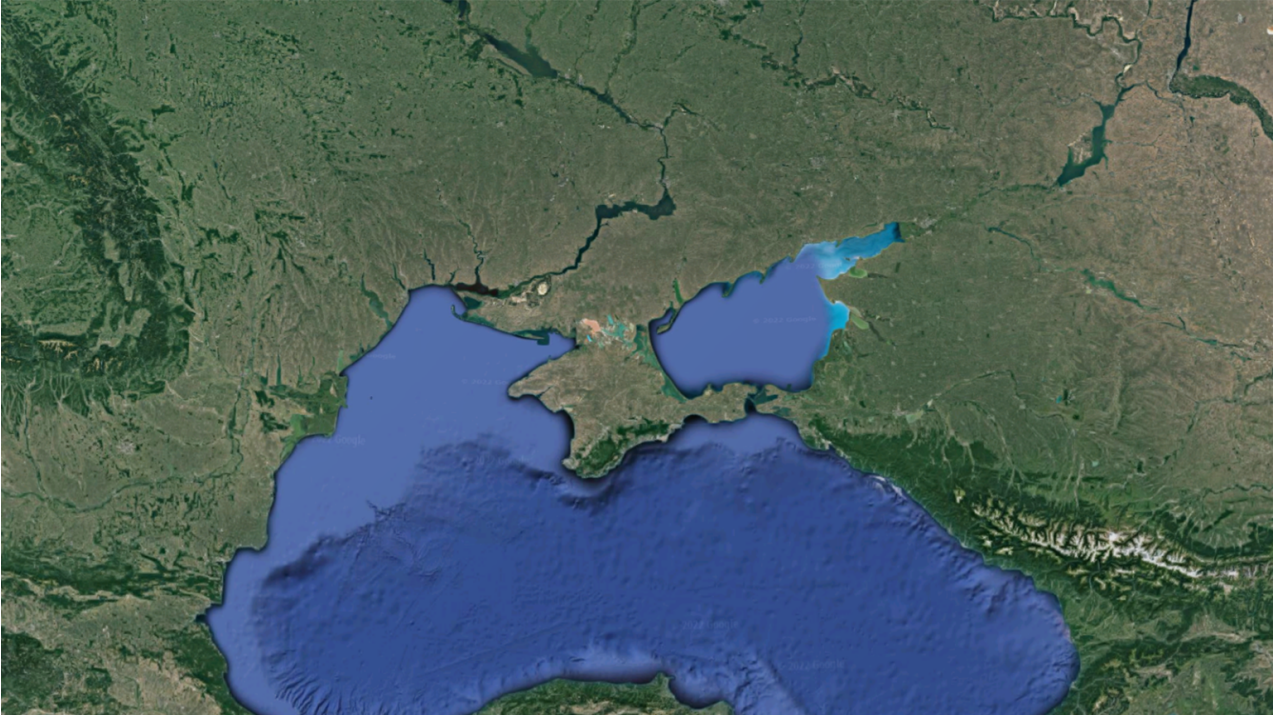


„Místní“ Ruské rušení GPS na Ukrajině zatím neovlivnilo americké podpůrné operace

breakingdefense.com/2022/03/local-russian-gps-jamming-in-ukraine-hasnt-affected-us-support-ops-so-far

1. března 2022



Satelitní pohled na Černé moře, jižní Ukrajinu a jižní Rusko. (Google maps)

WASHINGTON: Americké síly v regionu detekovaly lokalizované ruské rušení signálů GPS na Ukrajině, ale podle představitelů Pentagonu zatím nezasahovalo do amerických podpůrných operací.

Jeden vojenský zdroj řekl Breaking Defense, že rušení bylo zjištěno až v Černém moři americkými průzkumnými letadly, ale zdroj zdůraznil, že to nemělo žádný dopad na schopnost mise.

Podobně, když byl dotázán na ruské rušení, mluvčí amerického vesmírného velitelství řekl: "V tuto chvíli nemáme žádné dopady na americké a spojenecké síly v Evropě."

Vysoký představitel obrany dnes novinářům řekl, že USA podezřívají Rusko, že se zatím drží zpátky ve využívání své rozsáhlé sady nástrojů pro elektronickou válku.

"Neviděli jsme to, o čem jsme přesvědčeni, že [je] plný rozsah jejich schopností elektronického boje, které přinesly. Nedokážu posoudit, proč tomu tak je. Ale víme a máme náznaky, že na některých místech využili EW ve svůj prospěch, zejména při rušení, na místní úrovni," řekl vysoký úředník.

Není jasné, zda rušení mělo vliv na ukrajinské operace v zemi. To, že lokalizované rušení nebylo faktorem pro americké operace ve vzdálenějších oblastech, by nemělo být velkým překvapením, uvedli bývalí a současní úředníci ministerstva obrany s odbornými znalostmi v této problematice, vzhledem k výzvě pro protivníky rušit přijímače GPS používané v USA. vojenské síly – zejména vojenská letadla.

Kliknutím sem zobrazíte veškeré zpravodajství o situaci na Ukrajině Breaking Defense.

pozemní válka,
Sponzorováno



Poskytování základního a zaručeného PNT každému taktickému vozidlu je AC²ES (esa).

S armádním rekordním programem A-PNT, který se v současnosti zaměřuje pouze na zlomek taktických vozidel, je k dispozici dostupné dočasné řešení, jak této hrozbě čelit.

