J. Space Technol. Appl. 2(2), 169-186 (2022)
https://doi.org/10.52912/jsta.2022.2.2.169

우주기술과 응용
Journal of Space Technology and Applications
pISSN 2765-7469 eISSN 2799-3213

기고문

러시아-우크라이나 전쟁(러시아의 우크라이나 침공)의 우주전 분석 및 양상 그리고 우주기술 개발시 고려사항

최성환†

대한민국 공군본부 우주센터

Analysis and Aspects of Space Warfare in the Russia-Ukraine War (Russian Invasion of Ukraine) and Considerations for Space Technology Development

Seonghwan Choi†

[1]R.O.K Air Force H.Q. Space Center, Gyerong 32800, Korea

Received: April 29, 2022
Revised: May 6, 2022
Accepted: May 10, 2022

†**Corresponding author :**
Seonghwan Choi
Tel : +82-10-5082-9248
E-mail : kf2020@hanmail.net

Copyright © 2022 The Korean Space Science Society. This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

ORCID
Seonghwan Choi
https://orcid.org/0000-0002-5674-4207

요 약

본 글에서는 러시아의 우주위협 평가와 러시아-우크라이나 전쟁(러시아의 우크라이나 침공)의 우주전을 분석하고 양상에 대해 정리하였다. 우주전의 양상이 상용위성 또한 잠재적인 공격 대상이 될 개연성을 고려하여 우주기술 개발시 군용위성뿐만 아니라, 상용위성도 우주위협에 대비할 수 있는 우주기술을 개발하고 동일하게 적용해야 함을 제언하고 적용이 필요한 우주기술에 대해 열거하였다.

Abstract

In this article, Russia's space threat assessment and space warfare in the Russia-Ukraine war (Russian invasion of Ukraine) were analyzed and summarized. Considering the probability that commercial satellites will also be potential targets of space warfare, it is suggested that not only military satellites but also commercial satellites develop and apply space technology that can be applied equally to space threats when developing space technology. Necessary space technologies is listed.

핵심어 : 우주전, 우주기술, 우주위협, GPS 재밍, 사이버 공격, 인터넷 위성통신
Keywords : space warfare, space technology, space threats, GPS jamming, cyber attack, internet satellite communication

1. 서론

러시아-우크라이나 전쟁(러시아의 우크라이나 침공)은 지난 100년간 일어났던 전쟁의 종합판이다. 과거 전쟁에서 나타났던 모습들이 모두 등장해서다. 1940년대 제2차 세계대전 당시 독일이 기갑부대로 유럽 전역을 휩쓸었던 '전격전'과 양 진영 전투기간에 치열하게 벌어졌던 '공중전', 1970년대 캄보디아에서 자행된 '민간인 학살'과 미군이 베트남전에서 겪었던 '게릴라전', 그리고 1990년대 체첸전쟁에서의 격렬했던 '시가전' 등 20세기 전쟁 양상과 함께

2000년대 이라크전에서 등장한 압도적인 '정밀폭격'과 조지아전쟁에서 활발히 진행됐던 '심리전', 이스라엘의 시리아 폭격 당시 벌어졌던 '사이버전', 2010년대 미군이 오사마 빈라덴(Osama bin Laden) 제거를 위해 실시했던 '특수전'과 10년 후 가셈 솔레이마니(Qasem Soleimani) 제거를 위해 드론을 활용한 '유·무인 복합전'의 모습과 같은 현대전 양상도 보인다. 21세기 초반, 러시아는 '하이브리드전(Hybrid War)'이라는 군사적·비군사적 수단의 조합을 통해 목적을 달성하는 새로운 전쟁개념을 선보였고 이번 전쟁에서도 이 개념을 바탕으로 다양한 '작전'을 수행하고 있다. 이러한 시점에 우주위협에 대비할 수 있게 러시아의 우주위협 평가와 러시아-우크라이나 전쟁의 우주전을 분석하고 양상에 대해 정리하였다. 우주전의 양상이 상용위성 또한 잠재적인 공격 대상이 될 개연성을 고려하여 우주기술 개발시 군용위성뿐만 아니라, 상용위성도 우주위협에 대비할 수 있는 우주기술을 개발하고, 동일하게 적용해야 함을 제언하고 적용이 필요한 우주기술에 대해 열거하였다[1].

2. 러시아의 우주위협 평가

미 국방부 산하 국방정보국(Defence Intelligence Agency, DIA)이 최근 발간한 '2022년 우주안보도전(2022 Challenges to Security In Space)' 보고서에는 러시아는 미국의 위성 기술이 발전하고 위성에 대한 의존도가 높아지는 걸 역이용하려는 움직임이 있다고 분석했다. 보다 구체적으로 2020년대 중반에는 위성에 직접 타격을 가할 수 있는 지상기반 레이저를 사용할 가능성을 열어뒀다. DIA에 따르면 "러시아는 2018년 자국 우주군에 배치한 시스템을 포함해 이미 다양한 지상기반 레이저를 보유하고 있다고 밝혔고, 이중엔 위성 센서를 dazzling(눈부심, 촬영 거부)할 수 있는 장비도 있다."고 발표했다. 또한, 보고서는 "2030년이면 러시아는 이보다 고출력인 시스템을 배치할 수도 있다"면서 "이러한 경우 위협은 전기광학 센서뿐만 아니라 모든 위성의 구조물로 확장된다"고 했다. 그리고, 미국 국제전략문제연구(Center for Strategic & International Studies, CSIS)가 최근 펴낸 '우주위협 평가 2022(Space Threat Assessment 2022)' 보고서에 따르면 러시아는 우크라이나 침공시 GPS 재밍(jamming) 및 위성통신 전파방해가 계속되거나, 전쟁이 진행됨에 따라 증가하였다고 분석했다[2,3](Fig. 1).

Fig. 1. Up-to date space security / space threat analysis materials.

'우주위협 평가 2022'에 의하면 러시아는 2021년 저궤도(low earth orbit, LEO)에 대한 DA (Direct Ascnt)-ASAT(Anti-Satellite) 요격시험을 성공적으로 수행했으며, 지상기반 위성레이저거리측정(satellite laser ranging, SLR) 시설은 광학 이미지 위성의 센서를 dazzling시키는데 사용될 수 있으며, 전자전(electronic warfare, EW) 분야에서도 통신위성 및 GPS 수신기를 방해할 수 있는 다양한 시스템을 보유하고 있다고 평가하고 있다[4](Fig. 2).

3. 러시아-우크라이나 전쟁의 우주전 분석

3.1 통신분야: 러시아, 우크라이나 통신 · 인터넷 네트워크 물리적공격 자제

러시아-우크라이나 전쟁의 우주전 분석 중 통신 분야로 러시아군의 우크라이나 침공이 7주가 지나도록, 소셜미디어에선 파괴된 러시아군 탱크와 중화기에서부터 길거리의 수많은 민간인 시신들, 학살 현장, 병원·주거 단지 파괴 등 러시아군이 우크라이나에서 벌인 전쟁범죄의 모습들이 생생하게 전달됐다. 그래서 우크라이나가 군사력 열세에도 불구하고, 국제사회의 공분을 초래하는 소셜미디어 전쟁에선 압승했다고들 한다. 더 나아가, 우크라이나군은 인터넷으로 드론을 조종해 폭탄을 러시아군 장갑차·탱크 · 트럭에 투하하고, 볼로디미르 젤렌스키(Volodymyr Zelenskyy) 우크라이나 대통령은 텔레그램(telegram)으로 계속 국민에게 항전을 독려했다[5](Fig. 3).

