SISTEMELE DE NAVIGAȚIE CU SATELIȚI – O ȚINTĂ EVITATĂ? –

Colonel Dorian LUPARU

Agenția de informații geospațiale a apărării „General de divizie Constantin Barozzi", București

DOI: 10.55535/GMR.2022.3.04

În contextul geopolitic actual, regiunea Mării Negre a devenit scena conflictului în care se utilizează o gamă largă de armament și muniție, diferențiată categoric de dirijarea/ghidarea prin semnalele transmise de rețelele de navigație cu sateliți – GNSS. Aportul acestora s-a remarcat instantaneu, chiar dacă nu reprezintă o noutate, iar armele care au beneficiat de augmentarea semnalului satelitar și-au dovedit acuratețea loviturilor. Din acest motiv, în câmpul de luptă au apărut acțiunile de bruiere sau falsificare a semnalului satelitar și au fost lansate chiar amenințări de atac al GNSS. Prin prezentul articol îmi propun o dezambiguizare a subiectului, în încercarea de a delimita declarațiile și posibilitățile militare de cele politice în mediul spațial, devenit esențial în desfășurarea acțiunilor militare moderne.

Cuvinte-cheie: GNSS, bruiaj, semnal satelitar, spoofing, GLONASS.

INTRODUCERE

Regiunea Mării Negre a fost şi este un loc central al competiției dintre Rusia și Occident pentru viitorul Europei. Regiunea a experimentat două decenii de conflicte fierbinți chiar înainte de anexarea Crimeii de către Moscova, în 2014, iar Rusia a folosit forța militară împotriva țărilor din regiune de patru ori, începând din 2008. Trebuie remarcat, în contextul geopolitic actual, modul în care Rusia folosește o varietate de instrumente militare și nemilitare pentru a-și promova obiectivele, analizând felul în care cei trei aliați ai Organizației Tratatului Atlanticului de Nord – Bulgaria, România și Turcia – și cinci parteneri ai NATO – Armenia, Azerbaidjan, Georgia, Moldova și Ucraina – din regiunea Mării Negre percep și răspund la activitățile Rusiei și unde anume interesele acelor țări se aliniază sau sunt divergente. Fiind o putere economică şi militară mondială, există continuu temerea că, în plan strategic, deține mereu în stare latentă diverse posibilităţi de afirmare a puterii, iar o opţiune neconvenţională, dar de impact covârşitor este atacarea sistemelor de navigaţie cu sateliţi (GNSS – Global Navigation Satellite System), în mod particular GPS (Global Positioning System). Există această posibilitate?

Regiunea Mării Negre a experimentat două decenii de conflicte fierbinți chiar înainte de anexarea Crimeii de către Moscova, în 2014, iar Rusia a folosit forța militară împotriva țărilor din regiune de patru ori, începând din 2008.

Masarea unor convoaie militare ruseşti, la începutul acestui an, în zona oraşului rusesc Belgorod până la graniţa cu Ucraina a fost sesizată şi urmărită îndeaproape de întrega lume, cu vădite îngrijorări politice şi cu mare preocupare şi atenţie atât de către mediul militar, cât şi de cel civil. Poate părea surprinzător interesul civil, dar deplasările (marşurile), staţionările sau manevrele au fost analizate pe baza imaginilor satelitare obţinute din diverse surse, cele mai multe din mediul de înaltă tehnologie spaţială în care activează diverse companii comerciale. La un moment dat, la sfârşitul lunii februarie a.c., Google a declarat că va opri temporar actualizările live de trafic în Ucraina, *„după consultarea cu mai multe surse de pe teren, inclusiv autoritățile locale”* (Culliford, 2022), fără a da explicaţii referitoare la îngrijorările care au determinat această decizie. Declaraţiile au fost voalate şi au sugerat că Google nu ar dori să fie parte a furnizării de date de direcționare

într-un conflict internațional, dar analiștii au fost de părere că datele de trafic generate de companie pot dezvălui locațiile trupelor sau ale refugiaților şi ar putea fi folosite pentru loviturile militare.

Departe de a fi numit *„primul conflict pin satelit”*, această etichetă purtând-o Războiul din Golf desfășurat acum trei decenii, trebuie remarcat totuși că, în acest răstimp, mediul beligerant a cuprins şi segmentul spaţial, ca o componentă firească, evolutivă a conflictului modern şi a creat oportunitatea fructificării informaţiilor spaţiale oferite de sateliţi comerciali şi în scopuri militare. Publicul larg apreciază spectacolul, artificiile şi, de aceea, armamentul modern, mai ales muniţia (rachetele, bombele), care au suport satelitar, dau lovituri de mare acurateţe, denumite ca atare *„surgical strikes”*, într-un *„precision warfare”* (război de precizie), cu impact major în expunerea media. Un exemplu devenit celebru este eliminarea *„teroristului măcelar”* (Inside GNSS, 2007) Abu Musab al-Zarqawi; astfel, spre locuinţa acestuia din suburbia Hibhib, Irak, a fost lansată o *„bombă inteligentă”*, ucigându-l, împreună cu cei câţiva apropiaţi, în iunie 2006. Ideea este că a fost folosită o bombă cu încărcătură explozivă mică, precis dirijată prin GPS, în vederea obţinerii rezultatului dorit cu un minimum de daune colaterale sau chiar prin evitarea acestora. A fost considerat un succes şi o demonstraţie clară a suportului GNSS adus tehnologiei în domeniul militar.

