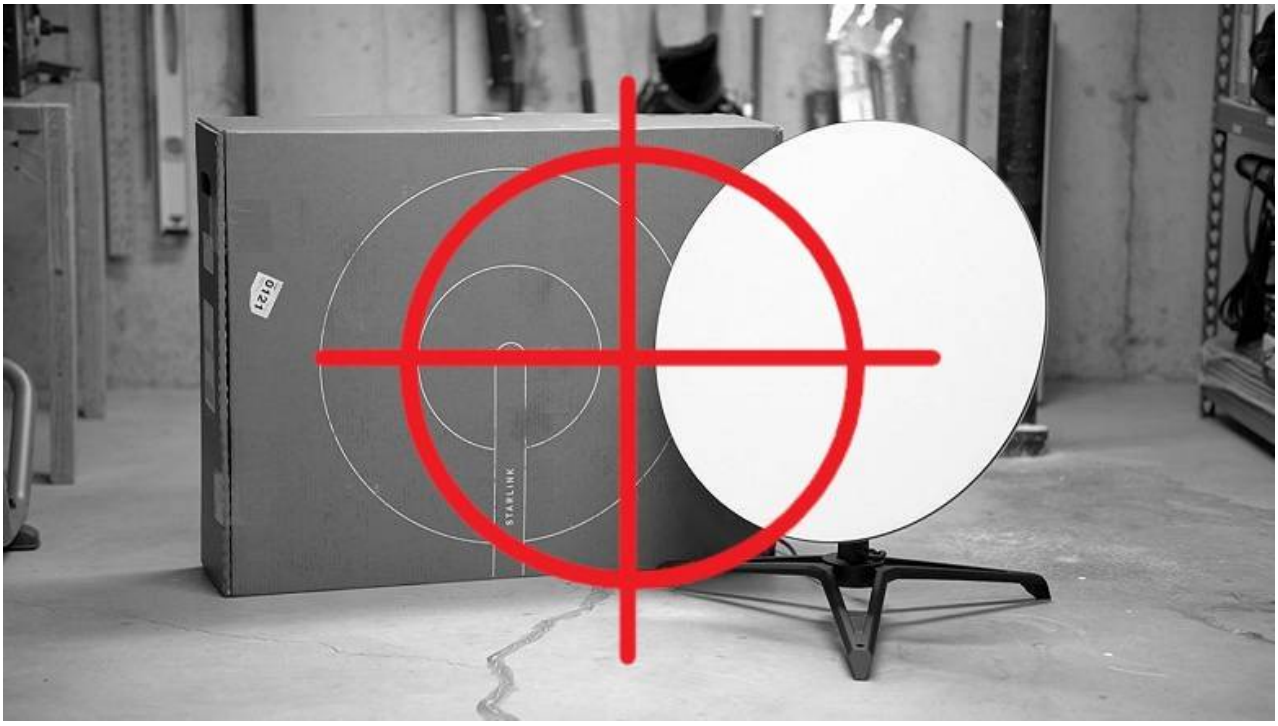
Hon na terminály Starlink a jejich provozovatele je prohlášen za otevřený

topwar.ru/207671-ohota-na-terminaly-starlink-i-ih-operatorov-objavljaetsja-otkrytoj.html

Andrej Mitrofanov 30. prosince 2022



Je docela těžké přeceňovat vliv komunikací na bojišti. Jde o stabilní spojení, které dokáže proměnit porážku ve vítězství a její absence naopak vítězství v porážku. Nejdůležitějším komunikačním faktorem je zajištění důvěrnosti kanálů přenosu dat a jejich odolnosti vůči přirozenému i umělému rušení.

V době zahájení ruské speciální vojenské operace (SVO) nepřesahovaly komunikační prostředky v ozbrojených silách Ukrajiny (AFU) a jejich schopnosti ty, které měly ozbrojené síly Ruské federace (RF ozbrojené síly). . Poté však západní země začaly pumpovat Ukrajinu nejmodernější vojenskou technikou včetně komunikačních systémů a také poskytovaly komplexní informační podporu vojenské a civilní infrastruktuře zemí NATO.

Pokud z rovnice vyjmeme vojenské a civilní zpravodajské satelity, pak nejvýznamnějším příspěvkem k boji proti SVO byl převod desítek tisíc vysokorychlostních satelitních komunikačních terminálů Starlink s placenými komunikačními službami. Ano, lze s vysokou mírou jistoty tvrdit, že právě toto vybavení vytváří nejvýraznější problémy ozbrojeným silám RF, a už vůbec ne raketám, dělostřelectvu a systémům protivzdušné obrany.

