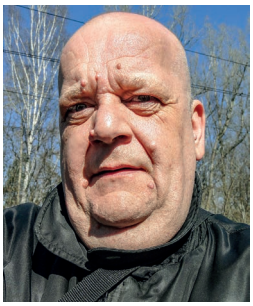
Znikający GPS

Konflikt Rosji z Ukrainą zmienił nasze postrzeganie wielu zagadnień, zwłaszcza w obszarze wojny elektronicznej. Bezprecedensowe działanie Rosji zmierzającej od początku wojny do całkowitego zakłócenia cywilnej i wojskowej łączności telekomunikacyjnej na Ukrainie nie tylko pokazało, że agresor nie liczy się z żadnymi skutkami swoich działań, lecz także ujawniło duże możliwości Rosjan w tym zakresie operacji wojennych.



Jacek Grabowski

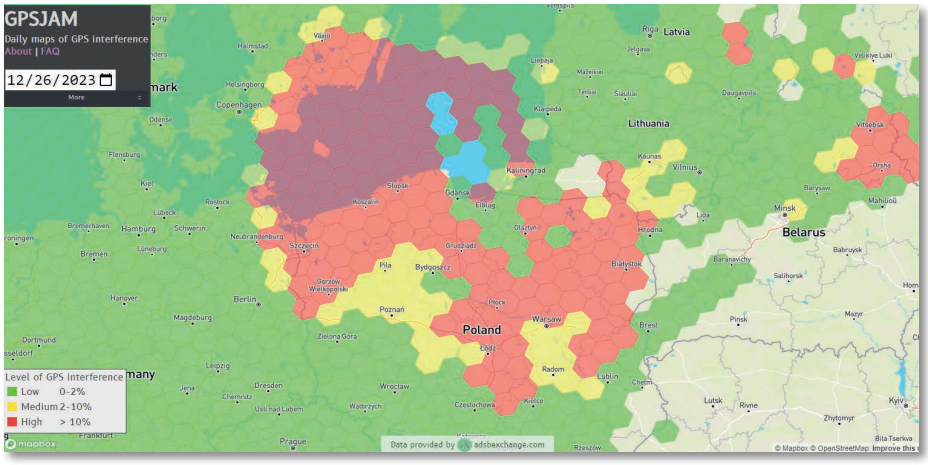
z wykształcenia specjalista gazownictwa i górnictwa naftowego, przygodę z informatyką rozpoczął w końcu lat 80. XX wieku od współpracy z wydawnictwem „Lupus", gdzie publikował teksty głównie w dwutygodniku „PCkurier" i miesięczniku „Enter". Współtwórca pierwszego w Polsce informatycznego czasopisma B2B „MRK" (1997). Były redaktor naczelny miesięcznika „Reset", współpracownik wielu innych tytułów (magazyn „WWW", „IT Reseller", „Komputer Świat"). Obecnie freelancer, współpracuje m.in. z warszawską komunikacją miejską.

Eskalacja napięcia poprzez deklarację przystąpienia do NATO krajów skandynawskich spowodowała szybki „odwet" Rosji objawiający się zakłóceniami sygnału GPS nad Finlandią. Już 5 marca 2022 r. fińscy piloci cywilni odnotowali poważne problemy z nawigacją. Na szczęście ich samoloty były wyposażone w alternatywne względem GPS systemy nawigacyjne, które pozwoliły kontynuować lot. Litewskie linie lotnicze musiały jednak z powodu zakłóceń odwołać kilka lotów do Finlandii i z powrotem. Sporadyczne zakłócenia GPS w obszarze Morza Bałtyckiego zdarzały się od tego czasu coraz częściej. Rosja nigdy oficjalnie nie przyznała się do prowadzenia działań utrudniających krajom NATO dostęp do systemu nawigacyjnego. Tym niemniej kolejna eskalacja zakłóceń nastąpiła w okolicy świąt Bożego Narodzenia 2023 r. Wtedy też anomalie sygnału GPS na rozległym terenie zauważono wtedy także nad Polską.