Semnalul satelitar susţine o multitudine de activităţi/ operaţiuni militare care includ domeniul informaţional, intelligence, pe cel al navigării, managementul transportului, al studiului terenului, al dinamicii acţiunilor şi multe altele, care conferă o poziţie privilegiată celui care îl posedă.

Dar, semnalul satelitar susţine o multitudine de activităţi/operaţiuni militare care includ domeniul informaţional, intelligence, pe cel al navigării, managementul transportului, al studiului terenului, al dinamicii acţiunilor şi multe altele, care conferă o poziţie privilegiată celui care îl posedă. Evident că această stare corespunde opusului adversarului, care va căuta să elimine acest avantaj sau să-l neutralizeze.

În mod evident, se nasc o serie de întrebări, dintre care menționăm:

1. *Este posibil ca reţelele de navigaţie prin sateliţi să fie atacate?*
2. *Poate să fie afectată întreaga lume de deteriorarea, alterarea sau sistarea suportului spaţial?*

În acest context, trebuie să precizez că, în acest articol, voi aborda sistemele de navigaţie cu sateliţi care operează pe orbite înalte, la aproximativ 20.000 de kilometri altitudine, excluzând sateliţii dispuşi pe orbita joasă (LEO sau Low Earth Orbit), o regiune care se întinde până la 2.000 de kilometri de Pământ, care au ca funcţiuni principale asigurarea comunicaţiilor, a internetului, observaţiilor meteorologice și altele.

SCENA SISTEMELOR DE NAVIGAŢIE CU SATELIŢI

În economia modernă mondială nu mai sunt de conceput o serie de activităţi majore fără ajutorul semnalelor sistemelor de navigaţie cu sateliţi, care ne influenţează şi au ajuns de mult timp să facă parte din cotidianul nostru. Astfel, infrastructura şi managementul transportului aerian, maritim şi terestru, comunicaţiile, cartografierea şi măsurătorile terestre, operaţiunile de căutare şi salvare şi multe altele au dezvoltat dependenţă de datele satelitare, fără a omite interesul militar concretizat pe aplicaţiile de localizare, urmărire, dirijare, ghidare a trupelor, materialelor, navelor, aeronavelor, echipamentelor, armamentelor şi muniţiei.

În lume, există șase sisteme de navigație prin satelit, care formează o comunitate aparte, diferenţiată în principal de sarcinile spaţiale (sateliţi orbitali sau geostaţionari) sau de acoperirea globală sau zonală. Cel mai cunoscut este GPS-ul american, dar există şi versiunea chineză – BeiDou (COMPASS), iar cel rusesc se numește GLONASS. Europenii au GNSS Galileo, însă acesta nu joacă un rol important în navigația prin satelit, deoarece este doar pentru uz civil, este limitat şi are o serie de restricții. Mai pot fi menţionate IRNSS indian şi Quasi-Zenith japonez, dar sunt sisteme zonale şi de augmentare. Sistemele de navigație prin satelit sunt investiţii costisitoare pentru orice deținător – SUA, China, Rusia sau Europa, prin urmare, țările încearcă să își combine eforturile atunci când sateliții unui sistem îl pot completa pe un altul. De exemplu, Rusia cooperează activ în această direcție cu China şi se presupunea că se vor face paşi similari cu Europa și SUA, dar nu mai poate fi un demers de actualitate, din motive geopolitice evidente.

În lume, există șase sisteme de navigație prin satelit, care formează o comunitate aparte, diferenţiată în principal de sarcinile spaţiale (sateliţi orbitali sau geostaţionari) sau de acoperirea globală sau zonală. Cel mai cunoscut este GPS-ul american, dar există şi versiunea chineză – BeiDou COMPASS, iar cel rusesc se numește GLONASS.

Evoluţia GLONASS a fost sinuoasă, a început în URSS, iar, după ani de decădere, în anii ’90, sistemul a fost revitalizat și, treptat, adus la deplină acoperire globală. Acum există o constelație completă de sateliți pe orbită, aceștia fiind utilizați atât în segmentul civil, cât și în cel militar. Nu există diferențe față de același GPS.

Avantajul GLONASS în zona nordică este de netăgăduit, în Scandinavia sistemul permițând obținerea coordonatelor mai rapid și mai precis, completând GPS-ul. De altfel, toți producătorii de chipset-uri adaugă soluțiilor lor suport pentru toate sistemele de navigație existente – este mai ieftin și mai ușor, iar consumatorul obține cu acuratețe mărită. Mai mult, chiar și aplicaţiile militare

au sisteme duale şi pot folosi semnale din altă constelaţie satelitară pentru navigație sau alte necesităţi, utilizarea tuturor datelor disponibile reprezentând un beneficiu.