Jde o to, že komunikační prostředky proměňují nesourodé jednotky v jedinou strukturu, která skutečně funguje „s jediným cílem, podle jediného plánu“. Komunikační prostředky výrazně zvyšují rychlost reakce na akce nepřítele, umožňují vám se vzdalovat, udeřit společně, vyhýbat se nepřátelským úderům a koordinovat akce k zásahu na nepřítele.

Jinými slovy, komunikace jsou katalyzátorem, který výrazně zvyšuje efektivitu jakýchkoli ozbrojených sil.

Na základě toho lze tvrdit, že ničení nepřátelských komunikačních sítí je strategickým úkolem ozbrojených sil RF.

Ale než budeme mluvit o Starlinku, podívejme se, jak jinak lze zajistit komunikaci v ozbrojených silách Ukrajiny?

Hra "prozradí"

A mohou komunikovat pomocí konvenčních prostředků mobilní komunikace. Ano přesně. Buněčná komunikační infrastruktura na Ukrajině je ruskými údery prakticky nedotčena. Pokud někdo mluví o „odposlechu“ takových sítí, pak bude muset být zklamán – přepínače jsou v rukou ukrajinských úřadů a VPN nikdo nezrušil.

V článku Rozklad Ukrajiny jako cesta k radikálnímu snížení schopností Ozbrojených sil Ukrajiny vzdorovat ruské speciální operaci jsme hovořili o třech pilířích, které nás mohou výrazně přiblížit k vítězství:

1. Regionální izolace – zničení mostů , především železnice, ale i další prvky dopravní infrastruktury.

2. Energetická blokáda – zničení energetických sítí Ukrajiny.

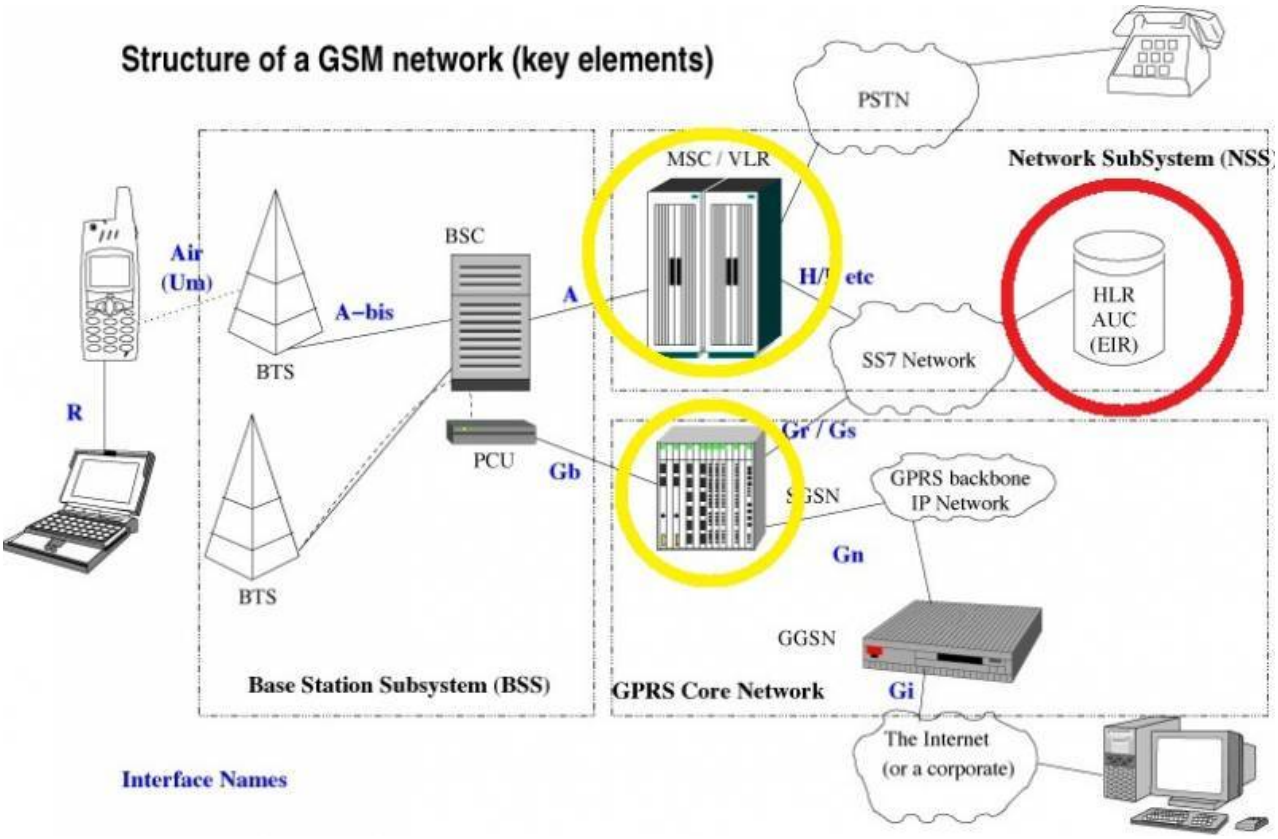
3. Potlačení informací – zničení zařízení televizního a rozhlasového vysílání a deaktivace mobilních sítí na celé Ukrajině.

