Institute For National Security Strategy
www.inss.re.kr

November 2024.
No. 290

INSS 전략보고

우주 사이버 위협의 난제와 한국의 대응 방안

윤정현 연구위원
yjh5791@inss.re.kr

Ⅰ. 문제 제기
Ⅱ. 뉴스페이스 시대의 우주 사이버 위협
Ⅲ. 한국의 우주-사이버 안보 환경 진단과 주요국의 대응 현황
Ⅳ. 우주 사이버 난제에 대한 대응 방안

국가안보전략연구원

November 2024.
No. 290

CONTENTS

우주 사이버 위협의 난제와 한국의 대응 방안

I. 문제 제기

II. 뉴스페이스 시대의 우주 사이버 위협

1. 우주-사이버-신기술의 연계가 초래한 불확실성
2. 우주 사이버 위협의 구조적 난제

III. 한국의 우주-사이버 안보 환경 진단과 주요국의 대응 현황

1. 한국의 우주 사이버 안보 취약성 진단
2. 주요국의 대응 : 현황과 함의

IV. 우주 사이버 난제에 대한 대응 방안

1. 다층적 위협 기반 사이버 방어모델 수립
2. 우주 사이버 위협의 비대칭성 완화
3. 국가안보전략 및 주요 지침과의 연계성 강화
4. 민관 우주 사이버 협력 기반 조성

우주 사이버 위협의 난제와 한국의 대응 방안

저자 | 윤정현

국문 초록

최근 우주 활동이 민간의 컴퓨팅 시스템 및 통신 네트워크로 확대됨에 따라 우주 사이버 안보의 중요성이 증대되고 있다. 우주, 사이버, 신기술이 결합되어 불확실성이 증대되고 있는 우주 공간의 취약성은 단순히 양적 위협으로 치환하기 어려운 복합적인 속성 또한 내재하고 있다. 이 같은 우주 사이버 안보 환경의 난제에 대비하기 위해 우리는 이들 복합 공간의 구조적인 취약점은 무엇이며 어떠한 경로로 위협이 발현, 확산되는지 선제적인 탐색이 필요하다.

본 연구는 우주-사이버 공간의 복합적 위협이 제기하는 양상과 난제적 속성을 기반으로 한국의 상황과 주요국의 대응현황을 진단하고, 각각의 구조적 위협에 조응하는 대응방안을 제시하고자 하였다. 한국의 우주 사이버 대응 역량 강화를 위해서는 첫째, 우주 시스템에 대한 사이버 위협에는 지상, 링크, 우주 부문을 포함해 전방위적 접근이 필요하다. 둘째, 우주 사이버 영역의 안보딜레마를 촉진하는 비대칭성과 주체의 다양성에 대비해야 한다. 셋째, 국가안보전략 및 사이버안보전략과 밀접히 연계된 국가우주안보전략 및 우주 사이버 대응방향이 정립되어야 한다. 넷째, 우주 사이버 안보 시대에 부합하는 민관군 파트너십을 강화하고 협력 거버넌스를 새롭게 정립해야 한다.

주제어: 우주 사이버 위협, 구조적 난제, 뉴스페이스, 우주안보전략, 민관협력

Ⅰ 문제제기

▪ 뉴스페이스 시대의 도래와 함께 우주-사이버-신기술이 결합한 우주 사이버 위협 이슈가 새로운 난제로 부상 중

- 최근 우주개발의 디지털 의존도 증가 및 사이버 공간과 연계된 우주 시스템의 확대는 우주-사이버 공격에 대한 취약성을 내재

  ※ 우주 공간의 활용 확대에 따라 이를 효과적으로 관리하기 위한 사이버 운용체계의 도입은 다차원적 사이버 공격에 대한 취약 표면을 노출

- 우주-사이버-지상 간 연계 심화와 AI 등 신기술의 적용 또한 운용 과정에서의 불확실성과 중요 정보 탈취의 가능성을 내포
- 또한, 위성정보 하이재킹, 전자파 교란 등 우주와 사이버 공간을 매개로한 회색지대에서 구조적 우위에 있는 다양한 공격행위자의 위협에 노출

  ※ △우주 자산 급증과 (비)국가 행위자 공격 가능성 증대, △통신·데이터 취약성으로 전주기(life cycle) 위협, △공격자 우위의 비대칭성으로 인한 위협, △AI 등 신흥기술와 융합에 따른 불확실성 등

▪ 최근 증대되고 있는 우주 사이버 위협들에 대한 면밀한 분석을 통해 복합 위협의 난제적 속성 분석과 대응 방안 모색이 시급

- 현재의 우주기술은 △공격·방어의 경계가 불확실하고, △이중용도로 활용 가능하며, △상대의 의도가 불확실하고, △피해의 원인이 불확실한 특징을 내재
- 이에 따라, △다차원적 연계의 취약성, △공수 비대칭 구조, △전략적 연계성 부족, △민관 파트너십 구축 곤란 등의 난제를 심화시킴

▪ 우주 사이버 위협에 대한 우리의 대응 환경 진단, 대응전략 체계 및 지침, 다층적 파트너십의 측면에서 종합적인 검토가 필요

- 우주-사이버 안보와 같은 공공분야에서 이해관계자들이 직면한 도전에 대한 공동의 인식, 상호 협력을 위한 역할의 조정, 이를 뒷받침하는 제도적 정합성을 확보할 것이 요구됨
- 따라서 본고는 최근 발생하는 우주 사이버 위협의 현황과 난제적 속성을 검토하고, 주요 우주 선도국들의 대응 시사점을 토대로 한국적 맥락에서의 우주 사이버 역량 강화 방향을 제언

