국가전략연구위원회 이슈브리핑 22호 (발간일: 2024.3.18.)

우주 사이버 보안 위협과 대책[1)]

류재철 (충남대학교)

1. 미·중 우주 동향

1.1 미국

미국은 아이젠하워 대통령이 NASA를 설립한 이후 우주 분야에서 광범위한 활동을 전개하고 있으며, 이러한 활동은 이전 행정부의 기조를 이어받아 연속성을 유지하고 있다. 우주 사이버 보안과 관련해서는 트럼프 정부가 2020년 SPD-5(Cybersecurity Principles for Space Systems), 2022년 바이든 정부가 S.3511-Satellite Cybersecurity Act를 통해 국가적 지침을 마련하였다.

미 의회는 우주 활동에 필요한 예산과 우선순위 확보를 위해 지속적으로 지원하고 있으며, 최근 몇 년 동안 미국은 우주 활동의 재조직과 강화에 상당한 주력을 기울이고 있다. 아폴로 프로그램 이후 약 50년 만의 달로의 복귀, 70년 만에 이루어진 우주군의 창설, 그리고 민간 부문의 우주 기술 발전이 이러한 노력의 주요 사례로 꼽힌다.

1.2 중국

중국 정부는 지난 수년간 우주항공 분야에서 주목할 만한 발전을 이루어냈으며, 이러한 발전을 공식적으로 세계에 알리기 위해 '우주백서'(中國的航天)를 발표해왔다. 2021년 발

1) 이 글은 2024년 3월 13일 제8차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.

표된 우주백서에 따르면, 2016년 이후 중국의 우주 분야는 주목할 만한 진전을 보였다. 베이더우 글로벌 위성 항법 시스템 가동 개시, 고해상도 지구 관측 시스템 구축, 위성을 통한 방송 통신 서비스의 안정성 및 능력 향상 등이 이루어졌다. 또한, 중국은 달 탐사 프로젝트를 '궤도 진입, 착륙, 귀환'의 세 단계로 구성된 과정을 성공적으로 완료하였다. 중국 우주 정거장의 건설이 본격적으로 시작되었으며, 화성 탐사선은 지구-달 시스템을 넘어 행성 간 탐사를 진행하여 세계적인 주목을 받은 성과를 달성하였다[2].

중국 지도부는 우주개발을 통해 공산당의 집권 체제를 강화하고 세계 초강대국으로의 도약을 목표로 하고 있다. 즉, 1958년 마우쩌뚱의 지시로 시작한 우주 개발을 시진핑 때 완성하고자 투자를 강화하고 있으며 일대일로와 더불어 '우주 굴기'를 실현하여 미국을 뛰어넘고자 하는 야심찬 계획인 것이다.

또한,《2015년 중국의 군사전략》 백서에서는 핵, 항공모함과 더불어 우주, 위성 분야에서 국방산업의 기술과 제품 개발이 전략적 우선순위로 설정되어 있다. 이는 국가 안보 차원에서 우주에 대한 지배권 확보의 중요성을 강조하는 것으로 우주 시스템에 대한 해킹 능력을 세계 최고 수준으로 유지함을 의미한다.

1.3 우주에서의 국제협력 강화

중국은 2022년 브릭스 우주협력기구를 구성하여 브라질, 러시아, 인도, 남아프리카공화국 등과 지구관측위성 및 통신위성 분야에 국제협력을 강화하고 있다.

이에 위기 위식을 느낀 미국에서는 '아르테미스'프로젝트을 통해 약30개국과의 교류를 강화하여 2030년까지 달 탐사 연구기지 건설을 목표로 하고 있으며, 24년 2월에는 국제 우주 훈련을 역대 최대 규모로 개최한 바 있다. 육·해·공에 이은 제4의 전장인 우주에서도 미중 경쟁이 치열해 짐에 따라 지금까지 우주 관련 기술 공유를 꺼려하였던 미국의 태도 변화가 주목받고 있다.

우주는 무주공산 그 자체의 공간으로 향후 관련 제도나 규제가 고도화 될 수 있다. 후발 주자에게는 불이익이 있을 수 밖에 없는 상황에서 국제 협력이 무엇보다 중요한 시점인 것이다.