ALTERAREA SEMNALELOR SATELITARE – BRUIAJ VERSUS FALSIFICARE

Pentru statele care nu au un sistem propriu de navigație prin satelit, în situaţia unui conflict, este posibil ca semnalul satelitar să fie sistat sau să conţină erori, adică să fie alterat, deteriorat sau falsificat. Un exemplu clar a fost în războiul din Kosovo, din 1999, când semnalul satelitar a fost oprit în timpul bombardării Iugoslaviei de către NATO, apoi a fost introdusă în mod deliberat o eroare în activitatea segmentului public civil GPS.

Există, în esență, două moduri de a interfera cu semnalele GPS: prin bruiaj și prin falsificare. Bruiajul blochează complet semnalul, iar acest tip de interferență este cunoscut din bazele militare. Spoofing-ul este o interferență mai avansată, în care un transmițător radio trimite semnale GNSS false, care îl fac pe receptor să creadă că sunt semnale de satelit reale.

Relativ recent, în perioada 22-24 iunie 2017, au fost raportate incidente având presupunerea falsificării semnalului GPS; concret, o serie de nave din Marea Neagră au raportat anomalii despre poziția lor derivată din GPS și s-au trezit aparent localizate în zona continentală, la un aeroport (Rogoway, 2017). Pe lângă evenimentele din Marea Neagră, au fost raportate și întreruperi ale GPS-ului şi în estul Finlandei, în estul Mediteranei, lângă Cipru, Turcia, Liban, Siria, Israel și în nordul Irakului.

Există, în esență, două moduri de a interfera cu semnalele GPS: prin *bruiaj* și prin *falsificare*. După cum sugerează cuvântul *bruiaj*, această metodă blochează complet semnalul, iar acest tip de interferență este cunoscut din bazele militare, unde nu s-ar dori să i se permită inamicului să urmărească mișcările, având suportul GPS. Bruiajul este chiar la îndemână, deoarece semnalele GNSS transmise de sateliți sunt relativ slabe; se spune că un bruiaj portabil de un kilowatt poate bloca un receptor GPS de la o distanță de până la 80 de kilometri!

Spoofing-ul este o interferență mai avansată, în care un transmițător radio trimite semnale GNSS false, care îl fac pe receptor să creadă că sunt semnale de satelit reale. Aceasta este o metodă de interferență semnificativ mai complexă, deoarece trebuie să fie capabil să reproducă mai multe semnale GNSS în paralel, astfel încât receptorul să nu detecteze că sunt semnale false.

Falsificarea (spoofing-ul) nu este o amenințare nouă – există de zeci de ani, dar abia în ultimii ani i s-a acordat mai multă atenție. Ca și în cazul tehnologiei de bruiaj și antiblocare și al mai multor subiecte din domeniul GNSS, spoofing-ul își găsește rădăcinile în epoca

radarului Războiului Rece. În acele vremuri, era adesea cunoscută sub denumirea de *„blocarea imaginii false”*, în cazul în care se transmiteau returnări radar denaturate pentru a crea o imagine falsă pe ecranul radar al adversarului.

Când a apărut GPS-ul, codul C/A (Coarse or Clear/Acquisition) a fost perceput ca fiind vulnerabil la falsificare, fiind un cod deschis, deci oricine este liber să-l reproducă; la urma urmei, ce este un simulator GPS? Un GPS spoofer! În mod obişnuit, receptoarele GPS se verifică folosind semnale test de la un simulator GPS. Desigur, tocmai acesta este motivul pentru care sateliții GPS transmit și codul militar P(Y) și continuă să facă acest lucru. Codul P oferă o precizie îmbunătățită și alte beneficii, dar, mai important, acesta este modulat cu secvența de criptare W pentru a oferi codul P(Y) criptat. De când modulul anti-spoofing a fost activat, cu excepția cazului în care există accesul de securitate, codul P(Y) nu poate fi falsificat.

Asadar, la momentul iniţial, se poate susține că amenințarea de falsificare a fost rezolvată, dar, abia când GPS-ul a devenit omniprezent în domeniul comercial și civil, falsificarea a devenit problematică. Faptul că marea majoritate a receptoarelor GPS din lume s-au bazat exclusiv pe codul C/A necriptat a devenit un motiv de îngrijorare – mai ales acolo unde acele receptoare GPS erau esențiale pentru infrastructura critică. Chiar şi aşa, ameninţarea falsificării semnalului satelitar a fost îndelung dezbătută, dar specialiştii au concluzionat că este o amenințare teoretică sau că este mult prea dificil spoofing-ul, deci nu ar exista motive de îngrijorare. Totuşi, în anul 2012, au fost realizate câteva demonstrații relevante de către Laboratorul de radionavigație al Universității din Texas, când personalul de laborator a efectuat un exercițiu la White Sands Missile Range, unde o dronă ghidată de GPS a fost supusă unui test de falsificare a semnalului satelitar de la distanță. Drona a fost păcălită, crezând că altitudinea sa crește, făcând-o să compenseze prin căderea sa. Apoi, în 2013, aceeași echipă a demonstrat modul în care un iaht ar putea fi îndepărtat de la cursul său printr-un atac de falsificare. Deci, ceea ce se credea improbabil a devenit real, ameninţarea spoofing-ului existând de la început şi dovedindu-şi potențialul de atac.

Când a apărut GPS-ul, codul C/A a fost perceput ca fiind vulnerabil la falsificare, fiind un cod deschis, deci oricine este liber să-l reproducă; la urma urmei, ce este un simulator GPS? Un GPS spoofer!