Ⅱ 뉴스페이스 시대의 우주-사이버 위협

1. 우주-사이버-신기술 연계가 초래한 불확실성

가. 우주자산의 양적 급증에 따른 취약성 심화

▪ '우주 新경제'로 상징되는 미래 시장으로서의 측면이 강조되면서, 공급망 확대, 민간의 우주개발 참여 등으로 인해 우주자산이 양적으로 증가하면서 우주가 안보적 측면의 핵심 공간으로 부상[1]

- 우주 기술의 고도화의 이면에는 네트워크 시스템에 절대적으로 의존하고 있는 우주자산, 우주 인프라의 운영 및 우주 통신체계의 취약성 내재
- 우주 공간은 위성의 설계에서부터 발사 및 비행 운영에 이르기까지 통신·제어 시스템과 네트워크에 의존, 개발·활용 전주기 단계에 걸쳐 광범위한 사이버 공격의 표면을 노출

※ 광범위한 데이터의 손실, 우주 시스템 또는 위성의 수명 및 기능 저하, 우주선에 대한 통제력 상실, 시스템에 대한 잠재적 손상이나 유해한 궤도 잔해물과의 충돌 가능성의 증가 등

나. 신기술과의 결합이 초래한 우주 공간의 안보 공백 증대

▪ 상업적·군사적으로 새롭게 부상하고 있는 우주 공간은 기술융합을 바탕으로 지상-디지털 세계와 긴밀히 결합 중

- 이종 영역 간의 취약한 연결고리가 유발하는 불확실성과 직간접적 연계 부문의 새로운 도전 이슈 제기
- 위성 네트워크를 활용하는 넓은 서비스 영역이 장기간의 치명적인 피해로도 직결되며, 지상 인프라에 대한 사이버 공격에도 비대칭적 취약성 내포

※ 최근 우주상황인식(space situational awareness)을 수행하는 위성은 운용 과정에서 AI의 도입에 따른 자율적 임무 수행을 확대하고 있으나 운용체계의 해킹이나 데이터 훼손의 공격 위협에 노출

1 윤정현·이성훈, "뉴 스페이스 시대의 민관협력 변화와 한국형 발전방향 모색", 『국가전략』, (2023 가을호), 제29권 3호, p. 183.

다. 우주 사이버 안보 공간의 안보 딜레마 심화

▪ 우주와 사이버 공간에서는 공격자 우위 구도의 속성을 안고 있으며, 우주-사이버-신기술 연계로 인해 불균형 심화

※ 익명성: 은밀성을 내재한 공격을 감행한 주체의 확인이 어려우며, 책임귀속의 난제 유발

※ 첨단 인프라의 역설: 고도로 정보화된 디지털 사회일수록 사이버 공격의 취약성은 증대

※ 억지 전략의 한계: 사이버 공격행위에 대한 적절한 억지와 처벌, 예방의 전략 수립을 불가능하게 함

- 인공지능(AI) 등 진화된 자동화시스템은 데이터·정보 위협과 통제의 문제를 초래하여,[2] 파급력의 불확실성과 공격자의 우위 구도를 강화

※ 접근 용이성: 국가, 전문집단 뿐만 아니라 비숙련 개인과 비인간 행위자가 전면에 등장

※ 통제 불확실성: 특정 데이터의 분석·처리를 넘어 시스템 자체를 운용·제어하는 수준으로 진화

※ 신뢰성 훼손: AI시스템 라이프 사이클 전주기 단계에서 데이터를 탈취, 유출, 조작 변조, 오염 가능

2. 우주 사이버 위협 대응의 구조적 난제

가. 위협의 다차원적 속성

▪ 새롭게 부상한 안보 영역으로서 우주-사이버-신기술의 결합은 물질적·비물질적 복합성으로 인한 구조적 취약성을 내재

- 이러한 구조적 취약성은 사안별, 혹은 이슈별 파편적 대응이 아닌, 복합적인 우주 사이버 위협 속성을 종합적으로 이해하고 시스템 차원에서 접근해야할 필요성을 제기
- 우주 사이버 위협의 복합적인 양상을 유형화하고 효과적 대응을 위한 분석틀의 수립과 핵심 쟁점들에 대한 탐색이 우선되어야 함

2 미국 우주군은 '2024 데이터-인공지능 전략 실행 계획(Data and Artificial Intelligence FY 2024 Strategic Action Plan)'을 수립, 데이터 최적화에 기반한 AI 기술을 우주 작전에 적용하려고 시도. US Space Force, "Space Force publishes Data, AI strategic action plan," May 14, 2024. https://www.spaceforce.mil/News/Article-Display/Article/3774329/space-force-publishes-data-ai-strategic-action-plan/ (검색일 : 2024. 5. 16)

▪ 우주 사이버 위협의 다차원적 연계 공격 위험

- 우주와 사이버 공간이 태생적으로 가지고 있는 취약성은 지상연계공격 또는 링크부문공격을 통해 증폭될 우려

〈표 1〉 우주 사이버 연계 공격 유형의 구분

구분	공격명	공격의 주요 특징
지상연계 공격	• 불법 접근	– 허가받지 않은 공격자가 명령어를 전송하거나 위성 혹은 지상국 데이터에 접근하는 것
	• 정보 유출	– 위성과 지상국 간의 명령어 및 데이터 송수신 과정에서 발생하며 특정 주파수를 청취하는 스니핑 공격을 통해 송수신 데이터에 대한 위치/운영정보 등 중요정보에 불법 접근하는 것
	• 서비스 거부(Dos)	– 위성 혹은 지상국에서 정상적인 기능을 수행할 수 없도록 지속적인 부하를 가하여 처리 능력을 마비시키거나 명령 송수신을 방해하는 공격
	• 소프트웨어 위협	– 위성 혹은 지상국에서 사용하는 소프트웨어의 취약점을 노린 공격으로 시스템을 파괴하거나 정보유출 및 변조 등의 형태로 공격 가능
	• 사회공학적 해킹	– 지상국 관리자와 사용자를 대상으로 원하는 정보를 얻어내기 위한 심리적 공격 기법
링크 부문 공격	• 재전송 공격	– 통신 내용을 가로채어 보관 후, 나중에 이를 재전송하는 공격
	• 트래픽 분석	– 통신 트래픽의 패턴을 분석하여 정보를 추출하는 것으로 추론을 통해 위성에 송수신되는 신호를 임의로 조작하거나 탈취하는 공격
	• 데이터 변조	– 정상적인 명령어 및 데이터의 일부 내용을 불법적으로 변경하는 공격
	• 재밍	– 무선 주파수(RF) 또는 광학 신호를 이용하여 의도적으로 통신 링크에 간섭을 주는 공격으로 통신 안정성 방해 및 링크 손실 유발