하지만, 현대 전쟁에서 상대국 군대의 지휘·통신 체계를 마비시키기 위해, 전쟁 초기에 통신 · 전력 네트워크를 파괴하는 것은 상식이다. 게다가 러시아는 우크라이나의 통신·인터넷 서비스를 차단·교란할 수 있는 가공할 해킹 능력과 폭격 능력을 갖추고 있다. 실제로, 전쟁 초기에 러시아는 우크라이나 정부 시스템을 파괴하는 '와이퍼웨어(wiper malware)' 공격을 했고, 웹사이트 접속을 막는 디도스(Ddos) 공격도 했다. 또한 미국의 민간 통신위성인 비아샛(Viasat)을 사이버 공격해 서비스에 일부 지장을 초래했으나 제한적이었다. 그러나, 러시아군은 통신 · 인터넷 · 전력 네트워크를 근본적으로 파괴하는 물리적 공격은 자제했다. 러시아군은 자체 통신을 우크라이나 민간 통신 네트워크를 사용하고 있었고 러시아군의 작전에 우크라이나의 민간 통신 네트워크가 필요하기 때문이었다. 서방 군사 전문가들은 러시아군이 대부분

	R&D	TESTING	OPERATIONAL	USE IN CONFLICT
LEO Direct Ascent	▲	▲	?	●
MEO/GEO Direct Ascent	■	–	–	●
LEO Co-Orbital	▲	▲	–	●
MEO/GEO Co-Orbital	■	–	–	●
Directed Energy	▲	■	?	●
Electronic Warfare	▲	▲	▲	▲
Space Situational Awareness	▲	▲	▲	?

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

Fig. 2. Russia space threat assessment [2].

Fig. 3. Ukrainian soldier is controlling a drone that will drop bombs on the Russian army while watching the screen through the Internet connected to a civilian news agency and Starlink [5].

특정 주파수 대역에서 암호화하지 않은 통신을 주고 받는다는 사실에 크게 놀랐다. 러시아군은 심지어 저가(低價)의 워키토키로 송수신했는데, 현대적인 군용(軍用) 통신 장비는 1초에도 수시로 주파수를 바꾸고 신호를 암호화한다. 우크라이나군은 전투 중에 열악한 러시아군 통신 주파수 대역에 헤비메탈 음악을 틀어 통신을 방해하거나, 통신 내용을 엿들었다. 러시아군의 작전 내용과 위치는 그대로 노출됐고, 지금까지 7명의 러시아 장군이 최전선에서 지휘하다가 숨진 배경엔 이 허술한 통신 탓도 있었다[6,7]. 그러다 보니, 러시아군은 민간 통신 네트워크에 의존하는 핸드폰에 매달렸다. 구글의 '위협분석그룹' 장인 셰인 헌틀리(Shane Huntley)는 폴리티코(Politico)에 "러시아군의 의도는 알 수 없지만, 작전을 하기 위해서라도 우크라이나의 민간 통신 네트워크가 필요했다"고 말했다[8].

3.2 인터넷 분야: 우크라이나, 미국 스타링크 서비스로 위성 인터넷 사용

러시아-우크라이나 전쟁의 우주전 분석 중 인터넷 분야로 우크라이나의 디지털 장관인 미하일로 페도로프(Mykhailo Fedorov)는 2월 26일 일론 머스크(Elon Musk)에게 트위터로 "당신이 화성을 식민지화하려는 동안, 러시아가 우크라이나를 점령하려고 한다고! 당신의 왕복 로켓이 우주에서 지상에 착륙하는 동안, 러시아 로켓이 우크라이나 민간인들에게 쏟아지고! 우크라이나에 스타링크 서비스를 제공하고, 제정신인 러시아인들도 푸틴(블라디미르 블라디미로비치 푸틴, Vladimir Vladimirovich Putin)에게 맞서게 좀 해주시오"라고 요청했다[9-11]. 다음날 머스크는 "스타링크 서비스는 이제 우크라이나에서 사용 가능하고, 더 많은 (수신기) 터미널이 가고 있소"라고 트윗했다. 이후 5,000개의 인터넷 수신을 위한 안테나 접시 모양의 터미널이 우크라이나에 제공됐고, 이 중 1,330개의 터미널 비용을 바이든 행정부가

Fig. 4. Terrestrial reception terminal/Starlink for Starlink satellite internet service provided by Elon Musk.

지불했다. 민간 통신서비스가 차단돼도, 통신 단절이 일어나지 않도록 한 것이다. 이처럼 우크라이나는 미국 스타링크 서비스로 위성 인터넷을 사용하여 우주정보지원을 받고 있다[5,12](Fig. 4).

3.3 GPS 재밍: 러시아, 우크라이나 침공일부터 본격적인 GPS 재밍공격 실시

2022년 2월 23일, NSSA(National Sequrity Space Association) 주최의 Defense And Intelligence Space Conference에서 크리스토퍼 스콜스(Dr. Christopher Scolese) 미국 국가정찰국(National Reconnaissance Office, NRO) 장관이 “러시아가 우크라이나 침공을 위해 위성을 과녁에 두고 통신 및 GPS 재밍(jamming) 공격을 가할 수 있다”고 경고했다. 스콜스 장관은 러시아가 구체적으로 어떤 행위를 할지는 언급하지 않았지만, 과거의 행동을 토대로 추측하기가 쉽다며, “예를 들어, 러시아는 이미 위성에 GPS 재밍 행위를 하고 있습니다”라고 언급하고 있고, GPS 재밍 가능성이 제기되고 있다. 스콜스 장관은 정부가 운용하고 있는 인공위성뿐만이 아니라, 민간의 위성도 러시아에 의한 공격의 표적이 될 가능성이 있다고 지적하고 있어, “중요한 것은 러시아가 효과적인 사이버 공격자인 것을 알고, 시스템을 안전하게 보호해, 주의 깊게 감시하는 것입니다”라고 위성 운영자에게 경고했다. 이처럼 러시아는 GPS 재밍으로 GPS 시스템 혼란은 물론, 위조된 위치 확인, 항법, 타이밍(PNT) 데이터를 이용해 미국 GPS 사용자를 속일 수도 있는데, GPS가 완전히 정지해 버리면 항공기, 배, 군수품, 육상 차량, 지상 부대를 포함한 모든 군사 활동에 대혼란을 초래할 수 있다. 최근 러시아는 우크라이나에 대해 몇 년 동안 GPS 재밍을 실시했고, 러시아가 우크라이나를 침공한 날부터 본격적인 GPS 재밍공격을 했다[6](Fig. 5).