Ulterior, a apărut o dovadă a ameninţării şi mai bizară, un joc pentru telefonul mobil, Pokemon GO, în care jucătorii călătoreau cu telefoanele lor, căutând anumite locaţii fixe şi obținând puncte prin

strângerea de creaturi, într-o lume a unei realități augmentate. Nu a durat mult până când oamenii au căutat noi modalități de a câștiga puncte în joc din confortul căminului propriu, fără a fi nevoiți să facă efortul de a călători în jurul lumii. Astfel, au făcut ca telefonul *„să creadă că este în altă parte”* prin denaturarea şi falsificarea locaţiei, ridicând, din nou, gradul de alarmă al ameninţării. Concret, nu se ştie *„cine a dat tonul”*, deoarece, în anul 2017, falsificarea semnalului GPS a provocat un haos pentru receptorii din aplicațiile de telefon din centrul Moscovei, determinându-i să prezinte rezultate eronate. Amploarea problemei a devenit evidentă când oamenii au jucat acelaşi Pokemon GO: semnalul fals, care părea să se concentreze pe Kremlin, muta pe oricine din apropiere la Aeroportul Vnukovo, la 32 km depărtare!

Eșecurile navigației ar putea duce la încălcări ale spațiului aerian. Spațiul aerian deasupra Ucrainei, Moldovei, Belarusului și în părțile de sud ale Rusiei este, în prezent, interzis operatorilor din cauza riscului de siguranță de a opera în sau în apropierea unei zone de război active.

VREMEA DEMONSTRAŢIILOR

În martie anul acesta, Agenția pentru Siguranța Aviației a Uniunii Europene (EASA) a avertizat, printr-un comunicat, că sistemele de navigație prin satelit – serviciul GPS american și semnalul Galileo similar din Europa – sunt afectate în zonele din jurul Rusiei şi există întreruperi ale echipamentelor vitale de siguranță a navigației aeriene de către ceea ce părea a fi o parte rău intenționată (Katz, 2022).

EASA sugerează că sunt cauzate probleme sistemului fie prin blocarea acestuia, fie prin furnizarea de date înșelătoare. Numărul de astfel de cazuri care au apărut s-a intensificat în regiuni apropiate de granițele Rusiei, de-a lungul provinciei Kaliningrad. Efectele falsificării au fost observate în diferite faze ale zborului, astfel că piloții au fost forțați să redirecționeze avioanele sau să schimbe destinația finală a unei aeronave în timpul zborului, după cum a comunicat EASA în buletinul de siguranță adresat operatorilor (Ib.). Impactul interferenței variază de la pierderea navigației de bază în punctele de referință până la prevenirea abordării pistei sau declanșarea falsă a avertismentelor de teren.

Eșecurile navigației ar putea duce, de asemenea, la încălcări ale spațiului aerian. Spațiul aerian deasupra Ucrainei, Moldovei, Belarusului și în părțile de sud ale Rusiei este, în prezent, interzis operatorilor din cauza riscului de siguranță de a opera în sau în apropierea unei zone de război active. De asemenea, Rusia a interzis aproape tuturor operatorilor europeni să zboare pe cerul său, după ce Marea Britanie, Uniunea Europeană și alții au sancționat companiile aeriene ruse.

Efectele bruiajului GNSS și/sau ale posibilului spoofing au fost observate de aeronave în diferite faze ale zborurilor lor, ducând, în anumite cazuri, la redirecționarea sau chiar schimbarea destinației din cauza incapacității de a efectua o procedură de aterizare în siguranță. *„În condițiile actuale, nu este posibil să se prezică întreruperile GNSS și efectele acestora. Amploarea problemelor generate de o astfel de întrerupere ar depinde de întinderea zonei în cauză, de durata și de faza de zbor a aeronavei afectate”.* (Johnson, 2022).

În astfel de circumstanțe, unele dintre problemele care au fost întâmpinate sau potențiale difuncţii care pot apărea din cauza bruiajului includ:

- pierderea capacității de a utiliza GNSS pentru navigarea în puncte de referință;
- pierderea capacității de navigație în zona de apropiere (RNAV/ Area Navigation);
- incapacitatea de a efectua sau de a menține operațiuni de performanță de navigație necesară (RNP[1]);
- declanșarea avertismentelor de teren;
- poziția inconsecventă a aeronavei pe afișajul de navigație;
- pierderea funcționalităților de supraveghere dependentă automată-difuzare;
- eșecul sau degradarea managementului traficului aerian (ATM/ Air Traffic Management), a serviciilor de navigație aeriană (ANS/Air Navigation Services), a sistemelor de comunicații, navigație și supraveghere (CNS) și a aeronavelor care utilizează GNSS ca referință temporală;
- potențiale încălcări ale spațiului aerian și/sau abateri de rută din cauza degradării GNSS (Matei, 2002).

„În condițiile actuale, nu este posibil să se prezică întreruperile GNSS și efectele acestora. Amploarea problemelor generate de o astfel de întrerupere ar depinde de întinderea zonei în cauză, de durata și de faza de zbor a aeronavei afectate”.