출처: 류재철(2023), 엄정식(2024), pp. 73-83을 토대로 재정리

- 통제의 불확실성과 예상치 못한 안보적 파급효과를 야기, 중대한 도전으로 부상

※ △내부 아이디를 통해 악성코드를 심어 위성에서 보내는 데이터 탈취, △지상관제소를 통한 데이터 손상 및 관제 오류 발생, △위성의 통제권 탈취하여 연료 소모 유도 및 우주에서 사고 발생 유도 등

나. 공수 비대칭성과 의도 파악의 난제

▪ 공격 주체의 다변화와 공격 방식의 유연성, 책임 귀속의 제한 등의 이유로 사이버 위협의 비대칭성 문제가 제기되고 있음[3]

- 우주력이 열세한 국가나 비국가 행위자(개인 해커, 민간 기업 등)도 강대국을 상대로 공격 감행이 가능

3 윤정현·이성훈(2023), p. 189.

※ 물리적 접근이 불가능한 우주 인프라에서 발생하는 피해는 장애 원인을 파악하기 어렵다는 근본적 한계를 내포

※ 또한, 익명성으로 인한 책임 귀속이 제한되어 보다 빈번한 공격을 유인하거나 은밀한 공격 능력 개발의 유인으로 작용[4]

- 특히 지상의 우주 제어 인프라에 타격을 가하는 방식으로 원거리 위성이나 우주비행체를 노릴 수 있어 공격 효과 대비 적은 비용을 수반

▪ 이는 우주 시스템이 체계적인 국가일수록 공격 표면이 증가하여 완벽한 방어가 어려운 '첨단 인프라의 역설' 상황을 유발

※ 우주개발 선도국들은 우주자산 및 우주 인프라에 대한 활용과 의존도 증대가 높을 수밖에 없으며, 이는 기존의 사이버 공격 목표가 주로 선진국의 우주 인프라로 전환되는 기제로 작용[5]

다. 민관 협력 확대를 제약하는 보안체계의 문제

▪ 민간 위성정보가 상업적 측면 뿐만 아니라 공공·안보적 측면에서도 활용성이 증대되면서 민관군 협력·공유의 필요성이 증대됨

- 그러나 사이버 위협에 대한 민간의 대응 체계와 보안 대책 역시 현재보다 높은 수준으로 확보되어야 한다는 것을 전제

※ 최근 민간의 참여 확대로 우주개발 전주기에서 오픈소스 소프트웨어, 상용 부품 사용, 클라우드 서비스의 아웃소싱, 다단계 하청 등이 빈번히 발생

▪ 이는 상대적으로 보안이 취약한 민간 부문, 특히 중소기업들의 사이버 공격 표면의 취약성 증대로 귀결

- 일정수준의 보안체계의 강화가 뒷받침되지 않은 민관협력은 생태계 전반의 해킹 위험성을 높이는 기제로 작용 위험성 내재[6]

4 엄정식(2024), p, 178; 운동성 공격은 몇 분 안에 발견되고 신뢰할 수 있는 출처가 밝혀지지만, 데이터 유출은 중요한 시스템에서도 평균 200일 동안 탐지를 피할 수 있다. B. I. Koerner, 'Inside the OPM Hack, the cyberattack that shocked the US government', Wired, 23-Oct 2016; T. Harrison, K. Johnson, and T. Roberts, 'Space Threat Assessment 2018', 2018; J. Sigholm, 'Non-State Actors in Cyberspace Operations', Joint Military Studies, Vol. 4, No. 1, pp. 1~37, Dec. 2013

5 엄정식, 『우주안보의 이해와 분석』, (서울: 박영사, 2024), p. 178.

6 김선우, "미래 우주경제를 위한 우주 안보와 우주 사이버보안: 주요 동향 및 시사점", 『제8차 사이버국가전략포럼 자료집: 우주 사이버 안보의 현황과 쟁점』, (2024. 3. 13.), p. 21.

Ⅲ 한국의 우주-사이버 안보 환경 진단과 주요국의 대응 현황

1. 한국의 우주 사이버 안보 취약성 진단

가. 전통적 경계 기반 접근방식의 한계[7]

▪ 현재 국가우주개발의 최상위 계획인 '제4차 우주개발 기본 계획'은 5대 임무 중 하나로 우주 안보를 제시하고 있으며 우주 자산과 위성 네트워크 확장이 사이버 위협을 배가시키고 있음을 경고

- 그러나 정부의 우주개발을 종합한 2024년 우주개발진흥 시행계획에 우주-사이버 안보 관련 연구개발 사업은 제외되어 있음

  ※ 우주 사이버 안보 역량 고도화와 능동적 보호시스템 구축 및 운영이라는 핵심 목표는 2030년 이후에 추진하는 중장기 과제로 남겨둔 상황

- 추진 중인 제3차 위성정보활용 종합계획('24~28) 또한 우주정보 활용 촉진과 인프라 역량 강화를 주요 사안으로 다루고 있으며 암호화 장비 등 우주 사이버 보안체계와 직결된 프로그램은 상대적으로 미흡[8]

