쟁의 대상이기도 하다. 데이터 경쟁력의 관점에서 볼 때 누가 앞서가고 있느냐가 쟁점이다. 그 현황을 보면, 구글, MS, 메타, 아마존, 애플 등과 같은 미국 빅테크가 앞서가고, 알리바바, 텐센트 등 중국 기업이 추격하고 있다. 그러나 미국의 플랫폼들이 이미 전 세계적으로 엄청난 영향력을 행사하고 있는 데 비해, 중국 플랫폼의 경우에는 틱톡이나 알리익스프레스 등과 같은 예외적인 경우를 제외하면, 해외 시장에서 아직은 제한적인 영향력만 행사하고 있다. 그런데 최근 전자상거래 분야에서 알리, 테무, 쉬인 등 이른바 '차이나 커머스'의 약진이 심상치 않다.

제2장 "데이터 경제와 데이터 권력"(서봉교)는 미국과 중국 플랫폼의 글로벌 경쟁력을 데이터 경쟁력의 측면에서 분석하였다. 기존의 연구는 플랫폼의 경쟁력을 참여자의 규모와 직결되는 네트워크 효과에만 주목하였기 때문에, 미국과 중국 플랫폼 경쟁도 양국의 데이터 확보 경쟁으로 인식되기도 하였다. 그러나 플랫폼의 경쟁 우위는 단지 데이터의 규모 경쟁이 아니라, 이 데이터를 효율적으로 활용하여 지속적으로 새로운 가치를 창출하는 혁신의 측면에서 창출된다. 첫째, 플랫폼은 자발적 참여자로 형성되기 때문에 참여자들에게 정보통신 기술의 발전에서 기인하는 혁신을 통해 지속적인 혜택을 제공하는 것이 중요하다. 둘째, 데이터 관련 디지털 인프라에 대한 투자를 통해 데이터 관련 비용 경쟁력을 확보해야 한다. 셋째, 데이터를 상업적으로 활용하여 수익을 창출할 수 있는 비즈니스 모델의 경쟁 우위가 중요하다. 넷째, 플랫폼의 혁신적인 비즈니스 모델의 수용성이나 국제결제, 데이터와 관련된 국제규범 등의 외부 경제환경의 경쟁력도 중요하다.

현재 미국 플랫폼은 국제 전자상거래, 소셜 미디어, 엔터테인먼트 등의 분야에서 글로벌 우위를 확보하고 있다. 하지만 중국의 플랫폼은 최근 동남아시아 등을 중심으로 해외 진

출을 적극적으로 추진하면서 글로벌 영향력이 확대되고 있다. 제2장에서는 이러한 중국 플랫폼의 데이터 경쟁력의 사례를 세 가지 측면에서 분석하였다. 첫째, 중국 플랫폼은 클라우드 인프라에 대한 대규모 투자를 통해 데이터 관련 비용 경쟁력을 높이고 있다. 둘째, 중국에서는 데이터의 상업적 활용에 대한 규범화가 진행되면서, 플랫폼이 맞춤형 광고 비즈니스를 통해 안정적인 수익 모델을 확보하였다. 셋째, 모바일 국제결제 영역에서 영국계 국제결제 솔루션 플랫폼인 월드퍼스트 인수, 중국 정부의 모바일 국제결제 제도환경 개선 등으로 외부경제 환경의 경쟁력이 높아지고 있다.

2. 데이터 거버넌스와 개인정보 보호

데이터 거버넌스와 개인정보 보호와 관련하여 각국은 서로 다른 법 · 제도와 이념을 갖고 있다. 최근에는 민간 기업이 다루는 데이터를 국가안보 차원에서 이해하는 경향도 부상하면서 이러한 차이는 더 복잡해졌다. 특히 해외 사업자의 국내 데이터 사업이나 자국 데이터의 해외 유출과 관련된 규범의 차이에 주목할 필요가 있다. 미중 디지털 패권경쟁의 맥락에서도 이러한 차이가 논란거리다.

미국은 개인 데이터를 수집하고 활용하는 데 있어 전통적으로 기업에 유리한 접근 방식을 취해 왔다. 미국은 국경 간 개인정보의 자유로운 이동을 허용하되, 오히려 자국의 안보를 위해 해외에 있는 데이터에 대한 접근권한을 강화하는 '자유유통 모델'을 채택하였다. 이에 비해 중국은 자국민의 데이터가 국경 밖으로 이전되지 못하도록 하는 규범체계를 채택하였으며, 예외적인 경우에만 허용하는 '국가통제 모델'이다. 이러한 정책과 제도, 규범의 차이는 미중 갈등의 소지를 제공하였다. 특히 2019년 오사카 G20 정상회의에서 미국과 중국은 데이터 초국적 이동과 데이터 국지화(localization) 문제를 놓고 설전을 벌이기도 했다.

미국형 자유유통 모델과 중국형 국가통제 모델 사이에, 데이터의 국외 이전 자체는 허용하되 국가가 정한 기준에 부합하는 경우에만 허용하는 유럽연합의 '상호적정성 모델'이 있다. 유럽연합은 개인정보 보호를 기본권 또는 인권의 시각에서 파악한다. 따라서 유럽 지역과 개인정보 보호 수준이 대등한 것으로 인정되지 않는 국가에 대한 유럽 시민의 개인정보 이전을 엄격히 제한한다. 예외적으로 정보 주체의 강력하고 명백한 동의를 획득한 경우에는 데이터의 국외 이전이 가능하다. 과거 한국은 국가가 사전에 개인정보의 국외 이전을 통제하지 않고, 전적으로 정보 주체의 동의에 의존하는 자유유통 모델을 취했지만, 최근에는 상호적정성 모델로 이행하였다.

제3장 "데이터 거버넌스와 개인정보보호"(김현경)는 여태까지 민간의 데이터 안보가 글로벌 경쟁 관계에 있는 기업 간 영업비밀 등 기업의 핵심 혹은 주요 전략 보호 차원에서

다루어져 왔다고 지적한다. 그러나 인공지능과 데이터를 기반으로 한 글로벌 플랫폼 기업이 국제경제에서 차지하는 영향력과 비중이 높아지면서 민간 기업이 보유하고 있는 '데이터' 역시 국가안보 차원에서 논의되는 경향이 있다는 것이다. 특히 개인정보는 자국민의 프라이버시권 · 개인정보자기결정권이라는 헌법상 기본권의 원천이 되므로 자국민의 기본권 보호 차원에서 개인정보의 국외 이전에 대한 관심이 고조되고 있다.

개인정보 국외 이전을 규율하는 유형은 국가의 개입 정도에 따라, 사적자치의 원칙을 우선시하는 '자유주의 모델', 이전 자체는 허용하되 국가가 정한 기준에 부합하는 경우에만 허용하는 '상호적정성 모델', 원칙적으로 국경 밖 이전을 허용하지 않되 지극히 예외적인 경우에만 허용하는 '국가통제 모델'로 나누어 볼 수 있다.

최근 '상호적정성 모델'을 채택한 유럽이 외국 정부기관이 유럽 개인정보에 접근할 수 있는 모든 위험을 '제거'하도록 요구하면서 많은 비유럽 기업은 유럽에 데이터를 국지화하는 이른바 '주권적 해결책(sovereign solutions)'을 실행하고 있다. 그러나 이러한 '위험 제로' 접근방식이 보안 친화적이며 실효적인지에 대해서는 의문이다. 그 이유로 우선 유럽의 데이터 컨트롤러 등은 종종 미국의 인적 관할권의 적용을 받으며, 미국 기업과 동일하게 역외 데이터 접근 요청에 직면할 수 있다. 또한 해외 정보기관이 데이터에 접근하는 방식은 반드시 기업에 강제적 요청을 통해서만이 아니라 자국의 기술적 수단에 의한 직접 접근 방식을 사용한다. 유럽의 데이터 프로세서들은 미국 등 외국의 인적 관할권에 속하는 것을 회피하더라도 해외 정보기관에 의해 '직접 접근'될 위험이 다분하다. 따라서 유럽에서 클라우드 서비스 제공자(CSP)에게 요구하는 '위험 제로' 요건의 충족은 궁극적으로 달성할 수 없는 것을 추구하고 있다고 볼 수 있다.

각 국가가 자국 내에서 데이터 활용의 기회 확대를 통해 국익을 극대화하고자 자국에 적합한 데이터 규범을 시행하는 것은 지당한 일이다. 한국도 무분별한 해외 벤치마킹이 아니라 국내 데이터 생태계에 대한 면밀한 분석을 전제로 한 합리적 규범의 마련이 필요하다.