Privite ca potenţiale ameninţări, dar nefiind considerate a fi o conduită, au fost emise o serie de măsuri de atenuare, printre acestea numărându-se solicitarea către autoritățile aviatice de a fi pregătite să furnizeze sisteme alternative de navigație terestră și non-satelit în zonele afectate și emiterea de instrucțiuni piloților pentru a fi pregătiți să revină la proceduri clasice de aterizare cu excepția serviciilor prin satelit.

[1] RNP AR/Required Navigation Performance – performanța de navigație cerută/autorizare cerută.

După izbucnirea conflictului din Ucraina, în zona Mării Negre a fost detectat un bruiaj de către avioanele de recunoaștere americane, dar acesta nu a interferat cu operațiunile de sprijin ale SUA, conform purtătorului de cuvânt al Comandamentului Spațial al SUA: *„Nu există niciun impact asupra forțelor americane și aliate din Europa în acest moment.”* (Hitchens, 2022). Nu este clar nici dacă bruiajul a avut un efect asupra operațiunilor ucrainene din țară.

Armata rusă a blocat în mod obișnuit receptoarele GPS în estul Ucrainei, de la conflictul din Crimeea din 2014, și adesea falsifică GPS-ul pur și simplu pentru a disimula mișcările președintelui Vladimir Putin în jurul Moscovei, potrivit unui raport din 2019 al Centrului nonprofit pentru Studii Avansate de Apărare. Bruiajul localizat al receptoarelor GPS terestre – în loc de bruiaj sau atacuri cibernetice asupra celor 30 de sateliți GPS operați în prezent de Forța Spațială – a devenit aproape obișnuit de la războiul din Kosovo, din 1998, în multe dintre zonele de conflict actuale, cum ar fi Siria, după cum spun experții.

Rusia poate construi și lansa sateliți pe cont propriu, iar complexul militar-industrial rusesc este imun la diverse sancțiuni din partea majorității statelor. Se pare că dezactivarea GLONASS este practic imposibilă, iar acest lucru conduce la imposibilitatea sancțiunilor împotriva constelației de sateliți ai Rusiei.

MODALITĂŢI DE CONTRACARARE – VIABILE SAU INUTILE?

Să ne imaginăm o situație în care sistemului de navigaţie cu sateliţi GLONASS i se impun sancțiuni și i se solicită să fie oprit sistemul. Având în vedere că acesta este un sistem rusesc, există o singură modalitate de a-l opri fizic, și anume de a distruge sateliții dispuși pe orbită. În prezent, nimeni nu deține astfel de arme, prin urmare este o opţiune inactivă. De asemenea, este imposibil să forţezi un stat să-şi abandoneze propriul sistem. Oricum, Rusia poate construi şi lansa sateliţi pe cont propriu, iar complexul militar-industrial rusesc este imun la diverse sancțiuni din partea majorității statelor. Se pare că dezactivarea GLONASS este practic imposibilă, iar acest lucru conduce la imposibilitatea sancțiunilor împotriva constelației de sateliți ai Rusiei.

Continuând scenariul, GLONASS nu va mai exista, dar este posibil ca noua configuraţie satelitară, formată din sateliții celorlalte sisteme, să nu schimbe nimic: un exemplu la îndemână sunt smartphone-urile, care, indiferent de naționalitatea proprietarului, de țara/zona/spațiul în care sunt active, vor avea suport pentru alte sisteme satelitare, vor funcționa și vor afișa coordonatele. Companiile private producătoare de chipset-uri ar putea fi forţate pentru a elimina suportul pentru GLONASS, dar, chiar dacă se întâmplă acest lucru, este imposibil să aibă loc instantaneu. Dezvoltarea de noi cipuri nu este un proces rapid, astfel încât ar putea dura câţiva ani până la dispariția

fizică a sistemului GLONASS în chipset-uri. Dezactivarea GPS-ului pe teritoriul Rusiei este dificilă și, cu siguranță, nu este necesară pentru nimeni, fiind puțin probabil ca SUA să o facă. În plus, există sistemul chinez, care nu poate fi influenţat.

Cel mai important indiciu că nu dezactivarea constelaţiei satelitare ruseşti este scopul care trebuie urmărit este faptul că Doctrina militară rusă presupune că GLONASS și alte GNSS nu vor fi disponibile odată ce începe o bătălie, așa că se va apela, în schimb, la Loran-C2 pentru navigare! (Cozzens, 2022). Cu alte cuvinte, forțele ruse, fiind experte în bruiaj și falsificare a semnalelor GNSS, consideră că semnalele din spațiu, inclusiv propriul GLONASS și alte GNSS, nu vor fi disponibile sau vor fi alterate odată ce începe o bătălie. Conform Planului de radionavigație pentru Rusia și Comunitatea Statelor Independente (CSI), sistemul terestru Chayka, o versiune a Loran-C, este menținut pentru a-și proteja teritoriul cu servicii de navigație și cronometrare atunci când semnalele din spațiu nu sunt disponibile. Există şi Sistemul portabil Skorpion, care este conceput pentru utilizare militară în timpul expedițiilor în zonele în care Chayka sau Loran nu sunt disponibile: *„Trei dintre stațiile Chayka/Loran din Rusia au înconjurat Ucraina”,* a explicat CEO-ul UrsaNav, Charles Schue, referindu-se la o grafică pe care a furnizat-o GPS World: *„Oferă o acoperire ideală și vor permite o precizie de navigare între 20 și 50 de metri pe cea mai mare parte a Ucrainei. Trecerea la un eLoran le-ar putea oferi o precizie de 5 până la 10 metri, dar sunt sigur că actuala configurație este mai mult decât adecvată pentru scopurile lor în acest moment”.* (Hovgaard, 2002).