Od Olsztyna do Lublina

Głównym źródłem informacji o zakłóceniach sygnału GPS stał się internetowy serwis *gpsjam.org*, który pokazuje na mapie obszary, gdzie występują nieprawidłowości w odbiorze sygnału GPS. 26 grudnia 2023 r. po raz pierwszy na mapie zakłóceń pojawiły się czerwone plamy na terenie Polski.

Tego dnia zakłócenia objęły olbrzymi obszar od Danii przez Morze Bałtyckie do praktycznie całego zachodniego wybrzeża morskiego Polski. Wdarły się głęboko na teren naszego kraju, zahaczając o Warszawę i Mazowsze, na południu dochodząc aż na wysokość Częstochowy i Lublina. Po tym incydencie przez pewien czas panował względny spokój, lecz już 10 stycznia 2024 r. znów obszar zakłóceń nad Polską sięgnął na południe aż do Łodzi, a na wschodzie znowu do Lublina. Przez kolejne dni zakłócenia GPS w Polsce występowały „wyspowo", w znacznie mniejszym zakresie, ale 19 stycznia br. znów doszło do nasilenia i obszar zakłóceń ponownie sięgnął od Danii aż do Gorzowa, Łodzi i Lublina.



Źródło: hjttps://gpsjam.org

Poniższe linki ilustrują największe zakłócenia GSP nad Polską:

14/02/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-14

10/02/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-10

02/02/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-02

19/01/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-19

16/01/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-16

10/01/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-01-10

26/12/2024 https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2023-12-26

Po kilku dniach spokoju sytuacja powtórzyła się 2 lutego, a następnie 10 i 14 lutego. Gdy kończyłem tekst, mapa *gpsjam.org* nad Polską była chwilowo czysta.

Ujawnienie informacji o zakłóceniach w grudniu ubiegłego roku spowodowało wysyp różnych komentarzy. Radio Zet łączyło przyczynę zakłóceń z odbywającymi się w tym okresie manewrami NATO, inne media donosiły także o „ćwiczącym" w rejonie królewieckim oddziale wojsk walki elektronicznej wyposażonych m.in. w system Borisoglebsk-2, w skład którego wchodzą dwa pojazdy dowodzenia oraz cztery pojazdy ze stacjami zagłuszającymi wyposażone w anteny.

Borisoglebsk

Źródło: Wikimedia Commons

System taki z powodzeniem może zakłócić sygnały radiowe na sporym obszarze, wymaga tylko podłączenia do źródła prądu, by po 15 minutach przygotowań zacząć pracę.

Kształt mapy zakłóceń pokazuje dużą powtarzalność granic terytorium objętego anomaliami sygnału. Mniemanie, że generuje je jakiś system umieszczony w rejonie królewieckim nie jest więc pozbawione podstaw. Tym niemniej do dzisiaj nie ma żadnego oficjalnego potwierdzenia, kto i w jaki sposób zakłócał GPS w naszym kraju i okolicach. Na Rosję wskazuje jednak nie tylko obszar zakłóceń, lecz także wiele innych poszlak.

Rosja straszy czy się boi?

John Wiseman, ekspert z portalu *gpsjam.org*, zwrócił uwagę, że skala zakłóceń jest bezprecedensowa. Według niego wskazuje to, że są one praktycznie na pewno wynikiem celowych prób zagłuszania sygnału lub ćwiczeń wojskowych. Szef szwedzkiej Wojskowej Służby Wywiadu i Bezpieczeństwa MUST generał broni Thomas Nilsson w grudniu ubiegłego roku mówił: „obserwacji dotyczących zakłóceń GPS dokonywaliśmy już wcześniej w związku z rosyjskimi ćwiczeniami wojskowymi. Uważam, że jest to przykład działania hybrydowego, którego celem jest tworzenie niepewności". Z kolei pułkownik Joakim Paasikivi, wykładowca z Zakładu Strategii Szwedzkiej Akademii Obrony, powiedział, że „za zakłóceniem działania systemu GPS w regionie Bałtyku mogła stać Rosja, której celem było pokazanie, że potrafi przeprowadzać tego rodzaju akcje". Stwierdził też, że Rosja już wcześniej ingerowała w północnoeuropejski system GPS. Również pułkownik Eero Rebo z estońskich wojsk obrony terytorialnej wysnuł zbliżoną teorię: „Rosja prawdopodobnie nie ma wystarczającej obrony powietrznej, więc aby uspokoić swój naród, zdecydowała się po prostu na działania zastępcze". Rebo zaznacza, że stwarza to dodatkowe ryzyko w lotnictwie, a także w żegludze i nawiązując do niedawnych ataków ukraińskich dronów na infrastrukturę w Rosji dodaje: „tłumienie sygnału GPS w rzeczywistości nie wpływa na działania dronów. Reżim Putina robi to raczej po to, aby pokazać, że robi się coś, by bronić kluczowych dla niego aktywów".