  ※ 주로 2030년대 국가위성 연간 획득 영상 용량 급증에 대비한 국가위성운영센터 내 서버 및 스토리지 확충에 초점을 두고 있음

나. 우주 사이버 활동의 공수 비대칭성 및 위험 식별 역량 부족[9]

▪ 현재 과학기술정보통신부를 중심으로 해킹 및 사이버 공격에 대비한 국가우주자산 및 지상 시스템, 우주통신 및 지상통신망 보안 가이드라인, 해킹 대응 시나리오 마련 등을 추진 중

- 그러나, 국가위성운영센터와 연계한 국가 핵심 인프라 및 지상국의 보안 취약성 문제가 지속적으로 제기되고 있으며, 점검 · 운영 대책 마련을 위한 제도 및 심층 연구 프로그램 등은 미흡

7 Junghyun Yoon, Jungsik Um, "Complex Challenges of Space Cybersecurity and Their Implications for ROK, *Korean Journal of Defense Analysis*, Vol. 36, No. 3 (2024), p. 355.

8 한국우주기술진흥협회, "제3차 위성정보 활용 종합 계획 안내" (2023. 5. 22.) http://www.kasp.or.kr/ kasp_news/ kasp_notice.html?ptype=view&idx=8098 (검색일: 2024. 8. 22).

9 Yoon and Um (2024), p. 356.

※ 우주위험 상황 인식을 종합적으로 다루는 법령과 추진정책이 부재하며, 『우주개발진흥법』 및 『우주위험 대비 기본계획』의 일부가 우주 감시를 통한 우주 위험 완화 정책으로 제한된 기능

다. 우주 사이버 전략과 국가안보전략의 연계 미흡

▪ 현재 국내 우주안보 관련 법제는 '국가정보원법', '우주개발진흥법', '우주항공청의 설치 및 운영에 관한 특별법'에 근거하고 있으나[10] 증대되고 있는 우주 사이버 대응체계 내용을 미포함

※ 2023년 6월 22일 시행한 우주개발진흥법에서 국가안보 관련 우주개발사업 추진 시 중앙행정기관의 장과 협의하고 보안 대책을 대통령령으로 정하도록 규정하였으나 그 실효성이 낮은 상황

※ 2024년 2월 20일에 마련한 우주개발사업 보안관리 규정 제15조에서 위성정보 데이터베이스 보호를 다루고 있으나 "해킹 등 불법 접근 및 컴퓨터 바이러스 예방 대책 강구"라는 원론적 언급에 그치고 있음

▪ 사이버 안보 정책의 최상위 전략서인'2024 국가사이버안보전략'에도 우주 사이버 안보 관련 내용은 부재

※ '국가 핵심인프라와 중요 시스템의 사이버 복원력 강화'를 주요 목표중 하나로 설정하였으나 대상 범위를 '스마트그리드 등 IT 기술이 접목된 기반시설 정도'로 명시[11]

- 이는 국가안보전략과 국가 사이버안보전략과 직결된 핵심 사안으로서 우주 사이버 역량 강화를 위한 지원 및 제도 마련의 실행 동력을 저해하는 요인으로 작용

라. 민간의 취약한 보안역량 제고를 위한 종합 가이드라인 부재

▪ 민간의 우주 사이버 위협 대응을 위한 종합 가이드라인의 부재는 민관의 긴밀한 우주 사이버 안보 협력 유인을 제약

- 현재 우주개발사업에 참여하고 있는 국내 기업들은 극소수를 제외하고는 인력 운용, 보유 기술의 축적과 관리 측면에서 공공에 비해 상대적으로 열악한 환경에 놓여있음
- 이러한 상황에서 우주시스템에 대한 민간 개방 및 기술 이전의 증가는 단기간의 사이버 공격에 대한 취약성을 높일 수 있음

※ 2024년 5월 민간 우주기업과 협업한 지구관측용 초소형 위성 성공적으로 발사, 2030년까지 민간 초소형 군집위성 등 총 100개 이상 발사 예정

10 오일석, "우주안보 발전을 위한 법제 개선: 「우주안보 업무규정」 개정의 시사점과 함의", 『INSS 전략보고』, (August 2024), No. 281, p. 1.

11 국가안보실, "국가 사이버안보 전략" (2024. 2), p. 27.

※ 발사체-위성체 제작 기업 간 자체 협업, 위성제작-위성활용 겸업 기업 등장 등 우주 시스템에 민간 기업 활동 증가 추세

▪ 민간 우주기업이 위성 설계 단계에서부터 우주 사이버 위협에 대비할 수 있도록 하는 범정부 차원의 실효적 지침이 부족한 상황

※ '우주 시스템의 사이버 안보 준수를 위한 가이드라인' 및 우주 사이버 위협 대응을 위한 민관 공동 협의체 등 부재

2. 주요국의 대응 : 현황과 함의

가. 지상-우주-사이버의 복합적 위협 대응 측면

▪ 미국은 국토안보부 산하 사이버보안 및 인프라보안국(CISA)은 우주시스템 핵심 인프라 워킹그룹을 구성하고, 우주전력망 등을 핵심 인프라로 규정, 지상과 같은 사이버보안 조치를 강화하고자 노력

- 2021년 6월 의회에서 발의한 '우주인프라법안(Space Infrastructure Act)'의 경우 국토안보부에 의해 핵심 인프라로 분류된 16개 부문[12]에 우주시스템을 추가할 것을 명시한 바 있음

▪ 또한 '국가사이버전략(National Cyber Strategy)'에 우주 자산과 인프라를 보호하며 진화하는 사이버 위협에 대응하기 위한 각 군의 다층적 협력체계를 강화하도록 명시('18. 6)[13]

- 미 국방부는 육해공, 사이버 및 우주 등 복합적 작전 영역에서 동시적으로 운영되는 작전 개념인 '다영역 작전(Multi-Domain Operations)'을 수립, 확대된 시공간과 군사적 영역이 교차하는 지점에서 군이 추구해야할 군사적 임무를 구체화[14]

▪ 중국은 효과적인 우주 사이버 안보 전략 수행을 위해 우주, 사이버, 전자, 심리전 대응 역량을 통합, 우주시스템부와 네트워크시스템부로 분할 운영되는 '중국인민해방군 전략지원부대(SSF)'를 신규 군종으로 창설

12 16개 핵심 인프라 부문은 화학, 산업시설, 통신, 핵심제조, 댐, 국방산업기반, 응급서비스, 에너지, 금융서비스, 농식품, 정부시설, 보건의료, 정보기술, 원자력, 운송시스템, 상하수도 등으로 열거된다.