3. 데이터 국제규범과 데이터 주권

최근 디지털 통상규범에 대한 논의는 소강상태이다. 다만 CPTPP, USMCA, USJDTA, DEPA, DEA 등과 같이 이미 체결된 디지털 통상협정에서 데이터 관련 쟁점으로 초국경 데이터 유통, 데이터 국지화 요구 금지, 소스 코드 공개 요구 금지, 인터넷 접근 및 이용 자유화, 인터넷 서비스 제공자(ISP) 책임 면제, 정부의 정보 공개, 암호화 기술을 사용한 ICT 제품 등이 제기되었다. 이들 안건에 대한 각국의 견해는 매우 다르다. 특히 데이터 국제규범 형성 과정에서 '데이터 주권'의 문제를 어떻게 이해할 것인가를 놓고 미국과 중국, 유럽연합

(EU)의 입장이 크게 대립한다.

최근에는 데이터 규범의 이슈가 경제적 시각에서 본 데이터 주권 문제로부터 국가안보 관점에서 본 데이터 안보 문제로 일행하는 경향을 보인다. 그 연장선에서 볼 때, 데이터 안보 관련 미국의 정책도 ICT 제품과 서비스의 데이터 안보 문제로부터 데이터 그 자체의 안보 문제로 변천하고 있다. 데이터 안보를 보는 정태적 프레임을 넘어서 좀 더 동태적인 프레임의 필요성이 거론되는 대목이다. 이러한 데이터 안보의 문제와 관련하여 최근 국내에서도 '클라우드 서비스 보안인증 제도(CSAP, Cloud Security Assurance Program)'가 주목을 받았다. CSAP는 공공기관에 안전성 및 신뢰성이 검증된 클라우드 서비스를 공급하기 위해 2015년에 만들어졌는데, 이것이 해외 사업자에 대한 시장 진입장벽으로 인식되면 논란이 되기도 했다.

제4장 "데이터 국제규범과 데이터 주권"(이효영)은 대표적인 데이터 안보 강화를 위한 정책 수단이라고 할 수 있는 데이터 국지화 조치에 주목한다. 이 조치는 자국민의 데이터가 역외로 이전되거나 역외에서 저장 · 처리될 경우 해당 데이터에 대한 통제권을 상실한다는 우려에서 비롯된다. 특히 데이터 국지화 조치는 국가안보의 관점에서 민감한 데이터에 대한 보호 수단으로서 신뢰할 수 없는 국가로부터 데이터 접근권을 제한하기 위해 도입되기도 한다.

빅데이터를 다루는 클라우드 컴퓨팅은 데이터를 인터넷상에 저장해 두고 인터넷에 접속만 하면 언제 어디서든 다양한 ICT 서비스를 활용할 수 있도록 하는 서비스인데. 자유로운 국경간 데이터 이전이 허용되는 환경에서 가장 효율적인 서비스가 제공될 수 있다. 이에 따라 데이터의 자유로운 국외 이전을 제한하는 데이터 국지화 조치는 클라우드 컴퓨팅 서비스 시장의 성장에 부정적인 영향을 줄 수 있다.

한편, 정부와 공공기관의 입장에서 볼 때, 클라우드 서비스의 활용을 위해 자국 밖에 저장한 자국민의 데이터에 대하여 외국 정부가 접근할 수 있다는 것은 리스크 요인이며 국가안보의 사안이다. 외국 클라우드 서비스 사업자들의 데이터센터에 정보를 저장할 경우 해당 정부의 열람 대상이 될 수 있다는 점이 특히 우려되고 있으며, 외국의 클라우드 서버에서 개인정보가 유출될 경우 구제받기 힘들다는 점도 우려된다. 결국 공공 데이터의 영역에서는 '공공이익' 및 '공공안전'의 관점에서 정책 방향성을 추구하고 외국이 통상현안으로 제기하고 있는 문제에 대하여 데이터 안보의 측면에서 대응할 필요가 있다.

4. 데이터 안보와 공급망 안보

데이터 안보와 공급망 안보 문제가 결합하여 지정학적 갈등에까지 이른 사례로는

2019년의 '화웨이 사태'를 들 수 있다. 중국 기업 화웨이가 5G 이동통신 장비에 숨겨놓은 백도어를 통해서 미국의 국가안보와 관련된 정보와 데이터를 빼갈지도 모른다는 논란이었다. 이후 사이버 및 데이터 안보 빌미로 화웨이에 대한 미국의 수출입 제재가 가해지기도 했다. 데이터 안보와 공급망 안보 결합의 또 다른 사례로는 중국 기업 DJI의 드론을 둘러싼고 펼쳐진 논란이 있다. 글로벌 상업용 드론 시장의 70%를 점유한 DJI가 자사 드론을 통해서 미국의 국가안보와 관련한 민감한 정보를 빼간다는 우려였다. 드론에 의한 밀수품 · 폭발물 · 무기 운송, 금지된 지역에 대한 악의적 목적의 정찰, 사생활 침해 등도 우려되었다. 최근에는 중국 기업인 ZPMC의 대형 항만크레인도 데이터 안보의 경계 대상이 되기도 했다.

중국계 기업 바이트댄스의 동영상 플랫폼 틱톡의 데이터 안보도 최근 큰 쟁점이다. 2024년 4월 미 의회는 1억 7,000만 명을 넘는 미국 내 틱톡 이용자의 성별, 거주지, 전화번호 등 개인정보가 중국에 유출돼 국가안보에 위협이 될 수 있다며 '틱톡 금지법'을 통과시켰다. 2025년 1월 19일까지 미국 기업에 매각하지 않으면 미국 내 서비스를 금지하겠다는 것이었는데, 이후 트럼프 행정부 2기에 접어들어 우여곡절을 겪고 있다. 이밖에 중국산 커넥티드카도 데이터 안보의 문제가 제기되었는데, 이전에는 중국산 자율주행차의 라이다(LiDAR)에 대한 데이터 안보 논란이 불거지기도 했다.

이러한 과정에서 한 가지 주목할 것은, 데이터 안보와 공급망 안보의 이슈가 동맹외교의 이슈로 비화되었다는 점이다. 화웨이 사태를 계기로 미국의 대응은 동맹 이슈가 되었는데, 미국의 정책에 파이브 아이즈(Five Eyes) 국가들이 동참하기에 이르렀다. 이후 사이버 동맹 전선의 균열 조짐도 발생했지만, 2019–20년 홍콩 사태와 코로나 사태를 겪으면서 재결속되는 양상이 나타났다. 또한 미국의 중국산 드론 규제에 대한 동맹국의 합류에도 주목할 필요가 있는데, 일본이 드론 공급망에서 중국산 배제를 고려한다고 발표하기도 했다. 이후 미국이 동맹국들에 '틱톡 금지' 행보에 동참할 것을 요구하여 EU, 캐나다, 일본도 퇴출 결정을 내린 바 있다. 이러한 조치들은 모두 데이터 안보와 공급망 안보 이슈가 일국 차원이 아닌 동맹외교의 차원에서 다루어지고 있는 사례들이다.

제5장 "데이터 안보와 공급망 안보"(유인태)는 미중 기술패권 경쟁 가운데, 첨단 디지털 기술의 공급망과 데이터 수집, 유출, 조작, 유포 등의 우려가 제기되는 과정에서 공급망 안보와 데이터 안보가 교차하는 양상에 주목하였다. 그런데 데이터 안보나 공급망 안보에 대한 연구는 각기 있었지만, 이 둘의 교차점에 초점을 맞춘 연구는 많지 않다고 지적한다. 여기서 다루는 데이터 안보 사안들은 정부뿐만 아니라 개인 혹은 민간 행위자들이 다루는 데이터들이 국가안보적 사안으로 전환되는 모습을 보인다. 이런 맥락에서 데이터 안보와 공급망 안보의 교차점은 더욱 특정화된다.

크게 두 가지 교차하는 방식으로 나눌 수 있는데, 한 부류는, 공급망 안보가 확보되지

않아, 데이터 안보가 우려되거나 침해되는 경우이며, 다른 부류는, 데이터를 겨냥한 사이버 공격으로 인해서 공급망 안보의 침해가 발생한 경우이다. 전자와 관련해서는 화웨이의 5G, ZPMC 항만 대형 크레인, 미래자동차의 핵심 기술 라이다, 중국산 DJI 드론, 틱톡의 사례들을 다루었다. 이러한 사례들의 의미를 부각시키기 위해 후자와 관련한 콜로니얼 파이프라인, 솔라윈즈 사태 등도 간략히 언급하였다.