Tento materiál byl zveřejněn v polovině dubna 2022 a co se od té doby změnilo?

Na dopravní infrastrukturu se prakticky nestávkuje, i když všechna neoficiální tematická média o tom nemluví – křičí o tom. Obecně je zde vše jasné - velcí strýcové vydělávají velké peníze, jak se říká: postavit se do cesty projektu, který přináší značný zisk, je stejné jako postavit se do cesty jedoucímu vlaku?

Energetická blokáda? Něco se v tomto směru dělá, ale jaksi pomalu. Jako drobné vedlejší účinky dochází k mírnému poklesu účinnosti celulární komunikace a internetových sítí a také k narušení pohybu elektrických vozidel. Efekt je však stále nepatrný - nepřítel buď rychle obnoví komunikační sítě, nebo vymění elektrické lokomotivy za dieselové lokomotivy (a dokonce i parní lokomotivy) - v extrémních případech civilisté nepojedou a granáty nepochybně dorazí včas. Tady přes rozhozený most neprojedou, ale o tom už jsme mluvili výše.

Co se týče celulárních sítí, nedochází k žádnému pokroku, i když je docela možné vyřadit databáze (HLR) a mobilní přepínací centra (MSC) celulárních operátorů pomocí Geranium.



Databáze (HLR) a mobilní přepínací centra (MSC) jsou nejzranitelnější a obtížně obnovitelné prvky celulárních sítí.

Proč to dělat, když ozbrojené síly Ukrajiny stále mají Starlink a civilní obyvatelstvo bude trpět?

Komunikace pro civilní obyvatelstvo rozhodně není důležitější než voda, proviant a teplo v domech, stejně jako celistvost domů samotných, takže o komunikaci mezi civilním obyvatelstvem - to není téma. Ale pro vládní agentury, ekonomiku, vojenské registrační a vojenské úřady a další vládní a komerční struktury je komunikace nesmírně důležitá.

Pokud jde o APU, zničení celulárních sítí výrazně zvýší zatížení sítě Starlink, intenzitu provozu terminálů a satelitů, což znamená, že se zhorší propustnost kanálů přenosu dat, zvýší se zpoždění a počet poruch terminálů. . Zvýší se i náklady Spojených států, SpaceX a Ukrajiny (pokud je ta vůbec ponese), což je důležité.

Bez ohledu na to, kolik terminálů Starlink Spojené státy dodají ozbrojeným silám Ukrajiny, stále jich nebude dostatek pro všechny, což znamená, že efektivita velení a řízení jednotek se nevyhnutelně sníží - vysílačky / radiostanice ne zcela kompenzují nedostatek celulární komunikace.

Mimochodem, odstavení celulárních sítí na Ukrajině ruskému velkopodnikateli nijak neublíží.

A nyní, když se Starlink stane hlavním, prakticky jediným způsobem pro ozbrojené síly Ukrajiny k rychlé výměně digitálních informací, přijde čas začít lovit terminály Starlink a jejich operátory.

Komplex "Borshchevik"

Terminály Starlink jsou aktivním rádiem emitujícím objektem, což znamená, že je lze detekovat a sledovat, jejich polohu lze určit s různou přesností.

V prosinci tohoto roku se v médiích objevila informace, že v Rusku se dokončují testy komplexu Borshchevik, určeného pro nasměrování satelitních internetových terminálů Starlink.