13 National Cyber Security of the United States of America (Sept. 2018).

14 U.S. Department of Defense 2018: U.S. Army Combined Arms Center 2021; RAND Corporation 2021.

- 우주시스템부와 네트워크 시스템부는 우주C4ISR·우주TT&C·우주 발사와 정보·사이버 해킹·전자전·심리전을 담당하며 공동으로 우주 대항과 전략정보를 관할[15]
- 전략지원부대를 중심으로 중국은 우주 사이버 분야에서의 통합 기술 역량을 강화하고 있으며 관련 인재 양성도 함께 진행 중

▪ EU 역시 주요 인프라의 우주 서비스에 대한 의존도를 식별하고 사이버 공격으로부터 우주 자산을 보호하는 것에 정책 우선순위를 검토

- 유럽우주국(ESA)의 공식문서인 'SPACE : The Five Dimensions of Space 4.0'을 통해 유럽이 추구하는 우주 안전 및 보안 방향을 제시하고, 유럽의 우주 인프라 보호, 우주기상 및 사이버 보안 등에 중점[16]

나. 비대칭적 우주 사이버 위협 대응 측면

▪ 미중은 통합작전에 기반하여 우주시스템의 비대칭적 사이버 위협에 대응

- 미국 바이든 정부는 2024 회계연도에서 우주군이 요청한 300억 달러의 예산에 '우주 작전과 관련된 중요 네트워크의 사이버 방어를 강화'하기 위한 예산을 포함, 통합작전에 기반한'우주 회복력'강조[17]
- 중국 정부 역시 우주 산업의 상업화가 진행될수록 저비용 위성 및 위성군이 사이버 공격에 취약하여 주요 공격 대상이 될 가능성이 높다고 판단,'우주-지상 통합정보 네트워크 구축을 핵심 사업으로 추진 중
- 중국은 과학기술혁신 2030'을 통해 통합 우주 시스템이 갖는 사이버 공격에 대한 노출 위험도와 취약성에 대비하고 우주 시스템의 생존 가능성을 극대화하기 위해 우주 사이버 보안 대비를 강조[18]

※ 위성인터넷·5G 이동통신망 기술·사물인터넷 등에 기반한 '新인프라'구축 및 차세대 우주 기반 정보 네트워크 기술을 응용하여 안전하고 빠른 통합 디지털 인프라 구축을 목표로 추진

15 Adam Ni, Bates Gill. "The People's Liberation Army Strategic Support Force: Update 2019." China Brief 19 (10). 2019.05.29. https://jamestown.org/program/the-peoples -liberation-army-strategic-support-force-update-2019/

16 오일석, "뉴스페이스 시대의 우주 사이버위협 대응 방안" 『INSS 전략보고』, (November 2023), p. 6.

17 https://spacenews.com/u-s-space-force-ramps-up-cybersecurity-spending/ (2023.03.28.)

18 김다혜, 백기연, 김성훈, "주요국 우주 사이버 시큐리티 정책 동향 조사 분석", 『한국인터넷진흥원』, (2024.3), p. 17.

다. 관련 국가안보전략과의 연계성 측면

▪ 미국은 우주 시스템에 대한 취약성을 최소화하고 회복력을 강화하며, 우주통신 체계의 신뢰성과 기밀성도 유지하기 위한 정책을 시행 중

▪ 2017년 '국가안보전략(National Security Strategy)'에 우주에서 리더십과 행동의 자유를 안정적으로 유지하도록 명시

▪ 특히, 우주정책지침-5(National Space Policy, SPD-5)을 통해 우주 시스템의 사이버 위협 대응을 위한 협력방식과 임무 수행 지침을 명시('21. 12)

※ SPD-5는 △민간 우주 사업자와 협력을 통한 최적의 관행 도출, △사이버 보안에 대한 규범 확립, △사이버 보안 행동 개선 촉진, △우주 시스템의 소유자와 운영자가 개발과 실행에 있어 우주 시스템이 제공하는 핵심 기능과 임무 서비스 및 데이터의 무결성·기밀성·가용성 등 검증 능력 확보, △위험 평가와 내구력 등을 반드시 포함하도록 명시[19]

- 미국은 SPD-5에 의거, 모든 국가의 우주 시스템에 간섭 없이 작전 수행 및 통과할 수 있는 권리를 주장, 우주 인프라에 대한 의도적 간섭은 미국과 동맹국의 국가이익 침해로 간주[20]

라. 민관 우주안보 협력 측면

▪ 우주에서의 사이버 위협 활동에 대한 민관 정보 공유 강화

- 미국 CISA, FBI는 러-우 전쟁 이후 자국 위성 사업자들에 대해 '미국과 국제 위성통신(satellite communication: SATCOM) 네트워크에 대한 사이버공격에 관련 주의를 촉구하는 보안 권고문'을 발표, 사이버 위협 활동에 대한 정보 공유 촉진을 강조[21]
- 2023년 3월 미국 국가사이버국장(ONCD)과 국가우주위원회는 우주 시스템 생태계의 사이버안보 강화를 위해 민간 기업을 대상으로 신흥기술 접목을 통한 우주 사이버 보안체계의 강화 필요성을 강조