제5장은 이러한 사례들의 발생에 대해 국가 차원에서 어떤 대응이 있는지 탐구하였고, 특히 어떤 나라들보다, 안보화하고 관련 대응책을 앞서 제시하고 있는 미국에 초점을 맞추었다. 대체로 행정명령을 통해 발 빠르게 대처하려는 모습과 사이버안보전략서 발간을 통해 전체적 노력을 체계화하고 있었다. 그리고 연방 예산안을 통해 공급망을 재편하려고 하였으며, NIST나 CISA를 통해 공급망의 데이터 안보 차원을 관리하기 위한 구체적인 표준, 규범, 규제를 설립해 나가고 있다.

Ⅲ. 공공 데이터 보안

1. 데이터 안보와 사이버 안보

최근 데이터 관련 사이버 공격은 해킹을 통해서 데이터를 탈취하는 방식에서, AI를 활용하여 데이터 자체를 조작 · 오염시키는 방식으로 변천하고 있다. 기존의 데이터 · 사이버 공격이 유무선 네트워크나 시스템, 단말기 등의 취약점을 공략하는 것이었다면, 새로운 공격은 AI 알고리즘에 내재된 취약점을 이용하는 방식이다. 새로운 데이터 · 사이버 공격은 AI가 머신러닝 과정에서 스스로 잘못된 판단을 하도록 유도하는 '적대적 공격(adversarial attack)' 방식을 취한다. AI가 부정확하거나 왜곡된 데이터를 학습하게 되면, 알고리즘의 오작동으로 이어지는 현상이 발생할 수 있다는 점을 이용하는 것이다. AI의 언어 구사 능력은 대규모 텍스트 데이터를 지속해서 학습하는 과정을 통해 갖춰진다는 점에서, 악의적 침투 가능성을 완전히 예방할 수는 없다. 이런 점에서 자연어 처리 기술을 활용한 AI 챗봇이 의도치 않게 적대적 공격의 대상이 될 위험이 있다.

최근 논란을 일으키고 있는 사이버 영향력 공작(influence operation)은 가짜뉴스나 허위조작정보 등을 생성하고 유포하여 심리적 교란을 노리는 사이버 공격인데, '소셜 엔지니어링' 공격으로도 불린다. 최근 사이버 영향력 공작이 AI와 데이터를 매개로 수행되면서 그 피해와 파장이 커지고 있다. 특히 생성형 AI 기술이 상용화되면서, '입력 데이터'에 대한 사

이버 공격의 범위를 넘어서, AI가 생성하는 '출력 데이터'가 가지는 사회적 영향과 관련한 새로운 안보 위협이 제기되었다. 대표적으로 AI가 생성한 데이터를 실제 데이터처럼 오인식하거나, 그렇게 인식하도록 악의적인 조작을 가하는 것이 가능해졌다. 말투, 어조, 음색 등의 면에서 AI가 인간에 버금가는 수준으로 언어를 구사할 수 있게 됨으로써 가짜뉴스와 허위조작정보를 생산하고 유포하는 수단으로 활용될 위험성이 커졌다.

'개인 데이터(private data)를 낚는다(fishing)'라는 의미의 피싱(phishing)과 AI의 결합은 큰 논란거리 중의 하나이다. 모든 사이버 공격 중에서 70% 이상을 차지하는 이메일 피싱은 생성형 AI의 출현 이후 더욱 증가하는 추세이다. 원래 피싱 수법은 정교하지 못한 언어 구사와 오타 등의 결함으로 인해서 그 효과가 제한적이었다. 그러나 최근 AI 기술을 활용하여 피싱 공격이 인간 행위자에 버금가는 수준의 자연어 능력을 갖추게 되면서 그 진위 분간이 어렵게 되었다. 생성형 AI를 활용해 인간이 작성한 것처럼 정교하고 설득력이 있고, 게다가 수신자별로 개인화된 피싱 이메일과 메시지를 대량으로 생성할 수 있게 된 것이다. 이외에도 AI를 활용한 음성 및 이미지 합성 기술을 통해 더욱 정교화된, 이른바 딥보이스(DeepVoice)와 딥페이크(DeepFake)의 파급력이 많이 늘어났다. 특히 딥페이크에 의해 조작된 영상 정보가 평판 저하나 신원 도용, 액세스 권한 탈취 등에 널리 활용되고 있다.

최근 AI 활용 영향력 공작은 개인과 조직의 권리나 이미지를 왜곡하는 수준을 넘어서 민주주의 체제 자체를 위협하는 요인으로 인식되고 있다. 정치적 목적을 달성하기 위해 감행되는 AI 활용 영향력 공작은 국가의 핵심 가치와 제도를 직접적으로 위협한다는 점에서 경계의 대상이 되었다. 더 나아가 이러한 위협의 확대는 이른바 '인지전(cognitive warfare)'이 새로운 전쟁의 양식으로서 부상하고 있다는 논의마저 촉발했다. 특히 AI를 활용하여 수행되는 인지전은 전시뿐만 아니라 평시에도 그 피해와 파장을 더욱 키울 가능성이 농후하다. 당장 러시아–우크라이나 전쟁에서 딥페이크 기술이 정치적 선동의 도구로 활용된 사례나 북한의 대남공작에 이와 관련된 AI 기술이 악용될 가능성을 어렵지 않게 떠올릴 수 있다. 또한 최근 중국의 AI 활용 영향력 공작이 중국과 갈등 관계에 놓인 국가들을 대상으로 이루어지고 있음에도 주목해야 한다.

제6장 "데이터 안보 이슈의 부상과 사이버 공격의 진화"(윤정현)는 오늘날 데이터가 경제·안보적으로 중요한 가치를 내재한 자원으로 인식되고 있다는 문제의식에서 출발한다. 특히 디지털 전환 사회에서 데이터는 필수 불가결한 자원으로 기능 중이다. 이와 같은 중요성 때문에 최근 데이터의 통제·활용 문제를 안보적 관점에서 다뤄야 한다는 주장이 제기되고 있다. 실제로 사이버 안보 이슈들을 살펴보면, 과거와 구별되는 특성들이 포착된다. 바로 데이터가 사이버 공간의 질서와 경쟁, 안보적 이해관계를 결정하는 주요 변수로 부상한 것이다. 그리고 이와 같은 흐름은 사이버 공간을 둘러싼 기술혁신과 주요 행위자의 변화 확장에

따라 더욱 가속화되고 있다.

동시에 데이터를 노린 사이버 공격 행위들도 진화하고 있다. 기술·군사 전문 집단을 노린 동시다발적 해킹, 군사기밀 정보 유출과 탈취, 삭제 등 '정보·데이터 무용화' 공격들이 대표적이다. 이제는 민간·개인정보 및 데이터의 조작, 오염, 영향공작 등 민간과 불특정 다중 이해관계자를 위협하고 사회공학과 결합된 공격 유형들도 중요한 고려 사안이 되고 있다.

이와 같은 환경변화에 따라 데이터를 둘러싼 접근 방식의 전환이 필요하다. 첫째, 사이버 공격의 진화가 보여주는 표적 대상에 대한 전환적 시각이다. 인프라 · 네트워크 · 소프트웨어 뿐만 아니라 비정형 개인정보 · 데이터에 대한 보호를 강화해야 한다. 둘째, 대응 주체로서 민간과 다중이해관계자를 포함한 다층적 거버넌스로의 전환이 필요하다. 셋째, 이 같은 복합적인 데이터 안보화의 메커니즘을 고려한 새로운 경쟁 구도에 대비해야 한다.

2. 데이터 안보와 인공지능 안보

데이터 수집 및 활용 역량의 핵심으로서 AI의 중요성이 주목받고 있다. AI를 활용하여 민감한 데이터가 의도적 · 비의도적으로 유출되어 악의적 세력에 활용될 경우, 국가안보뿐만 아니라 개인의 안전과 집단의 보안을 해칠 가능성이 우려된다. 특히 AI 기반 데이터를 활용하여 정치적 반대자를 억압하고 정치적 성향까지도 예측하고 조작할 가능성이 제기되면서 AI가 민주주의에 위협을 가할 위험성이 우려된다.

