Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전연구센터 연구위원 워킹페이퍼 No.19.(발간일: 2025.2.7.)

뉴스페이스 시대 우주 안보와 데이터 안보 연계의 동학

정헌주 연세대학교 행정학과 교수

1. 서론

지상으로부터 수백 혹은 수만 km 떨어진 우주공간에 있는 인공위성을 통해서 생성 · 수집되고, 전송되는 막대한 양의 데이터는 그 자체로 혹은 분석 · 가공된 후 다른 데이터와 결합 · 융합되어 다양한 가치를 창출함으로써 국가안보와 경제발전, 환경문제 인식 · 대응에 매우 중요한 영향을 미치고 있다. 이러한 데이터에는 위성을 통해서 생성된 다양한 기상, 해양, 지형 · 지리, 농업 · 산림 데이터 및 건축물, 차량, 사람 등을 식별 · 추적하는 데이터, 위치 · 항법 · 시각(positioning, navigation, timing, PNT) 데이터, 통신데이터 등이 포함된다. 한 보고서에 따르면, 위성 데이터 서비스 시장은 2020년 약 60억 달러 규모였지만, 2030년에는 약 458억 달러로 성장(2021년~2030년 연평균 성장률 22.5%)할 것으로 전망되었다(Allied Market Research 2024).

이러한 우주 파생 데이터 혹은 우주 기반 데이터(space-derived/space-based data, 이하 우주 데이터)는 상업적 가치를 창출함과 동시에 새로운 기술과 혁신을 통해서 경제활동의 전반적인 생산성을 향상시키고 지속가능한 경제발전의 기반을 구성하는 역할을 수행하고 있다. 예를 들면, 글로벌항법위성시스템(global navigation satellite system, GNSS)이 제공하는 PNT 데이터와 지구관측위성 데이터를 함께 활용하면, 농약 및 연료 절감 효과와 농작물 생산량 증가 등으로 인해서 10% 이상의 농업생산성 향상이 발생하는 것으로 보고되었다(UN 2018). 또한, 17개 우주기관이 참여하는 "The International Charter Space and Major Disaster"(2024)는 태풍, 지진, 홍수, 화산폭발, 해양오염 사고 등 자연재해 또는 인간에 의한 재해에 관한 지구관측 데이터를 해당 국가와 지역에 제공함으로써 재해를 예측하

고, 대응하는데 기여함으로써 다양한 사회적 · 경제적 가치를 창출하고 있다.

무엇보다 우주 데이터는 군사적, 안보적 측면에서 그 중요성이 커지고 있다. 특히, "궁극의 군사적 고지(ultimate military high ground)"로서 우주에서 생성되고 전달되어 축적 · 활용되는 다양한 데이터는 현재와 미래의 전쟁을 대비하고 수행하는 데 필수적 자산과 역량이 되고 있다.[1] 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 확보하는데 결정적 역할을 수행하기 때문이다(정헌주 2021, 22–23). 이는 2022년 발발한 러시아–우크라이나 전쟁이나 2023년에 시작된 이스라엘–하마스 전쟁에서도 명확하게 드러나고 있다.

이러한 점에서 우주 데이터를 어떻게 수집 · 분석 · 활용할 것이며, 이를 보호할 것인가는 매우 중요한 안보적 차원의 문제로 부상하였다. 하지만, 우주 안보와 데이터 안보의 다양한 관계를 체계적으로 분석하고, 이를 기반으로 정책적 함의를 도출한 연구를 찾기는 쉽지 않다. 체계적 분석이 부재할 경우, 우주 안보와 데이터 안보 및 이들의 역동적 관계 속에서 발생하는 취약점을 정확하게 식별하지 못한다는 점에서 본 연구의 중요성이 있다. 이러한 점을 고려하여, 본 연구는 우주–데이터 안보의 관계를 크게 3가지, 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 살펴본다. 특히 본 연구는 뉴스페이스 시대 민간행위자의 우주활동이 증가하고 이에 따른 우주 데이터의 양이 급증하고 질적으로도 향상되는 맥락을 고려하여 우주 안보와 데이터 안보가 맺는 이러한 각각의 관계를 구체적 사례와 함께 분석한다. 나아가 우주–데이터 연계의 세 가지 차원에서 한국의 현황을 살펴보고 취약점을 식별한 후 정책적 함의를 도출한다.

본 연구의 구성은 다음과 같다. 먼저, 제2장에서는 우주 데이터의 특징과 특징으로부터 도출되는 다양한 함의를 살펴본다. 제3장은 우주 안보와 데이터 안보의 관계를 크게 3가지로 구분한 후, 각각의 관계를 다양한 사례를 통해서 분석한다. 제4장에서는 한국의 우주–데이터 안보 현황을 분석하고 취약한 부분을 식별함으로써 우주–데이터 안보를 제고하기 위해 필요한 방안을 구체화한다. 마지막 장에서는 연구를 요약하고 연구의 함의를 제시한다.

[1] 우주는 다수의 학자, 전략가들에 의해서 "궁극의 (군사적) 고지"로 표현되었으나, 이에 대한 반론 역시 존재한다(Meyer and Stallings 2011).

2. 우주 데이터: 특징과 함의

기존의 지상, 해상, 공중 기반 데이터 및 이에 대한 보안 · 안보와 비교하였을 때, 우주공간, 우주자산의 특성으로 인해서 우주에서 생성되는 다양한 데이터와 이에 대한 보안과 안보는 새로운 기회임과 동시에 도전이다. 이를 위해서 먼저 우주 데이터의 개념과 특징을 살펴보고, 그 군사안보적 함의에 대한 분석이 필요하다.

우주 데이터(space data)에 대한 명확한 정의는 없지만, 대부분 위성, 우주비행체 등 우주 기반 자산으로부터 생성되는 다양한 데이터를 의미한다. 하지만, 보다 확장된 정의에 따르면, 우주 데이터는 인간의 우주활동으로부터 생성되는 데이터뿐만 아니라 우주활동 자체에 대한 데이터 및 우주에 대한 데이터 역시 포함한다. 이러한 점에서 우주 데이터는 PNT, 지구관측, 우주상황인식, 통신, 신호정보, 원격탐사(remote sensing) 및 관련 R&D와 관련된 데이터를 포함한다(UK Legislation 2021).

이러한 우주 데이터는 위성의 숫자가 빠르게 증가하고 고성능화되면서, 그 절대적 규모가 급증하고 있다. 한 보고서에 따르면, 2020년부터 2030년까지 지상과 우주 사이에서 이동하는 데이터의 양은 500엑사바이트(exabytes)를 넘어설 것으로 전망된다(Northern Sky Research 2021/12/6).[2] 이러한 우주 데이터의 급격한 증가는 위성에 탑재되는 센서의 가격이 하락하고, 다양화, 고성능화, 소형화되는 현상과도 연계된다. 특히, 저궤도(low Earth orbit, LEO)에서 운영되는 위성은 지구궤도를 더 자주, 빠르게 회전하면서, 데이터를 생성하고, 낮은 지연율(latency)로 지상에 전달함으로써 다양한 가치를 창출하고 있다.

이러한 우주 데이터는 다른 종류의 데이터와는 차별적인 중요한 특성이 있다. 먼저, 우주 데이터는 기본적으로 민군겸용기술(dual-use technology)의 특성을 지닌다. 대표적으로는 지구관측위성이 지구 표면의 물체, 장소, 특정 사건, 상황 등과 관련하여 생성한 지리공간(geo-spatial) 데이터는 민군겸용으로 활용될 수 있다. 2016년 구글이 상세 지도데이터(5,000:1 수준)를 국외로 반출할 것을 요청한 것에 대해 한국 정부가 불허한 사건은 이러한 특성을 잘 보여준다(조선비즈 2016/11/18). 구글은 2007년부터 상세 지도데이터를 국외로 반출하여 본사 데이터센터에 저장하는 것을 요청하였으나, 한국 정부가 이를 불허한 이유는 국내법상 해외 반출이 가능한 지도는 축적 25,000:1 수준 이하라는 점과 더불어 국내 주요 군사기지의 위성사진 삭제 여부와 관련되었다고 보도되었다(동아사이언스 2016/11/18). 즉, 구글이 요청한 5,000:1 수준의 상세 지도데이터에는 이미 군사 · 안보 시설이 삭제된 상태였지만, 해외에서 제공되는 데이터와 결합될 경우 민감 정보 유출이 가능하다는 점을 둘러싼 이견이 협상 결렬의 주요 요인이었다는 것이다. 즉, 이는 민간 위성 데이터와 국가안보

[2] 엑사바이트는 페타바이트(petabyte)의 1024배로, 이는 약 10억 기가바이트, 약 100만 테라바이트에 해당한다.