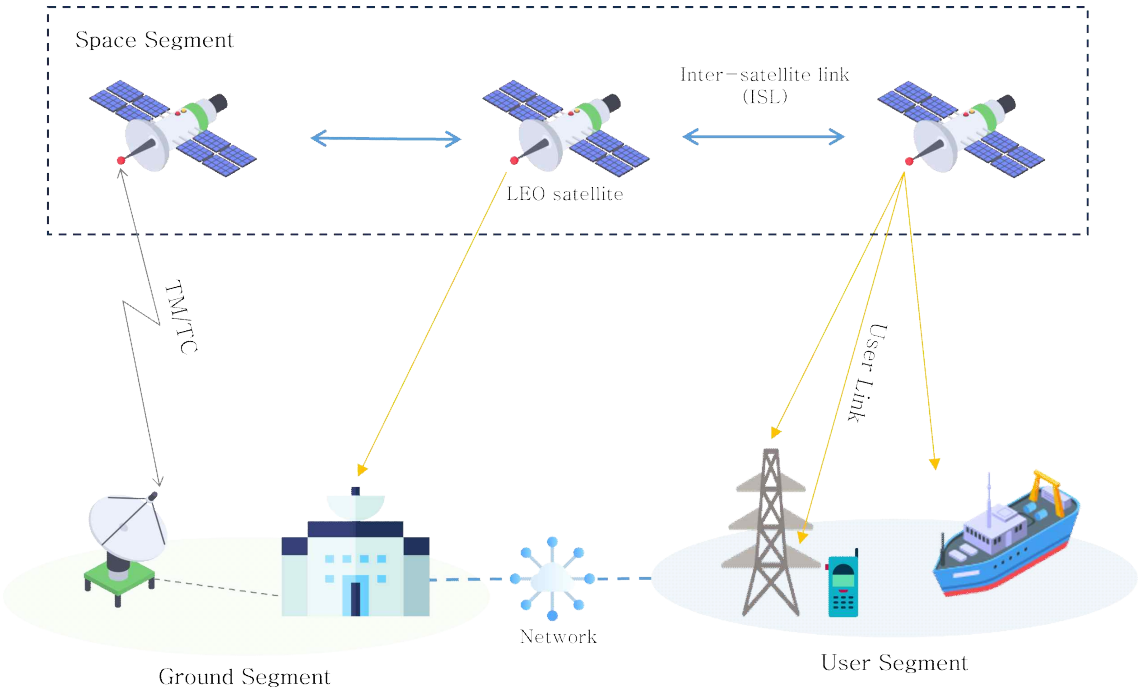
현재 우주 공간에서의 물리적 충돌을 제한하는 우주조약 외에는 명확한 기준이 없으며, 우주조약조차도 강제할 수 있는 현실적 방안이 없기 때문에 향후 강대국들이 자신들의 편의 위주로 관련 법이나 조약을 만들 가능성이 있다. 이에 비록 유망한 기술을 개발한 기업이 있다 하더라도 국적에 따라 해당 기술의 확장이나 효용이 제한될 수 있는 것이다. 한편, 우주 쓰레기, 천체관측 방해, 궤도 선점과 주파수 간섭 문제가 향후 주요 안건으로 거론될 것으로 예상되고 있다.

---

[2] 임강희; 이진성. [2021 년 중국의 우주] 백서. 국방과 기술, 2022, 518: 116-127.