AI 기술을 사용하여 데이터를 무단 취합하여 정치적 감시에 활용할 가능성이 제기된 사례는 중국의 CCTV 감시망을 들 수 있다. 중국의 쑤저우(苏州)시는 CCTV를 활용한 이른바 천망(Skynet) 시스템을 도입하여, 감시데이터로 1초 만에 특정인을 식별할 수 있는 것으로 유명하다. 이에 미국 정부는 2017년부터 하이크비전, 다후아 등과 같은 중국 CCTV 업체들이 수집하는 데이터가 중국 정부로 유출될 수 있다는 의혹을 제기하였다. 미국 곳곳에도 설치된 중국산 CCTV에 찍힌 영상이 백도어를 통해 중국으로 유입된다는 의혹을 제기한 것이었다.

중국 기업들은 CCTV뿐만 아니라 안면인식이나 사람들의 버릇과 신체 특성 등을 고려해 특정 인물을 식별하는 AI 기술로도 유명하다. 중국 정부는 이를 데이터 감시도구로 활용하여 소수민족이나 반체제 세력을 통제하는 것으로 알려지면서 미국 간에 인권로 비화되었다. 2019년 10월 미국 정부는 인권 탄압과 미국의 국가안보 및 외교 정책에 반한다는 이유로, 중국 신장위구르 자치구의 불법 감시에 연루된 지방정부 20곳과 기업 8곳을 블랙리스트에 올렸는데, 여기에는 센스타임, 메그비, 이투 등 중국의 대표적 AI 기업들이 포함되었다.

최근에는 생성형 AI, 그중에서도 거대언어모델(LLM)이 초래하는 데이터 안보가 쟁점

으로 부상했다. AI 모델을 개발하고 이를 실제 서비스에 적용하는 과정은 여러 단계를 거쳐서 이루어지는데 각 단계에 모두 취약점이 존재한다. 따라서 효과적인 방어를 위해서는 모든 단계에 걸쳐서 안전한 AI 시스템 개발 및 운영에 대한 고려가 필요하다.

AI의 머신러닝 과정에서 발생하는 적대적 공격은 크게 두 가지 범주로 나누어 볼 수 있다. 그 하나가 데이터와 AI 모델을 추출하여 '기밀성'을 공격하는 방식이라면, 다른 하나는 데이터를 오염시키고 변조시켜 '무결성'을 공격하는 방식이다. 이러한 적대적 공격은 데이터 수집, 데이터 전처리, 모델 훈련, 모델 추론, 시스템 통합 등으로 구별되는 AI 시스템의 라이프 사이클 전체에 걸쳐서 발생한다. 특히 다음과 같은 네 가지 유형의 데이터 · 사이버 공격에 주목하고자 한다(유지연, 2024).

첫째, 데이터 '수집' 단계에서 감행되는 학습 데이터의 '추출 공격(inversion attack)'인데, 학습 데이터를 구축하는 단계에서 여러 차례의 쿼리를 하면서 AI 모델의 응답으로부터 거꾸로 학습 데이터를 추출하는 방식이다. 주소를 묻는 데서 시작해서 결국에는 아파트 동호수까지도 알아내는 방식으로 이해하면 될 것 같다.

둘째, AI 모델의 '훈련' 단계에서 악의적인 학습 데이터를 주입해 머신러닝 모델을 망가뜨리는 '오염 공격(poisoning attack)'인데, 이를 통해 AI 모델의 정확도를 낮추거나 오류를 유발하는 방식이다. 잘 알려진 데이터 오염 공격 사례로는 2016년에 마이크로소프트가 출시한 챗봇인 테이(Tay)를 유도하여 결국에는 인종 · 성차별적 발언을 쏟아놓게 한 사건이 있다.

셋째, AI 모델의 '테스트' 단계에서 데이터를 변조해 머신러닝을 속이는 '회피 공격(evasion attack)'인데, 입력값에 노이즈를 추가하여 AI 모델이 정확한 판단을 하지 못하도록 유도하는 방식이다. 이른바 '적대적 스티커(adversarial patch)'를 붙이는 방식이 잘 알려져 있는데, 사람의 눈으로는 구분되지 않는 약간의 노이즈만 추가해도 오류가 발생할 수 있다.

끝으로, 역공학(reverse engineering)을 이용해 머신러닝 AI 모델 전체의 추출을 시도하는 '모델 추출 공격(model extraction attack)'인데, AI 모델에 쿼리를 반복하면서 모델의 특징을 파악하는 방식으로 이해하면 된다. 이러한 시도를 통해서 아예 AI 모델 전체를 추출하려는 방식이라고 할 수 있다.

제7장 "데이터 안보와 인공지능 안보"(송태은)는 인공지능 기술은 이미 현대 전쟁의 무기체계에 본격적으로 적용되고 있다고 주장한다. 인공지능 기술의 정밀탐지 및 실시간 정보 분석 능력은 정보의 우위가 곧 전장의 우세이며 앞으로 미래전쟁의 승패는 화력에 앞서 정보전과 사이버전이 좌우할 것임을 예고하고 있다.

인공지능 기술은 국가안보와 직결되고 있고, 이러한 인공지능 기술의 기계학습 대상인 '데이터'는 궁극적으로 국가안보의 핵심적인 변수가 된다. 즉 '인공지능 기술을 보호하는

인공지능 안보'와 '데이터를 보호하는 데이터 안보'는 사실상 동일한 일이다. 인공지능의 성능을 보장하는 것은 데이터의 '규모'와 '질(quality)'이 되기 때문에 국가는 인공지능 기술의 발전을 결정짓는 학습 데이터를 확보하고 이 데이터가 오염되지 않도록 보호하고, 그러한 기술에 의해 생성된 데이터를 관리하고 보호하는 활동을 수행하게 된다. 또한 국가는 자국 개인의 정보를 보호해야 하는 동시에 자국 개인의 정보를 수집하여 인공지능 기술과 자국 산업의 발전을 도모해야 하는 이중적인 책임을 수행하는 위치에 놓여 있다.

아직 기술 발전 자체가 완성되지 않은 인공지능 기술 및 관련 데이터로부터 발생하는 다양한 문제는 아직 국가 및 국제사회의 통제 밖 문제가 아니다. 인공지능 기술을 개발하고 소유하고 있는 기업이나 국가는 기술 사용의 수단적 측면뿐 아니라 '책임 있는', '믿을 수 있는' 기술 사용의 목적 측면을 적극적으로 다룰 수 있는 관련 원칙과 규범을 구축해 나가기 위한 다양한 의제와 아이디어를 국가적으로 그리고 국제사회의 차원에서 지속적으로 발굴하고 제기해야 한다.

3. 데이터 안보와 우주안보

우주공간에서 생성되는 데이터가 국가안보에 미치는 영향이 매우 커졌다. 이러한 맥락에서 최근 다양한 수법의 해킹 공격을 통해서 위성 시스템을 교란하거나 무력화시켜 물리적 손실을 일으킬 우주 사이버 안보 위협에 관한 관심도 커졌다. 지상 시스템에 대한 사이버 공격도 큰 위협이다. 위성과 지상국 사이에서 주고받는 데이터는 그 생성과 송수신, 활용 등 각 단계에서 보안에 매우 취약하다. 특히 위성 정보 · 데이터의 탈취 · 손실 · 조작이 쟁점이 됐다. 전자기파 공격으로 인한 위성 전파의 방해 · 교란 · 변조도 위성 해킹과 맥을 같이 한다.

우주자산에 대한 의도적인 공격으로 인해 발생하는 안보 위협 외에도 군사 및 민간 인공위성에서 생성되는 정보 · 데이터 그 자체가 지니는 안보적 함의에도 주목해야 한다. 지구궤도 상에 떠다니는 지구관측 및 원격탐지위성, 통신위성, 글로벌항법위성 등은 다양한 데이터를 생산하고 이는 매우 중요한 군사적 · 경제적 · 사회적 가치를 창출한다. 군 정찰위성의 경우, 우주 기반 정보감시정찰(ISR) 자산과 군사위성을 이용한 미사일 발사 징후, 군부대 이동 및 해상의 군사활동 추적 등이 활용된다. 우주의 군사화라는 시각에서 볼 때, 정찰위성, 정찰기 활용 군사 정보 · 데이터의 수집은 전시뿐만 아니라 평시에도 전략적 우위를 창출하는 핵심역량이다.