19 The White House, "National Space Policy of the United States of America," (December 9, 2020), pp. 3-4.

20 The White House, "National Space Policy of the United States of America," (December 9, 2020), pp. 3-4.

21 CISA, Strengthening Cybersecurity of SATCOM Network Providers and Customers, May 10, 2022(Alert Code: AA22-076A), https://www.cisa.gov/news-events/cybersecurity-advisories/ aa22-076a

※ '양자 내성 암호와 알고리즘의 개발과 적용', '오픈소스 라이브러리 보안 강화 필요성' 및 '우주 사이버위협의 측정과 우주 사이버 공급망 문제를 해결하기 위한 전략'을 포함한 다양한 사이버 보안 관행이 논의됨

▪ 우주안보 및 국방 전략적 차원에서 '미 우주 우선순위 프레임워크(United States Space Priorites Framework)'를 발표[22]

- 우주 활동이 급속도로 가속화되고 있으며, 우주 산업 및 기타 비정부 우주 개발자 및 운영자와의 협력이 보다 중요해지고 있음을 강조

※ 민감한 우주자산과 우주시스템에 대한 사이버보안을 개선하고 효율적인 접근 통제를 보장하며 우주 산업 기반 전반에 걸쳐 공급망의 탄력성을 강화할 것임을 천명

▪ 일본은 일찍이 2008년부터'우주기본법'을 제정하였으며, 2023년 6월 5차 개정안을 통해 우주 활동의 자주성 확보와 우주 사이버 위협에 대한 대응을 주요 국가 과제로 설정[23]

- 특히, 민간 기업을 대상으로 하는 우주 사이버 보안 위협 증대에 대응하고자 2023년 3월 일본 경제 산업성 제조산업국 우주산업실에서'민간 우주시스템 사이버보안 대책 가이드라인'을 발표[24]

※ 가이드라인에서는 우주 시스템과 관련된 보안상의 위험, 우주시스템 관련 민간 사업자가 확보해야 할 기본적인 보안 대책 및 매뉴얼을 정리하여 제시

22 https://www.whitehouse.gov/wp-content/uploads/2021/12/united-states-space-priorities- framework-_december-1-2021.pdf

23 김다혜, 백기연, 김성훈(2024), p. 14.

24 Japan Space Industry Office. (2023). Cybersecurity Guidelines for Commercial Space Systems (ver.1.1). Ministry of Economy, Trade and Industry

Ⅳ 우주-사이버 난제에 대한 대응 방안

1. 다층적 위협 기반 사이버 방어 모델 수립

가. 지상, 우주, 링크 부문의 사이버 위협 취약점 개선

▪ 우주-사이버 위협은 취약한 연결고리가 우주 시스템 전체에 치명적 영향을 줄 수 있으므로 네트워크 경로의 전방위적 대응 필요

- 최근 위성 소프트웨어는 링크 부문에서 데이터 업로드를 통해 업데이트를 하고 있는 수준으로 발전하고 있으나, 위성 간, 지상-위성 간 네트워크를 공격하는 사이버 위협 대응에 대한 대비는 상대적으로 미흡

▪ 위성 간, 지상-위성 간 전송에 활용되는 데이터 암호화와 호스팅 서비스를 안전하게 처리하는 위성용 보안 네트워크 적용 시급

※ 최근 스페이스X는 지구관측, 통신, 데이터 전송 과정에서 선단 간 고신뢰 암호화 기능을 적용한 위성 네트워크 스타실드(Starshield)를 개발, 정부 공공 목적 위성에 우선 적용('22. 12)[25]

나. 우주 사이버 위협의 취약성이 두드러진 구형 시스템을 중심으로 군집위성 운용의 보안체계 강화

▪ 구형 시스템은 방어나 복원 능력이 부족할 뿐만 아니라 연결된 신형 시스템 취약성을 유발할 수 있음

- 특히, 다수의 위성이 함께 기능하는 군집 위성의 경우 구형과 신형 시스템이 혼합되어 보다 취약하여 우선순위의 보안개선이 요구됨

25 https://zdnet.co.kr/view/?no=20221209081331

2. 우주 사이버 위협의 비대칭성 완화

가. 우주 사이버 운용체계의 전주기 취약점 진단 및 개선

- 우주 시스템 개발과 생산, 유지보수 및 운영 주체까지 포함된 우주 사이버 운용 체계의 취약점 진단 매뉴얼 수립 필요
  - 우주항공청은 국가 우주시스템의 컨트롤타워로서 우주-사이버 위협에 대한 연구개발과 정책 마련을 주도, 보안 취약성 점검 및 대책 마련의 주체로서 우선적으로 가이드라인을 마련

- 최근 ICT · 제조 · 의료 기기 등에 의무화되고 있는 '소프트웨어 자재 명세서(Software Bill Of Materials)' 지침과 같이 개발 · 설계 과정의 전주기 공급망의 투명성과 보안성을 보다 강화할 필요

나. 북한의 우주 사이버 공격 가능성 대비

- 최근 북한은 우주 사이버 공간에서의 은밀한 도발행위를 시도한 바 있으며, 러북 밀착에 따라 향후의 위협 가능성 다대
  - 우주 사이버 공격은 적은 비용과 책임 귀속의 제한, 공격 시차 지연으로 은밀성이 높다는 점에서 핵티비스트, 해커 뿐만 아니라 북한에게도 우주 사이버 공격의 유인을 제공[26]
    ※ 또한, 북한은 다양한 해킹그룹을 운영하여 협업을 강화하고 중소 방산 업체 등 다소 방어가 약한 대상으로 공격 표적을 확대하고 있는 추세[27]