2. 우주 사이버 보안 위협과 대책

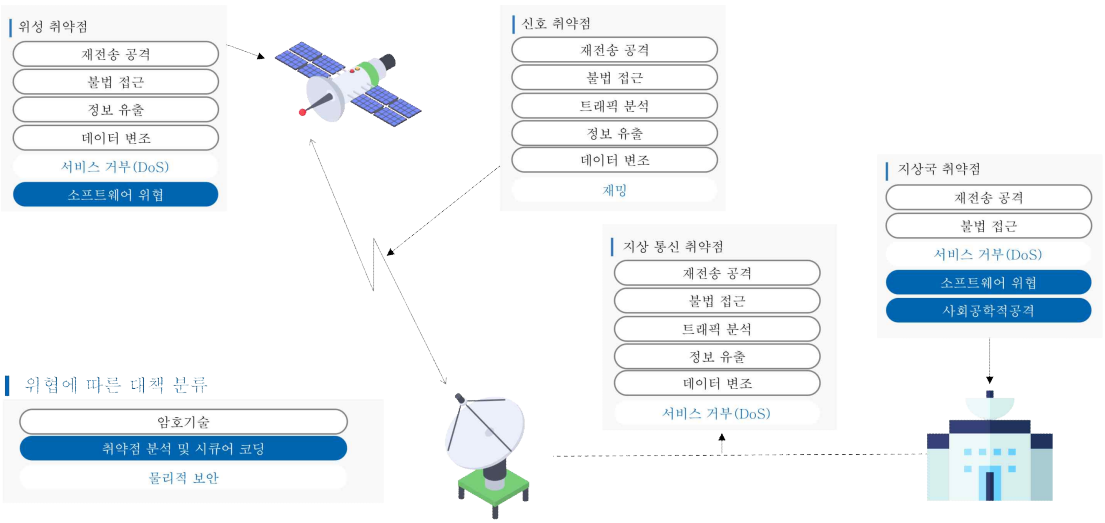
2.1 우주 시스템 구조



우주 시스템의 구성은 크게 3가지로 스페이스, 그라운드, 사용자 부문으로 이루어진다. 스페이스 부문은 위성들 간의 통신을 위한 Inter-Satellite Link(ISL)와 지상 부문으로부터 올라오는 명령어를 처리하고 그 결과를 전달하는 기능이 구현되어 있으며, 사용자 부문은 다양한 단말기 형태로 위성에서 전달하는 데이터를 수신하는 기능을 담당하게 된다. 그라운드 부문은 위성을 제어하고 관리하는 기능을 수행하며 통상적으로 그라운드 부문의 위성 제어 시스템과 사용자 부문의 수신 기능을 통합하여 지상국이 구축되는 경우가 일반적이다.

저궤도 위성은 지구 주위를 빠르게 도는 특성으로 인해 하루에 1~2회, 5~8분 정도의 짧은 주기 동안 통신이 가능하다. 이러한 특성으로 인해 지속적인 데이터 전송과 통신을 위해 다수의 위성을 띄어 군집 위성 형태로 운영하게 되고 전 세계에 분포된 다수의 지상국의 활용을 필요로 한다. 이러한 지상국 네트워크는 통신망의 취약점으로 작용할 수 있으며 이를 통한 지상국 해킹은 우주 시스템 전체에 영향을 줄 수 있다.

2.2 우주 시스템에서의 사이버 보안 위협과 대책



우주 데이터 표준을 위한 CCSDS(Consultative Committee for Space Data Systems)에서는 다음과 같은 우주 위협을 제시하고 있다.

- 재전송 공격은 통신 내용을 가로채어 보관한 후, 나중에 이를 재전송하는 공격으로 수신하는 곳에서 재전송 공격을 탐지할 수 없다면 해당 통신 내용을 다시 처리하게 된다.
- 불법 접근은 허가 받지 않은 공격자가 명령어를 전송하거나 위성 혹은 지상국 데이터에 접근하는 것을 말한다.
- 정보 유출은 위성과 지상국 간의 명령어 및 데이터 송수신 과정 중에 발생할 수 있다. 특히 RF 통신 링크를 통해 할당된 특정 주파수를 청취하는 스니핑 공격을 통해 송수신되는 데이터를 수집하고 분석함으로써 위치 정보, 운영 정보, 과학적 데이터 등의 중요 정보의 불법 접근을 가능하게 한다.
- 트래픽 분석은 통신 트래픽의 패턴을 분석하여 정보를 추출하는 행위로, 추론을 통해 위성에 송수신되는 신호를 임의로 조작하거나 탈취하는 형태의 공격이다.
- 데이터 변조는 정상적인 명령어 및 데이터의 일부 내용을 불법적으로 변경하는 공격이다.
- 서비스 거부(DoS) 위성 혹은 지상국에서 정상적인 기능을 수행할 수 없도록 만드는 공격으로, 지속적인 부하를 가하여 처리 능력을 마비시키거나 명령 송수신을 방해한다.
- 소프트웨어 위협은 위성 혹은 지상국에서 사용하는 소프트웨어의 취약점으로 인해 발생할 수 있는 공격으로 시스템을 파괴하거나 정보 유출 및 변조 등 다양한 사이버 공격이 가능하다.
- 사회공학적공격은 지상국 관리자 및 사용자를 대상으로 원하는 정보를 얻어 내기 위한

심리적 공격 기법이다.

- 재밍은 무선 주파수(RF) 또는 광학 신호를 이용하여 의도적으로 통신 링크에 간섭을 주는 공격으로, 이는 통신의 안정성을 방해하여 링크 손실을 야기할 수 있다.