의 관계를 명확하게 보여준 사례였다.[3)]

우주 데이터의 또 다른 특징은 데이터가 생성되는 우주 기반 자산과 지상 사이 공간적 거리와 연관되어 있으며, 이러한 공간적 이격은 몇 가지 중요한 함의를 갖는다. 먼저 이로 인해 신호(업링크와 다운링크) 전송이 필수적이다.[4)] 따라서, 신호 전송 과정에서 사이버공격 등 우주 자산 운영자 및 이용자의 의도와 목적에 반하는 의도적 행동이나 비의도적 · 자연적 방해의 가능성이 매우 높다. 둘째, 공간적 이격으로 인해 데이터를 생성하는 우주부문(space segment)은 물리적 설계와 탑재체에 변화를 주기가 어렵다는 점이다. 즉, 소프트웨어적 변화(업데이트 등)는 가능하지만, 물리적 변화는 매우 어렵다는 점에서 우주 자산이 설계 · 제작 · 전개되는 시점과 데이터 생성 시점 사이의 시간적 거리는 지속적으로 증가한다. 셋째, 경계와 주권의 영향이 미치지 않는 우주에서 데이터가 생성되지만, 많은 경우 이 데이터가 활용되기 위해서는 주권과 경계로 구분된 지상으로 전송되어야 한다.[5)] 만약에 어떤 국가의 우주 자산이 지구궤도를 돌면서 우주 데이터를 생성하더라도, 이 데이터를 전송받고 활용하는 지상국이나 사용자는 주권 국가 내에 위치할 수밖에 없다.[6)] 따라서, 어떤 국가나 기업이 자국이나 자사의 위성에서 생성되는 데이터를 자국의 영토가 아닌 곳에서 전송받기 위해서는 국제협력이 필수적이다. 물론 이러한 우주 데이터의 특성은 다양한 기술적 발전에 의해서 약화될 수 있다. 하지만, 지상과 우주라는 공간적 이격으로 인해서 우주 데이터는 사이버안보와 매우 밀접한 관계를 갖을 수밖에 없고, 다른 어떤 시스템보다도 보안설계(security by design)가 매우 중요하다는 점 등은 이러한 특성이 갖는 안보적 함의이다.

마지막으로, 지상과 우주 사이의 공간적 이격이라는 특징과 연계되지만, 위성 등 우주부문에 특수하게 연계된 특징도 있다. 먼저 지구궤도의 특성상, 정지궤도 위성을 제외한 대부분의 위성은 특정 지역에 대한 데이터를 생성 · 전송할 수 있는 시간적 제약, 즉 재방문 주기(revisit frequency)가 있다. 즉, 대부분의 위성은 개발단계에서부터 위성의 목적과 탑재체 등 다양한 요소를 고려하여 재방문주기를 계획한다.[7)] 따라서, 대부분의 우주 데이터는 특정 지역, 특정 시간이라는 시공간적 특수성을 지니고 있다. 이를 극복하기 위해 다수의 위성을 다양한 궤도에서 함께 운영하거나 위성 자세 · 탑재체 제어를 통해서 재방문주기 감소 효과를 창출하기 위한 노력은 이러한 특징에서 기인한다. 특히, 지구관측 데이터의 경우, 재방문주

3) 이러한 맥락에서 한국은 위성 데이터가 해외로 반출되는 문제를 막기 위하여 "위성정보 보완관리 규정"(과학기술정보통신부훈령 제211호)를 통해서 위성정보심의위원회 설치, 위성정보의 종류, 비공개 및 공개 제한 위성정보의 국외 반출 금지 등을 명시하고 있다.

4) 물론 우주상황인식과 관련된 데이터의 경우, 순수히 지상에서 생성 · 활용되는 경우도 있지만, 이는 전체 우주 데이터 중 일부에 해당된다.

5) 정지궤도 위성이 제공하는 데이터와 서비스의 경우는 해당되지 않는다.

6) 공중에서 이용되는 PNT 데이터 등은 예외이다.

7) 물론 운용단계에서 재방문주기를 변경할 수도 있지만, 이를 위한 추진체 사용과 궤도 재진입 등 다양한 비용이 발생한다.

기뿐만 아니라, 관측 폭(field of view), 궤도, 공간해상도(spatial resolution), 분광해상도(spectral band) 등에 의해서 차이가 발생한다(김은정 2015). 이 중에서도 공간해상도는 데이터의 양과 질에 결정적 역할을 수행한다. 즉, 해상도의 차이에 따라서 관측하는 물체를 어느 정도 정확하게 식별할 수 있는가가 결정되며, 이는 개발단계에서 매우 중요한 고려사항이다. 동시에 높은 해상도는 보다 정밀한 사진을 제공하지만 데이터의 양을 고려하였을 때, 관측폭이 좁은 반면, 낮은 해상도는 보다 넓은 지역에 대한 데이터를 창출할 수 있다는 점에서 상충관계(trade-off)가 존재한다. 물론 최근 이러한 상충관계는 다양한 저해상도 데이터를 융합하여 고해상도 데이터를 생성하는 초해상도화(super resulution) 기법 등 기술적 발전으로 인해서 완화되고 있다(강종구 · 이양원 · 김대선 2023, 542).

이렇듯 민군겸용기술의 특성과 공간적 · 기술적 특성으로 인해 우주 데이터는 기존의 데이터와는 차별적인 특성이 있다. 이러한 특성을 고려하였을 때, 우주 데이터를 보호하고, 이를 활용해 안보를 증진시키는 우주 안보와 데이터 안보 사이의 관계는 매우 복잡하며 이를 체계적으로 이해하기 위해서는 우주-데이터 안보의 관계를 세부적으로 나눠서 살펴볼 필요가 있다.

3. 우주 안보와 데이터 안보의 연계

우주 안보와 데이터 안보 사이의 관계를 좀 더 체계적으로 살펴보기 위하여, 이를 세 가지로 구분할 수 있다. 첫째, 우주 데이터를 활용하여 (국가)안보를 제고하는 것(security by space data)이다. 둘째는 우주 파생 데이터의 안보(security for space data)이다. 마지막으로는 우주 안보를 위한 데이터(data for space security)이다. 각각을 구체적으로 살펴보면 다음과 같다.

(1) 우주 데이터를 활용한 안보(security by space data)

우주 안보와 데이터 안보가 가장 밀접하게 연계되는 방식은 군사용 위성뿐만 아니라 다양한 공공 · 민간 · 상업용 위성을 통해서 생성되는 데이터를 활용하여 (국가)안보를 제고하는 것이다. 대부분의 군사용 우주 자산의 경우, 지상에서의 안보를 제고하기 위해 설계 · 제작되고 운용되고 있다는 점에서 이러한 데이터는 직접적이고 즉각적으로 안보에 영향을 미친다. 2023년 현재, 군사용 위성의 경우, 미국이 가장 많은 247개를 보유 · 운영하고 있으며, 그 다음으로 중국(157개), 러시아(110개), 프랑스(17개), 이스라엘(12개), 이탈리아(10개)

등의 순으로 알려졌다(WPR 2024).

최근 주목되는 점은 민간행위자에 의해서 생성 · 전송 · 저장 · 활용되는 우주 데이터가 상업적 가치와 함께 군사 · 안보적 가치를 창출하는 사례가 점차 증가하고 있다는 것이다. 예를 들면, Orbital Insight라는 회사는 원유 저장 탱크 지붕에 있는 그림자를 분석해서 원유 저장량을 분석하고,[8] 이를 통해 석유 수요를 예측하여 유가를 전망하는 서비스를 제공하는 것으로 알려졌다(연합인포맥스 2020/4/13; KBS 2020/4/28). 이러한 원유 저장량을 분석하는 데 활용된 우주 데이터는 경제적 가치를 창출하지만, 동시에 한 국가가 얼마나 많은 원유를 저장하고 있는지를 통해서 해당 국가의 군사적 역량(전쟁수행능력)을 엿볼 수 있다는 점에서 안보적 함의가 있다.

〈그림 1〉 Orbital Insight의 "Floating Roof Oil Tan Computer Vision"

출처: Orbital Insight 구글드라이브 파일(Media kit)

나아가 지리공간 데이터는 PNT 정보와 연계되어 다양한 위치기반 서비스를 가능하게 한다. 이러한 위치기반 서비스는 적의 위치와 이동에 대한 정보감시정찰(intelligence, surveillance, and reconnaissance, ISR) 역량, 무인무기체계 및 정밀유도무기 등에 활용되고 있다. 러시아–우크라이나 전쟁 초기 Maxar Technology가 촬영한 키이우 주변 위성 이미지는 상업적 서비스를 제공하는 민간기업의 우주 데이터가 군사적으로 충분히 활용될 수

8) 원유 저장 탱크는 증발과 폭발의 위험을 제거하기 위하여 뚜껑이 없는 원통형이며, 부유식 지붕을 활용하고 있다. 따라서 원유 탱크의 위치와 특정 시각의 태양 위치, 저장량에 따라 저장 탱크 상단에 생기는 초승달 모양의 그림자 크기가 달라지고, 이를 통해서 저장량을 분석할 수 있다.

있음을 보여주었다. 또한, SpaceX가 제공하는 스타링크 서비스는 우크라이나의 파괴된 통신망을 대체하였고, 우크라이나 군은 이 서비스를 활용해 무인기를 통제하는 등 군사적 목적으로 민간 서비스를 사용하였다(Peperkamp and Bolder 2024, 260–263). 최근에는 서방의 제재를 우회한 러시아 역시 스타링크 서비스를 활용하고 있는 것으로 보도되었다(연합뉴스 2024/3/27).