Także służby niemieckie przyznały, że od pewnego czasu w rejonie Morza Bałtyckiego poważnie zakłócany jest sygnał nawigacji GPS. W związku z tym Bundesnetzagentur (Federalna Agencja ds. Sieci), odpowiedzialna m.in.

za ochronę elektromagnetyczną, wszczęła dochodzenie w porozumieniu z Bundeswehrą. Niemieckie służby mają zdolność precyzyjnego zlokalizowania źródeł zakłóceń, jednak żadne informacje dotyczące wyników ich badań nie są udostępniane publicznie. Podobnie jak w przypadku wspomnianych służb szwedzkich i estońskich, podejrzenia Niemców kierują się w stronę Rosji, która prawdopodobnie chroni swoje miasta pewnego rodzaju tarczą zagłuszającą, mającą skutecznie zabezpieczać przed atakami, takimi jak te przeprowadzane przez Ukrainę za pomocą dronów. Dla rosyjskiej armii zakłócenia GPS nie mają znaczenia, gdyż korzysta ona z własnego systemu nawigacji satelitarnej GLONASS, wspieranego w zakresie synchronizacji naziemnym radiowym systemem Czajka, a do prowadzenia działań wojskowych może ona również używać dużej liczby rozproszonych w sieci Internet TCP/IP publicznych serwerów NTP (NTPPOOL). Od wybuchu wojny ich widoczna liczba wzrosła ze 150 do 200 (25 proc.) i nadal wzrasta. Eksperci ze Szwecji szacują, że liczba ta może być 2–3-krotnie większa, ponieważ Rosjanie umiejscawiają swoje serwery NTP również poza granicami Rosji i pod domenami zagranicznych firm (źródło: https://gist.github.com/mutin-sa/eea1c396b1e610a2da1e5550d94b0453).

Jamming i spoofing

Choć istnieje wiele teorii i prób wytłumaczenia domniemanego postępowania Rosji prowadzącego do błędnego działania NATO-wskiego system nawigacyjnego, to w rzeczywistości oficjalnie nie znamy nawet rodzaju zakłóceń, które występowały na naszym terenie. Istnieją bowiem dwie metody zakłócania GPS: zagłuszanie sygnału (*jamming*) i fałszowanie wskazań odbiorników poprzez podawanie nieprawdziwych danych (*spoofing*).

Głównym celem zagłuszania jest uniemożliwienie dekodowania jakiegokolwiek sygnału GPS przez odbiorniki. Zakłócenia mogą jednak doprowadzić nawet do uszkodzenia odbiornika. Najprostszą metodą *jammingu* jest nadawanie fali elektromagnetycznej na częstotliwości nośnej L1 (1575,42 MHz). Przeprowadzone badania pokazują, że zależnie od tego, czy emitowane zakłócenia mają charakter ciągły czy impulsowy oraz czy częstotliwość fali zakłócającej pozostaje niezmienna, czy też lekko zmienia się w czasie, *jamming* może być bardziej lub mniej efektywny. Niezależnie jednak od tego, jakiego sygnału użyjemy, skutek pozostaje ten sam – odbiornik nie jest w stanie podać nam czasu UTC ani swojej pozycji. Obie wielkości są ze sobą ściśle związane, ponieważ aby wyznaczyć pozycję, odbiornik musi najpierw pozyskać z systemu satelitarnego GPS czas. Wiele wskazuje na to, że zakłócenia GPS obserwowane na terytorium Polski były spowodowane właśnie przez *jamming*.