이에 따른 보안 대책으로는 다음과 같다. 암호기술은 정보 유출 방지를 위해 절대적으로 필요할 뿐만 아니라 사용자 인증을 통한 불법 명령 전송을 방지할 수 있어 우주 시스템에서 가장 중요한 기술로 간주되고 있다. 국내에서도 이미 관용암호방식을 이용한 연구는 진행된 바 있으며 향후에는 관용암호방식이외에 공개키암호방식을 사용하여 암호키관리를 안전하면서 효율적으로 수행하는 연구가 필요하다. 또한, 우주 공간의 특성상 전력 사용을 최소화 하며 암호 기능이 빠르게 작동할 수 있는 저전력 기술이 필요로 하고 있다. 중국에서는 양자암호통신기술을 활용한 연구를 진행하고 있어 향후 양자컴퓨터 시대에 대비한 암호기술의 진화도 함께 준비해야 한다.

취약점 분석 및 시큐어 코딩은 우주에 장착되는 모든 응용소프트웨어, 펌웨어, FPGA, ASIC의 안전성을 분석하여 취약점을 제거하고 해킹이 용인되지 않는 안전한 프로그래밍 기술을 의미한다. 이런 기술 확보가 쉽지 않아 스페이스X에서는 버그바운티를 공개적으로 운영하며 지속적으로 취약점을 관리하고 있는 실정이다. 특히, 위성에서의 취약점을 이용한 해킹보다는 각종 SW가 많이 사용되는 지상국 해킹이 보다 수월하게 진행될 것으로 예상되어 이에 대한 대비책이 필요하다.

물리적 보안은 통신의 신뢰성과 안정성을 보장하는 핵심 요소로 외부에서의 의도적인 재밍(jamming)에 대응하여 통신을 보호하는 항재밍 기술이 중요하다. 주파수 호핑, 확산 스펙트럼, 에러 정정 부호 등 주로 전자전과 관련된 기술로 사이버 보안 범위 밖의 기술로 간주되고 있으나 해킹에 효과적으로 대응하기 위해서는 통합 관리할 필요성이 증가하고 있다.

3. 국내 우주 사이버 보안을 위한 제언

3.1 위성 해킹 테스트 환경 구축

국내 대부분의 우주 분야 종사자들은 위성 해킹에 대한 가능성을 매우 낮게 보고 있다. 암호인증 기술이 적용되어 있고 폐쇄적으로 운영하고 있는 지상국을 대상으로 해킹은 거의 불가능하다고 간주한다. 따라서 이러한 인식 전환을 위해서는 무엇보다 실제 위성이 해킹될 수 있음을 보여주는 것이 무엇보다 중요하다.

지난 1월에 발표된 조선일보 기사에 따르면 "중국인으로 추정되는 해커가 국내 기관이 사용 중인 위성통신 신호를 수집분석한 뒤 정상 장비인 것처럼 위장해 지상의 위성망 관리 시스템에 무단으로 접속한 뒤 최초로 정부 행정망 침투를 시도"한 것을 확인되어 전국 위성

통신망 운영 실태를 종합 점검하기로 한 바 있다.

북한, 중국 해커로부터 공격을 받기 이전에 우리 스스로 위성 해킹 가능성을 확인하고 그 중요성을 인식하는 것이 필요한 바, 실제 위성 운용 환경을 대상으로 각종 해킹 기법을 테스트 할 수 있는 환경 구축이 필요하다.

RHEA System Luxembourg S.A.는 우주, 정부 및 방위 조직에 맞춤형 보안 솔루션 및 서비스를 제공하는 회사로 우주 사이버 훈련장 서비스인 Cyber Integration, Test and Evaluation Framework (CITEF)를 통해 우주 사이버 보안 역량을 강화할 수 있는 프로그램을 운영하고 있다.

위성의 수명은 3-5년이었으나 최근에는 기술의 발전으로 5-10년으로 연장되었다. 수명이 다하였다고 바로 폐기 처분 되는 것은 아니고 주어진 임무를 수행하지 않을 뿐이다. 따라서 수명이 다한 위성을 대상으로 해킹 테스트를 할 수 있다면 이 분야의 연구 활성화에 큰 도움이 될 것으로 판단된다.

3.2 우주 전문가와 사이버 보안 전문가의 협업을 위한 해킹대회 개최

우주 분야는 기계공학, 전자공학, 천문학, 컴퓨터공학 등 다양한 학문이 결합하여 발전하고 있다. 최근에는 소프트웨어의 중요성이 커지면서 컴퓨터 프로그래머의 역할이 커지고 있는 가운데 취약점 발생에 따른 해킹 위험이 증가하고 있어 사이버 보안 전문가와의 협업이 절대적으로 필요한 상황이다.