- 최근 러북 정상회담 및 북한군의 우크라이나 파병에 따라 양국의 군사 무기 개발 분야에서의 밀착 가능성 증대
  - 특히, 첨단 발사체와 인공위성 개발 기술의 북한 제공 가능성이 어느 때보다도 높은 상황으로, 북한이 이를 활용하여 우주개발 프로그램을 강화 시, 우주 사이버 위협은 보다 고도화될 가능성

---

26 실제로 북한은 지난 2024년 3월 한미 연합 '자유의 방패(FS)' 훈련 기간에 위성항법장치(GPS) 전파 교란을 시도한 바 있으며, 미국 우주사령부(U.S. Space Command) 스티븐 와이팅(Stephen Whiting) 사령관 역시 북한이 미국 우주 시스템을 위협할 지상 기반 전자전 역량을 보유하고 있음을 언급하였다. 문화일보, "우주 사이버 안보, 발등의 불 됐다" (2024. 4. 16.)

27 김보미, "진화하는 북한의 사이버 공격 현황과 대응," 『이슈브리핑 472호』, 국가안보전략연구원, 2023, pp. 2~3; 조재학, "북한 해킹조직, K-방산 10여곳 털었다," 『전자신문』, (2024. 4. 23.)

3. 국가안보전략 및 주요 지침과의 연계성 강화

가. 국가안보전략, 사이버안보전략과의 정합성 확보

▪ 우주 사이버 전략은 국가안보전략과 사이버안보 전략과의 긴밀한 연계에 기반하므로 대응체계의 정합성 강화에 초점을 둘 필요

- 우주 시스템에 대한 사이버 안보 대응은 상위 국가안보 전략 및 국가 사이버 전략 방향과 부합하여야 하므로, 공세적 대응과 기반 조성, 능동적 국제협력의 전략기조를 염두에 둔 실행방안이 필요

※ △우주 시스템 생산·유지 공급망 안정, △우주 시스템의 활용에서 비롯되는 우주 산업과 경제 발전, △우주 시스템 활용에 바탕이 되는 국제규범과 우방국 협력 등 국가 차원의 대응 방향과 체계 구축 등

▪ 우주 사이버안보 대응체계 개선을 통해 궁극적으로 우리의 우주정보수집 역량 및 보호활동 범위를 확장하는 방향으로 추진 필요

- 최근 정부는 정부는 우주안보 역량을 강화하기 위하여 「우주안보 업무규정(대통령령 제34434호)」을 전면 개정, 우주에서의 정보생산 및 보호활동 범위를 구체화('24. 4. 23.)[28]

※ 우주 안보 강화를 목표로 '위성자산 및 안보 관련 우주 정보 수집·작성·배포 업무' 이외에 '위성자산 등의 안보 관련 위협에 대한 대응 및 보안 업무'를 추가[29]

나. 국가우주안보 전략 내 우주 사이버 대응임무 강화

▪ 현재 국방우주전략서가 존재하나 이는 군사적 관점에 기반한 국방부 임무 중심의 전략서로, 주요 실행체계가 비밀로 관리되어 우주 사이버 안보 차원의 범용적 활용에 제약

▪ 따라서, 우주의 안전과 번영 확보를 위한'국가우주전략'의 수립이 시급하며, 이를 위한 우주 사이버 안보 역량을 강화할 필요

- 다영역에서의 우주활용 능력 강화, 우주안보자산의 생존성과 복원성 강화를 위한 실천원칙과 세부 추진과제를 모색할 필요

※ ①우주 시스템에 대한 사이버 안보의 기초가 되는 주요 원칙 확립, ②미국 중심 위성항법 정책 수립 및

28 오일석(2024), p. 2.

29 오일석, "우주안보 위협, 국가적 대비 태세 갖췄다", 아시아경제(2023년 5월 3일).

GPS 성능과 사이버 보안 수준 개선, ③민간 우주 사업자 간 협력으로 최적의 관행 도출, ④사이버 안보에 관한 규범 확립, ⑤사이버 안보의 행동 개선 촉진 등

4. 민관 우주 사이버 협력 기반 조성

가. 민관의 우주 사이버 위협 대응 임무와 거버넌스 정립

▪ 우주 영역에서의 민간 역할을 강화하기 위해 우주 사이버 위협에 대한 민관군 협력체계를 개선할 필요

- 우주-사이버 안보에 대한 정부 기관별 이해(利害)는 민간과 협력에 장애가 될 수 있으므로 임무와 거버넌스를 정립할 필요가 있음
- 특히 실질적인 우주 시스템의 개발과 운영에 민관군 주체들이 중복되는 부분은 협력하고 공백 영역에서의 책임을 명시해야 함
- 현재 국내 우주안보는 「우주항공청법」과 「국가정보원법」에 근거한 「우주안보 업무규정」에 의해 구체적으로 추진 예정[30]

▪ 국가정보원의 위성정보 보안관리 규정 및 위성정보 보안지침에 따라 우주 사이버 위협 임무체계 구체화

※ 현행 「우주안보 업무규정」은 국정원장으로 하여금 위성자산 등 및 안보 관련 우주정보 보호를 위한 보안지침을 수립·시행해야 한다고 규정하고 관계기관과 협의할 것을 규정

나. 민관 사이버 위협 탐지 및 식별 활동 공유

▪ 민관이 함께하는 우주 시스템에 대한 사이버 위협 탐지 및 정보 수집, 식별 활동의 종합 관리 메커니즘 강화

- 우주 자산이 증가하고 이해관계자가 다양화되고 있음을 고려하여 노력의 중복과 비효율성에 대비할 필요가 있음. 동시에 민관군 우주 자산이 중복 및 교차 운영 시 정보의 질이 높아질 수 있음
- 따라서 민관군이 처할 수 있는 우주-사이버 위협을 공동으로 분석하고 그 결과를 설명하여 위협 인식을 공유할 수 있어야 함
- 이 과정에서 경직된 보안을 이유로 정보공유나 기술지원 등을 제약하지 않도록 적절한 제도적 보완책이 필요

30 오일석(2024), p. 8.

