

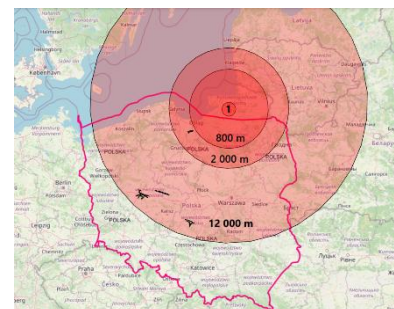
Zakłócenia systemów nawigacji satelitarnej na Pomorzu i nad Bałtykiem

Co właściwie dzieje się dziś na Pomorzu i czy to tylko „lepsza widoczność”?

Obecnie Polska znajduje się w jednym z najbardziej narażonych na zakłócenia sygnałów satelitarnych regionów świata. Mamy do czynienia z bezwzględny, obiektywnym i skokowym nasileniem celowych zakłóceń. To nie jest tak, że nagle zaczęliśmy je tylko lepiej dostrzegać. Rzeczywista skala i moc ataków drastycznie wzrosły. Zakłócenia obserwowane w regionie Morza Bałtyckiego uderzają w infrastrukturę krytyczną, istotnie utrudniają prowadzenie żeglugi na Bałtyku, wpływają na lotnictwo, a ostatecznie uderzają w codzienne usługi.

Oczywiście, zjawisko to stało się bardziej „namacalne” z dwóch powodów. Po pierwsze, tanie i wszechobecne technologie oparte na lokalizacji (od aplikacji transportowych po drony) zaczęły masowo zawodzić pod wpływem tak silnego promieniowania. Po drugie, jako państwo zaczęliśmy ten problem aktywnie mapować. Właśnie w tym celu budowana jest Polska Tarcza PNT, na którą składają się oddany już do użytku system RTGMS (rtgms.pl) oraz rozwijany System Monitorowania Zakłóceń Sygnałów GNSS (SMZSG), czyli pilotażowa sieć 100 sensorów Polskiej Agencji Kosmicznej. Działają one jak system wczesnego ostrzegania, który daje nam coraz pełniejszy obraz sytuacji.

Zasięg zakłóceń: Ponad dwie trzecie terytorium kraju na wysokości przelotowej znajduje się w zasięgu środków zakłócających rozmieszczonych w Obwodzie Królewieckim oraz na obiektach tzw. floty cieni¹.



Rosjanie najprawdopodobniej wykorzystują również własnego satelitę wojskowego KOSMOS 2546², znanego także jako EKS-4 lub Tundra 14L, do zagłuszania sygnałów GNSS. Jeżeli technologia ta zostanie dopracowana, mogą uzyskać zdolność do „wyłączenia” GNSS, na przykład na obszarze Europy.

Paraliż żeglugi: Ruch morski na Morzu Bałtyckim od kilku lat jest silnie zaburzany. W tym obszarze na masową skalę stosowany jest spoofing (fałszowanie sygnału), co sprawia, że cywilna żegluga morska nie może już polegać na niezakłóconych sygnałach GNSS.

Potężne spadki mocy sygnału: Pomiary z krajowych stacji referencyjnych wskazują, że odbiorniki w regionie bałtyckim konsekwentnie odnotowują największe spadki współczynnika CNR (Carrier-to-Noise Ratio). W 2024 roku na terytorium Polski zarejestrowano spadki tego parametru sięgające nawet 10 dB.

Aby zrozumieć, co dokładnie uderza w odbiorniki i dlaczego niektóre incydenty są groźniejsze od innych, przełożmy te inżynierskie pojęcia na codzienne sytuacje:

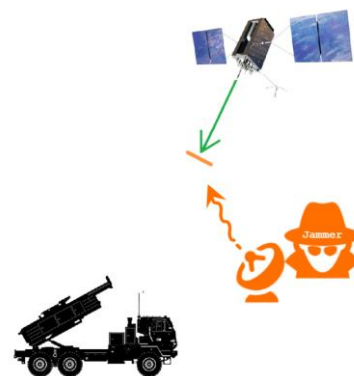
¹ Około 1,5 tys. tankowców, często starszych jednostek pływających pod fałszywymi banderami.

² [Ryzyko rosyjskich zagłuszeń GNSS z orbity](#)

1. Jamming (Zagłuszanie) – „Krzyk, który zagłusza szept”

Sygnały z satelitów docierające na Ziemię są niezwykle słabe. Jamming to po prostu brutalne wyemitowanie silnego szumu radiowego na tej samej częstotliwości. Wyobraź sobie, że stoisz w tłumie i próbujesz usłyszeć szept z drugiego końca pokoju, a nagle ktoś staje obok ciebie z wielkim megafonem i zaczyna wrzeszczeć. Nic nie słyszysz.