지금까지 우주 분야에서의 보안은 물리적 보안, 인적 보안, 폐쇄적 운영 등의 개념으로 이루어져 왔다. 다만, 통신채널을 통한 도청이 이루어 질 수 있어 암호 및 인증 중심으로 기술이 개발되어 왔으나 이마저도 민간용 위성에서는 제대로 사용하지 않은 상태로 운영되고 있다.

통신채널을 통한 해킹이 가능할 뿐만 아니라 지상국에서 사용하는 각종 소프트웨어의 취약점을 이용한 공격 가능성도 입증되면서 사이버 보안 전문가와 우주 전문가의 협업을 통해 실효성 높은 대책을 마련해야 한다.

미국의 경우 2020년부터 4년 동안'Hack-A-Sat' 해킹대회를 개최하여 우주 커뮤니티와 사이버 보안 커뮤니티 간의 지식 격차 해소 및 혁신을 장려한 바 있으며 프랑스에서도 2022년부터 매년 'CYSAT'행사를 통해 이 분야에 대한 관심과 중요성을 높이고, 다양한 전문가들 간의 지식 공유와 협력을 촉진하는 데 기여하고 있다.

국내에서도 우주 사이버 보안에 대한 해킹대회를 정기적으로 개최하여, 국제 커뮤니티와의 지식 공유 및 협력을 강화하고, 국내 우주 보안 연구의 발전을 촉진할 필요가 있다. 이를 통해 우주 기술과 사이버 보안 기술이 융합된 새로운 연구 분야를 개척하고, 우주 환경에서의 안전과 보안을 보장하기 위한 첨단 기술과 정책의 발전을 이끌어낼 수 있다.

3.3 우주 사이버 보안 가이드라인 제시

뉴스페이스 시대를 맞이 하여 우주 분야에 대한 관심은 민간 영역으로 확장되고 있다. 특히, 위성통신 기반의 6G 시대에서는 민간 위성 통신 사업자의 역할이 무엇보다 중요해 질 것으로 예상된다.

위성 기술의 발전은 우주 시스템의 제조 과정을 간소화하고 통신을 표준화하는 등 비용 절감을 위한 노력을 하고 있다. 특히, NASA의 오픈 소스 핵심 비행 시스템(cFS)과 같은 "plug and play" 시스템의 도입은 편의성을 제공하지만, 많은 보안 취약성에 노출되는 원인이 되고 있다. 따라서 우주 산업 분야에서 DevOpsSec 접근 방식의 적용을 통해 개발 초기 단계에서부터 보안을 내재화함으로써 보다 안전한 소프트웨어 배포가 가능하도록 해야 한다.

2022년 미 우주작전사령부 사령관 스티븐 화이팅은"위성 시스템을 운영하는 지상 시스템과 네트워크 장비가 사이버 공격자에게 많은 진입점을 제공함으로 미사일이나 레이저보다 훨씬 쉽게 접근할 수 있다"며 우주 사이버보안 대책 강구를 지시한 바 있으며, 2023년 NIST에서는 'Cybersecurity for Commercial Satellite Operations'문서를 통해 우주 사이버 위협 환경에서 지속적으로 관리할 수 있는 프레임워크를 발표한 바 있다.

국내에서는 우주 보안에 대한 조치로 정보통신망기반시설로 지정하는 것 이외에는 체계적인 보안 가이드라인이 마련되지 않은 상태이다. 따라서 우주 시스템 개발 및 운영자를 위한 보안 요구사항 제시를 통해 우주에서의 안전성 확보 뿐만 아니라 미래의 우주 산업 발전의 기초를 닦아야 한다.

3.4 우주 사이버 보안 평가체계 구축

사이버 보안 분야에서는 제3자의 객관적인 평가를 중요시하고 있다. 예를 들어, 암호기술 구현의 적합성을 확인하는 KCMVP(Korea Cryptographic Module Validation Program), 보안 제품이 개발자가 의도한 대로 제대로 구현되었는지를 평가하는 CC(Common Criteria) 인증 제도가 운영되고 있다. 또한, 조직 및 기관의 보안 활동이 정해진 규정대로 진행되었는지를 평가하는 ISMS(Information Security Management System) 제도가 우리에게 익숙한 사이버 보안 평가체계이다.