Podle vývojářů komplexu Borshchevik je schopen zjistit polohu terminálu Starlink do patnácti minut na vzdálenost asi deseti kilometrů v sektoru 180 stupňů, přičemž chyba v určení souřadnic nepřesáhne šedesát metrů.

Je pravda, že na internetu jsou také prohlášení, že Borshchevik je schopen detekovat pouze signál Wi-Fi, prostřednictvím kterého terminál Starlink distribuuje internet předplatitelům. Pokud ano, pak potenciální hodnota Borshchevik výrazně klesá.

Pokud Borshchevik detekuje postranní laloky radiačního diagramu kanálu terminál-satelit, pak se operátoři Starlink již mohou stát potenciálními cíli pro ozbrojené síly RF, alespoň podél linie

kontaktu.

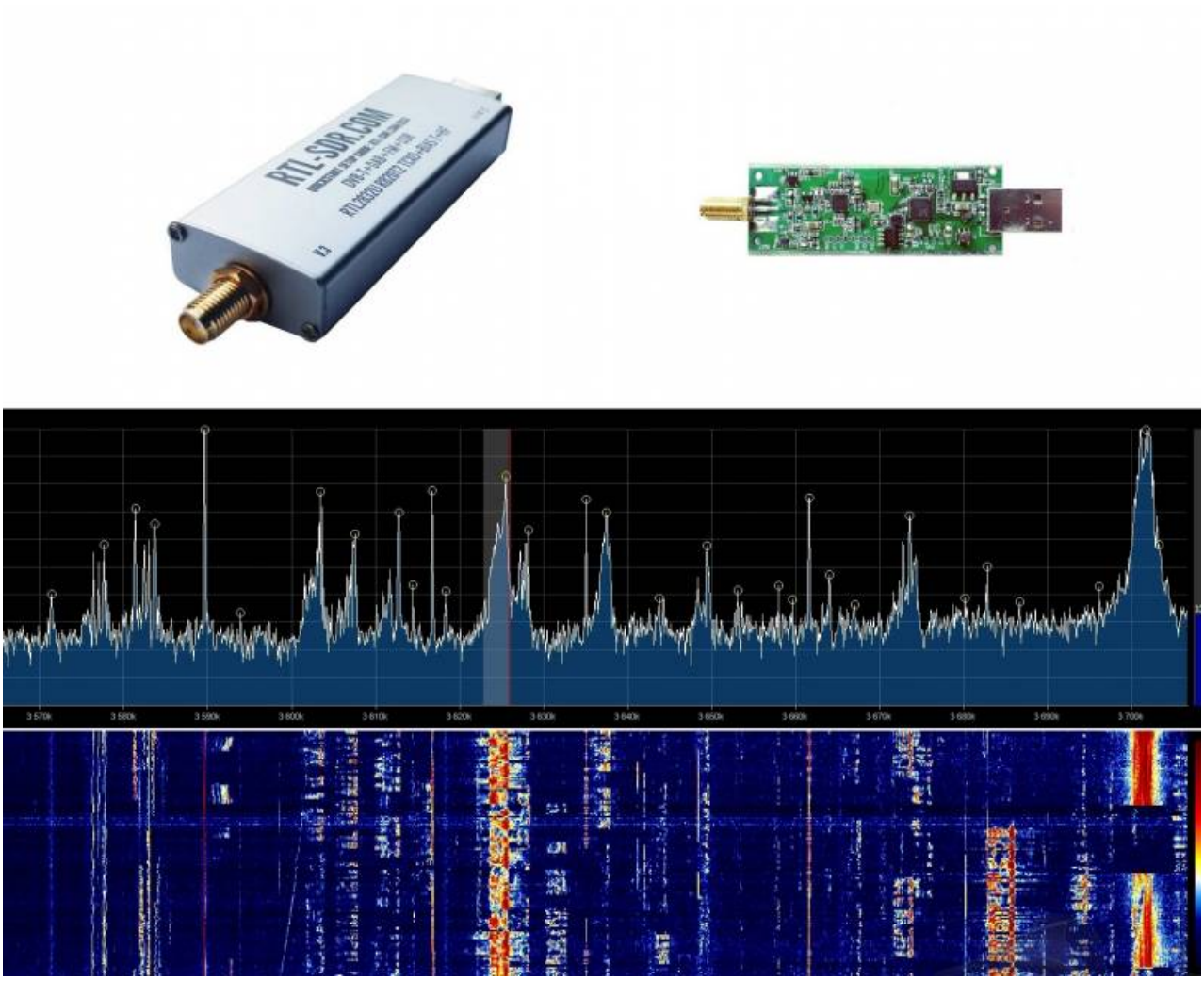
Jaké další alternativy máme?