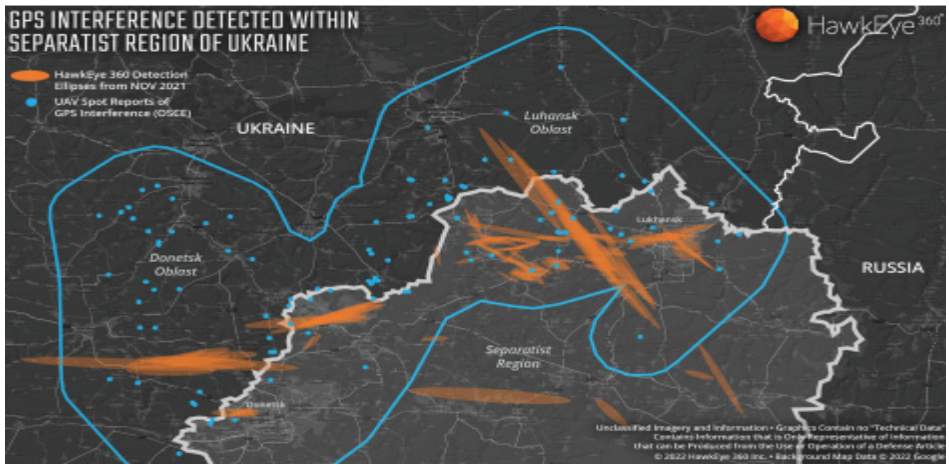

Fig. 5. Russia jammed GPS for NATO.

3.4 사이버공격: 러시아, GPS/상업위성통신 신호교란용 사이버 공격 시도

러시아와 우크라이나 전쟁을 계기로 인공위성과 이를 기반으로 하는 통신망의 보안과 복원력의 강화가 필요하다는 주장이 힘을 얻고 있다. 러시아의 침공 전후로 우크라이나와 주변 지역에 공급되는 GPS와 상업 위성통신의 신호를 교란하는 사이버 공격이 있었고, 그 배후에 러시아의 사주를 받은 해커집단이 있다는 주장이 제기되었다. 실제로 개전 초반 미국의 통신기업 비아샛이 운용하는 통신위성 KA-샛(KA-SAT)의 기능이 한동안 마비됐고, 그 결과 이 위성과 연결되어 우크라이나와 주변 나라에 설치된 다수의 위성통신용 모뎀이 먹통이 됐다. 그리고 해당 위성을 이용해 풍력 발전용 터빈을 작동시키는 독일의 에너지 회사 에너콘도 피해를 본 것으로 알려졌다. 또한, 스페이스X의 '스타링크' 우주 인터넷도 공격의 대상이 됐다. 러시아의 공격으로 파괴된 우크라이나의 통신망 복원을 위해 스타링크 서비스를 무상으로 제공한 일론 머스크는 5일 트위터를 통해 "(우크라이나) 전투 지역 근처의 몇몇 스타링크 단말기들이 몇 시간 동안 동시에 전파 방해를 받았다"면서 "전파 방해를 피할 수 있도록 최신 소프트웨어 업그레이드를 했다."고 전했다[6,12](Fig. 6).

Fig. 6. Russian cyberattacks.

4. 러시아-우크라이나 전쟁의 우주전 양상

4.1 러시아, 우크라이나 접경지역 정찰위성에 대한 재밍으로 탐지마비 시도

지난 '21년 7월 25일, 다수의 러시아 언론은 ESA의 센티널-1 위성이 우크라이나 인근 로스토프 온 돈(Rostov-on-Don) 남부지역을 스캔하던 중 반복적으로 전자전 공격을 받았다고 보도했다. 그동안 러시아는 인공위성을 활용한 서방세계의 첩보 활동에 대해 민감하게 반응한 것은 물론 정보수집 활동을 방해하기 위해 다양한 방법을 동원해 왔다. 하지만, 여러 정보를 교차 검증한 결과 이번 ESA의 센티널-1 위성에 대한 러시아의 전파 교란(SAR 위성 재밍)은 지금까지와는 비교 불가능한, 가장 강력하고 독특한 형태인 것으로 일시적으로 위성의 탐지능력을 마비시켰기 때문이다. 국적을 초월한 집단지성을 추구하는 트위터 OSINT(Open Source INTelligence: 공개출처정보) 전문가들은 러시아가 5.405 GHz 대역의 새로운 위성교란 전자전 시스템을 시험하고 있으며, 구체적 성과를 거두고 있다는 데 의견을 일치했다. 이제 러시아가 마음만 먹으면, 언제든 러시아 영공을 통과하는 서방세계 인공위성을 무력화시킬 수 있는 능력을 갖추게 됐다는 것을 증명하는 것으로, 특히 전파 교란이 일어난 우크라이나 인근 로스토브 온 돈 남부지역은 최근 러시아군의 대규모 이동과 재배치로 인해 군사적 긴장감이 고조되고 있는 지역이다. 이 때문에 일부 군사전문가들은 러시아가 본격적인 군사행동에 앞서 인공위성을 활용한 서방세계의 조기경보 및 감시체계를 무력화하려는 단계적 도발이 아닌지 의심하고 있다[7](Fig. 7).

4.2 우크라이나, 미국의 위성 지원을 받아 우주기반 영상정보 수신

미국 '워싱턴포스트(The Washington Post)'에 따르면 미하일로 페도로프(Mykhailo Fedorov) 우크라이나 부총리(디지털혁신부 장관)가 실시간 고해상도 위성 이미지를 요청한 업체 가운데 미국과 유럽 기업 총 5곳이 위성 영상을 공개하고 있다. 영상 이미지를 촬영하는 위성은

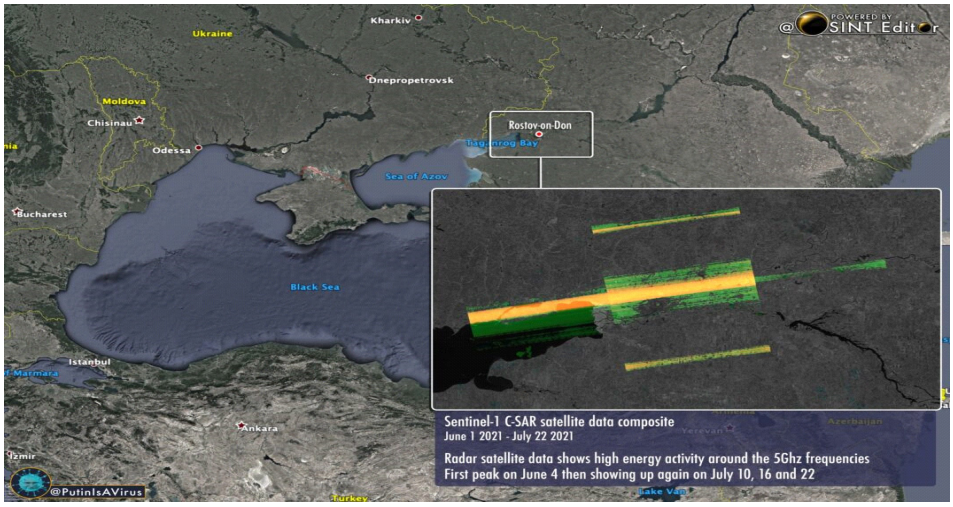

Fig. 7. Russian jamming evidence of the European Space Agency's Sentinel-1 radar imaging satellite released by Russian scientists and the media.