우주 분야에서도 사이버 보안 제품 혹은 운영관리 상의 취약점이 없는 지를 확인하는 우주 사이버 보안 평가체계를 구축할 필요가 있다. 이를 위해서는 보안 요구사항들이 명확히 제시되어야 하고 평가를 수행할 기관이 선정되어야 함으로 이를 위한 법적, 제도적 검토가 필요하다. 이때 기존의 보안 평가체계에서 이를 수용할지 아니면 별도의 평가체계를 통해 우주 분야의 고유성을 유지하는 것이 타당한지 검토가 필요하다.

또한, 제시된 보안 요구사항을 만족하는 제품만이 공급 될 수 있도록 공급망 보안과

연계할 필요도 있고 위성운영관리 평가 대상을 민간 기업까지 포함 한다면 그 기준을 어떻게 할지 등 고려할 사항이 많음으로 신중한 접근이 필요하다.

우주 공간의 특성상 방사능에 의한 성능 저하 및 장애 발생이 문제가 되고 있다. 이를 해결하기 위해 방사능에 강한 HW 부품을 사용하기도 하고 이중화, 삼중화 등 Fault Tolerant 기능 구현이 무엇보다 중요하다. 이에 따라 보안 요구사항은 일반적인 시스템과 차별화 될 것으로 판단됨에 따라 해당 분야의 전문가들의 기술적 검토가 요구된다.

아마존, MS 등 주요 클라우드 회사에서는 지상국 혹은 위성 서비스를 대여해 주는 사업을 진행하고 있다. 필요에 따라 국내 위성 서비스도 이와 같은 해외 위성 서비스를 이용해야 하는 경우도 있어 우주 사이버 보안 평가를 국내 뿐만 아니라 해외 국가들과 함께 수행할 필요가 있다. 따라서 국제 협력의 주요 안건으로 부상될 수 있어 이에 대한 체계적인 준비가 요구된다.

3.5 우주 사이버 보안 전문 회사 육성

스페이스X의 발사체 재사용과 버진 갤럭틱의 민간인 우주 여행은 상업우주 1.0 시대를 개시하였다. 스페이스X의 기업가치가 우주산업 전통의 강자인 보잉과 록히드 마틴을 넘어서면서 상업우주는 이제 새로운 국면에 접어들어 상업우주 2.0 시대를 맞이하고 있다. 즉, 상용화 단계에 들어선 발사체, 저궤도 위성통신의 개화, 우크라이나 전쟁으로 인한 우주 안보의 중요성에 따른 세계 각국의 우주 투자 확대 등이 그 주요 요인이다.

상업우주 시대를 위한 우주 보안 전문회사들도 등장하고 있다. 유럽의 RHEA System Luxembourg S.A., 제로트러스트 기술 기반의 OrbitSecure을 개발한 미국의 SpiderOak 등이다. 이들 기업은 우주 보안 산업에서 혁신적인 서비스와 솔루션을 제공함으로써, 군사 및 안보 목적을 위한 우주 기술의 운영 능력을 강화하고 전략적 우위를 확보하는 데 중요한 역할을 하고 있다.

우주 분야의 특수성을 이해하고 보안 솔루션을 개발할 수 있는 국내 민간 산업체가 필요하다. 상업우주 2.0 시대에 걸맞는 국내 우주 사이버 보안 전문회사를 통해 우주 산업의 보안 역량을 강화하고, 관련 기술과 서비스를 개발해야 한다. 이들을 통해 앞에서 제시한 우주 사이버 보안 평가를 수행한다면 보다 전문적이고 객관적인 평가가 이루어질 것으로 예상된다.

현재 위성통신 분야 예타 사업이 5개년 약5천억 규모로 진행되고 있다. 기술성 평가는 통과된 상태에서 경제성 평가를 앞두고 있는 가운데 사이버 보안에 대한 고려는 전무한 것으로 알려지고 있다. 우주 분야의 또 다른 예타 사업인 KPS(Korean Positioning System) 사업에서는 암호 및 인증을 고려하여 진행되고 있으나 사이버 보안과 관련해서는 어떤 예타 사업에서도 고려하지 않고 있는 실정이다.

따라서 위성통신 예타 사업에 사이버보안을 추가함으로써 국내에서도 우주 분야의 사

이버 보안 전문회사가 육성될 기회 마련이 필요하다.

<참고자료>

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.