Protiterminální munice

Teoreticky by signál vysílaný terminálem měl nést informaci o přesné poloze terminálu, aby satelit "věděl", kde vytvořit a udržovat obrazec paprsku kanálu přenosu dat. Vzhledem k tomu, že během komunikační relace je signál terminálu postupně zachycován satelity, které nad ním létají, musí být informace o poloze terminálu přenášeny neustále.

Ideálním řešením by bylo vytvoření levného zařízení, které detekuje signál terminálů Starlink a zajišťuje navádění nosiče (munice) na nich, podobně jako to dělají samonaváděcí hlavice (GOS) antiradarových střel (PRR).

Existují takové zajímavé produkty, jako jsou přijímače RTL-SDR a spektrální analyzátory, které dokážou skenovat vzduch a detekovat elektromagnetické záření v širokém frekvenčním rozsahu. Na jejich základě již existují projekty detekce bezpilotních letounů (UAV), které jsou realizovány i na amatérské úrovni.



Přijímač RTL-SDR a „vodopád“ jím přijímaných signálů

Na jejich základě by bylo potenciálně možné vytvořit nástroje pro detekci terminálů Starlink, nicméně přijímače známé autorovi RTL-SDR pracují v rozsahu s horní hranicí šesti gigahertzů a relativně kompaktní a levné spektrální analyzátory pracují v rozsahu s horní hranicí dvanáct gigahertzů. Současně terminál a satelity Starlink „komunikují“ v pásmech Ku a Ka - terminál přenáší informace v pásmu 12 až 24 GHz a satelit od 27 do 40 GHz (údaje o frekvenčních rozsazích terminály a satelity se mohou lišit, navíc se mohou lišit frekvence různé modifikace terminálů a satelitů).

Spektrální analyzátor

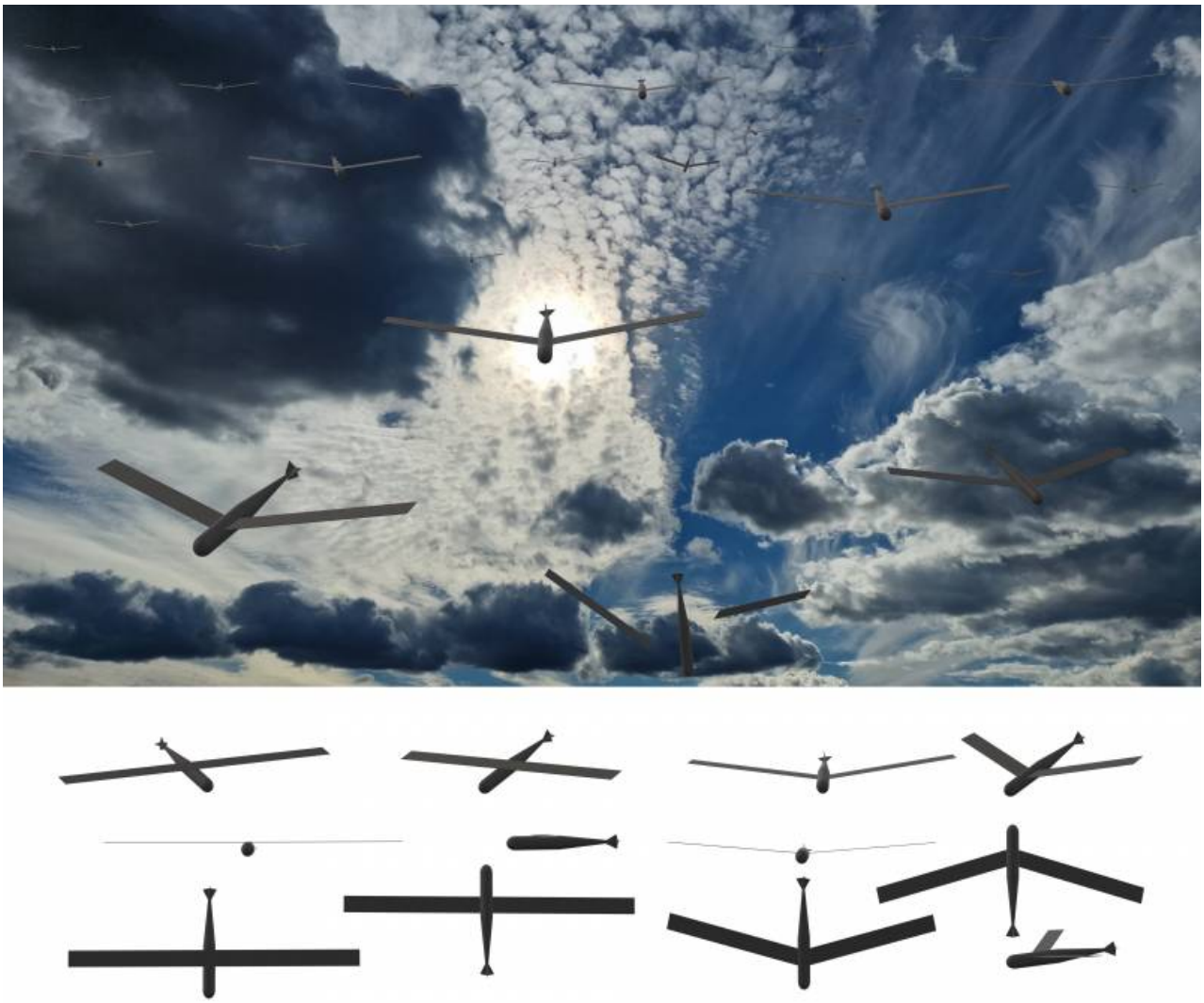
Možnosti zde však jsou. Stávající přijímače RTL-SDR jsou založeny na čipech pro digitální televizory. V současné době se aktivně rozvíjejí řady satelitních přijímačů, satelitních komunikačních terminálů, mobilních telefonů s funkcí satelitní komunikace. Široké používání družicových komunikačních technologií v civilním průmyslu vede a možná již vedlo ke vzniku elektronických součástek schopných pracovat v požadovaném frekvenčním rozsahu 12-40 GHz.