Od prolomení obrany

„Moderní antény GPS pro letadla mají schopnost vynulovat několik rušících signálů GPS současně – což přispívá k přirozené odolnosti správně naklíčovaného a uzamčeného přijímače GPS, takže je téměř

nemožné rušit letadla, pokud nejsou extrémně blízko rušičky. (v několika kilometrech),“ řekl jeden bývalý představitel Pentagonu.

Ruská armáda běžně ruší GPS přijímače na východní Ukrajině od krymského konfliktu v roce 2014 a často falšuje GPS jednoduše proto, aby zamaskovala pohyb prezidenta Vladimira Putina po Moskvě, podle zprávy neziskového Centra pro pokročilé obranné studie z roku 2019.

Lokalizované rušení pozemních přijímačů GPS – spíše než rušení nebo kybernetické útoky na 30 satelitů GPS, které v současnosti provozují vesmírné síly – se od války v Kosovu v roce 1998 v mnoha dnešních konfliktních zónách, jako je Sýrie, stalo téměř rutinou, říkají odborníci. .

Například americký námořní úřad „má určitý druh stálých varování“ pro lodě plující ve východním Středomoří o degradaci signálu GPS, vysvětlila Dana Goward, prezidentka nadace Resilient Navigation and Timing Foundation.

Doporučeno



Se sny o JADC2 Pentagon znovu spouští experimenty velení a řízení řízené umělou inteligencí

Globální experimenty informační dominance V až VIII se snaží přenést těžkopádné procesy Pentagonu do věku umělé inteligence, velkých dat a cloudu, v naději, že budou informovat budoucí metasíť nazvanou Joint All Domain Command and Control.

Autor : Sydney J. Freedberg Jr.

A i když je extrémně těžké rušit šifrované funkce GPS nasazené americkou armádou, civilní uživatelé takové štěstí nemají.

„Pokud jde o civilní versus vojenskou GPS... civilní GPS je relativně snazší narušit a podvrhnout. Rusové to dělají celkem pravidelně po celém světě,“ řekl Breaking Defense Ganesh Pattabiraman, generální ředitel NextNav.

NextNav poskytuje pozemní přijímače, které poskytují alternativní signály určování polohy, navigace a časování (PNT) pro použití v městských kaňonech, kde se často ztrácí přístup GPS, a Pattabiraman řekl, že firma se zapojila do armádních experimentů hledajících alternativní řešení PNT.

Několik expertů poznamenalo, že „spoofing“ civilních signálů GPS změnou dat tak, aby se zařízení objevilo v jiném místě nebo časovém pásmu, je pro zlomyslné aktéry ještě snazší, a z tohoto důvodu je to znepokojení i pro ministerstvo obrany. Obranná inovační jednotka Pentagonu dne 10. února udělila zakázku na bližší nespecifikovanou částku společnosti Orbital Insight na odhalení falšování globálních navigačních družicových systémů (GNSS), včetně GPS.

Zpráva nadace Secure World Foundation 2021 Global Counterspace Capabilities uvádí minulé incidenty se spoofingem v Černém moři a Sýrii ruskými silami, Íránem v Hormuzském průlivu a Čínou na Spratlyho ostrovech.

V roce 2021 Trumpova administrativa vydala novou politiku Space Policy Directive 7 (SPD-7) s cílem zlepšit GPS a také nastartovat investice do alternativních systémů PNT. Směrnice zejména přiměla ministerstvo obrany, aby se stále více soustředilo na to, aby signály GPS byly odolnější proti rušení a také na zlepšení kybernetické bezpečnosti.

Současně byla vydána dlouho očekávaná zpráva o demonstraci doplňkových technologií PNT a GPS Backup Technologies ministerstva dopravy, která doporučila, aby vláda USA jako celek

více investovala do komerčních alternativ navzdory skutečnosti, že žádný aktuálně dostupný systém nemůže poskytnout samostatná záloha do GPS.

Odborníci však uvedli, že došlo jen k malému posunu vpřed směrem k tomu, jak zálohovat GPS pro civilní a komerční použití v USA.

Bidenova administrativa navrhla v rozpočtu ministerstva dopravy na fiskální rok 2022 financování ve výši 17 milionů dolarů na odolnou civilní PNT, oproti 5 milionům v roce 2021.

„Bohužel, od té doby Kongres nezbytně nepodnikl kroky, aby, víte, poskytl finanční prostředky, aby se z něj skutečně stala celostátní kapacita,“ řekl Pattabiraman.

Kromě toho neexistuje žádné kontaktní místo, které by dokonce varovalo komerční operátory v USA nebo v zahraničí na problémy s GPS.

"Existují vládní agentury, které mají odpovědnost varovat lidi," řekl Goward, včetně Národní Geospatial-Intelligence Agency (NGA) a ministerstva pro vnitřní bezpečnost. „Ale problém je v tom, že mnoho zdrojů, které používají, jsou tajné zdroje ke zjištění těchto informací. Můj dojem je... za prvé se nerozhodli, že je dostatečně důležité poskytovat tato varování, a za druhé, nepřišli na způsob, jak smíchat open source a klasifikaci dohromady a vytvořit varování.“

Mluvčí NGA nebyl schopen poskytnout komentář.