크게 두 가지로 분류할 수 있다. 합성 개구면 레이더(synthetic aperture radar, SAR) 위성은 물리적 특성을 감지하기 위해 지구 표면에 마이크로파 레이더 신호를 보낸다. 마치 박쥐가 어둠 속에서 탐색하는 것과 유사한 방식으로, 신호를 보내고 반사돼 돌아오는 신호를 통해 지구 표면의 소규모 움직임을 포착하고 매핑(mapping)하는 기술이다. 광학영상으로는 불가능한 야간은 물론, 구름과 연기도 꿰뚫고 촬영할 수 있어 구름이 자주 끼는 우크라이나 기상 조건에서 특히 요긴하다. 군사적 이동이나 장비 활동, 연료 보급 작업과 관련된 정보를 수집할 수 있다. 카펠라스페이스(Capella Space), 아이스아이(ICEYE), 에어버스(Airbus) 등이 SAR 위성을 사용하고 있다. 기존 광학영상 위성은 가시광선, 근적외선, 단파장 적외선 센서를 사용해 이미지를 생성한다. 플래닛랩스(Planet Labs)와 맥사테크놀로지스(MAXAR Technologies) 위성이 여기에 해당한다. 우크라이나 상황을 관측 중인 월드뷰(WorldView)-1, 2, 3 위성은 2007년 이후 발사돼 고도 496~770 km에서 작동하고 있으며, 지표면에 있는 약 30 cm 크기의 물체까지 구별할 수 있다[8](Fig. 8).

4.3 러시아, 우크라이나에서 GPS 재밍, 위성통신방해, 인터넷폐쇄, 전자공격 감행

러시아군은 GPS 재밍(jamming) 및 기타 형태의 전자 공격을 전쟁 초기 적극적으로 수행했는데, 특히, 전파방해 장비를 군대가 먼저 집결하는 지역에 배치하여 운영하기도 했다. 구체적으로 알아보면 러시아는 우크라이나 침공이 시작되기 전인 2022년 2월 24일에는 우크라이나 지역 전체에 GPS 신호 재밍을 실시한 바 있고, 러시아군이 조기경보통제기나 정찰 위성과 같은 정찰감시 수단의 SAR 레이다를 재밍하기 위해 개발한 크라슈하(Krasukha)-4와 통신 방해를 위해 개발된 R-330ZH 지텔(Zhitel)을 우크라이나 접경에 배치하였다. 또한, 러시아군에 2015년부터 배치되기 시작한 보리소글렙스크(Borisoglebsk)-2 다목적 전자전 차량도 배치해 운용했다[9](Fig. 9 and 10).

Fig. 8. Worldview-2 satellite image of Ukraine's Antonov Airport, with buildings and fuel tanks engulfed in flames [Maxa Technologies].

Fig. 9. Russian Electronic Warfare Assets. Russian SATCOM (Satellite Communication) jammer (left) Krashuka-4 jammer (right).

Fig. 10. Russian Army's newest Borisoglebsk-2 electronic warfare vehicle.

4.4 스타링크를 중심으로 한 저궤도 위성인터넷 서비스 효과성에 주목

그동안 스타링크 위성들은 밤하늘의 천문 관측에 방해가 된다는 이유로 천문학자들의 우려를 샀던 것이 사실이다. 하지만, 위급한 상황에는 위성 인터넷이 효과적일 수 있다는 것을 이번에 제대로 보여준 것이다. 스타링크 위성의 무게는 227 kg으로 1만 2,000여 개의 위성을 지구 저궤도인 550 km에 띄워 전 세계의 인터넷망을 촘촘히 연결하는 것을 목표로 한다. 현재까지 약 2,000여 개의 위성을 지구 저궤도에 쏘아 올렸으며, 서비스를 이용하려면 위성의 통신 신호를 받을 수 있도록 소형 안테나와 무선 인터넷 액세스포인트(AP) 역할을 하는 셋톱박스가 있어야 한다. 안테나와 셋톱박스만 있으면, 광통신망이나 기지국, 중계기 등의 인프라 없이도 전 세계 어디에서도 무선 통신이 가능해진다. 2020년 10월 베타 서비스를 시작한 이후 올해 1월 기준으로 14만 5,000명이 스타링크 서비스를 이용하고 있다. 이번 우크라이나 전쟁으로 스타링크를 중심으로 한 저궤도 위성 인터넷 서비스가 더욱 주목받게 되었고, 위성 인터넷의 등장으로 현대전에서 외부와의 연결은 이제 더 이상은 막을 수 없는 일이 되었다 [10](Fig. 11).

Fig. 11. Low Orbit Satellite Internet Service. (left) Destroyed Ukrainian telecommunication facility (right) Starlink satellite dish.

4.5 민간 지구관측위성으로 촬영한 러시아군 관련 고해상도 사진 일반공개

우크라이나의 부총리 겸 디지털혁신부 장관인 미하일로 페도로프는 러시아의 침공이 시작되자 플래닛랩스(Planet Labs), 맥사테크놀로지스(Maxar Technologies), 에어버스SAS(Airbus SAS), SI이미징서비스(SI Imaging Services, SIIS), 블랙스카이글로벌(BlackSky Global), 아이스아이(Iceeye), 스페이스뷰(SpaceView), 카펠라스페이스(Capella Space) 등 위성기술을 보유한 민간기업들에 위성 이미지 공유를 촉구하는 탄원서를 보냈다. 적시에 자료를 제공받아 전략적으로 활용하기 위해서다. 실시간으로 전체 상황을 들여다볼 수 있다면 군대 이동이나 증강, 난민 흐름 등을 파악하는 주요한 정보원으로 활용이 가능하다. 특히 불빛이 없는 야간에는 위성 이미지를 통해 러시아군의 이동과 전황을 파악하는 것이 필요하다. 민간 위성기업들은 지구관측 위성으로 촬영한 러시아군 관련 고해상도 사진을 연이어 공개하고 있는데, 이 이미지가 일반에 공개되고 인터넷에 게시되면서 전쟁에 관한 실시간 미디어가 형성됐다. 러시아의 공격으로 우크라이나 수도 키이우가 무참히 폭격당한 모습이 위성사진으로 생생히 포착되거나, 도심 곳곳은 물론, 국경지대에서도 화염과 연기가 피어오르는 위태로운 상황이 일반에 공개되었다. 과거에는 이러한 장면을 미국 CIA(중앙정보국) 같은 국가정찰국이 비밀리에 촬영했다면 이제는 위성기술을 보유한 민간기업이 고화질 이미지로 촬영하고 있다. 사실상 전쟁상황이 생중계되는 셈이다(Fig. 12).