Je možné, že na elektronických součástkách, které jsou součástí těchto satelitních přijímačů, satelitních komunikačních terminálech, mobilních telefonech s funkcí satelitní komunikace nebo jejich funkčních analogech zkopírovaných v hlubinách čínského průmyslu, mohou být vytvořeny slibné prostředky pro detekci a zničení satelitních komunikačních terminálů Starlink. .

Potenciálně, na základě levných civilních elektronických součástek, mohou být vytvořeny naváděcí hlavice určené k zacílení ničení terminálů Starlink.

Kromě RTL-SDR přijímačů s rozšířeným frekvenčním rozsahem mohou obsahovat počítač malých rozměrů, například založený na jednodeskovém řešení, jako je Raspberry Pi.

Cena takových řešení může být dostatečně nízká na to, aby mohla být nasazena na stejných bezpilotních letounech typu Geranium nebo na těch, o nichž pojednává článek Project Condor: smrt z nebes plánování kamikadze bezpilotních letounů implementovaných na základě civilních technologií a určených pro výrobu v množství desítek na stovky tisíc jednotek ročně.



Koncept projektu UAV "Condor"

Algoritmus pro provoz munice vybavené antiterminálním vyhledávačem může být následující.

Zpočátku jejich GOS, který funguje na principu navádění podle souřadnic globálního satelitního navigačního systému (GLONASS), zadá souřadnice konečného cíle - elektrické rozvodny, mobilního přepínače, mostu nebo Zelenského rezidence .

Během letu hledač protiterminálu skenuje vzduch, a pokud je detekován signál z terminálu Starlink, munice změní priority a udeří na něj. Vzhledem k tomu, že údery na cíle musí být prováděny s

rezervou, to znamená, že na ně musí být vynaloženo několik Geranií nebo Condorů, lze ztrátu jednoho nebo dvou výměnou za zničení terminálů Starlink a jejich operátorů považovat za přijatelné řešení.

Takovými produkty budou ve skutečnosti antiterminální munice, jejíž logika bude zahrnovat prioritní zničení terminálů emitujících Starlink a v případě nepřítomnosti jejich signálu na trase bude munice pravidelně porážet stacionární cíl, jehož souřadnice byly původně uloženy v jeho paměti.