민군겸용의 성격을 강하게 지니는 민간 위성의 영상 및 데이터 서비스의 안보적 함의도 매우 크다. 특히 우크라이나 전쟁은 군사뿐만 아니라 민간 우주 정보자산의 영향력을 새

삼 확인한 계기를 마련했다. 미국의 우주 자산을 활용하여 러시아군의 정보를 공개하고 러시아 침공 임박을 탐지했다. 민간 위성정보가 군과 정보기관 활동을 보완했다. 러시아의 맹공 속에서도 우크라이나 인터넷은 건재했는데, '스타링크'의 민간 우주자산이 중요한 역할을 했다. 맥사테크놀로지와 플래닛랩스 등 실리콘밸리 기업의 민간 위성 이미지 분석이 한몫을 담당했다. 미국의 지구관측위성 제작기업인 카펠라스페이스의 전천후 정찰 가능 위성영상레이더(SAR) 군집위성도 중요한 역할을 했다. 구글맵을 통해서는 러시아 전차부대의 진군, 우크라이나 피란민 행렬, 도로 폐쇄 상황 등도 실시간 파악했다. 이러한 정보와 데이터가 틱톡, 유튜브, 페이스북 등 SNS를 통해서 전세계로 전파된 것도 큰 변화다.

최근 위성항법시스템(GNSS: Global Navigation Satellite System)을 활용한 우주 기반 항법(PNT) 정보의 군사활동 지원 및 경제, 교통안전, 국토안보 관련 서비스 등이 큰 주목을 받고 있다. 또한 위성을 활용하여 지구의 관측 영상을 제공하고 데이터를 분석하는 서비스를 통해서 기상위성, 지구관측 위성의 날씨, 토지, 자연재해, 작물 수확량, 동물 서식지, 토지이용 변화 관측 등이 이루어진다. 위성정보는 환경 · 에너지 · 자원 · 식량안보 · 재난 등의 신흥안보 문제 해결에 이바지하는 필수요소이다. 특히 정밀한 위성 데이터는 사물인터넷, 빅데이터, 인공지능 딥러닝 등의 기술과 융합되어 다양한 분야에 정보를 제공함으로써 4차 산업혁명의 중요한 인프라를 형성한다.

제8장 "뉴스페이스 시대 우주안보와 데이터 안보 연계의 동학"(정헌주)은 지상으로부터 수백 혹은 수만 킬로미터 떨어진 우주공간에 있는 인공위성을 통해서 생성 · 수집되고, 전송되는 막대한 양의 데이터에 주목한다. 그 데이터는 그 자체로 혹은 분석 · 가공된 후 다른 데이터와 결합 · 융합되어 다양한 가치를 창출함으로써 국가안보와 경제발전, 환경문제 인식 · 대응에 매우 큰 영향을 미치고 있다. 무엇보다 우주 데이터는 군사적 · 안보적 측면에서 그 중요성이 커지고 있는데, 이는 대량살상무기 발사 징후, 실시간 상황인식, 정밀유도무기 운영, 효과분석 등 전장에서 우주 기반 데이터의 활용도가 높을 뿐만 아니라 (잠재적) 적국의 군사대비태세, 군사력 평가 등에 이용됨으로써 군사적 우위를 확보하는 데 결정적 역할을 하기 때문이다. 이러한 점에서 우주 데이터를 어떻게 수집 · 분석 · 활용할 것이며, 이를 보호할 것인가는 매우 중요한 안보적 차원의 문제로 부상하였다.

이러한 문제의식을 바탕으로 제8장은 우주 안보와 데이터 안보의 관계를 크게 세 가지 측면, 즉 우주 데이터를 활용한 안보(security by space data), 우주 데이터의 안보(security for space data), 우주 안보를 위한 데이터(data for space security)로 구분해서 각각을 살펴보았다. 특히 뉴스페이스 시대 민간 행위자의 우주활동이 증가하고 이에 따른 우주 데이터의 양이 급증하고 질적으로도 향상되는 맥락을 고려하여 우주 안보와 데이터 안보가 맺는 이러한 각각의 관계를 구체적 사례와 함께 분석하였다. 더 나아가 우주–데이터

연계 차원에서 한국의 현황을 살펴보고 정책적 함의를 도출하였다.

4. 데이터 안보와 정보기관 첩보

최근 데이터는 좀 더 본격적으로 국가정보기관이 벌이는 활동의 대상이 되었다. 이러한 현상을 데이터(data)와 첩보(intelligence)의 합성어인, '데이터 첩보(data intelligence)' 또는 '데이틴트(DATINT)'로 부를 수 있다. 데이틴트는 '데이터'에서 '정보(information)'를 추출하고, 그 정보에서 '첩보'를 추출하는 과정에서 발생하는 국가정보활동의 디지털 전환을 배경으로 출현한다. 이러한 관점에서 본 데이틴트는 AI 기반 테킨트(TECHIT)에 의한 오신트(OSINT)의 수집 · 처리 · 분석을 그 내용으로 한다.

첫째, 데이틴트는 스몰데이터를 넘어서는 빅데이터 시대의 도래를 기반으로 한다. 스몰데이터 시대의 첩보활동은 휴민트(HUMINT)를 기반으로 비밀스럽게 숨어 있는 데이터와 정보를 발굴하여 처리하는 작업이었다면, 빅데이터 시대에는 무수히 쏟아져 나오는 데이터와 정보 중에서 옥석을 가려내는 활동이 주를 이룬다.

둘째, 데이틴트는 테킨트, 그중에서도 AI를 활용한 첩보, 즉 '에이아인트(AIINT)'의 형태로 이루어진다. 예전에는 아무리 좋은 원천 데이터가 있어도 이 데이터에서 정보와 첩보를 추출할 기술이 없어서 불가능했을 일을, 이제는 머신러닝과 딥러닝을 바탕으로 개발된 AI 기술을 활용하여 예전에는 인간의 지적 능력으로는 할 수 없었던 분석 작업을 할 수 있게 되었다.

끝으로, AI를 활용한 데이틴트는 많은 부분에서 오신트(OSINT), 즉 공개출처정보에 대한 분석을 통해서 이루어진다. 특히 기존에는 안보 이슈로 다루어지지 않았던 민간 분야의 정보 · 데이터가 사이버 공간과 SNS의 오픈 플랫폼을 통해서 제공되고, 그 정보 · 데이터의 생성과 수집 속도와 질에 있어서 국가기관이 아닌 민간 행위자들이 중요한 역할을 담당하게 되었다.

데이틴트를 통해서 수집 · 분석 · 공유된 데이터 그 자체를 안전하게 지키는 것도 중요한 데이터 안보의 문제다. 이는 사이버 안보 활동과도 상당 부분 중첩된다. 데이터 유출을 방지하는 문제뿐만 아니라 데이터 안보 강화를 위한 암호 체계 구축, ICT 기기나 네트워크 장비의 공급망 안보 등 다양한 대응책이 필요하다. 더 나아가 데이틴트를 효과적으로 추진할 국가정보기관의 디지털 전환도 중요한 과제로 제기된다. 데이터 공유 플랫폼이나 민관협력 체계의 구축, 탄력적인 조직개편, 관련 법제도 정비 등이 쟁점이다.

제9장 "데이터 안보와 정보기관 첩보"(오일석)는 정보기관이 정보화와 지구화 및 비대면 사회에 적응하여 경쟁력을 확보하기 위해서는 디지털 전환을 실현하는 동시에 휴민트

(HUMINT), 테킨트(TECHINT) 및 오신트(OSINT) 사이의 유기적인 협력과 상호보완적인 관계를 구축 · 운영해야 한다고 주장한다. 이러한 다양한 정보활동의 대상인 동시에 수단이 되면서도 그 협력과 상호보완성의 교차점에 데이터 기반 정보활동, 즉 데이틴트(DATINT)가 자리잡고 있다. 정보활동의 수행으로 구축되는 결과가 데이터이며, 정보활동은 정확한 데이터를 적시에 확보하는 것이 기본이 되기 때문이다. 정보활동으로 생성된 데이터를 상호 비교 보완함으로써 더욱 가치가 있는 새로운 데이터도 생산할 수 있기 때문이다.

데이틴트는 크게 데이터의 처리에 기초한 수집 · 분석 · 공유 활동과 데이터 지배력 강화를 위한 데이터 보호 활동 및 데이터 공작 활동으로 나누어 볼 수 있다. 첫째, 정보의 처리 과정에 따른 데이터에 대한 수집 · 분석 · 공유 활동은 컴퓨터 네트워크 탐사, 사이버 공격, 인공위성과 드론, 오신트 활동 등을 통하여 이루어진다.

둘째, 수집 · 분석 · 공유된 데이터를 어떻게 보호할 것인지가 데이터 지배력 강화를 위한 정보활동의 중요한 한 축이라고 할 것이다. 데이터 보안 활동은 사이버 안보 활동과 상당 부분 중첩된다고 할 수 있다. 우선 네트워크 보안 활동이 중요하다. 이와 관련하여 클라우드 환경에서 데이터 보안과 활용을 확대할 수 있는 '제로 트러스트'로 패러다임을 전환할 필요가 있다. 데이터 보안을 위해 보다 강화된 암호 체계를 구축할 필요도 있다. ICT 및 사이버 안보 관련 하드웨어나 소프트웨어에 대한 공급망 안전성을 강화하여야 데이터에 대한 지배력을 확보할 필요가 있다.