Warto zauważyć, że Rosja ma niemałe doświadczenie w zagłuszaniu fal radiowych. Już pod koniec minionej dekady Izrael doświadczał podobnych zakłóceń GPS, które docierały tam z sąsiedniej Syrii, objętej wojną domową, wspieraną przez siły zbrojne Putina. Zakłócenia ruchu lotniczego i silnie zautomatyzowanego przemysłu oraz rolnictwa w Izraelu były bolesnym doświadczeniem. Tradycja zakłócania sygnałów radiowych przez Rosję jest jednak znacznie dłuższa. Już w czasach „zimnej wojny" dysponowała rozległą siecią „zagłuszarek" skutecznie eliminujących z eteru wiadomości nadawane przez zachodnie i amerykańskie stacje radiowe typu „Radio Wolna Europa" czy „Głos Ameryki". Choć oficjalnie „zagłuszarki" wyłączono w 1989 r., pracujący w nich specjaliści znaleźli łatwo zatrudnienie w armii. W efekcie Rosja dysponuje kilkoma różnego rodzaju systemami zagłuszania i zakłócania fal radiowych, których kryptonimy budzą respekt wśród ekspertów NATO. Poza wspomnianym już systemem Borisoglebsk-2 jest to np. system Krasucha C-4 użyty w Syrii i w Ukrainie do zagłuszania telefonii komórkowej.

Krasucha

Źródło: Wikimedia Commons

Są to systemy stacjonarne, rozmieszczone na samochodach lub ciągnikach gąsienicowych, jednak wiadomo, że Rosjanie dysponują także co najmniej jednym przenośnym systemem zagłuszającym mieszczącym się w plecaku.

W *spoofingu* Rosjanie również okazują się mistrzami. W 2017 r. francuski tankowiec Atria płynący do rosyjskiego portu Noworosyjsk napotkał niespodziewane problemy z nawigacją GPS. Urządzenia nawigacyjne tankowca wskazywały, że znajduje się on na lądzie, na terenie lotniska w pobliskim uzdrowisku Gelendżyk. Inne statki na Morzu Czarnym również zgłaszały niejednokrotnie podobne anomalie. Ponieważ (według Aleksandra Nawalnego) w Gelendżyku znajduje się tajna rezydencja Putina, Amerykanie wysnuli z tego zdarzenia teorię, że naziemne

stacje spoofingowe chronią przed „namierzeniem" miejsca przebywania rosyjskiego prezydenta. Przypuszcza się także, że powodem spoofingowania GPS w tamtej okolicy może być port w Noworosyjsku, ważny z punktu widzenia wojskowego. To, co chroni, może również służyć do ataku jako broń ofensywna. Zbyt zależna dziś od GPS automatyka przemysłowa jest podatna na desynchronizacje. Okazuje się, że źródło czasu i synchronizacja opierają się najczęściej na GPS, a są one niezbędne dla każdej rozproszonej architektury IT. Jest to szczególnie ważne dla telekomunikacji, w energetyce, transporcie (kierowanie ruchem lotniczym i kolejowym). Z GPS do synchronizacji korzysta: administracja publiczna, banki, wojsko i policja. Jej desynchronizację można wywołać *jammingiem* i *spoofingiem* sygnałów GPS. Działa to jak arytmia serca. Może boleć (incydent bezpieczeństwa) lub prowadzić do złego samopoczucia obniżającego naszą wydajność pracy, ale może również prowadzić do poważnych zapaści, a nawet śmierci. Za pomocą desynchronizacji można wywołać poważne awarie prowadzące do blackoutu w energetyce i telekomunikacji.

Co z tym zrobić?

Przeciętnemu człowiekowi zakłócenia GPS mogą wydawać się właściwie mało szkodliwe, efektowne czerwone plamy na mapie, ciekawe jako sensacja wojenna w mediach, ale mające mały wpływ na życie. Czasami przy okazji zakłóceń GPS zauważyć możemy, jak nasz samochód „znosi z drogi" i podążamy poza jej obszarem. Na mapach telefonów komórkowych obserwować możemy dziwne skoki naszej pozycji.