이는 뉴스페이스(New Space) 시대 민간 우주 자산으로부터 파생된 데이터의 양이 급격히 늘어나고 이를 처리하는 새로운 방식—클라우드 컴퓨팅, 인공지능 등—이 등장함에 따라 민간 · 상업용 우주 데이터의 활용도가 매우 높아졌음을 의미한다. 과거 고성능, 고가의 감시정찰 위성과 이를 통해서 생성된 데이터는 국가가 독점하는 전략자산이었다. 하지만, 최근 민간기업의 지구관측위성은 저궤도에서 상대적으로 낮은 해상도의 이미지를 다수 촬영하여, 이를 합성함으로써 고가의 감시정찰 위성으로 생성된 데이터(이미지)에 못지않은 높은 가치의 데이터를 생성하고 있다. 이는 곧 민간용 우주 데이터의 군사적 활용도가 더 높아짐을 의미한다. 또한, 군사용 PNT 서비스보다 높은 신뢰도와 정확도를 추구하는 민간기업—Xona Space Systems 등—이 추진하는 저궤도위성군 기반 초정밀 PNT 서비스는 자율주행 차량 및 드론에게 보다 정확한 위치 정보를 제공하는 목표를 가지고 있지만, 그 군사 · 안보적 함의는 매우 크다(Spacenews 2024/3/19).

우주 데이터는 실제로 민간 · 상업용 우주 데이터와 군사용 우주 데이터가 융합(data fusion)되어 더욱 큰 군사적 가치를 창출할 수 있다. 예를 들면, 군사적으로 중요한 (잠재적) 적의 특정 지역을 관찰하는데 이러한 민군 데이터 융합이 활용될 수 있다. 즉, 이 지역에 발생하는 모든 변화를 관측하기 위해서는 높은 해상도의 군사용 정찰위성을 다수 운용하는 것은 매우 큰 비용이 발생한다. 대신 낮은 해상도이지만 해당 지역을 매우 자주 방문하면서, 넓은 지역을 관찰하는 민간기업의 우주 데이터를 우선적으로 활용하고, 어떠한 중요한 변화—전력 이동, 새로운 무기체계 등장, 새로운 시설 공사 등—가 발견된다면, 그때 이 변화가 무엇이었는지를 보다 정확하게 분석하기 위하여 높은 해상도의 군사위성을 본격 활용하거나 궤도 변경을 통해서 해당 지역을 자세히 관찰하는 것이다. 이렇게 함으로써 처리해야 할 막대한 양의 데이터 처리 비용과 시간을 줄이고, 효율성을 제고할 수 있다(European Commission and European Investment Bank 2019, 37–38).

게다가 과거에는 효용성이 낮았던 데이터가 컴퓨팅 기술의 발전과 함께 새로운 군사 · 안보적 가치를 창출할 수도 있다. 많은 우주 데이터는 1970년대부터 축적되어 있으며, 누구에게나 무료로 공개되는 자료 역시 방대한 양이다. 이러한 데이터를 분석하여, 현재의 데이터와 결합한다면 (잠재적) 적의 행동 패턴과 군사적 역량을 파악할 수 있다는 점에서 데이터 우위 혹은 지배(data superiority, data dominance)를 통한 군사적 우위를 도모할 수 있다.

무엇보다 중요한 점은 우주 기반 이미지정보(imagery intelligence, IMINT)와 지리공간정보(geo-spatial intelligence, GEOINT)가 신호정보(signal intelligence, SIGINT), 오픈소스정보(open source intelligence, OSINT)나 다른 사회적 정보(소셜미디어 등)와 결합되어 국가안보 및 인간안보에 중요한 영향을 미칠 수 있다는 것이다(Peperkamp and Bolder 2024; Dolce et al. 2020). 러시아-우크라이나 전쟁에서의 다양한 사례들은 신호정보나 소셜네트워크서비스(SNS) 정보가 우주 데이터와 결합되는 사례를 잘 보여준다. 러시아군의 임시훈련소에서 한 병사가 스마트폰으로 가족과 안부 전화를 한 이후 우크라이나의 정밀유도무기가 해당 훈련소를 정밀타격한 사례나 친러 체첸 병사가 동료의 사진을 틱톡에 올린 후 해당 건물이 정밀타격을 받았던 사례 등은 OSINT나 SNS 정보가 즉각적으로 우주 데이터와 결합되어 군사작전에 활용되고 있음을 보여준다(중앙일보 2023/4/29). 위성 데이터와 소셜미디어 정보를 결합하여 홍수 등 긴급상황에 실시간 혹은 준실시간으로 효과적 대응이 가능함을 보여주는 연구는 다양한 정보와 데이터의 융합과 이를 활용한 즉각적인 군사적 행동이 충분히 가능함을 보여준다(Li et al. 2017). 만약 OSINT, SIGINT, 소셜미디어 정보와 IMINT · GEOINT를 결합하여 특정 상황에서의 개인이나 집단의 행위 패턴을 파악한다면, 그 자체로서 안보적 함의가 있을 뿐만 아니라, 군사적 · 작전적 가치 역시 높을 것이다.

(2) 우주 데이터의 안보(security for space data)

우주 안보와 데이터 안보가 연계되는 두 번째 지점은 우주 데이터의 안전과 완전함(integrity)과 관련된 우주-데이터 안보이다. 일반적인 데이터의 생애주기와 마찬가지로 우주 데이터 역시 데이터를 획득하고, 분석 · 가공 · 저장하며, 이를 활용하는 일련의 과정이 있으며, 이를 신속하고 안전하게 수행하는 것은 매우 중요하다. 물론 주의할 점은 데이터 획득 · 생성 단계, 데이터 분석 · 선별가공(curation), 저장 및 활용 단계는 일반적으로 데이터의 가치사슬에 따른 단계 분류이며, 모든 단계는 때로는 동시다발적 · 연속적으로 일어남과 동시에 이러한 단계 사이를 연계하는 데이터 전송(transfer) 역시 고려해야 한다는 것이다. 이러한 일련의 과정에서 우주 데이터의 안보에 대한 위협은 다양하고 실제적이다.

첫째, 데이터 획득 · 생성 단계에서의 위협으로 데이터 획득을 방해하거나, 데이터 자체를 왜곡시키거나 오류를 유발하는 방식으로 데이터의 정확성과 신뢰성을 저하시키는 것이다. 우주 데이터의 종류는 매우 다양하여, 해당 데이터가 획득, 생성되는 단계에서의 위협 역시 매우 다양하다. 대표적인 우주 데이터라고 할 수 있는 PNT 서비스와 관련하여 생성 단계에서는 GNSS에 대한 직접적인 데이터 오염 또는 실수에서부터 가짜 PNT 정보를 제공하는 방식 등이 주요한 위협이 될 수 있다. 2016년 1월에 발생하였던 GPS 비정상작동 사례(UTC

offset anomaly)는 실수로 GPS 위성에 탑재된 부정확한 시각정보(약 백만 분의 13초)로 인해서 동기화 문제가 발생하고, 이로 인해 해당 GPS 위성의 PNT 데이터에 의존하는 전 세계의 기기가 12시간 정도 오작동하는 등 매우 큰 파급효과가 발생함을 보여주었다(Glass 2016/6/13).

지구관측 또는 감시정찰 위성의 경우, 데이터 획득 · 생성 단계에서의 위협은 물리적 방식과 지향성 에너지 또는 사이버 공격을 통한 데이터 오염의 가능성이 존재한다. 전통적으로 감시정찰 위성의 활동을 무력화하기 위하여, 은폐, 엄폐, 기만, 은닉 방식이 사용되었다. 러시아–우크라이나 전쟁에서 양국은 모형(decoy) 무기를 활용하여, 위성 및 드론을 활용한 상대의 감시정찰을 기만하고, 모형 무기를 파괴하는데 고가의 무기를 사용하도록 유도하고 있다(Rivero 2024). 또한, CSIS 리포트에 따르면, 중국 인민해방군은 최근에도 "적국"의 ISR 위성이 감시활동을 수행할 때, 장비를 철수하거나 신속하게 기동하고, 무선침묵(radio silence)를 유지하는 등의 훈련을 실시하는 것으로 보도되었다(Swope et al. 2024, 10). 나아가, 지향성 에너지(레이저빔 등)를 통해서 감시정찰 위성에 탑재된 광학렌즈 혹은 레이더를 교란함으로써 ISR 데이터 획득을 방해할 수 있다. 하지만, 이러한 방식은 최근 군용뿐만 아니라 민간 위성을 활용한 ISR 역량이 강화되면서, 전술적, 작전적 수준에 비해 전략적 수준에서의 활용도는 낮아지고 있다. 그럼에도 불구하고, 최근 딥페이크 이미지를 활용하여 민간 ISR 데이터의 신뢰성을 저하시키고, 데이터의 진위를 입증하기 위한 비용을 추구하게 만든다는 우려 역시 존재한다(Swope et al. 2024, 36).