끝으로, AI를 활용하여 데이터를 오염시킴으로써 특정 국가에 유리한 영향력이 발휘되도록 하는 데이터 공작이 활성화될 수 있다. 데이터 공작에 공세적으로 대응하기 위한 데이터 정보활동에 대해서도 관심이 필요할 것으로 보인다. 결국 데이터에 대한 지배력을 바탕으로 정보활동의 우위를 확보하기 위해서는 국가 간의 데이터 이전이나 데이터 공작에 대하여 정보기관이 관여할 수 있는 공간을 마련할 필요가 있을 것으로 보인다.

Ⅳ. 국방 데이터 안보

1. 국방 데이터 관리체계 구축

미래전의 승패는 고성능 AI 알고리즘과 이를 구동시키는 컴퓨팅 파워, 그리고 양질의 데이터에 의해서 갈릴 것이다. 그중에서도 양질의 국방 데이터를 확보하는 것은 우선적 과제가 아닐 수 없다. 무엇보다도 전략적 목적에 맞는 데이터를 구축하고 활용하는 것이 중요

하다. 현재 국방 분야에는 AI 알고리즘은 있지만 쓸만한 데이터가 없고, 있더라도 담당자가 그 데이터를 어디에 쓸지 모른다는 지적이 나오는 게 현실이다.

단순히 국방 데이터를 구축하는 것만큼 이를 효과적으로 다루는 국방 데이터 관리체계 구축도 중요하다. 다시 말해, 데이터의 품질관리만큼 표준화가 중요하다. 그런데 현재는 통일된 국방 데이터 아키텍처가 부재하다는 지적이다. 데이터가 기능별로 분절되어 있고, 플랫폼별 데이터 구조 등이 다르다. 특히 AI가 학습할 수 있는 형태로 레이블링이 된 데이터가 부족하다. 데이터 수명주기별로 데이터를 체계적으로 관리하는 것도 중요하다. AI 학습용 데이터 구축 및 공유를 위한 메타 데이터 표준화도 중요하다는 지적이 나오는 이유다.

국방 클라우드 구축도 중요한 문제다. 다원적인 센서를 통해 수집된 전장 데이터가 국방 빅데이터로 통합되어야 하는 것은 물론, 빅데이터가 전장 사용자에게 실시간으로 전달해야 한다. 이런 점에서 국방 클라우드는 전장 데이터의 수집과 저장 및 처리, 그리고 전장 빅데이터를 사용자(무기, 부대, 병력)에게 전달하는 문제를 해결하는 기반이다. 국방 클라우드 구축 방식으로는 중앙집중형 '데이터 레이크' 이외에도 '데이터 패브릭'이나 '데이터 메쉬' 등과 같은 분산형 또는 메타형이 거론되고 있다.

이러한 과정에서 많이 지적되는 것이 국방 분야 데이터의 저장 · 공유 · 협업을 위한 보안 문제의 개선이다. 비밀로 분류된 데이터는 따로 관리되며, 보호기간이 지나면 파기되도록 구조화되어 관리가 부족한 실정이다. 민감한 데이터 비식별화, 합성데이터 생성, 국방 데이터 보안 등급 관리 등도 중요한 과제다. 이러한 과정에서 개방과 폐쇄의 적절한 조화가 필요하다. 이를 위해서는 데이터 개방과 공유를 위한 문화 조성 및 제도 개선 등이 필요하다. 이밖에 민군협력을 바탕으로 한 데이터 구축과 분석 플랫폼 구축 및 기반 환경의 마련도 필요하다.

제10장 "지능화 전장 시대 국방 데이터 관리체계구축: 데이터 축적 · 운용 플랫폼 발전을 중심으로"(배학영)는 국방 분야 데이터의 민감성을 고려하여 국방 데이터는 국방부에서 따로 추진하고 있다고 지적한다. 국방부 최초의 데이터를 인공지능의 관점에서 접근한 것은 '국방 인공지능 추진 전략(2020년 12월)'이 발표되면서이다. 이후 국방부에서 '국방 데이터 관리 및 활용 활성화 훈령(2021년 12월)'을 제정하여 데이터의 생애주기별 관리 및 활용 방안 등 정책적 근거 마련하였다. 이후 '인공지능 추진전략 2.0(2022년 1월)'을 수립하고, 국방 분야 AI 정책의 기본지침을 제공하고 국방부 · 합참 및 각 군의 중장기 AI 정책 추진의 기준을 마련하였다.

2022년 국방 데이터 발전의 핵심인 '제1차 국방데이터관리위원회(2022년 12월)'가 국방부 차관 주관으로 열리면서 국방 데이터만을 위한 정책 방향을 공유하였다. 실제 데이터 관리를 위한 기관으로 2023년 1월 30일에 '국방데이터분석센터'를 한국국방연구원

(KIDA)에 신설하고 2024년 4월 국정과제 및 '국방혁신 4.0' 과제 중 하나로 국방과학연구소(ADD) 내에 '국방AI센터'가 신설되었다. AI 등 첨단과학기술 기반 국방력 혁신을 목표로 AI 소요기획 · 모델 개발 및 핵심기술 확보, 사업 수행을 위한 전담 업무 수행 중이다. 플랫폼, 표준 · 품질, 보안 · 권한권리, 분석 · 서비스, AI 학습 데이터, 방산 데이터로 나누어 발전 방향을 제시하였다.

지능전 시대에서 데이터는 전략적 자산이며 실제 그렇게 인식되고 관리되어야 한다. 데이터는 단순한 정보의 집합이 아닌, 국방과 안보 분야에서 우위를 확보하기 위한 핵심적인 요소로, 데이터의 수집, 처리, 분석 및 활용 전반에 걸쳐 전략적으로 관리되어야 한다. 그래야만 지능화된 전장에서 전략적 의사결정을 지원하고, 작전 수행의 효율성을 극대화하는 데 기여할 수 있다. 이러한 관점에서 국방 데이터의 가치와 중요성을 재평가하고, 데이터 기반의 의사결정 시스템을 강화함으로써 미래 전장에서의 우위를 확보하는 것이 중요하다.

2. 데이터 기반 국방 서비스 확산

국방 전 영역으로 데이터 기반 서비스가 확산하면서 데이터 기반 군수, 인사, 정비, 보급, 복지, 공급망 및 재고관리, 인력의 효율성, 정책 등에 걸쳐서 다양한 논의가 진행되고 있다. 특히 군수혁신의 차원에서 본 데이터 기반 운영유지는 데이터를 활용한 정비예측, 공급망 및 재고관리, 인력 효율성 제고, 가동 중지시간 최소화 등에 있어서 획기적인 효과를 거둘 것으로 기대된다. 이러한 과정에서 '디지털 트윈'은 데이터 기반 군수관리 체계의 혁신 기반을 제공하는 대표적인 사례 중의 하나다.

데이터 중심 국방 상호운용성의 발전 차원에서 국방 데이터 분야 한미 협력에 대해서도 고민이 필요하다. 육 · 해 · 공뿐만 아니라 우주 · 사이버 공간을 포함하는 다영역작전을 수행함에 있어서 한미 동맹 간의 상호운용성이 중요한 문제로 부상한 가운데, 사이버 동맹나 우주동맹 등에 대한 논의와 함께 한미 데이터 동맹도 고민해 볼 문제가 아닐 수 없다. 특히 국방 데이터 주권의 관점에서 볼 때, 무기체계와 관련된 데이터뿐만 아니라 AI 알고리즘의 기반이 되는 데이터를 한미 양국 간에 얼마나 공유하고 제공할 수 있는지의 문제가 향후 동맹 협력을 진행해 나가는 쟁점이 될 것이다.