Existuje možnost, že nebude možné prodávat levnou antiterminální munici. V tomto případě může být řešením v „opakovaně použitelných“ nástrojích elektronické inteligence (RTR) navržených speciálně pro detekci terminálů Starlink a umístěných na maximálním možném počtu nosičů.

lov na lišku

V SSSR, zejména v radioamatérských kruzích, byla poměrně známá hra „hon na lišku“, při které bylo třeba pomocí rádiového přijímače se směrovou anténou najít někde na zemi ukrytý rádiový vysílač. Vzhledem k důležitosti odhalování a ničení terminálů Starlink by všechny složky ozbrojených sil RF měly tak či onak hrát „hon na lišku“.

To vyžaduje vytvoření protiterminálních prostředků RTR, které lze umístit na taktická letadla a vrtulníky , bezpilotní prostředky, pozemní vozidla a případně jako součást individuální výbavy jednotlivých stíhaček.

Pokud není možné implementovat levná řešení založená na přijímačích RTL-SDR založených na čipech satelitních přijímačů, satelitních komunikačních terminálů, mobilních telefonů s funkcí

satelitní komunikace nebo jiného civilního vybavení, pak přichází na pomoc profesionální vybavení. Zde je to, co bylo nalezeno na internetu:

Původní přenosné automatizované zařízení pro rádiové a rádiové řízení „Bars“ vytvořil 5. ústřední výzkumný ústav Ministerstva obrany Ruské federace a VNIIS. Poskytuje: **přehled v pásmu 30 MHz–30 GHz** , vyhledání směru zdrojů rádiového vyzařování s přesností 2–8 stupňů, měření charakteristik rádiového signálu (frekvence a výkon signálu, doba trvání pulzu a perioda opakování, intenzita pole), identifikaci typu radiového vyzařování s pravděpodobností alespoň 0,9 vytvoření databáze s alespoň 100 standardy. Zařízení Bars se skládá z anténního napáječe, výměnných vysokofrekvenčních jednotek, jednotek pro rychlou časově-frekvenční a přesnou analýzu, zpracování dat, řízení a monitorování a také napájecí zdroj. Princip budování hardwaru a softwaru umožňuje přizpůsobit zařízení konkrétním podmínkám.

Uvedené zařízení je zjevně určeno k detekci rádiových záložek, jinými slovy, tzv. "hmyz". Je možné, že nástroje detekce terminálu Starlink mohou být vytvořeny na jeho základě nebo na základě jiného zařízení podobného účelu. Tak či onak by mělo být docela možné detekovat signál terminálů Starlink. Anti-terminální prostředky RTR budou zvláště účinné, pokud je možné izolovat informace o umístění zemních svorek Starlink od struktury signálu, jak jsme již diskutovali výše.