이번 러시아-우크라이나 전쟁에서는 구글맵으로 우크라이나 국경지역에서 러시아군의 대규모 차량이동을 확인하고, 민간 소형위성군을 활용하여 24시간 우크라이나에 대한 위성감시가 가능했다. 특히, 민간 소비자에게 90분 이내 해당 영상 이미지 제공이 가능할 정도로 인공지능 기술 발전으로 위성 이미지를 근실시간으로 분석지원되었다. 특히, 이번 러시아-우크라이나 전쟁에서 특이한 점은 기존의 군사용으로만 사용되었던 SAR 위성이 민간분야에도 활용되면서 우크라이나의 기상이 좋지않은 낮(80%가 구름에 덮여 있는 상황)과 야간에도 러시아군대의 이동을 감시할 수 있게 SAR 위성영상이 활용되었다는 점이다(Fig. 13 and 14).

Fig. 12. SAR high resolution satellite image of Ukraine. SAR, synthetic aperture radar.

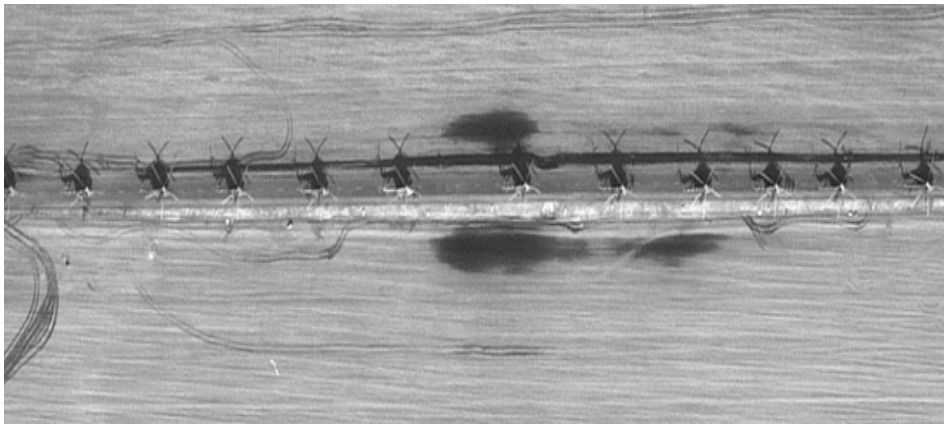

Fig. 13. SAR satellite sensor image (exhibits Russian military movement status). SAR, synthetic aperture radar.

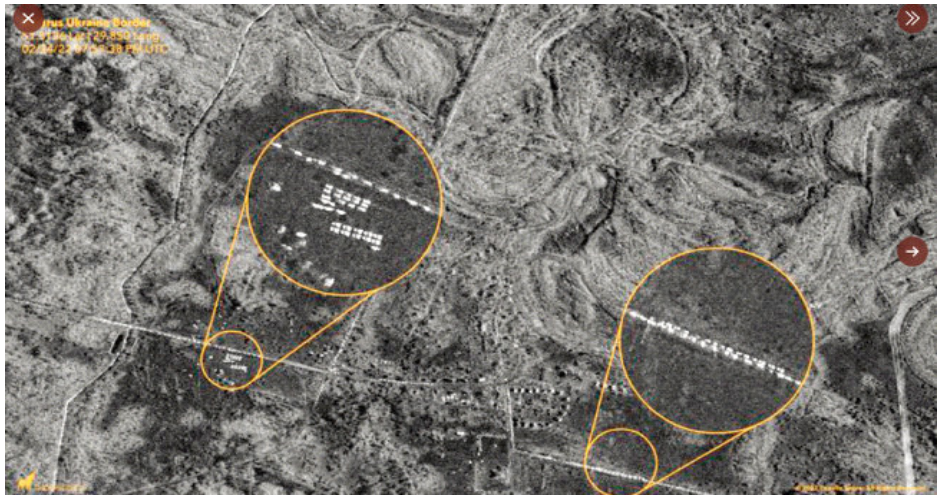

Fig. 14. Synthetic aperture radar (SAR) image of the Belarus–Ukraine border released on February 24 by Capellaspace [Capella Space].

5. 결론

지금까지 본 글에서는 러시아-우크라이나 전쟁(러시아의 우크라이나 침공)의 우주전 분석 및 양상에 대해 알아 보았다. 본인은 우주전의 양상이 상용위성 또한 잠재적인 공격 대상이 될 개연성을 고려하여 우주기술 개발시 군용위성뿐만 아니라, 상용위성도 우주위협에 대비할 수 있는 우주기술을 개발하고 동일하게 적용해야 함을 제언하고, 적용이 필요한 우주기술에 대해 열거하였다.

5.1 잠재적 우주위협에 대응가능 위성 자체방어 우주기술 개발적용 필요

최근 우주위협 사례로 러시아는 지상형 SAR 재머로 우크라이나 정부군/나토군 C4I 체계 교란(2015~16년)하거나, 유럽(ESA) 정찰위성을 재밍(jamming)하여 촬영을 거부(2022년)하였으며, 중국은 위성레이저 거리측정기(지상 레이저 시스템)로 중국본토 상공을 통과하는 미국과 프랑스 위성에 대한 재밍(dazzling: 눈부심, 촬영거부)을 시도(2005~6년)하였다. 또한, 인도-중국 위기 상황간 중국 지상군 이동상황을 촬영 거부하기 위해 지상 이동형 위성 재머를 인도 접경지역에 배치(2020년)하기도 했다. 이러한 배경에 미 정보국(DIA)은 “중국은 2020년대 중반에서 후반에 이르기까지 미국 위성에 대한 위협을 확대하기 위해 더 높은 전력의 지상 레이저 시스템을 배치할 수 있다”고 경고했고, 나아가 “정찰위성도 계속 우주로 발사해 1월 현재 250개 이상의 위성이 구축돼 있다”며 “이는 미국에 이어 세계에서 두 번째로 큰 규모”라고 설명했다. 이어 “특히 정찰위성 대부분은 인도 태평양 지역 전역에서 미군과 연합군을 감시하고 한반도와 대만, 남중국해를 비롯한 분쟁 잠재지역을 감시할 수 있다”고 덧붙였다. 러시아의 경우는 미국이 우주 산업과 관련해 자신들에게 의존하는 것을 아킬레스건으로 삼는 상황으로, 당장 우크라이나 전쟁에 대러 제재가 이행되는 상황에서 미국 우주인이 지구로 귀환할 때 러시아 소유스선을 타고 돌아오는 등 미국은 러시아의 도움이 필요한 상황으로, DIA는 “러시아는 미국의 우주 기반 서비스를 무력화하거나 미국 요청을 거부하기 위한 우주 시스템을 구상하고 있다”며 “러시아도 2020년대 중후반 미국 위성에 큰 피해를 줄 수 있는 지상 레이저를 활용할 것”이라고 전망했다. 이어 “2030년까지 모든 인공위성에 위협을 가하는 고출력 레이저 무기를 배치할 수도 있다”고 덧붙였다[10]. 이처럼 중국과 러시아의 우주위협은 가까운 미래에 우리의 우주자산에게 위협이 될 수 있다. 즉, 분쟁국 상공을 통과하는 아측 위성(SAR/EO 정찰위성)에 대한 추적 및 지상 SAR 재머 공격 혹은 레이저 공격(dazzling 눈부심, blinding 눈을 멀게 함)으로 아측 위성의 적성국 정찰에 대해 거부 개연성이 상존한다. 아래 그림은 가장 가능성이 높은 우주위협 유형으로 재밍(jamming)에 의한 공격 가능성이 높을 것을 확인할 수 있다(Fig. 15).