제11장 "데이터 기반 국방 서비스 확산: 데이터 군사혁신의 과제"(윤대엽)는 빅테크 기업의 데이터 혁신 요인에 대한 분석을 통해 빅데이터 기반 국방체계 구축과 데이터 군사혁신의 과제를 역사적 · 비교적 시각에서 검토하였다. 4차 산업혁명 기술의 무기화를 위한 군비경쟁이 본격화되면서 빅데이터 기반 국방체계 구축이 추진되고 있다. 빅데이터는 클라우드와 함께 인공지능 지원 자율무기와 군사체계를 구축하는 핵심 기반이다. 역사적으로 디

지털 기술과 네트워크 혁신은 군대가 주도했다. 핵 군비경쟁의 우위를 위해 연구개발된 감시정찰, 무기체계는 디지털 기술을 혁신했고, 무기체계의 지휘통제를 실시간으로 연결해야 하는 목적에 따라 C2–C3–C4ISR 등의 지휘통제 체계가 구축되었다. 그러나, 디지털 플랫폼에 기반하여 데이터를 축적하고 이를 활용하는 데이터 혁신에 있어서는 빅테크 기업이 선도했다.

그러나 디지털 네트워크를 빅데이터 기반으로 활용하는 데이터 군사혁신에 있어서는 빅테크 기업이 오히려 추격자가 되었다. 인공지능 기반 무기체계와 군사체계 구축에 있어 클라우드와 빅데이터 기반 구축이 필요하다는 점에서 빅테크는 데이터 군사혁신에 함의를 제공한다. 디지털 기술과 네트워크 혁신을 선도했던 군대가 플랫폼 기반 빅데이터 전환의 후발주자가 된 것은 감시–정찰 체계의 하드웨어 기반 네트워크가, 육해공 사용자 간의 폐쇄적, 경직성에 따라 플랫폼화가 지체되었으며, 이 때문에 다양한 사용자의 상호운용적인 데이터를 공유하는 유저인터페이스의 혁신이 부재했기 때문이다.

인공지능의 기반으로서 데이터 군사혁신을 위해서는 보안성, 폐쇄성과 상호보완적인 데이터 군사혁신 목표가 추진될 필요가 있다. 첫째, 비대칭 억지력의 기반으로서 데이터 군사혁신이다. 데이터의 신뢰성, 보안성을 우선해야 하는 군사체계의 특성상 데이터의 신뢰성, 군사적인 효과성에 우선하여 데이터 군사혁신 목표가 추진될 필요가 있다. 이미 제한적으로 OODA 루프의 자동화 체계(automated system)가 구축되어 있는 3축 체계가 우선적인 대상이 될 수 있다. 아울러 데이터 군사혁신을 위해서는 군–빅테크의 협력과 함께 동맹의 데이터 상호운용성을 위한 과제도 검토될 필요가 있다.

3. 데이터 기반 지능형 통합체계 구축

데이터 기반 지능형 통합체계 구축을 위한 노력은 대략 네 단계로 나누어 진행되고 있는데, 1) 초연결 네트워크 및 데이터 관리 등 통합환경 구축. 2) 공통된 전장인식 및 전 영역 실시간 전장가시화. 3) 인공지능을 활용한 지휘결심체계 구축. 4) 유 · 무인 복합전투체계 등 첨단기술 전력의 효과적 운용 등이다. 이러한 체계의 도입을 통해서 궁극적으로 전력 운용 효과의 극대화가 추진된다. 이러한 데이터 기반 지능형 통합체계 구축을 보여주는 대표적 사례가 최근 미국이 추진하고 있는 합동전영역지휘통제(JADC2, Joint All–Domain Command and Control)이다.

JADC2는 합동 전장정보를 활용하여 실시간 전장을 가시화하고, 인공지능 기반의 지휘결심체계를 통해 효율적인 전력 운용을 보장함으로써 전 영역에서 우세 달성을 위한 차세대 지휘통제의 개념이다. JADC2는 지상, 해상, 공중, 우주, 사이버 등 전 영역 공간에서 센

서들을 연결하고 데이터를 실시간으로 공유해서 전체 합동전력의 통합 운용능력을 향상시키고, 결심과정 시간을 최소화함으로써 미래 지휘통제체계 능력을 확보해서 전장우위를 달성한다. JADC2 체제 구축을 위한 노력은 데이터 표준화. 연결성 증진. 데이터 체계 통합. 데이터 보안 강화 등과 같은 활동을 핵심으로 한다. JADC2는 미 공군이 추진해 온 다영역지휘통제(MDC2)가 합동 수준으로 채택되어 발전된 것으로 현재 미국 미래전 수행체계의 핵심이 되고 있다.

제12장 “미래전과 데이터 기반 지능형 통합체계 구축: 미 합동전영역지휘통제(JADC2) 사례 분석을 중심으로”(설인효)는 미중경쟁이 치열하게 전개되면서 군사 분야에서는 미래전을 둘러싼 군사혁신 경쟁도 본격화되고 있음을 지적하였다. 인공지능 기반 군사혁신은 알고리즘 발전을 위해서도, 인공지능이 활용할 정보의 확보와 환류를 위해서도 데이터 기반 체계 구축이 선행되어야 한다. 지난 수년간 지속된 인공지능 군사혁신 논의는 그 첫 단계로 데이터 기반 지능형 통합체계 구축으로 수렴되고 있으며 미국의 합동전영역지휘통제 추진 노력은 이러한 과정을 잘 보여준다. 데이터 기반 체계 구축에는 방대한 예산이 소요되고 광범위한 조직의 저항이 발생하며 상당한 시간이 소요된다. 과거 수십 년간 군별, 기능별로 발전해 온 정보체계를 하나의 통합체계에 연동하고 정보의 표준화를 추진하는 것은 지난한 과정이다.

미국은 이러한 과정을 효과적으로 추진하기 위해 국방부 및 합참 차원에서 지속적으로 확고한 의지를 표명하고 선도군을 중심으로 문제 식별 및 성공 사례를 발굴하는 등 다양한 접근법을 취해왔다. 특히 영역 및 업무별로 상대적으로 경험이 많고 앞선 군에게 해당 업무를 부여하고 주도하게 하여 군 간 선의의 경쟁을 유발하고 선행 사례를 통해 문제를 예견하고 대처하게 한 것은 주목할 만하다. 한국군은 향후 세계적 군사표준으로 부상할 인공지능 기반 군사혁신을 수용, 발전시키는 과정에서 데이터 기반 체계 구축의 중요성을 확고히 인식하고 이 단계의 고유한 속성과 도전을 명확히 이해할 필요가 있으며 미국의 사례에서 얻을 수 있는 교훈을 활용하여 체계적인 혁신전략을 수립해 나가야 한다.

Ⅴ. 맺음말

기술경쟁이 지정학 경쟁의 시각에서 이해되는 시대가 되었다. 과거 지구화 시대처럼 과학기술 담당 실무부처의 국제협력 업무 정도로만 과학기술외교를 대하던 시절은 지났다. 마찬가지로, 외교안보 부처에서 기왕에 담당했던 과학기술 관련 협정 체결이나 국제기구 활동 정도로만 볼 일도 아니다. 최근 지정학 환경의 출현으로 인해서 이제 과학기술외교는 국

가 간 갈등을 관리하고 분쟁을 조정하는 지정학적 권력경쟁의 핵심 사안이 됐다. 게다가 신흥기술 분야를 중심으로 해서 미국과 중국이 벌이는 경쟁의 최근 양상을 보면, 실제로 제기되는 객관적 안보위협에 대응하는 수준을 넘어서 미래의 상황을 미리 상정하고 주관적으로 안보위협을 구성하는 '안보화(securitization)'의 양상이 나타나기도 한다.

이러한 시각에서 볼 때 최근 반도체, AI 등과 함께 주목을 받는 중요 주제 중의 하나가 데이터이다. 그러나 산업의 원유라는 별명을 얻으며 각광의 대상이 된 데 비해, 데이터 대한 기존 학계의 연구는 많이 진행되지 않아 아쉽다. 이 글은 신흥안보의 시각에서 본 데이터 안보 연구에 초점을 두었다. 사실 기존의 연구는 '데이터 경제' 연구와 '데이터 국방' 연구의 중간지대에 자리 잡은 공공데이터의 보안/안보 연구를 등한시해 왔다. 이런 맥락에서 이 글은 복합지정학의 시각에서 데이터 안보와 관련된 어젠다를 개발하고 이 이면의 동학을 분석하여 향후 연구를 위한 플랫폼을 마련하고자 하였다.

미중 경쟁의 사례 중의 하나가 데이터 안보 문제이다. 2024년 2월 21일 바이든 대통령은 데이터 안보와 사이버 위협을 이유로 중국산 항만크레인을 규제하는 행정명령에 서명했다. 26일에는 유전자 · 위치 정보 등 미국인의 민감한 개인정보가 중국 등 적대국으로 이전되는 것을 금지하는 행정명령에 서명했다. 29일에는 중국의 '커넥티드 카'가 미국에 안보위협을 초래하는지 조사하라고 지시했다. 또한 2023년 12월에는 중국산 자율주행차 센서장비 라이다(LiDAR)가 데이터 유출 시비의 표적이 되기도 했다.