잠재적이지만 더 광범위한 위협은 궤도상 다수의 민간 · 군용 감시정찰 자산뿐만 아니라 대부분의 우주 자산의 작동을 일시에 무력화할 수 있는 (핵 · 非핵)EMP 공격의 가능성이다. 최근 러시아는 우주에서 인공위성을 파괴하거나 기능을 마비시킬 수 있는 핵EMP 무기개발에 상당한 진전을 이룬 것으로 보도되었다(KBS 2024/2/17). 핵무기 등 대량살상무기(WMD)를 우주에 배치하는 것을 금지하는 「달과 기타 천체를 포함한 외기권의 탐색과 이용에 있어서의 국가 활동을 규율하는 원칙에 관한 조약」(약칭: 우주조약, 1967년 발효)에 미국과 러시아를 포함한 주요 우주강국이 서명하였다는 점을 고려한다면, 非핵EMP 항우주무기체계(counter–space weapon system)의 등장 가능성을 배제할 수는 없다.[9)]

또 다른 방식은 위성체에 탑재되는 부품(반도체 등)에 악성코드를 탑재하거나, 해킹을 통해 데이터 획득 · 생성을 방해하는 것이다. 즉, 위성을 해킹하여 통제권을 장악한 적대적 행위자가 자신이 원하는 특정 지역에서 위성 데이터를 활용할 위험이 존재한다. 특히, 뉴스페이스 시대 다양한 민간기업과 대학, 연구소 등이 보안시스템이 취약한 저가의 위성을 궤도

9) 특히, EMP 차폐 기술은 이미 확보되었지만, 중량 증가를 고려하였을 때, 저궤도에서 활동하는 위성의 경우, EMP에 매우 취약할 수 있다.

상에서 운용함에 따라 이러한 위험성은 더욱 높아지고 있다. 위성의 제작 단계에서 악성코드가 탑재된 부품이 활용될 가능성도 있다. 물론 최근 미중 전략경쟁이 심화함에 따라 우주에 탑재되는 기술과 부품, 즉 우주 관련 공급망에 대한 통제가 강화되면서 이러한 가능성은 상대적으로 감소하고 있다는 주장 역시 가능하다. 2020년 9월 미국은 우주정책지침(Space Policy Directive–5: Cybersecurity Principles for Space Systems)을 통해서, 우주시스템의 사이버보안에 영향을 미칠 수 있는 공급망을 관리하도록 하였고, 여기에는 제조된 품목을 추적하고, 신뢰할 수 있는 공급자로부터 구입하고, 위조, 사기, 악의적 장비를 식별하는 등의 조치를 요구하고 있다. 나아가, 우주시스템을 구성하는 각 부문(segment)에서의 논리적 · 물리적 망분리, 물리적 보안 등도 강조하고 있다(U.S. White House 2020/9/4). 그럼에도 불구하고, 뉴스페이스 시기 다양한 민간행위자의 비용절감 노력에 따라, 기성제품을 이용하는 경우가 늘어나고 있다는 점에서 위성체에 탑재되는 부품을 통한 데이터 안보 위협 가능성을 배제할 수는 없다.

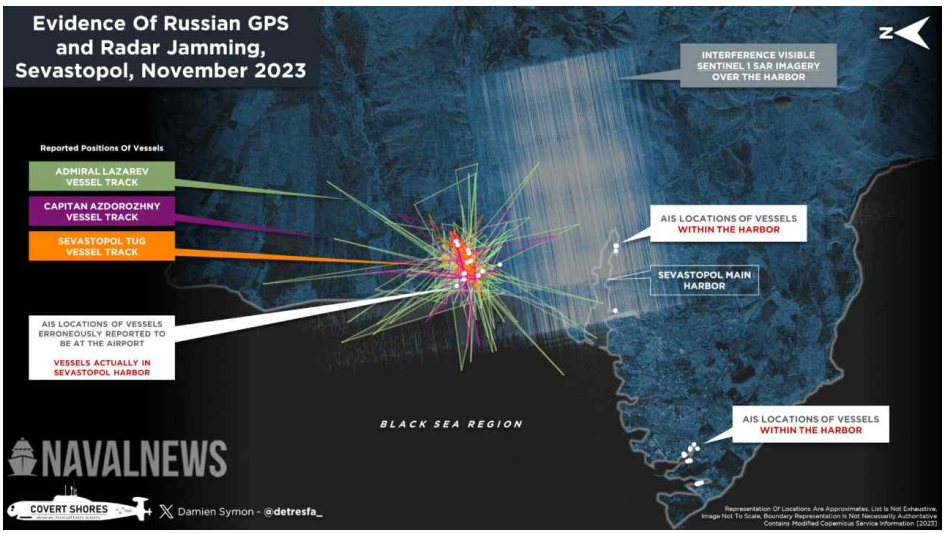
둘째, 데이터 분석 및 선별가공, 저장 단계에서의 위협이다. 이 단계에서의 위협은 위성으로부터 파생된 데이터가 지상으로 전송되어 지상부문(데이터센터 등)에서 데이터가 분석, 선별가공되고 저장되는 과정에서 발생하는 위협이다. 대부분의 위협은 지상부문을 대상으로 발생하는 사이버 공격으로 인해 데이터 위변조, 탈취 등이다. 예를 들면, 한국의 저궤도 위성을 운영 · 관리하며, 위성으로부터 수신받은 데이터가 저장된 국가위성운영센터(Korea Satellite Operations Center, 제주 구좌읍 위치)가 2023년 12월경 해킹 공격을 받은 것으로 수개월 뒤 밝혀졌다(조선비즈 2024/3/26). 과학기술정보통신부와 국가정보원이 협력해 설립하고 항공우주연구원이 운영하는 국가위성운영센터는 다목적실용위성인 아리랑3호와 아리랑3A호를 관제하고, 고해상도의 지구관측 영상 데이터를 수신하고 관리하는 역할을 담당하고 있으며, 2030년까지 저궤도 위성 70기에 대한 운영을 담당할 예정이다. 문제는 지난 20여 년에 걸쳐 축적된 위성 데이터가 탈취되었을 가능성이 있고, 더욱 중요한 것은 이를 통해서 한국의 지구관측 · 감시정찰 능력과 더불어 의도가 파악될 수 있다는 점이다.

이러한 외부로부터의 해킹 위협은 우주 부문의 특징과 최근의 변화로 인해서 더욱 악화되고 있다. 먼저 과거 우주 자산의 전략적 중요성으로 인해서, 이를 통제, 관리하는 지상국의 경우, 대부분은 확장된 네트워크 또는 공공 네트워크와 분리되어 운영되었다. 하지만, 최근 지상국에 대한 원격 접근과 실시간 데이터 공유의 수요가 증가하면서 지상국은 과거에 비해서 훨씬 더 연결되어 있고, 접근가능하다. 게다가 기존 망분리에 의해서 유지되었던 보안과 달리 연결성이 높아진 상황으로 변화하였지만, 기존 기지국의 경우, 여전히 오래된 운영시스템을 활용하는 경우가 많아 보안패치가 업데이트되지 않아 보안에 취약성이 높아지는 등의 문제가 발생할 수 있다(Heideman 2024/6/4).

외부로부터의 해킹뿐만 아니라 내부로부터의 위협 역시 충분히 가능하다. 여기에는 내부자 위협(insider threat), 즉 우주 데이터를 다루는 조직 내 합법적인 권한이 있는 사용자가 실수 혹은 고의로, 또는 합법적 권한이 없는 사용자가 내부의 느슨한 보안을 악용하여 고의로 데이터에 접근하고 이를 오용하는 가능성이다. 특히, 민간부문이 주도하는 우주 데이터의 양이 방대해지고, 군사안보적 용도로 사용될 수 있는 우주 데이터를 다루는 민간부문의 취약한 보안시스템, 보안의식 등으로 인해 민감한 데이터가 유출될 수 있다.

셋째, 데이터가 최종사용자에게 전송되어 활용되는 단계에서의 위협이다. 신호를 방해·교란하는 재밍(jamming), 실제 신호를 가로채 의도적으로 시간차를 두고 재송신함으로써 위치 측량에 혼선을 유도하는 미코닝(meaconing)이나 가짜 PNT 데이터를 생성하여 기만하는 스푸핑(spoofing)은 이 단계에서 발생하는 위협으로 볼 수 있다. 아래 〈그림 2〉는 2023년 11월 세바스토폴에서 수행된 러시아의 GPS 및 레이더 위성 재밍을 보여주고 있다.

