국가전략연구위원회 이슈브리핑 24호 (발간일: 2024.3.18.)

우주 전자전 분석 및 사이버 우주안보: 우주 전자전 및 사이버 공격을 중심으로[1)]

최성환 (한화시스템)

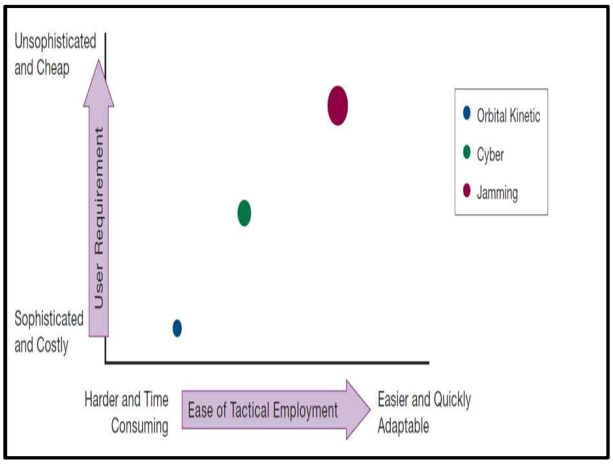
1. 머리말

위성이 제공하는 전략적 이점 때문에 중국, 러시아 등은 분쟁시 우위를 확보하기 위해 상대국 위성에 대한 물리적 공격 능력을 확보하거나, 그 역량을 지속 발전시키고 있다. 하지만, 최근 우주공간에 위성 등 우주물체의 급속한 증가로 우주 쓰레기(debris) 문제가 국제적인 주요 도전과제로 부각되고 있고, 이에 지난 2022년 9월 뉴욕에서 열린 유엔총회에 한국을 포함한 유엔 회원국들이 수직발사식 위성요격 미사일(anti-satellite, ASAT) 실험을 더 이상 실시하지 않도록 하는 결의안 채택을 통해, 전세계 13개국(23년 6월 기준)이 ASAT 실험을 실시하지 않기로 했다. 이는 앞으로의 전쟁 양상이 물리적인 공격보다는 우주 전자전, 사이버공격으로 진행될 개연성이 높아짐을 보여 준다.(그림 1)[2)] 이러한 배경에 우주 전자전과 사이버공격은 최근 전쟁에서 실행·가능한 옵션으로 빠르게 떠오르고 있는데, 그 이유는 물리적 공격에 비해 저렴하고 쉽게 접근할 수 있기 때문으로, 현재 진행 중인 러시아-우크라이나전의 양상이 되기도 하였다. 본 글에서는 러시아-우크라이나전의 우주 전자전을 분석하고

1) 이 글은 2024년 3월 13일 제8차 사이버 국가전략 포럼에서 발표된 발표문을 수정보완한 것이다.
2) JFQ / issue 69, 2nd quarter 2013 p.62, ndupress.ndu.edu

사이버공격 현황에 대해 알아보고, 우주 전자전과 사이버 우주안보의 시사점을 제언하고자 한다.

[그림 1] 우주 전자전, 사이버공격 개연성



[그림 2] 인터넷으로 드론을 조종하는 장면

2. 러시아-우크라이나 전쟁의 우주 전자전 분석

2-1. 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 투하(그림. 2)하고, 볼로디미르 젤렌스키(Volodymyr Zelenskyy) 우크라이나 대통령은 텔레그램(telegram)으로 계속 국민에게 항전을 독려했다. 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 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.[3] 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.[4]

2-2. 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 왕복로켓이 우주에서 지상에 착륙하는 동안, 러시아 로켓이 우크라이나 민간인들에게 쏟아지고! 우크라이나에 스타링크 서비스를 제공하고, 제정신인 러시아인들도 푸틴(블라디미르 블라디 미로비치 푸틴, Vladimir Vladimirovich Putin)에게 맞서게 좀 해주시오"라고 요청했다.[5]

---

3) 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
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

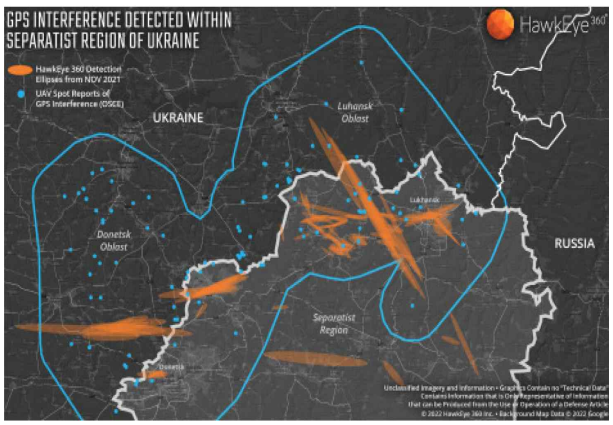
4) Park SS, Cyberattacks targeting artificial satellites are becoming a reality (2022) [Internet], viewed 2022 Feb 8, available from: https://news.v.daum.net/v/20220325091752213