지상에서 우주공간으로 공격에 대한 대응 시나리오를 상정해 지상 고출력 레이저로 위성의 센서를 dazzling(눈부심)/ blinding(눈을 멀게 함)하여 촬영거부를 시도할 시 방어할 수 있는 우주기술의 개발적용이 필요하다. 이에 대한 방어기술은 탑재체 센서에 대한 필터링, 차단막 작동(filtering & shuttering)기 설치가 있고, SAR 재밍(jamming)의 경우 재밍신호 차폐를 위해 안테나 빔 패턴의 Nulling(널링, null-steering 기법), 적응 필터링과 위성본체에 대한 전자기 차폐(shieldling) 등의 방안이 있겠다. 대위성 미사일(ASAT)의 최종요격 접근시에는 최종적으로 추력기를 사용하여 공격을 회피하는 우주기술 적용도 필요하다(Fig. 16).

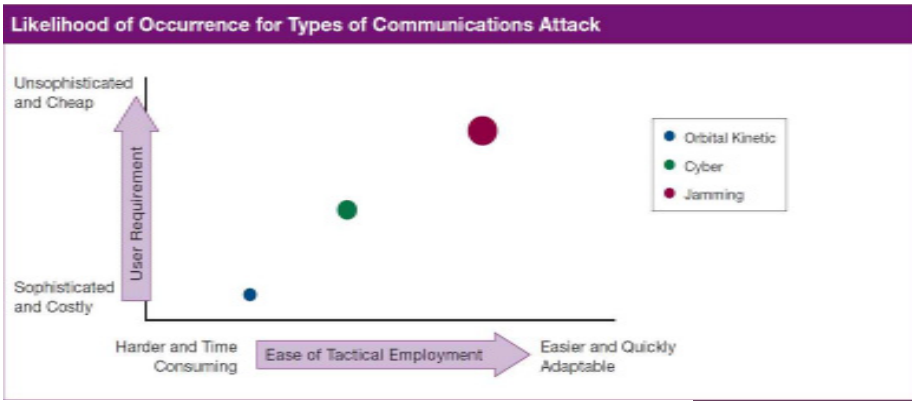

Fig. 15. Likelihood of occurrence for types of communications attack.

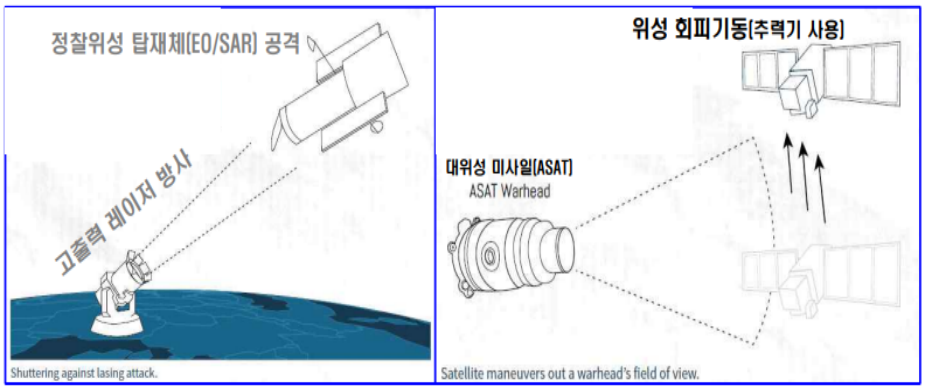

Fig. 16. Response scenarios for attacks from ground to orbiting satellite.

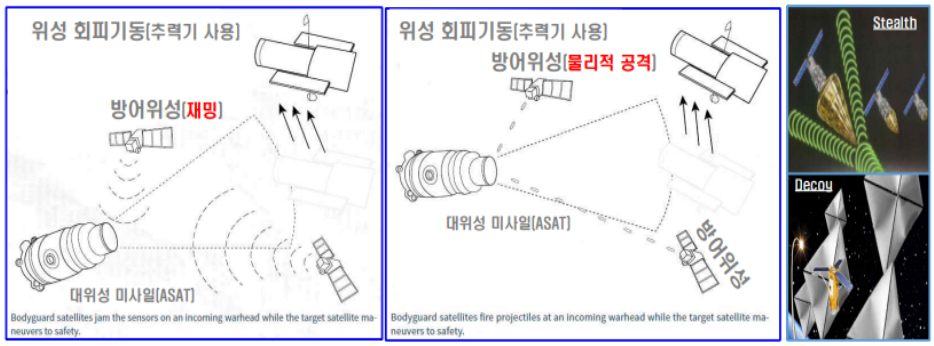

Fig. 17. Response scenarios for attacks from orbital warfare.

우주 공간 上 공격에 대한 대응 시나리오로 我 위성 활동 탐지/추적 시에는 위성을 최대한 RF/IR 센서에 발견되지 않게 Stealth 기술을 적용하여 설계하고, 궤도 정보 등을 비공개하거나, 궤도를 수시로 변경하는 등 기만(deception) 기법을 적용하여 운영하는 것을 고려해야 한다. 또한, 물리적인 대위성미사일(anti-satellite, ASAT)로 위성요격에 대비하여 전자기 기만기(Electro-magnetic Decoy) 탑재도 고려해 볼 필요가 있다. 최악의 경우, 대위성 미사일(ASAT)로 위성 요격 시에는 방어위성에 의한 ASAT 재밍(jamming)이나 목표위성이 직접 추력기를 사용해 회피기동을 실시하는 상황까지 고려해야 한다(Fig. 17).