▪ 민간 우주기업과 이들의 우주 자산을 국가안보 차원에서 적극 활용하는 동시에 안보 자산으로서의 보호 대책 역시 강화되어야 함

- △국가안보 차원의 임무 우선순위 선정, △합리적 최종 결정 권한, △민관군 전문 인력 양성과 인적 교류, △합동 기술 개발 방향 등이 정립될 필요
- 또한 우주 시스템의 공급망 보안을 유지하여 우주 기술을 보호하고 국가 차원에서 기술 주권을 강화하여야 함

참고문헌

관계부처합동, 2022, “제4차 우주개발진흥 기본계획”

국가안보실, 2023, “윤석열 정부의 국가안보전략”

———, 2024, “국가 사이버안보 전략”

김보미, 2023, “진화하는 북한의 사이버 공격 현황과 대응,” 『INSS이슈브리핑 472호』

김선우. 2024, “미래 우주경제를 위한 우주안보와 우주사이버보안: 주요 동향 및 시사점”, 『제8차 사이버국가전략포럼 자료집: 우주 사이버 안보의 현황과 쟁점』

류재철, 2024, “우주 사이버 보안 위협과 대책”, 『제8차 사이버국가전략포럼 자료집: 우주 사이버 안보의 현황과 쟁점』.

문화일보, 2024, “우주 사이버 안보, 발등의 불 됐다” (2024. 4. 16.)

엄정식, 2024, 『우주안보의 이해와 분석』, (서울: 박영사, 2024)

———, “우주안보의 3축과 사이버 안보,” KACA-KASS 공동 컨퍼런스 발표자료, (2024. 5. 8)

오일석, 2021, “우주 정보활동과 위성자산의 보호,” 『INSS 이슈브리핑 240호』

———, “우주안보 위협, 국가적 대비 태세 갖췄다”, 아시아경제(2023년 5월 3일).

———, 2023, “뉴스페이스 시대의 우주 사이버위협 대응 방안” 『INSS 전략보고』, (November 2023).

———, 2024. “우주안보 발전을 위한 법제 개선: 「우주안보 업무규정」 개정의 시사점과 함의”, 『INSS 전략보고』, (August 2024).

윤정현 • 이성훈, 2023, “뉴 스페이스 시대의 민관협력 변화와 한국형 발전방향 모색”, 『국가전략』, 제29권 3호.

이성훈, 2023, “우주자산 위협 양상과 주변국의 대응 정책 및 시사점”, 『INSS 전략보고』, No. 228

박은주, “우주에서도 지금 사이버 보안이 필요하다”, 『보안뉴스』, (2023. 3. 20.)

조재학, “북한 해킹조직, K-방산 10여곳 털었다,” 『전자신문』, (2024. 4. 23.)

한국우주기술진흥협회, “제3차 위성정보 활용 종합 계획 안내” (2023. 5. 22.) http://www.kasp.or.kr/kasp_news/kasp_notice.html?ptype=view&idx=8098 (검색일: 2024. 8. 22).

Jervis, Robert, 1978, “Cooperation under the Security Dilemma”, *World Politics*, Vol. 30, No. 2.

Harrison, T., K. Johnson, and T. Roberts, 2013, ‘Space Threat Assessment 2018’, 2018; J. Sigholm, ‘Non-State Actors in Cyberspace Operations’, Joint Military Studies, Vol. 4, No. 1.

Koerner, B. I. 2016, "Inside the OPM Hack, the cyberattack that shocked the US government", Wired, 23-Oct 2016.

National Cyber Security of the United States of America (Sept. 2018).

Yoon, Junghyun. Jungsik Um, 2024. "Complex Challenges of Space Cybersecurity and Their Implications for ROK, Korean Journal of Defense Analysis, Vol. 36, No. 3 (2024), p. 339-367.

U.S, Space Force, 2024, "Space Force publishes Data, AI strategic action plan," Secretary of the Air Force Public Affairs, (May 14, 2024).

The White House, 2020, "National Space Policy of the United States of America," (December 9, 2020). https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/09/Factsheet-SPD-5.pdf (검색일: 2024. 8. 10.).

https://zdnet.co.kr/view/?no=20221209081331

Abstract

Challenges of Space Cyber Threats and Korea's Response Strategies

Junghyun Yoon
(Institutue for National Security Strategy)

As recent space activities expand into civilian computing systems and communication networks, the importance of space cybersecurity is growing. To prepare for the challenges posed by this space cybersecurity environment, it is necessary to proactively explore the structural vulnerabilities of these interconnected domains and identify the pathways through which threats emerge and spread.

This study examines the patterns and complex attributes of threats in the space-cyber domain and diagnoses Korea's situation as well as the response measures of major countries. Based on this, it aims to propose response strategies that address each structural threat. First, cyber threats to space systems require a comprehensive approach that encompasses the terrestrial, link, and space segments. Second, it is essential to prepare for the asymmetry and diversity of actors that promote the security dilemma in the space-cyber domain. Third, a national space security strategy and a space-cyber response direction must be established in close alignment with the national security strategy and cybersecurity strategy. Fourth, public-private-military partnerships that are suitable for the era of space-cybersecurity must be strengthened, and new cooperative governance frameworks must be established.

Keywords: space cyber threats, structural challenges, new space, space security strategy, public-private cooperation

Institute For National Security Strategy

www.inss.re.kr

INSS 전략보고

November 2024.
No. 290

06295 서울시 강남구 언주로 120 인스토피아 빌딩
02-6191-1000 02-6191-1111 www.inss.re.kr

국가안보전략연구원