〈그림 2〉 러시아의 GPS 및 레이더 위성 재밍 사례(세바스토폴, 2023년 11월)



출처: Naval News(2023/11/28)

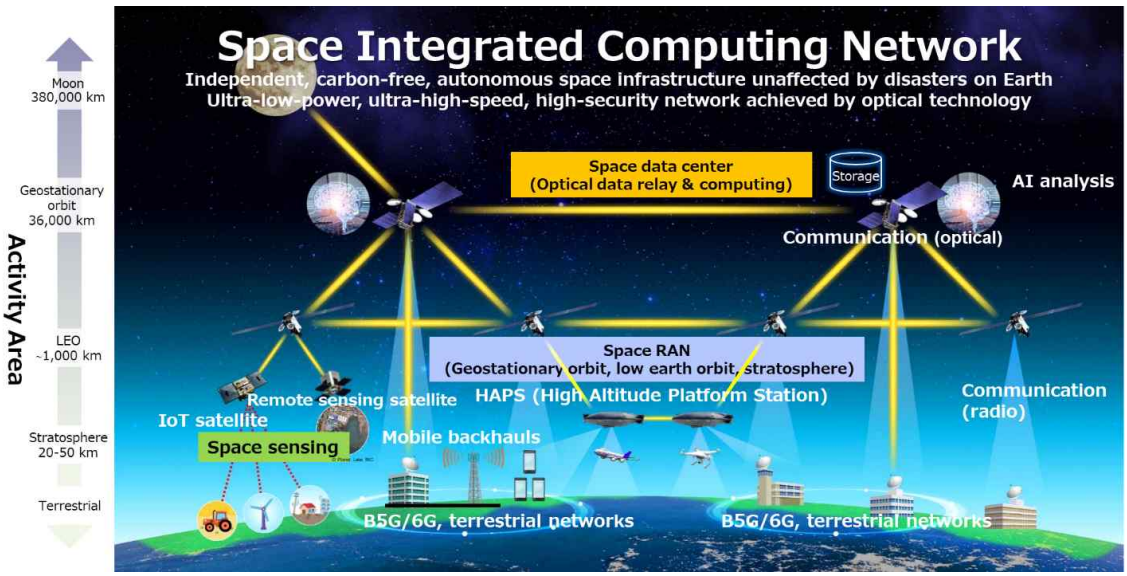
더욱 중요한 사실은 일단 최종사용자에게 전송이 되면 해당 우주 데이터가 원래의 목적 이외의 용도, 즉 군사·안보적 용도로 활용되는지를 사전에 예측·예방하는 것은 매우 어렵다는 점이다. 공공 및 상업용 우주 데이터를 활용하여 새로운 군사적 가치를 창출하는 사례는 최근 러시아–우크라니아 전쟁에서 여실히 드러났다. 또한, 앞서 소개한 원유 저장 탱크의 위성 데이터를 활용한 사례는 데이터가 일단 공개되면, 이를 창의적으로 활용하여 군사적, 안보적 목적으로 충분히 활용될 수 있음을 보여준다.

특히, AI 기술이 발전하고 우주 데이터의 종류와 양이 방대해지면서, 별 의미가 없었던 우주 데이터가 군사적으로 활용될 가능성은 더욱 커지고 있다. 즉, 미시적 차원에서 개별 기업이 상업적 목적으로 수집하고 활용하던 위성 데이터의 양이 폭발적으로 증가하고, 다른 데이터 및 인공지능 기술과 융합되면서, 초기 의도와는 전혀 다른 거시적 차원에서의 군사안보적 가치가 생성되는 "창발(emergence)"의 가능성이 충분하다(김상배 2020). 결국, 거시적 관점에서 이러한 상황은 우주경제 육성과 우주 안보 강화라는 두 가지 가치가 상충될 수 있음을 의미한다.

이상에서 살펴본 우주 데이터에 대한 안보 위협을 획기적으로 줄이기 위한 노력 역시 진행되고 있다. 이는 우주라는 공간적 특성을 활용함으로써 우주-데이터 안보를 제고하려는 노력이다. 앞서 살펴보았듯이 우주시스템은 다양한 하위부문(segment)로 이뤄져 있고, 각 부문 고유의 취약성과 이를 연계하는 전송 단계에서의 취약성이 존재한다. 또한, 데이터 획득 · 생성, 분석 · 선별가공 · 저장, 활용, 전송 등 각 단계에서 데이터 보안의 취약성은 매우 다양하며 실제적이다. 최근 이러한 단계는 빠르게 융합되고 있으며, 그 과정에서 새로운 기회가 생겨나고 있다. 즉, 데이터 분석 및 선별가공, 저장 단계가 기존에는 주로 지상부문(데이터센터 등)에서 이뤄졌다면, 최근 우주 공간에서 수집된 데이터를 우주에서 분석, 선별가공, 저장하는 기술에 대한 개발과 투자가 진행되고 있다.

우주 클라우드(space cloud) 혹은 우주 데이터센터(space data center)는 통신위성, 지구관측위성, 컴퓨팅 위성, 데이터 저장 위성 등으로 구성되어, 우주공간에서 데이터를 분석, 가공하여 사용자에게 신속하게 전달되어 즉각적으로 활용이 가능한 수준의 데이터를 지상으로 전송하는 개념이다(CIO 2024/2/20). 통상 지구관측 · 감시정찰위성에서 파생되는 방대한 양의 데이터 중 절반 이상은 불필요한 자료임에도 모든 데이터를 일단 지상국으로 전송하기 위해서는 이를 위한 에너지, 시간, 통신탑재체, 저장공간 등이 필요하다(정보통신산업진흥원 2024). 하지만, 최근 AI 등 컴퓨팅 능력이 향상되면서 이러한 데이터 분석, 선별가공 기능을 위성에 탑재(onboard computing)하고, 저장소 역시 다른 위성에 탑재한 후, 레이저 통신 기술을 활용하여 위성 간 데이터를 전송한다면, 최종 가공된, 즉 용량이 획기적으로 줄어든 데이터는 사용자가 바로 이용할 수 있게 되는 것이다.

〈그림 3〉 일본 NTT사의 우주 컴퓨팅 네트워크 개념도



출처: NTT(2022/4/26)

빠르면 수년 내로 현실화할 것으로 예상되는 수십에서 수백 개의 위성—지구관측위성, 통신위성, 컴퓨팅 프로세싱 위성, 데이터 저장 위성, 데이터 노드 위성 등—으로 구성된 우주 데이터센터는 꼭 필요한 데이터만 전송함으로써 속도를 획기적으로 향상시킬 수 있다. 그뿐만 아니라, 데이터 분석 · 식별가공 · 저장 과정에서 필요한 막대한 에너지를 태양으로부터 확보하고, 발생하는 열을 우주로 배출함으로써 경제적 가치뿐만 아니라 환경적 가치도 추구할 수 있다. 이러한 데이터센터는 지상에서의 자연재해, 테러 공격 등으로 인해 서비스가 중단될 가능성도 낮다는 장점도 있다. 게다가 가공된 데이터를 필요한 사용자가 지구상에 어느 곳에 있더라도 바로 전송할 수 있다는 장점이 있다. 따라서, 미국, 유럽, 일본 등 국가와 공공기관, 민간기업들은 우주 데이터센터를 구축하기 위해 노력하고 있다. 나아가 이러한 "우주 데이터센터"는 군사적 활용도가 높다는 점을 인식한 미국과 영국 등은 감시정찰위성이 직접 가공된 데이터를 지상으로 전송하는 개념을 발전시키고 있다(아시아경제 2024/3/3).

우주 데이터센터가 현실화된다면 우주 데이터에 대한 안보 위협의 성격은 크게 변화할 가능성이 높다. 즉, 데이터 생성, 분석, 식별가공, 저장이 수십에서 수백 개의 위성을 통해 분산되어 이뤄지고, 최첨단 레이저 통신으로 이들 간 데이터 전송이 이뤄진다면, 데이터를 위변조, 탈취, 오용하기가 어려워진 반면, 일단 해킹이 성공할 경우, 즉각적인 군사적 활용이 가능하다는 위험이 존재한다. 나아가, 충분한 회복탄력성이 보장되지 않을 경우, 소수의 데

이터 노드 위성, 저장 위성 등의 물리적, 비물리적 파괴를 통해서 우주 데이터의 활용을 저해할 수 있다.

(3) 우주 안보를 위한 데이터(data for space security)

우주 안보와 데이터 안보가 연계되는 또 다른 차원은 우주 안보를 위한 데이터이다. 이는 우주 안보의 핵심요소인 우주시스템, 특히 우주부문(space segment)에 대한 위협으로부터의 안전와 안보를 제고하는데 필수적인 데이터와 관련된다. 매우 적대적인 환경인 우주 공간에서 태양풍, 태양흑점, 플레어, 지자기 폭풍 등은 우주부문뿐만 아니라 업링크 · 다운링크, 그리고 심지어 지상에까지 부정적 영향을 미친다. 이러한 자연적인 영향뿐만 아니라 인간의 의도적이고 비의도적인 활동 역시 위성과 발사체 등을 위협한다. 따라서, 우주 파생 데이터와 서비스를 지속적이고 안전하게 이용하기 위해서는 이에 대한 위험과 위협 등에 대한 정보가 매우 중요하다.