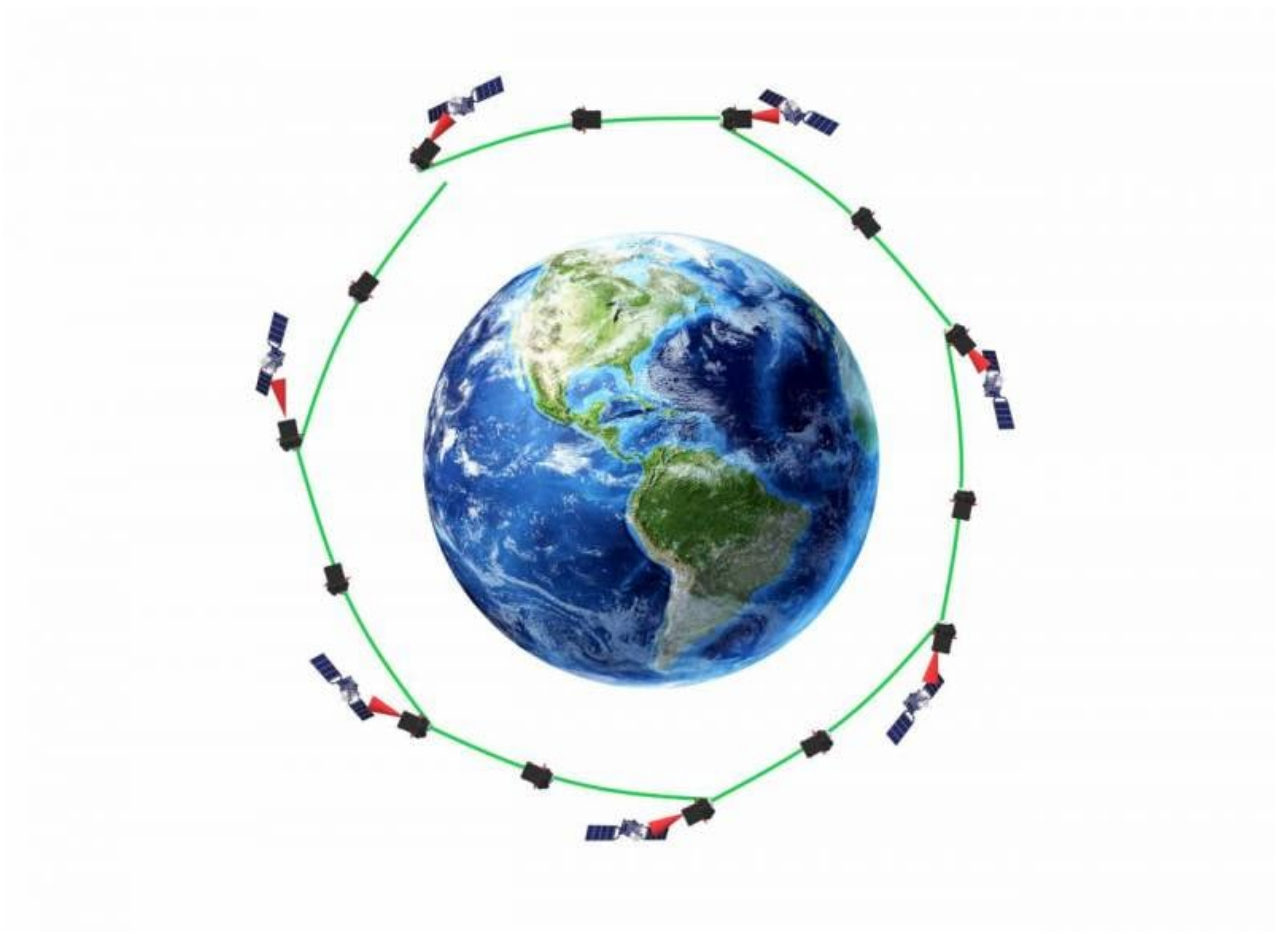
Pro letectví mohou být protiterminální prostředky RTR umístěny ve specializovaných kontejnerech, které musí být instalovány na všech letounech operujících v prostoru protivzdušné obrany. Zničení terminálů Starlink by pro ně mělo být nejvyšší prioritou. Su-34 létá, detekoval signál terminálu Starlink - shodil na zamýšlené místo několik vysoce výbušných bomb FAB-500. Ka-52 letí, zachytil signál terminálu Starlink - potenciální zónu svého nasazení pokryl

neřízenými letadlovými střelami S-130 (NAR) nebo protitankovými řízenými střelami Whirlwind (ATGM). Totéž platí pro pozemní jednotky: detekce - úder, detekce - úder, detekce - úder ...

závěry

Je možné, že navrhované možnosti neumožní vytvoření účinných protiterminálních RTR zbraní nebo munice, ale jedná se pouze o „náčrty tužky“. Lze pouze jednoznačně konstatovat, že terminály Starlink lze detekovat a je nutné je zničit všemi dostupnými prostředky. Hlavním závěrem, který je třeba vyvodit, je potřeba aktivně studovat tuto možnost, a to za účasti veřejných i soukromých podniků, vojenského i civilního rozvoje. Je důležité nezavěsit se na jedno řešení, ale hledat různé způsoby, jak problém vyřešit.

Dříve v materiálu „Reaper“ vyčistí oběžnou dráhu: satelity Starlink můžete sestřelit rychleji, než je Elon Musk dokáže vypustitjiž jsme řekli, že v případě eskalace konfliktu existuje technická možnost hromadného ničení satelitů Starlink. V Project Anxiety: Disrupt Starlink Satellites Without Destroying them jsme se podívali na způsoby, jak této konstelaci družic uškodit, což lze samozřejmě využít už nyní, pokud alespoň začnou pracovat tímto směrem.



Koncept zničení satelitů Starlink v rámci projektu Reaper

Do doby, než budou vytvořeny výše uvedené systémy nebo jejich alternativy a dokud nebude rozhodnuto o fyzickém zničení nebo alespoň částečném znefunkčnění konstelace družic Starlink, je nutné zajistit co nejefektivnější detekci a zničení pozemních terminálů sítě Starlink zde na Zemi, před časem, kdy se zahrnutí pozemního terminálu Starlink nestane pro nepřítele synonymem slova „sebevražda“.