한편, 수년 전부터 개인정보 유출 논란이 있었던, 중국 바이트댄스의 동영상 플랫폼 틱톡의 미국 내 유통 금지법이 2024년 3월 13일 미 하원을 통과했다. 2023년부터 중국 전자상거래 플랫폼인 테무와 쉬인도 개인정보 관리와 사이버 안보 문제로 경계 대상이 되었다. 더 거슬러 올라가면, 제일 큰 사건은 중국 화웨이의 5G 이동통신 장비를 둘러싸고 터졌다. 중국산 드론과 감시용 CCTV를 통한 데이터 유출이나 안면인식 AI를 활용한 감시 · 통제도 쟁점으로 불거졌다. 이외에도 네트워크에 연결된 거의 모든 중국산 제품에 '백도어'가 있다는 의심이 끊임없이 제기되었다. 향후 생성형 AI의 '딥페이크'도 초유의 데이터 안보 문제를 야기할 것이고, 인공위성의 정보 · 데이터도 새로운 안보 논란을 일으킬 것으로 예견된다.

빅데이터 세상에서는 국가안보와 무관해 보이는 민간 데이터의 안전 · 보안 문제가 언제든 지정학적 안보 문제로 '창발(emergence)'할 수 있다. 이러한 시각에 근거하여 미국은 중국산 제품의 수입규제에서 서비스의 사용금지로, 그리고 개인정보 · 데이터 자체의 이전금지로 '안보화'의 전선을 확대 · 심화하고 있다. 미국 정부가 국가안보라는 시장 외적 잣대를 동원해서 중국 기업들의 기술추격과 미국 시장 진입을 견제한다는 비난도 없지 않다. 그러나 중국으로의 데이터 유출 그 자체가 미국에 큰 자원손실이자 안보위협이 되는 것은 사실이다. 중국이 국가주권 논리를 내세우며 이미 인터넷상의 장벽을 세운 마당에, 미국마저도

국가안보 논리에 기대어 데이터 유통을 통제한다면, '반쪽인터넷(Splinternet)'의 세상이 현실화될 수도 있다.

한국의 전략적 고민도 깊어질 수밖에 없다. 실제로 한국은 이미 미중 5G 갈등의 와중에 화웨이 장비 도입 문제로 몸살을 앓았다. 국내에 들여온 중국산 드론의 정보 유출이 우려되면서 그 사용을 배제했고, 중국 서버로 연결된 CCTV의 백도어 위험성도 심각하게 거론되었다. 최근에는 기상청에 납품된 중국산 기상관측장비에서 악성코드가 발견되기도 했다. 중국산 크레인도 국내 항만의 절반가량을 장악하고 있다. 한국에서 틱톡은 아직 큰 소란을 일으키진 않았지만, 알리익스프레스와 테무, 쉬인 등 중국 전자상거래 플랫폼의 개인정보 관리 부실은 분란의 소지를 안고 있다. 가성비 좋은 중국산 제품 · 서비스를 사용할 것이냐, 아니면 동맹국인 미국의 안보 우려 기조에 동조할 것이냐를 놓고, 기술 · 경제적 선택이 아닌 안보 · 외교적 결정을 내려야 할 상황이 언제 닥칠지 모른다.

데이터를 안보 · 외교의 시각에서 보는 인식의 제고가 필요하다. 여태까지 한국은 국가가 개인정보 국외 이전의 안전성을 보장하지 않고, 정보 주체의 동의에 의존해서 개인에 위험과 책임을 부과하는 기조를 취해왔다. 국가가 나섰더라도 경제적 관점에서 데이터 주권을 거론하는 정도였다. 그러나 이제는 개인정보 · 데이터의 국외 이전을 새로운 안보의 프레임으로 봐야 하는 세상이 되었다. 게다가 데이터 안보는 미중 두 강대국 사이에서 한국이 고민할 동맹외교의 사안으로 부상했다. 새롭게 전개되는 '데이터 지정학'의 지평 속에서 안보 · 외교의 숨은 코드를 읽어내는 국가적 혜안이 필요한 때다.

'국가 데이터 전략'의 연장선에서 본 '데이터 안보의 국가전략'이 필요하다. 데이터 안보 전략의 추진체계 정비도 큰 과제다. 신흥안보 전략의 컨트롤타워 가동 차원에서 좀 더 적극적으로 데이터 안보 이슈를 챙겨야 할 뿐만 아니라. 여러 부처의 업무를 조정하는 '메타거버넌스(meta governance)'의 역할도 발휘해야 한다. 외교 전담 부처도 데이터 안보 이슈에 좀 더 적극적으로 접근할 필요가 있다. 데이터 경제 관련 실무부처에서도 단순한 국제협력의 차원을 넘어서는 '데이터 외교'의 발상이 필요하다. 데이터의 국외 이전 이슈와 관련해서도 유연하고 개방적 발상을 갖는 것도 중요하다. 더 나아가 새롭게 펼쳐지는 데이터 안보 세계질서의 지평에서 중견국으로서의 한국의 외교적 리더십을 발휘할 기회도 놓치지 말아야 할 것이다.

이 책은 2024년도 서울대학교 미래전연구센터의 총서 제11권 프로젝트의 일환으로 기획되어 진행한 연구의 결과물이다. 이 책에 실린 글들은 2023년 11월부터 2024년 1월에 미래전연구센터에서 개최한 특별세미나를 바탕으로 연구의 방향을 정리하는 과정에서 구상되었다. 당시 세미나에 참여하여 발표해 주신 이 책의 필자를 포함한 여러 전문가께 감사의

말씀을 전한다. 이후 특별세미나 참여자를 근간으로 하고 몇 명의 필자를 추가로 더 모셔서 프로젝트팀을 구성했고, 2024년 1학기 미래전연구센터에서 개최하는 미래군사전략과정 세미나에서 그간 작업 중이던 원고들의 중간발표회를 진행하였다. 2024년 9월 6일(금) "데이터 안보의 복합지정학: 신흥안보론의 시각"이라는 제목으로 개최된 2024년 정보세계정치학회 추계대회에서 최종원고가 발표되었다. 최종발표회 직후 2024년 하반기에는 각 원고의 핵심 주장을 추려서 '보안뉴스'(https://www.boannews.com)에 '정보세계정치학회 칼럼 시리즈'로 실었다. 특집 시리즈를 제안해 주신 보안뉴스 김경애 팀장께 감사드린다. 그 이후 필자들의 수정작업과 보완 과정을 거쳐서 이렇게 편집 단행본의 형태로 세상에 나오게 되었다.

이 책이 나오기까지 도움을 주신 많은 분께 드리는 감사의 말씀을 빼놓을 수 없다. 무엇보다도 길지 않은 시간에 아직 국제정치학계에는 생소한 주제의 연구를 수행해 주신 열한 분의 필자들께 깊은 감사의 말씀을 드린다. 또한 이 책의 구상을 다듬던 시기에 세미나 발표를 해 주신 전문가들과 이 책의 초고가 발표되었던 2024년 정보세계정치학회 추계대회에 사회자와 토론자로 참여해 주신 여러 선생님께 감사드린다. 직함과 존칭을 생략하고 가나다 순으로 언급하면, 강하연(정보통신정책연구원), 김민호(성균관대), 김세용(국방부), 김소정(국가안보전략연구원), 김용신(인하대), 김주연(네이버), 김준연(소프트웨어정책연구소), 김재오(인하대), 박주희(국가보안기술연구소), 손한별(국방대), 신범식(서울대), 안형준(과학기술정책연구원), 양희동(이화여대), 이종진(서울대), 정대원(국가위성정보활용지원센터), 정용찬(정보통신정책연구원), 정태진(평택대), 최낙중(합동참모본부), 홍건식(국가안보전략연구원), 홍정희(한국국방연구원) 등 여러분께 감사드린다. 또한 이 책의 출판 과정에서 교정 총괄을 맡아준 서울대학교 김명하, 이수연 두 박사과정에 대한 감사의 말도 잊을 수 없다. 끝으로 출판을 맡아주신 한울아카데미 관계자들께도 감사의 말씀을 전한다.

〈참고문헌〉

김상배. 2016. "신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해."『한국정치학회보』50(1), pp.75–102.

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

유지연. 2024. "인공지능(AI)과 사이버 안보." 한국사이버안보학회 제7차 사이버 국가전략 포럼 발표문. 2월 6일.