5) 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
Lee JR, Satellite image to broadcast live Ukrainian tragedy: Planet Labs, Maxa Technologies,

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 터미널(그림 3)이 우크라이나에 제공됐고, 이 중 1,330개의 터미널 비용을 바이든 행정부가 지불했다. 민간 통신서비스가 차단돼도, 통신 단절이 일어나지 않도록 한 것이다. 이처럼 우크라이나는 미국 스타링크 서비스로 위성 인터넷을 사용하여 우주정보지원을 받고 있다.[6)]

[그림 3] Star Link 안테나

[그림 4] 러시아의 GPS 재밍 공격



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
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

6) 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

2-3. 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 재밍 공격(그림 4)을 했다.[7)]

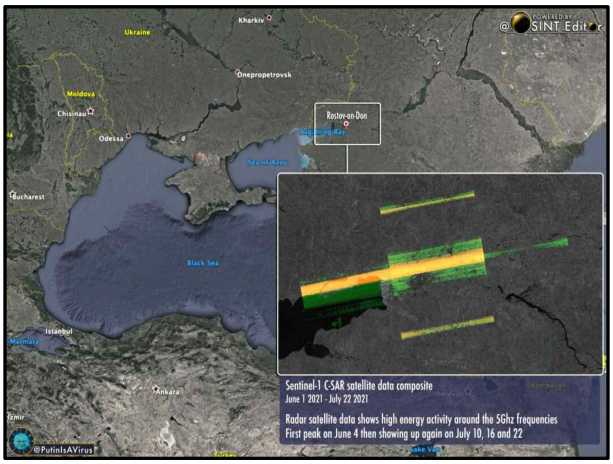
2-4. 러시아, 접경지역 유럽 정찰위성에 대한 재밍으로 위성관측 방해 시도

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.(그림 5) 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 러

7) 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

시아가 본격적인 군사행동에 앞서 인공위성을 활용한 서방세계의 조기경보 및 감시체계를 무력화하려는 단계적 도발이 아닌지 의심하고 있다.[8)]

[그림 5] 러시아의 센티널-1 위성 재밍공격 증거



[표 1] 최근 사이버공격 현황

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 용량 데이터, 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
<우크라이나 사이버 공격>		
22년 2월	KA-SAT 통신위성 네트워크 시설 사이버 공격	미국 Viasat 기업
22년 3월	우크라이나 통신 서비스사 사이버 공격	우크라이나 통신 서비스 기업

3. 러시아-우크라이나 전쟁의 사이버공격 현황

러시아와 우크라이나 전쟁을 계기로 인공위성과 이를 기반으로 하는 통신망의 보안과

8) 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

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.(표 1) 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.[9] 이처럼 사이버 공격자는 특정 임무에 대한 정보를 수집하여 목표로 삼으려고 한다. 즉, 사이버 공격자는 펌웨어(firmware), 소프트웨어(software), 하드웨어(hardware), 주파수(frequencies), 프로토콜(protocols), 암호화 알고리즘(fcryptographic algorithms) 임무에 사용된 우주선 설명자 및 우주선 설계, 아키텍처, 위치 및 궤적과 같은 기타 지식에 대한 정보를 찾을 수 있다. 또한, 공급망에서 해킹 기술을 적용하면 소프트웨어(software)/도구(tools)/데이터시트(datasheets) 또는 설계 노출이 발생할 수 있는데, COTS(상용) 또는 오픈소스 구성 요소(open-source components)를 사용하면 온라인 또는 생산 회사에서 정보를 쉽게 수집할 수도 있다.

4. 우주 전자전/사이버 우주안보 시사점

4-1. 우주 시스템(위성 등), 생존성 향상 우주장치 개발탑재 필요

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.(그림 6) 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

9) 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

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.

[그림 6] 잠재적 우주위협에 대응가능 위성 자체방어 우주기술 적용방안(예)

4-2. 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 공개협조문에서 "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 '이상징후'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 접

속하는 경우, 통신위성 네트워크에 강제적인 접속을 시도하는 경우가 포함됐다. 러시아-우크라이나 전쟁 이전에도 미국은 민간 인공위성의 보안을 강화하기 위해 다양한 정책을 추진해 왔다. 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.[10] 이와 관련 한반도 분쟁시 적성국의 전자전 무기에 의한 아측 위성에 대한 전자/통신 공격의 양상을 고려해 아측 위성(up/downlink 신호)에 대한 재밍(jamming) 등에 대비할 수 있는 보안기술 개발에 꾸준한 투자가 필요하다.[11] 또한, GPS 재밍(jamming)과 한국 우주체계의 위성-지상통제소에 대한 사이버(해킹 등) 공격 대비를 위한 기술적인 투자를 철저히 해야 한다.

10) 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

11) 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/

<참고자료>

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