Unul dintre cele trei locuri de transmisie a Loran se află în Crimeea, teritoriu anexat de Rusia în 2014. *„Motivul principal pentru care a fost alipită Crimeea poate să fi fost asigurarea accesului la ocean”*, a mai spus Schue, *„dar le-a permis și să recâștige controlul asupra locului de transmisie Loran de acolo. Acest lucru le-a asigurat PNT terestru suveran (poziționare, navigare și sincronizare) pentru întreaga regiune, inclusiv Marea Neagră”* (Cozzens, ib.).

Conform Planului de radionavigație pentru Rusia și Comunitatea Statelor Independente (CSI), sistemul terestru Chayka, o versiune a Loran-C, este menținut pentru a-și proteja teritoriul cu servicii de navigație și cronometrare atunci când semnalele din spațiu nu sunt disponibile. Există și Sistemul portabil Skorpion, care este conceput pentru utilizare militară în timpul expedițiilor în zonele în care Chayka sau Loran nu sunt disponibile.

[2] *Long RAnge Navigation/LORAN* este un sistem de navigație hiperbolic dezvoltat pentru prima dată în timpul celui de-Al Doilea Război Mondial, în SUA, care îi oferea unui receptor posibilitatea de a-și determina poziția ascultând semnale radio de joasă frecvență transmise de radiofaruri terestre fixe. Loran-C a combinat două tehnici diferite pentru a furniza un semnal care avea rază lungă de acțiune și era foarte precis, caracteristici care erau incompatibile. Dezavantajul său a fost costul echipamentului necesar pentru interpretarea semnalelor. A fost depășit de GPS. (https://lwvworc.org/ro/which-is-the-counterpart-system-of-loran, accesat la 22 august 2022).

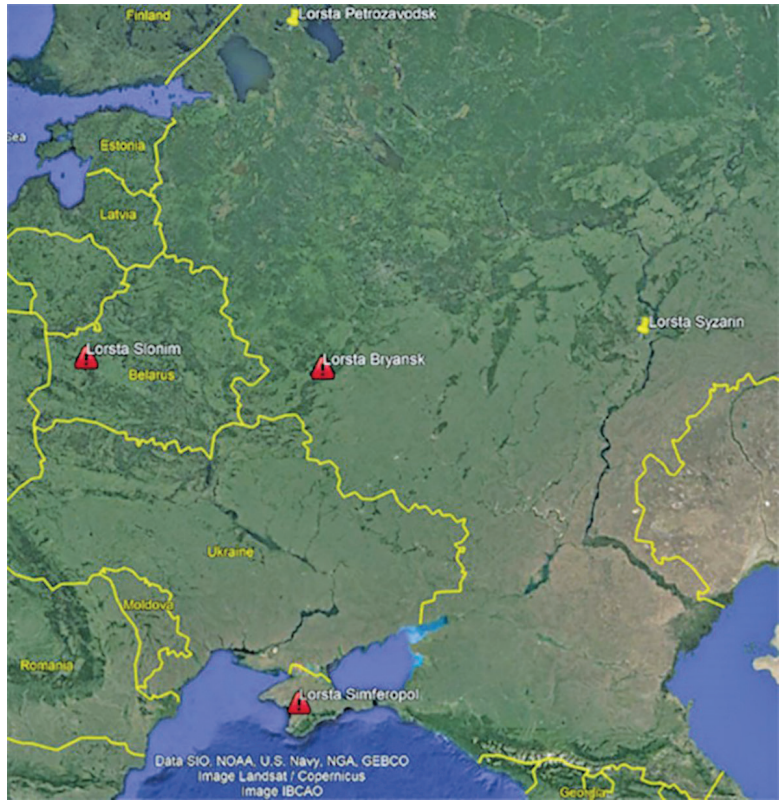

Figura nr. 1: Potrivit GPS World, Rusia are trei staţii Loran în jurul Ucrainei. Cele trei staţii ar trebui, teoretic, să poată acoperi toată Ucraina.
Foto: Charles Schue, UrsaNav (preluare de pe site-ul https://www.gpsworld.com/russia-expected-to-ditch-glonass-for-loran-in-ukraine-invasion/, Hovgaard, ib.).

Un atac asupra GPS-ului ar fi un atac asupra SUA şi riscul evident este să atragă NATO în conflict. Dar, este foarte puţin probabil să se recurgă la un pas atât de dramatic doar pentru a împiedica atacurile ucrainene, acţiunea practicată rămânând la nivelul alterării semnalelor satelitare la receptori.