따라서, 안전하고 지속가능한 우주 활동을 수행하기 위해서는 우주 공간에서 움직이는 물체들과 이들의 움직임에 영향을 미칠 수 있는 다양한 자연적 환경적 변수들에 대한 정확하고 시의적절한 데이터가 매우 중요하다. 일반적으로 우주상황인식(space situational awareness, SSA)은 우주 물체들의 위치, 방향, 속도 등에 대한 정보 및 우주 기상에 대한 (준)실시간 지식을 의미한다. EU의 경우, SSA를 “우주 물체 간의 충돌, 파편, 우주 물체의 대기권 재진입, 우주 날씨 현상, 근지구 물체 등을 포함한 주요 우주 위험 요소에 대한 포괄적인 지식과 이해를 포함하는 종합적(holistic) 접근”으로 정의한다(EU Law 2021). 이와 유사하지만 군사적 관점에서 미국 합참은 “우주 작전을 수행하는데 우주 물체와 작전 환경에 대한 필수적인 기반이 되며, 현재 상태와 예측을 포함하는 지식과 특성으로, 여기에는 우주 작전을 수행하거나 준비 중인 모든 주체의 모든 요소, 활동, 사건도 포함”하는 것으로 SSA를 정의한다(U.S. Joint Chiefs of Staff 2020).[10] 보다 구체적으로, SSA는 대체로 3개의 하위 요소를 포함하는데, 먼저 지구궤도 상 우주 물체들을 감시하고 추적하는 데이터, 정보, 서비스를 생성하고, 활용하는 우주 감시 · 추적이다. 둘째, 우주 기상 환경을 관측하고 관련 데이터를 만들고 활용하는 것이다. 셋째 지구에 접근하는 물체의 위험을 모니터링하는 것이다.

먼저 우주 물체를 감시 · 추적하는 데이터는 우주 안보를 위해서 매우 중요하다. 지구궤도를 따라 움직이는 우주 물체는 현재 작동하는 위성뿐만 아니라 무수히 많은 우주 잔해

[10] 이와 유사하지만, 보다 군사적 의미에서 우주 활동 주체의 특징과 의도를 파악하고 이해하는 것은 우주영역인식(space domain awareness, SDA)이라고 불리며, SSA보다 더 포괄적인 개념으로 받아들여진다.

(space debris)를 포함한다. 궤도상에서 떠돌아다니는 1cm 이상 크기의 우주 잔해의 숫자는 110만 개 이상으로 추정되며(European Space Agency 2024), 향후 10년 내로 2만여 개 이상의 위성이 발사될 것으로 예측된다. 이러한 상황에서 위성끼리 혹은 위성과 잔해가 충돌할 가능성과 함께 이러한 충돌로 인해 연쇄적 충돌이 일어날 가능성 역시 증가하고 있다. 군사용 위성이 이러한 충돌에 관여된다면 안보에 직접적인 영향을 미칠 것이고, 만약 직접 충돌을 하지 않고 충돌의 가능성이 있다고 하더라도 회피기동이 필요하다면 안보적 관점에서 손실이 클 수 있다(정헌주 2024). 이러한 충돌 가능성을 미리 파악하기 위해서는 다양한 방식을 통해서 우주 물체를 식별하고, 구분하며, 위험을 평가하고, 경고하고, 대응하는 일련의 과정이 필요하다.

또한, 우주 기상에 대한 정보 역시 우주 안보를 위해서 중요하다. 태양 플레어로 인한 양성자 방출이나 코로나질량방출, 고속태양풍 등과 같은 태양활동뿐만 아니라 지구 자기권에서의 자기폭풍 등은 위성체 및 위성 운영에 영향을 주거나 통신 장애, PNT 수신 장애, 정전 사태 등을 일으키기도 한다. 이를 모니터링하고 예측하며 대응하는 것은 우주 안보와 경제를 위해서 중요하다. 마지막으로, 우주에서 지구로 접근하는 물체의 위험을 모니터링하고 예측하는 것 역시 중요한데 특히, 우주 공간을 경유하여 지상으로 재진입하는 탄도미사일의 경우, SSA의 중요한 대상이다. 이렇듯 우주 안보를 위한 데이터는 이러한 점에서 매우 중요한 안보적 함의를 갖는다.

동시에 SSA는 다른 데이터와 다르게 국제협력이 꼭 필요한 영역이기도 하다. 실제로 보다 정확하고 실시간에 가까운 SSA를 위해서는 전지구 및 궤도에 분산되어 있는 센서들의 네트워크와 함께 위성 운영자들과의 데이터 공유가 필요하다. 이러한 센서들은 지상 혹은 우주에 기반을 둔 광학장비나 레이더이며, 최근에는 무선주파수나 적외선 등이 이용되기도 한다. 미국과 EU 등은 다양한 지상 기반 센서들과 우주 기반 우주감시(space-based space surveillance, SBSS)시스템을 통해서 SSA 역량을 갖추기 위해서 노력하고 있다. 특히 SBSS는 날씨나 대기, 시간에 의해서 방해받지 않고 우주 상황을 인식할 수 있다는 점에서 매우 활용도가 높은 것으로 알려졌다. SSA와 관련된 미국의 대표적인 시스템은 미국은 우주감시네트워크(Space Surveillance Network, SSN)이며, 미국 우주군에 의해서 운영되고 있다(송태은 2023).

이러한 SSA 관련 데이터는 매우 중요하며 공공재적 성격을 지니고 있다. 이러한 점에서 미국은 SSA와 관련된 데이터 중 비밀을 제외하고는 웹사이트(www.space-track.org)에 공개하고 있다. 또한, 미국의 우주사령부(US Space Command)는 다양한 우주행위자들—국가, 정부간기구, 민간기업, 학계 등—과 '우주상황인식 정보 공유 협정(SSA information sharing agreement)'를 맺고 있는데, 2024년 4월 현재 약 185개 이상의 협정을 맺은 것으

로 알려졌다(U.S. Southern Command 2024/4/11). EU의 경우, EU Agency for the Space Programme이 운영하는 EU Space Surveillance and Tracking(EU SST) 서비스를 통해서 SSA 데이터를 제공하고 있다(EUSPA 2024). EU SST의 경우, EU 회원국으로부터 제공되는 40개 이상의 센서를 통해서 수집된 정보를 200 이상의 조직에게 서비스를 제공하고 있으며, 400개 이상의 위성을 충돌 위험으로부터 보호하는데 기여하고 있다.

4. 한국의 우주-데이터 안보: 현황과 과제

한국은 우주 안보와 데이터 안보의 연계를 인식하고, 이러한 연계를 통해서 국가안보를 제고하기 위해 노력하고 있다. 특히, 북한의 핵 · 미사일 능력이 고도화되고 있고, 동아시아 안보의 불안정성이 높아짐에 따라 군사용 우주시스템을 획득하고 활용하고 있다. 동시에 국가가 운용하는 우주시스템이 증가함에 따라 이들의 안전을 보장하기 위한 노력과 우주-사이보안보 역량 강화 노력 역시 전개하고 있다. 이를 구체적으로 살펴보면 다음과 같다.

첫째, 우주 데이터를 활용한 안보(security by space data)이다. 한국의 경우, 북한의 핵 · 미사일 위협을 가장 중요한 안보위협으로 간주하고 있으며, 특히 이에 대응하기 위한 한국형 3축체계 중 "킬체인(Kill Chain)"과 "한국형미사일방어(Korea Air and Missile Defense, KAMD)"에서 우주 데이터는 핵심적 역할을 수행한다. 한국군의 대북 감시정찰을 위한 핵심 전력인 정찰위성을 확보하고자 하는 소위 425사업은 이러한 노력을 대표하는 사업이다. 2025년까지 군사용 정찰위성 5대—전자광학/적외선(EO/IR) 위성 1기와 합성개구레이더(SAR) 위성 4기—를 저궤도에서 운용하는 425사업의 일환으로 2023년 12월 EO/IR 위성인 1호기가 발사되었고, 2024년 4월에 SAR를 탑재한 2호기가 성공적으로 발사되었다(중앙일보 2024/4/8). 3호기~5호기는 2024년과 2025년에 발사되어 전력화될 예정이다. 이와 더불어 2030년까지 50~60기의 (초)소형위성을 활용한 감시정찰 위성군, 조기경보위성 등을 확보하기 위한 사업도 진행 중인 것으로 알려졌다.

우주시스템을 활용한 통신 역시 이러한 노력의 일환이다. 2006년 8월 발사된 무궁화 5호는 민군겸용 정지궤도 통신위성으로, 여기에 군용 통신위성인 아나시스 1호가 탑재되었다. 아나시스 1호는 기존의 군 통신반경을 획기적으로 확대하고 보안성을 강화하였지만, 민군겸용이라는 한계가 지적되었다. 이에 군 전용 통신위성인 아나시스 2호가 2020년 7월 정지궤도로 발사되어 보다 향상된 통신거리, 데이터 전송 용량, 보안성을 확보하였다. 한국 국방부는 현재 군 전용통신 위성인 아나시스 3호를 2030년까지 전력화하기 위해 노력하고 있으며(한국경제 2024/5/12), 저궤도위성군을 활용한 군 통신체계 구축사업도 진행하고 있는

것으로 알려졌다. 해양 감시를 위한 위성의 통합운영 노력 역시 이러한 우주시스템을 활용하여 국가안보를 제고하기 위한 방안으로 추진되고 있다.[11] 나아가, 2030년대 중반 운영을 계획하고 있는 한국형위성항법시스템(Korean Positioning System, KPS)는 보다 정확하고 탄력적인(resilient) PNT 세비스 제공을 통해서 한국의 국방안보뿐만 아니라 경제, 사회 전반에 활용될 것이다.