5.2 전자공격/GPS 재밍/사이버공격에 대비가능 보안기술 적용필요(지상체)

우크라이나 전쟁 발발 이후 미국은 자국 인공위성의 보안 강화를 위해 적극적으로 움직였다. 국토안보부 내에서 사이버 보안을 담당하는 '사이버 보안 및 인프라 보안국'(Cybersecurity & Infrastructure Security Agency, CISA)은 지난 17일 자국 인공위성 운영사들에 보낸 공개 협조문에서 "평상시보다 더욱 민감하게 통신망의 상태를 관찰해달라"며 "아주 작은 이상 징후라고 발견되면 바로 상황을 공유해 달라", "접수된 내용에 대해서는 미 CISA와 FBI(Federal Bureau of Investigation)가 공동으로 사이버 보안 경보를 발령해 다른 업체들이 이에 신속히 대처할 수 있도록 하겠다"라고 했다. CISA는 업체들이 각별히 주의해서 지켜봐야 하는 '이상 징후'도 공유했다. 여기에는 FTP(file transfer protocol)처럼 보안이 취약한 프로그램을 통해 위성통신망에 접속하는 경우와 위성통신망을 통해 통상적으로 예상외로 네트워크를 접속하는 경우, 위성통신망을 통해 비공개된 그룹의 위성통신 네트워크를 접속하는 경우, 통신위성 네트워크에 강제적인 접속을 시도하는 경우가 포함됐다. 러시아-우크라이나 전쟁 이전에도 미국은 민간 인공위성의 보안을 강화하기 위해 다양한 정책을 추진해왔다. 대표적인 것이 미 우주군이 올해 1월부터 시행한 '인프라 자산에 대한 사전평가 프로그램'(Infrastructure Asset Pre-Assessment Program, IA-PRE)이다. 이 제도에 따르면 미국 연방정부 및 군은 자신들에게 적용되는 최고 수준의 사이버 보안력을 인증받은 인공위성 운영사와만 거래를 할 수 있다. 철저한 검증을 위해 18개 분야에 900개 이상의 세부 평가대상을 지정했다. 미 우주군이 자국 인공위성이 적국에 의해 공격당한 상황을 가정한 시뮬레이션 훈련도 정기적으로 실시하고 있다. 이를 통해 미군의 위성이 누군가에 의해 격추되거나 원하는 대로 작동하지 않는 경우 어떻게 대응할지에 대해 훈련하고 있다[11]. 이와 관련 한반도 분쟁시 적성국의 전자전 무기에 의한 아측 위성에 대한 전자/통신공격의 양상을 고려해 아측 위성(up/downlink 신호)에 대한 재밍(jamming) 등에 대비할 수 있는 보안기술 개발에 꾸준한 투자가 필요하다[13](Fig. 18).

또한, GPS 재밍(jamming)과 한국 우주체계의 위성-지상통제소에 대한 사이버(해킹 등) 공격대비를 위한 기술적인 투자를 철저히 해야 한다. 인공위성에 대한 보안 강화가 필요한 이유는 크게 세 가지다. 우선 뉴스페이스 시대의 도래와 함께 우주로 발사된 인공위성의 수가 최근 몇 년 새 급격히 증가했고, 이것이 국가안보와 산업에 미치는 영향도 커졌기 때문이다. 두 번째 이유는 경제성과 효율성 등의 이유로 정부와 군의 민간 위성 사용이 증가하고 있다는

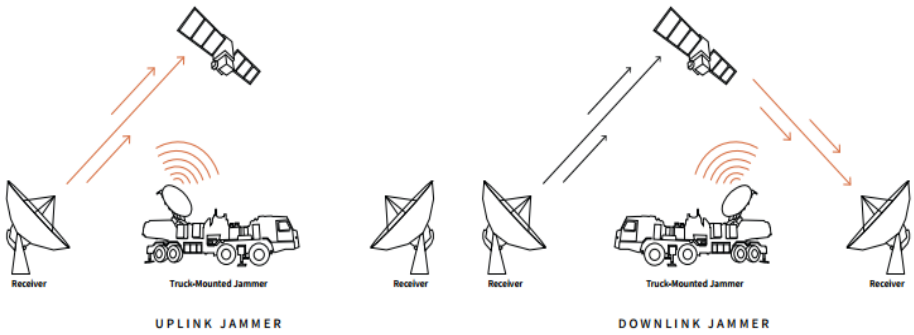

Fig. 18. Uplink and downlink jamming are two forms of electronic counterspace attack [2].

것이다. 군사위성과 민간 위성을 통합 운용하는 '하이브리드 전략'을 통해 지구관측과 통신, 첩보의 정확도를 높이려는 국가와 기관이 늘어나고 있다. 이러한 상황에서 정부나 군 위성보다 상대적으로 보안성이 취약한 민간 위성에 문제가 발생하면 그 피해는 공공 시스템으로 확대될 수밖에 없다. 마지막 이유는 인공위성이 '무기화' 될 수 있다는 우려 때문이다. 만약 누군가 악의를 갖고 특정 국가의 인공위성을 해킹해 통제권을 확보한 후 고의로 경쟁국의 위성과 충돌시키면 이는 최악의 경우 양국 간 외교·군사적 갈등의 단초가 될 수 있다. 더불어 불필요한 우주 쓰레기를 만들어 전 세계에 민폐를 끼칠 수도 있다[6,12](Table 1).

5.3 군용 위성, 생존성 향상 우주장치 개발탑재 필요

러시아는 우크라이나 침공에 NATO가 전쟁에 개입시, EU GPS 위성체계(Galileo)에 대한 공격을 경고하였다. 이러한 러시아의 사이버 공격은 NATO 국가들의 위성통신체계에 손상을 유발시킬 수 있다. 이와 관련 잠재적인 우주위협에 대비하기 위해 군 위성에는 공격받은 상황을 기록하는 장치 탑재를 고려할 필요가 있다. 또한, 우주공간에서 킬러위성의 접근이나 공격 의도를 사전에 인지할 수 있게 SAR 재밍(jamming)이나 고출력 마이크로웨이브 공격을 경보하기 위한 위성탑재 레이더경보수신기(radar warning receiver, RWR)와 고출력 레이저에 의한 SAR 정찰위성 EO/IR 재밍(jamming) 등의 경보를 위한 위성탑재 레이저경보수신기(laser warning receiver, LWR)를 장착하여 생존성을 향상할 필요가 있다. 또한, 군 위성은 평시 궤도정보 노출을 최소화하기 위해 위성 추적시에만 활성화(잠망경)하는 위성용 레이저 반사경을 개발하여 운영하는 것도 제안해 본다(Fig. 19).

Table 1. Examples of cyber attacks on space systems

연도	주요 내용	피해 기관
07/08년	미국 랜드샛-7 지형분석 위성 사이버 공격시도 (12분 이상 간섭)	노르웨이 지상통제소
08년	미 항공우주국(NASA)의 지형감시위성 사이버 공격(관제권 획득)	미 항공우주국(NASA)
09/11년	22 GB 용량의 데이터가 중국 IP로 전송('09년)/18개 서버 접근('11년)	미 제트추진연구소(JPL)
14년	위성정보 및 기상체계 사이버 공격(이틀간 체계 다운)	미 국립해양대기국(NOAA)
17년	정부 고위급 화상회의가 중국 해커의 공격에 노출 (4-5분간)	인도의 사이버 보안대
18년	위성을 관제하는 컴퓨터를 감염	미국 소프트웨어 기업

Fig. 19. Radar warning receiver & laser warning receiver for satellite.