Există posibilitatea, cel puţin din punct de vedere teoretic, ca Rusia să fie capabilă să facă inutili sateliţii GPS, folosind un atac cibernetic. Aşa cum am mai spus, suprimarea fizică este puţin probabilă, chiar dacă sunt declaraţii beligerante în acest sens, orbitele pe care activează sistemele de navigaţie cu sateliţi aflându-se la o altitudine de circa 20.000 de kilometri faţă de Pământ. Chiar dacă ar exista o astfel de lovitură, nu se poate suprima întreaga constelaţie satelitară, există sateliţi de rezervă, pot fi lansaţi alţii şi trebuie ţinut cont şi de celelalte sisteme de navigaţie existente. Altfel, un atac asupra GPS-ului ar fi un atac asupra SUA şi riscul evident este să atragă NATO în conflict. Dar, este foarte puţin probabil să se recurgă la un pas atât de dramatic doar pentru a împiedica atacurile ucrainene, acţiunea practicată rămânând la nivelul alterării semnalelor satelitare la receptori.

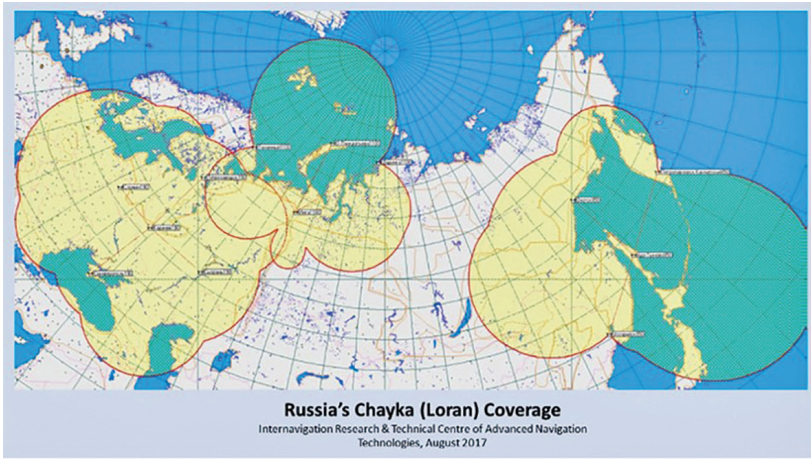

Figura nr. 2: Hartă de acoperire (2017) de la Centrul de Cercetare Internavigație și Centrul Tehnic de Navigație Avansată din Rusia, care arată că sistemul Chayka deservește Europa de Est, vestul Rusiei și aproape toată Marea Neagră (Cozzens, ib.)

În luna iunie a acestui an, Forțele Aeriene ale SUA și-au efectuat testul final al unui sistem de țintire asistat de radar pentru bombardier B-2A, care permite ghidarea cu precizie a armelor într-un mediu degradat de GPS.

Și totuși, Rusia a făcut o demonstraţie de forţă distrugând un satelit propriu pe orbită! Aşa era menționat într-o ştire din 2016, de altfel reală: *„Rusia a efectuat în mod nechibzuit un test devastator de arme antisatelit împotriva unuia dintre sateliții săi”*, a declarat Ned Price, reprezentant al departamentului diplomatic american (Amos, 2021). Nu doresc să dezvolt subiectul din perspectivă politică, prin care au fost relevate consecinţele grave asupra mediului orbital prin deşeurile produse, ci să exprim ceea ce se înţelege în unanimitate: dezvoltarea armelor anti-satelit generează şi teste, ca o demonstrație de putere. De aceea trebuie reamintit că, pe această tablă de şah, China a fost cea care a mutat prima, în 2007, urmată de SUA, în 2008, şi de India, în 2019, fiecare doborându-şi sateliţii dezafectaţi. În 2020, Londra și Washingtonul au acuzat Moscova că a testat un satelit – *„păpușă Matrioșca”*, aceasta deschizându-se și eliberând o navă de dimensiuni mai mici, pentru a urmări un satelit american; deci, cât mai rămăsese până la testul Rusiei? Însă, toate demonstraţiile prezentate au avut loc pe orbite la aproximativ 500 de kilometri de Pământ, iar GNSS se află la atitudini de 40 de ori mai mari!

Pentru a contracara o astfel de amenințare, şi SUA au dezvoltat alternative la navigația prin satelit, chiar dacă au renunţat la LORAN. Astfel, în luna iunie a acestui an, Forțele Aeriene ale SUA și-au efectuat testul final al unui sistem de țintire asistat de radar pentru bombardier B-2A, care permite ghidarea cu precizie a armelor într-un

mediu degradat de GPS. Bombardierul echipat cu Radar Aided Targeting System (RATS) a aruncat o bombă nucleară B61-12 în timpul testului final de la Tonopah Test Range, Nevada. Testul a fost prima versiune de unitate de producție a ansamblului de testare comun (JTA) B61-12, a cărui producție la scară largă a început în mai a.c.: *„Am efectuat mai multe ieșiri testând noua capacitate RATS în ultimele nouă luni și am colectat puncte de testare privind performanța acesteia”*, a spus comandantul de zbor al armelor B-2 al Escadrilei de Testare și Evaluare (TES) 72d, căpitanul David Durham. TES a testat, de asemenea, un instrument software proiectat intern, care oferă indicații timpurii despre funcționalitatea RATS, verificând dacă sistemul funcționează corect înainte de lansarea armei (Bisht, 2022).