하지만, 이러한 군사용 우주시스템을 통해서 제공되는 데이터를 활용할 계획만으로는 한계가 존재한다. 즉, 군사용 우주시스템을 획득하고 활용하기까지 걸리는 시간 및 예산 확보, 기술 개발 과정 등에서의 불확실성을 고려해야 한다. 그렇다면, 현재의 안보를 위해서는 이미 시장에서 구득이 가능한 우주 데이터, 즉 국내외 민간기업 및 공공부문이 제공하는 다양한 우주 데이터를 어떻게 적극적으로 활용해서 군사안보적 가치를 창출할 것인가를 고민해야 한다. 다시 말해 한국 독자적인 군사안보용 우주시스템도 중요하지만, 어떻게 민간 자산을 활용하고, 이를 한국의 국방 우주자산과 융합하는 역량을 기르는 것은 미래의 과제가 아니라 지금 당장의 과제이다.

둘째, 우주 데이터의 안보(security for space data)이다. 우주 데이터의 안보는 한국의 우주–데이터 안보에서 취약한 부분이다. 앞서 살펴보았듯이, 국가위성운영센터가 해킹 공격을 받았던 사례에서 알 수 있듯이, 우주 데이터의 획득과 생성, 분석 · 가공, 저장, 활용 등의 단계에서 방해받거나 데이터가 오염 · 탈취될 가능성이 매우 높다. 이러한 점에서 한국 정부는 「제4차 우주개발진흥 기본계획」(2022)에서 우주 안보의 중요한 목표로 우주사이버안보 역량 고도화를 제시하였고, 장기과제로 우주–항공–지상–해양 초연결 사이버안보 체계를 확립할 계획을 세우고 있다. 이를 구체화하기 위한 노력 중 하나로 2024년 6월 국가정보원은 우주 사이버보안 대응체계를 수립하기 위하여 다양한 이해관계자—국방부, 외교부, 국토교통부, 해양수산부, 과학기술정보통신부, 우주항공청 등 관계부처와 항공우주연구원, 국방과학연구소, ETRI, KAIST 등 20개 기관—가 참여하는 협의체를 출범하였다(국가정보원 2024/6/4).

하지만, 이러한 협의체를 통해서 우주 데이터의 안보를 효과적으로 제고할 수 있을지는 의문이다. 먼저 북한의 사이버공격 역량뿐만 아니라 한국 대비 우주 역량의 비교 열위를 고려하였을 때, 우주 데이터에 영향을 미치려는 북한의 시도는 계속될 것이다. 특히, 북한은 보다 정교해진 사이버공격 역량을 기반으로 우주 관련 기술을 탈취하고, GPS 재밍 등을 시도하는 것으로 알려졌다(Swope et al. 2024, 27). 더욱 중요한 점은 한국의 우주 데이터를 탈취, 조작, 침해하려는 행위자는 단지 북한뿐만이 아니라 다양한 잠재적 적국, 경쟁국, 그리고 사적 행위자(경제적 목적뿐만 아니라 명성 등 비경제적 목적의 활동) 등이 포함된다는 것

[11] 우주 데이터를 다양한 방식으로 활용할 계획 역시 존재한다(「제4차 우주개발진흥 기본계획」 참조).

이다. 나아가, 우주시스템을 구성하는 각 하위부문에서 생애주기 상 보안취약성을 식별하고 대응하기 위한 노력이 필요하다. 이러한 점에서 우주 데이터의 안보를 위해서는 전정부적(whole-of-government) 관점이 반드시 필요하다.

셋째, 우주 안보를 위한 데이터(data for space security)이다. 관련해서 한국 정부는 우주 감시체계(광학, 레이더, 레이저, 전자기 관측 장비 등)을 확보함으로써 SSA와 나아가 우주교통관제(space traffic management, STM)을 강화하기 위해 노력하고 있다. 「제4차 우주개발진흥 기본계획」(2022)에 따르면, 한반도 상공을 통과하는 우주물체를 감시하기 위해서는 "고출력 레이저 위성추적 체계, 레이더 우주감시 체계, 전파감시체계 등"을 2027년까지 확보할 계획이다. 또한, 우주 기상 관측을 위해 2024년까지 실시간 예 · 경보체계를 구축하려고 한다. 현재 기상청은 우주기상 예 · 특보 서비스를 제공하고 있다(항공기상청 2024). 나아가 부족한 SSA 역량을 보완하기 위하여 국제협력을 강화하고 있다.

우주-데이터 안보를 위한 이러한 노력에서 중요한 점은 한 국가의 노력으로 안 되는 부분들이 많으며, 이를 위해서는 국제협력, 특히 국제규범을 창출하고 준수하기 위한 협력이 필요하다. 예를 들면, 우주시스템에 대한 물리적 공격이 가져올 수 있는 파멸적 결과를 방지하기 위하여 직접상승 반위성무기(direct-ascent anti-satellite weapon, DA-ASAT) 실험을 금지하는 노력에 많은 국가들이 동참하였다(박시수 2023/8/27).[12] 또한, 유엔 COPOUS는 10여 년 간의 노력 끝에 2019년 "우주활동의 장기지속가능성(LTS)" 가이드라인을 공식 채택하였다. 비록 강제력은 없지만 국가들이 국내적으로 가이드라인을 이행함으로써 안전하고 지속가능한 우주 활동이 가능하도록 규범적 영향력을 가하고 있다.

5. 결론

우주를 통해서 생성되는 데이터의 중요성은 갈수록 커지고 있다. 우주 데이터를 어떻게 안보를 위해서 활용할 것인가에 대한 고민 못지않게 이러한 데이터를 어떻게 보호하고 다른 데이터들과 융합하여 새로운 군사안보적 가치를 창출할 것인가도 중요하다. 하지만 이러한 노력에 대한 도전 역시 증가하고 있다. 특히 도전자들은 다른 국가의 우주-데이터 안보 취약성을 찾기 위해 노력할 것이다. 무엇보다 우주시스템을 직접 운영하는 것에 비해 상대국의 우주시스템에 의해서 창출되는 데이터에 영향을 미치는 비용이 월등히 적다는 점 역시 이러한 취약성을 활용하려는 인센티브를 강화시킨다.

[12] ASAT 실험 금지(포기) 선언을 한 국가는 미국(2022년 4월)을 포함하여, 한국, 오스트리아, 프랑스, 독일, 이탈리아, 일본, EU 모든 회원국 등이다.

나아가 우주 데이터 우위(space-derived data superiority)의 군사적 중요성을 고려하였을 때, 지배적인 국가와 도전국 사이의 격차가 커진다면, 도전국은 자국의 우주 자산 피해를 감내하더라도 지배적 국가의 우주 자산과 데이터에 대한 접근을 막기 위하여 (핵 · 非핵)EMP 또는 ASAT 미사일을 활용할 가능성도 배제할 수 없다. 나아가 현재 운용되는 위성에 적용된 데이터 보안 기술은 발사 당시의 기술을 반영한다는 점에서 빠르게 변화하는 현재와 미래의 사이버 공격에 취약할 가능성이 높다. 따라서, 우주-데이터 안보의 다양한 측면을 고려한 역량 강화와 대비가 필요하다.

우주-데이터 안보와 관련하여 또 하나의 중요한 고려사항은 뉴스페이스 시대 민간의 역할이다. 어떻게 민간부문에서 창출되는 막대한 우주 데이터를 군사안보를 위해서 활용할 것이며, 새로운 지식을 창출할 것인가는 한 국가의 군사안보역량에 중대한 영향을 미칠 것이다. 또한 잠재적 경쟁국 역시 민간에 의해서 제공되는 우주 데이터를 활용하기 위해 노력할 것이며, 이에 대해서 어떻게 대응할지는 또 다른 과제이다.

한반도와 동북아시아의 평화와 안정을 위해서 우주 안보와 데이터 안보의 중요성은 갈수록 커지고 있다. 한국은 우주 안보와 데이터 안보의 다양한 연계—우주 데이터를 이용한 안보, 우주 데이터의 안보, 우주 안보를 위한 데이터—를 고려하여, 현재와 미래의 상황에 대비해야 한다. 나아가 국가안보뿐만 아니라, 안전하고 안정적이며 지속가능한 우주환경을 조성하기 위한 국제규범 형성에 적극적으로 참여하고 양자-다자간 국제협력을 강화하는 우주 외교(space diplomacy) 역량 역시 강화할 필요가 있다.

〈참고문헌〉

강종구 · 이양원 · 김대선. 2023. “Sentinel-2 위성과 국토위성에서의 딥러닝 기반 초해상화 기법 비교 연구.”『국토지리학회지』제57권 4호.