> *W rzeczywistości system nawigacyjny GPS jest podstawą wielu systemów gospodarki cywilnej, dawcą czasu wzorcowego UTC, istotnym elementem wszystkich form transportu publicznego i indywidualnego.*

Nawigacja GPS zastępuje żyroskopy i używa się jej: do stabilizacji torów jazdy, w medycynie nuklearnej, odpowiada za stabilność komunikacji radiowej, wspiera systemy informacyjne. Stosuje się ją w komunikacji miejskiej, na kolei, w żegludze i lotnictwie. Często nie zdajemy sobie sprawy, że od czasu z GPS zależą nawet systemy baz danych SQL i ich archiwizacja.

Tak więc zakłócenia GPS występujące na dużym obszarze i z taką intensywnością mogą budzić poważny niepokój. Nie są to zakłócenia występujące stale, ale ich powtarzalność i losowe momenty występowania osłabiają dziś zaufanie do GPS-u, powoli „podmywają" fundamenty współczesnej informatyki (IT) i przemysłu OT (technologie operacyjne), które dziś bazują wyłącznie na rozproszonej architekturze. Sam system GPS trudno byłoby dziś ad hoc czymś zastąpić.

Niepokój budzi również to, że w Polsce głównym źródłem informacji o zakłóceniach tak istotnego dla naszej gospodarki systemu nawigacyjnego stał się internetowy serwis *gpsjam.org* stworzony w sumie amatorsko przez jedną osobę na podstawie publicznych danych zgłaszanych przez linie lotnicze!

> *Siłą rzeczy nasuwa się pytanie, czy nasz kraj dysponuje systemem umożliwiającym wykrycie anomalii działania GPS-u, a jeśli nie, to czy taki system nie powinien w obecnej sytuacji być jak najprędzej zakupiony.*

System taki, o nazwie ARGOS, proponuje i może w trybie pilnym wdrożyć w Polsce firma ELPROMA (https://www.elpromaelectronics.com/category/elproma-time/) – polski producent serwerów czasu NTP/PTP, którego urządzenia posiadają atestacje NATO. Proponowane rozwiązanie posiada funkcję generowania alarmów z powiadamianiem wskazanego centrum zarządzania kryzysowego, które powiadomi przedmiotowe dla NIS2 infrastruktury krytyczne energetyki, telekomunikacji, transportu, banki i GPE o trwającym ataku radiowym *jamming/spoofing* GPS, wskazując siłę i zakres terytorialny ataku. To pozwoli uruchomić procedury cyberbezpieczeństwa i zapewni autonomię pracy systemów informatycznych, odcinając je od GPS na czas trwania ataków radiowych zakłócania.

Są jeszcze dwie ważne kwestie. Pierwsza to mało znany fakt istnienia dyrektywy prezydenckiej G.W. Busha z 2004 r., umożliwiającej wyłączenie amerykańskiego systemu GPS Navstar w dowolnym regionie świata, a więc również nad Polską. Świadomość takiej możliwości daje Polsce długi czas, który krajowa gospodarka powinna wykorzystać na przygotowanie się do pracy w rzeczywistości, którą dziś nakreśla nowa światowa geopolityka i ataki radiowe zakłócania GPS. Druga to miła niespodzianka i fakt, że na dwa tygodnie przed pierwszym incydentem GPS nad Polską, Główny Urząd Miar RP oddał do użytku na początku grudnia 2023 r. naziemny system synchronizacji czasu o nazwie eCzasPL. Jest to nieodpłatna dla krajowego przemysłu usługa naziemnej synchronizacji UTC z użyciem protokołów NTP i PTP IEEE1588. Głównym wykonawcą systemu jest firma ELPROMA, która wcześniej zrealizowała narodowe systemy czasu i synchronizacji, w tym obsługę synchronizacji energetyki i telekomunikacji w Europie, w krajach Azji i w Afryce.