„Asigurați-vă că sistemele dumneavoastră sunt securizate și că le urmăriți îndeaproape, deoarece știm că rușii sunt actori cibernetici eficienți”.

CONCLUZII

Starea de conflict generează provocări reale care demontează sau confirmă scenarii pregătite în timp de pace, dar istoria ne arată că, de cele mai multe ori, nici agresorul, nici agresatul nu au avut în mod oportun datele necesare pentru obţinerea rezultatelor scontate. Succesul a fost obţinut aproape mereu de cel care a ştiut să se adapteze, să folosească cu discernământ informaţiile aflate la dispoziţie, să exploateze intensiv şi să securizeze ceea ce posedă.

„Este greu de spus cât de departe va ajunge pentru a-și atinge obiectivele, dar este mai bine să fii pregătit decât surprins”.

În zilele dinaintea invadării Rusiei, oficialii americani din domeniul spaţial au avertizat companiile prin satelit că acest conflict s-ar putea extinde în spațiu: *„Asigurați-vă că sistemele dumneavoastră sunt securizate și că le urmăriți îndeaproape, deoarece știm că rușii sunt actori cibernetici eficienți”*, a spus directorul Oficiului Național de Recunoaștere, Chris Scolese, la o conferință a Asociației Naționale de Securitate Spațială din 23 februarie a.c.: *„Este greu de spus cât de departe va ajunge pentru a-și atinge obiectivele, dar este mai bine să fii pregătit decât surprins”.* (Erwin, 2022).

Sistemele de navigaţie cu sateliţi îşi vor continua nestingherite misiunile, deoarece nu există arme atât de sofisticate, capabile să le atace, dar nici nu există intenţia vreunui stat de sistare a acestora. Deziderатul sinergic este de cooperare GNSS în beneficiul umanităţii prin creşterea calităţii vieţii pe Pământ, având în vedere că soluţiile satelitare devin mult mai precise şi rapide atunci când semnalele sunt receptate de la mai mulţi sateliţi; dacă, pentru acoperirea globală, este necesară o constelaţie de minim 24 de sateliţi, trebuie să ne închipuim

cum ar fi rata de actualizare a informaţiilor dacă am primi semnale de la *„constelaţiile satelitare unite”*, ceea ce ar însemna, la acest moment, în jur de 75 de sateliţi.

BIBLIOGRAFIE:

1. Amos, J. (2021). *Russian anti-satellite missile test draws condemnation*, https://www.bbc.com/news/science-environment-59299101, accesat la 21 august 2022.
2. Bisht, I.S. (13 iulie 2022). *USAF Tests B-2 Bomber System for GPS-Denied Environments*. The Defence Post.
3. Cozzens, T. (2022). *Russia expected to ditch GLONASS for Loran in Ukraine invasion*, https://www.gpsworld.com/russia-expected-to-ditch-glonass-for-loran-in-ukraine-invasion/, accesat la 17 august 2022.
4. Culliford, E. (2002). *Google temporarily disables Google Maps live traffic data in Ukraine*, https://www.reuters.com/technology/google-temporarily-disables-google-maps-live-traffic-data-ukraine-2022-02-28, accesat la 12 iunie 2022.
5. Erwin, S. (2022). *NRO warns satellite operators of possible Russian attacks*, https://spacenews.com/nro-chief-warns-satellite-operators-to-secure-their-systems-as-ukraine-crisis-unfolds, accesat la 12 iunie 2022.
6. Hitchens, T. (2022). *Local Russian GPS jamming in Ukraine hasn't affected US support ops, so far*. Breaking Defense.
7. Hovgaard, L. (2002). *Russia does not trust satellite navigation: Revives old land-based radios*, https://ing.dk/artikel/russia-does-not-trust-satellite-navigation-revives-old-land-based-radios-254607, accesat la 22 iulie 2022.
8. Johnson, K. (2022). *Airlines Report Russian GPS Jamming in Four Regions*, https://www.flyingmag.com/airlines-report-russian-gps-jamming-in-four-regions, accesat la 22 iulie 2022.
9. Katz, B. (2022). *Someone Appears to Be Messing With GPS Near Russia, Europe's Air Safety Agency Warns*. În *The Wall Street Journal*, https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-17/card/someone-appears-to-be-messing-with-gps-near-russia-europe-s-air-safety-agency-warns-KVcaNmYR7uzWOiuiyPLu, accesat la 22 iulie 2022.
10. Matei, A. (2022). *Posibile interferențe* în *transportul aerian*, https://traficmedia.ro/posibile-interferente-in-transportul-aerian/, accesat la 12 iunie 2022.
11. Rogoway, T. (2017). *Russia may be testing its GPS spoofing capabilities around the Black Sea*, https://www.thedrive.com/the-war-zone/13549/russia-may-be-testing-its-gps-spoofing-capabilities-around-the-black-sea, accesat la 21 iulie 2022.
12. Inside GNSS (2007), *Why War, Precisely?*, https://insidegnss.com/why-war-precisely/, accesat la 22 iulie 2022.
13. https://lwvworc.org/ro/which-is-the-counterpart-system-of-loran, accesat la 22 august 2022.