국가정보원. 2024. “국정원, 위성 사이버보안 강화를 위한 관계기관 협의체 출범(2024.6.4.).” https://www.nis.go.kr/CM/1_4/view.do?seq=296(검색일: 2024년 8월 2일).

김상배. 2020. “데이터 안보와 디지털 패권경쟁: 신흥안보와 복합지정학의 시각.”『군사전략』제26권 2호.

김은정. 2015. “위성 특성에 따른 위성영상 차이.” https://www.kari.re.kr/cop/bbs/BBSMSTR_000000000064/selectBoardArticle.do?nttId=5150(검색일: 2024년 8월 10일).

동아사이언스. 2016. “정부, 구글 지도 반출 불허 “위성 사진 때문에…”(2016.11.18.).” https://m.dongascience.com/news.php?idx=14815(검색일: 2024년 1월 15일).

박시수. 2023. “EU 모든 회원국, ‘인공위성 요격 미사일 시험’ 중단 선언.”『SpaceRadar』8월 27일.

송태은. 2023. “우주안보와 정보 · 데이터 안보.” 서울대학교 국제문제연구소 이슈브리핑, No. 208.

아시아경제. 2024. “인공위성 수백개로 우주에 데이터센터 만든다(2024.3.3.).” https://www.asiae.co.kr/article/2024022911000624452(검색일: 2024년 4월 25일).

연합뉴스. 2024. “우크라 드론전 핵심 머스크 스타링크 장애…러도 사용 의혹(2024.3.27.).” https://www.yna.co.kr/view/AKR20240327144200009(검색일: 2024년 4월 2일).

연합인포맥스. 2020. “그림자로 원유재고 알아낸다…데이터 분석의 진화(2020.4.13.).” https://news.einfomax.co.kr/news/articleView.html?idxno=4082410(검색일: 2024년 2월 20일).

정보통신산업진흥원. 2024. “글로벌 ICT 주간동향리포트: 미국 주요 테크기업, 우주 클라우드 시장 주도(2024.2.16.).” https://www.globalict.kr/news/trend/weekly.do?menuCode=010200&knwldNo=143644(검색일: 2024년 8월 10일).

정헌주. 2021. “미국과 중국의 우주 경쟁과 우주안보딜레마.”『국방정책연구』제37권 1

호.

정헌주. 2024. “우주 환경 안보의 국제정치: 우주잔해 국제협력에 대한 국제정치학적 접근.”『국가안보와 전략』제24권 2호.

조선비즈. 2016. “[구글지도 반출불허] 정부, 구글에 퇴짜놓은 이유는…안보 위험 가중 우려 (2016.11.18.).” https://biz.chosun.com/site/data/html_dir/2016/11/18/2016111801241.html(검색일: 2024년 1월 15일).

조선비즈. 2024. “한국 위성 운영의 심장 해킹에 뚫렸다…우주청 설립 앞두고 보안 ‘구멍’ (2024.3.26.).” https://biz.chosun.com/science-chosun/science/2024/03/26/QH6X2YD5A5FLDJLDYJXJPMJA5M/(검색일: 2024년 4월 5일).

중앙일보. 2024. “韓 정찰위성 2호 발사…악천후에도 北 감시할 '고성능 눈' 생겼다(2024.4.8.).” https://www.joongang.co.kr/article/25240990#home(검색일: 2024년 6월 10일).

한국경제. 2024. “軍전용 통신위성 아나시스 3호 2030년 띄운다(2024.5.12.).” https://www.hankyung.com/article/2024051240221(검색일: 2024년 6월 20일).

항공기상청, “우주기상(국가위성센터),” https://amo.kma.go.kr/weather/aviation/aviation-space-nmsc.do(검색일: 2024년 8월 20일).

KBS. 2020. “원유 탱크 ‘지붕 그림자’로 보관량 안다…‘원유개미’ 살 길은?(2020.4.28.).” https://news.kbs.co.kr/news/pc/view/view.do?ncd=4434570(검색일: 2024년 3월 2일).

KBS. 2024. “러시아, 인공위성 파괴 가능할 핵 전자기파 무기 개발 중(2024.2.17.).” https://news.kbs.co.kr/news/pc/view/view.do?ncd=7892710(검색일: 2024년 4월 15일).

Allied Market Research. 2024. “Satellite Data Services Market Statistics 2021-2030.” https://www.alliedmarketresearch.com/satellite-data-services-market-A06428(검색일: 2024년 4월 10일).

CIO. 2024. “Data centers in space(2024.2.20.).” https://www.cio.com/article/1308658/data-centers-in-space.html(검색일: 2024년 4월 20일).

Dolce, Ferdinando, Davide Di Domizio, Denis Bruckert, Alvaro Rodríguez, and Andrea Patrono. 2020. "Earth Observation for Security and Defense," Kai-Uwe Schrogl, Maarten Adriaensen, Christina Giannopapa, Peter Hays, Jana Robinson, and Ntorina Antoni (eds.). Handbook of Space Security: Policies, Applications and Programs. 2nd ed. New York: Springer.

EU Law. 2021. "REGULATION (EU) 2021/696 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL(2021.4.28.)." https://eur-lex.europa.eu/eli/reg/2021/696/oj(검색일: 2024년 7월 10일).

European Commission and European Investment Bank. 2019. The Future of the European Space Sector: How to leverage Europe's technological leadership and boost investments for space ventures. European Investment Bank.

European Space Agency. 2024. "Space Environment Statistics." https://sdup.esoc.esa.int/discosweb/statistics/(검색일: 2024년 7월 10일).

EUSPA. 2024. "EU SST." https://www.euspa.europa.eu/eu-space-programme/ssa/eu-sst(검색일: 2024년 8월 12일).

Heideman, Matthew. 2024. "Why we need to take satellite ground station security seriously," SpaceNews. June 4.

Li, Jun, Zhi He, Javier Plaza, Shutao Li, Jinfen Chen, Henglin Wu, Yandong Wang, and Yu Liu. 2017. "Social Media: New Perspectives to Improve Remote Sensing for Emergency Response," Proceedings of the IEEE. Vol. 105, No. 10: pp. 1900-1912.

Meyer, Gregory, and Francis Stallings. 2011. "Is space the ultimate high ground?" Proceedings SPIE 8044, Sensors and Systems for Space Applications IV. , 80440K.

Naval News. 2023. "Russia's Powerful Invisible Defenses Around Sevastopol Rendered Visible(2023.11.28.)." https://www.navalnews.com/naval-news/2023/11/russias-powerful-invisible-defenses-around-sevastopol-rendered-visible/(검색일: 2024년 6월 10일).

Northern Sky Research. 2021. "Space Traffic Data Volumes Increase 14X Over the Next Ten Years(2021.12.6.)." https://www.nsr.com/space-traffic-data-volumes-increase-14x-over-the-next-ten-years/(검색일: 2024년 3월 10일).

NTT. 2022. "NTT and SKY Perfect JSAT Agree to Establish Space Compass

Corporation: Novel Space Integrated Computing Network Enterprise to Aid Realization of a Sustainable Society(2022.4.26.)." https://group.ntt/en/newsrelease/2022/04/26/220426a.html(검색일: 2024년 4월 30일).

Peperkamp, Lonneke, and Patrick Bolder. 2024. "The Space Domain and the Russia–Ukraine War," Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (eds.). Reflections on the Russia–Ukraine War. Leiden University Press.

Rivero, Jorge. 2024. "Decoy Warfare: Lessons and Implication from the War in Ukraine," U.S. Naval Institute Proceedings. Vol. 150/4/1,454.

Spacenews. 2024. "Aerospacelab to build Xona Space's first navigation satellite(2024.3.19.)." https://spacenews.com/aerospacelab-to-build-xona-spaces-first-navigation-satellite/(검색일: 2024년 4월 15일).

Swope, Clayton, Kari Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo. 2024. Space Threat Assessment 2024. Washington DC: Center for Strategic & International Studies.

The International Charter Space and Major Disasters. 2024. "About the Charter." https://disasterscharter.org/web/guest/about-the-charter(검색일: 2024년 1월 14일).

U.K. Legislation. 2021. "The National Security and Investment Act 2021." https://www.legislation.gov.uk/uksi/2021/1264/schedule/14(검색일: 2024년 5월 1일).

U.S. Joint Chiefs of Staff. 2020. "Space Operations." Joint Publication 3-14, April 10, 2018, Incorporating Change 1, October 26, 2020.

U.S. Southern Command. 2024. "USSPACECOM advances space partnerships in South America as part of Space Symposium 39 international engagements(2023.4.11.)." https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3739638/usspacecom-advances-space-partnerships-in-south-america-as-part-of-space-sympos/(검색일: 2024년 8월 10일).

U.S. White House. 2020. "Space Policy Directive-5: Cybersecurity Principles for Space Systems(2020.9.4.)." https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/(검색일: 2024년 6월 10일).

UN. 2018. European Global Navigation Satellite System and Copernicus: Supporting the Sustainable Development Goals. United Nations Office for Outer Space Affairs.

WPR. 2024. "Military Satellites by Country 2024." https://worldpopulationreview.com/country-rankings/military-satellite-by-country(검색일: 2024년 7월 10일).