5.4 위성통신의 군사적 활용증대에 따른 복원력 방안 우주기술 발전 필요

스타링크는 러시아의 침략 전에 우크라이나에서 서비스를 하고 있지 않았다. 하지만, 민간인 보호를 위한 통신수단이 필요하다는 우크라이나 정부의 요청을 받아들여 스페이스X는 우크라이나에서 서비스를 긴급하게 시작했다. 우크라이나에서 스타링크 서비스를 요청한 이유는 통신 인프라 시설의 파괴로 전쟁에서 민간인이 위급 상황에 제때 대처하는 것이 어려워졌기 때문이다. 평상시에도 개인과 세상을 연결해 주는 인터넷은 중요하지만, 전장에서 인터넷 연결과 통신망 제공은 헤어진 가족, 부상자를 찾거나 전쟁의 진행 상황을 실시간으로 국민들이 공유하고, 올바른 정보를 전 세계에 알리기 위해서 반드시 필요하다. 사실, 이번 전쟁이 길어지고 있는 큰 원인 중 하나는, 러시아의 의도대로 초기에 통신망을 마비시켜서, 전장의 실상을 외부에 알리지 못하도록 하는 것에 실패한 까닭도 있을 것이다[7]. 앞으로 전쟁에서 인터넷 위성통신의 군사적 활용 증대가 예상됨에 따라 인터넷 서비스를 지속적으로 제공하기 위한 안테나와 셋톱박스에 공급할 전력이 필요하다. 전장에서 안정적인 전원을 확보하는 일은 쉬운 일이 아니다. 전력을 얻기 위해서 이동형 태양광 패널과 배터리 팩, 디젤엔진을 사용하는 이동형 발전기 등을 활용하는 대안을 생각해 볼 필요가 있다. 이처럼 향후 한국도 저궤도 인터넷 통신위성 구축시 적 공격에 손실하게 될 경우에 대비한 복원력 방안을 강구하는 우주기술 발전도 필요해 보인다. 이러한 복원력 방안은 신속하게 위성을 우주공간에 투입할 수 있는 것으로 한반도의 지리적 여건(발사각 및 발사장소 제한)을 고려시 공중 및 해상발사체에 대한 투자가 필요함을 강조한다(Fig. 20).

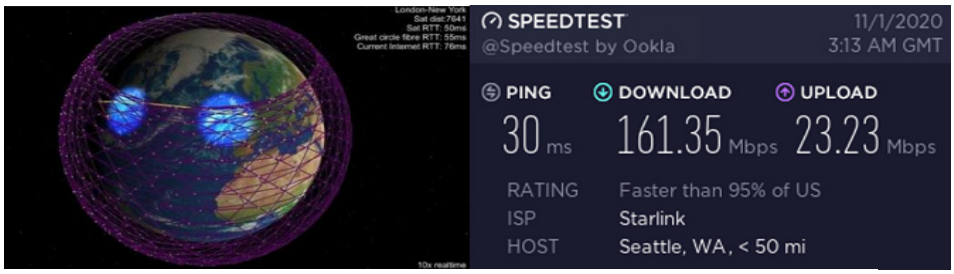

Fig. 20. Starlink Internet Servive. Starlink orbit (left) and internet service speed (right).

감사의 글

본 글은 우주산업 분야 민 · 군 협력 체제 강화의 필요성에 대한 공감대를 형성하기 위해 작성하였으며, 공군 우주전력 소요를 구상하거나 우주전력 소요제안서 작성간 도움이 되는 '우주기술과 응용' 저널지에 감사하고자 한다.

References

1. Weeden B, Samson V, Global counterspace capabilities 2022 (2022) [Internet], viewed 2022 Feb 8, available from: https://swfound.org/counterspace/
2. Harrison T, Johnson K, Young M, Space threat assessment 2022 (2022) [Internet], viewed 2022 Feb 8, available from: https://www.csis.org/analysis/space-threat-assessment-2022
3. Defense Inteligence Agency, 2022 Challenges to security in space, space reliance in an era of competition and expansion (2022) [Internet], viewed 2022 Feb 8, available from: https://www.dia.mil/Military-Power-Publications/
4. Yoo SK, Russia-Ukraine war from the perspective of military operations (2022) [Internet], viewed 2022 Feb 8, available from: https://kookbang.dema.mil.kr/newsWeb/20220413/7/BBSMSTR_000000010026/view.do
5. Lee CM, Drone bombing, live broadcast of massacre... Why are Ukrainian telecommunication services working? (2022) [Internet], viewed 2022 Feb 8, available from: https://www.chosun.com/international/europe/2022/04/13/DMQ4L5PHFBEX7OBYE3VKSVJ37E/?utm_source=daum&utm_medium=referral&utm_campaign=daum-news
6. Eyefun, It could even attack satellites for Russia's invasion of Ukraine... (2022) [Internet], viewed 2022 Feb 8, available from: https://eyefun.tistory.com/667
7. Hwang JA, Satellite internet 'Starlink' shines on the battlefield in Ukraine (2020) [Internet], viewed 2022 Feb 8, available from: https://news.v.daum.net/v/20220328190024530
8. Park SS, Cyberattacks targeting artificial satellites are becoming a reality (2022) [Internet], viewed 2022 Feb 8, available from: https://news.v.daum.net/v/20220325091752213
9. Kookbangilbo, Universe! Are you okay··· (2022) [Internet], viewed 2022 Feb 8, available from: https://kookbang.dema.mil.kr/newsWeb/20211222/1/BBSMSTR_000000010443/view.do
10. Lee JR, Satellite image to broadcast live Ukrainian tragedy: Planet Labs, Maxa Technologies, SpaceX··· Modern warfare is a satellite technology war (2022) [Internet], viewed 2022 Feb 8, available from: https://weekly.donga.com/3/all/11/3272350/1
11. Go DY, U.S., China, Russia Star Wars intensify in Ukraine war... "Deployment of satellite attack weapons" [Internet], viewed 2022 Feb 8, available from: https://m.etoday.co.kr/view.php?idxno=2123618
12. Guk NP, Musk's Ukrainian space internet emergency support 'behind the scenes' (2022) [Internet], viewed 2022 Feb 8, available from: https://news.v.daum.net/v/20220314100605782

13. Hill J, Jewett R, Cybersecurity US Space Force to kick off IA-PRE program in January 2022, via satellite news (2021) [Internet], viewed 2022 Feb 8, available from: https://www.satellitetoday.com/cybersecurity/2021/10/07/us-space-force-to-kick-off-ia- pre-program-in-january-2022/

Author Information

최 성 환 Kf2020@hanmail.net

공군사관학교에서 1994년도에 외국어학 학사학위를 취득하였으며, 2015~2017년 동안 합참 전력기획부에서 근무하면서 군정찰위성 사업을 담당하였다. 2017~ 2021년 공군본부 우주센터에서 우주전력발전과장으로서 초소형위성체계, 한국형위성항법체계(KPS) 등 우주전력 소요를 제안하였고, 우주정보상황실장으로서 중국 창정5B 로켓 추락과 같은 우주위험 상황에 대응하였다. 2021년부터 현재까지 우주센터장 직을 수행하며, 공군 우주력 발전을 위해 노력 중이다.