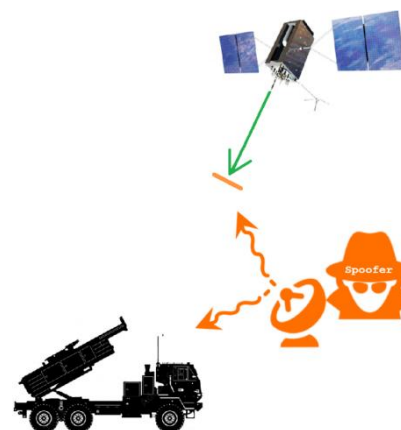
Efekt: Odbiornik zostaje „oślepiiony”. Na mapie w telefonie masz ciemność, a aplikacja krzyczy „Brak sygnału GPS”. Samochód przestaje nawigować, a dron po prostu zatrzymuje się w miejscu lub dryfuje z wiatrem, bo traci orientację w przestrzeni.



2. Spoofing (Falszowanie) – „Oszust na linii”

Jest to zdecydowanie najbardziej niebezpieczne zjawisko. Napastnik nie krzyczy, lecz dzwoni do ciebie, doskonale naśladowując głos twojego znajomego, i podaje fałszywy adres spotkania. Komputer spoofera generuje od zera fałszywy, ale bardzo wiarygodny sygnał, dopasowując się do prawdziwego.

Efekt: Urządzenie jest przekonane, że wszystko działa idealnie, i nie podnosi żadnego alarmu. Fizycznie jesteś w Gdyni, ale mapa nagle pokazuje środek lotniska w Królewcu. Systemy autonomiczne ślepo ufają tym danym. Dron zaprogramowany tak, aby unikać lotnisk (strefy zakazu lotów, tzw. No-Fly Zones), „myśli”, że złamał prawo, inicjuje twarde lądowanie i spada w lesie.

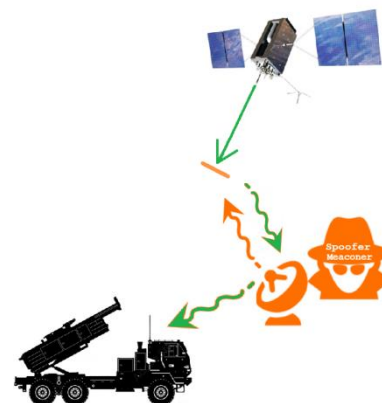


3. Meaconing (Odtwarzanie z taśmy) – „Spóźniona transmisja na żywo”

To atak typu „nagraj i odtwórz”. Wyobraź sobie, że ktoś z ukrycia nagrywa na dyktafon w 100% autentyczne przemówienie, a potem puszcza je z głośnika w zupełnie innym mieście. Sygnał w meaconingu jest prawdziwy, kosmiczny, ale napastnik odbiera go za pomocą własnej anteny (np. na dachu w Obwodzie Królewieckim), mocno wzmacnia i puszcza w eter wokół.

Efekt: twój telefon czy system na statku łapie ten wzmocniony sygnał i myśli, że znajduje się tam, gdzie faktycznie stoi antena oszusta odbierająca sygnał z kosmosu. System pozycjonowania przeskakuje. Jest to groźne i stosunkowo proste do przeprowadzenia, bo atakujący nie musi umieć generować fałszywego sygnału, wystarczy mu antena i potężny wzmacniacz.

Powinniśmy pamiętać, że to, co dziś dzieje się nad polskim wybrzeżem, to regularne działania hybrydowe w cyberprzestrzeni w warstwie fizycznej, uderzające zarówno w dostępność sygnału (jamming), jak i jego wiarygodność (spoofing i meaconing). Narzędzia, które budujemy jako odpowiedź, mają kluczowe znaczenie, by odróżnić kosmiczny szept od krzyku i kłamstw dobiegających z wrogich anten.



Typ zakłócenia	Źródło/Pochodzenie	
Antropogeniczne	Niecelowe	
	Celowe	jamming
		spoofing
		meaconing
Naturalne	Układ Słoneczny: koronalne wyrzuty plazmy, promieniotwórczość	
	Przestrzeń międzygwiazdowa: szerokopasmowe emisje	

Czy zakłócenia GPS to tylko problem z niedziałającą mapą w telefonie i zagubionymi dronami?

Zdecydowanie nie. Zepsuta nawigacja w smartfonie podczas powrotu z wakacji czy utrata kontroli nad rekreacyjnym dronem to tylko wierzchołek góry lodowej. W rzeczywistości współczesna cywilizacja opiera się na sygnałach, których nie widzimy, a które decydują o funkcjonowaniu niemal każdej dziedziny naszego życia.

Dziś sygnały satelitarne (GNSS) to niewidzialny fundament dla transportu, energetyki, telekomunikacji, rolnictwa, logistyki oraz finansów. Uderzenie w ten system to uderzenie w krwiobieg nowoczesnego państwa.

Aby to zrozumieć, podzielmy zagrożenia na dwie główne kategorie: transport oraz „ukryty zegar”.

Widoczne zagrożenie: transport (lotnictwo, morze i autonomia)

Kiedy sygnał znika lub jest fałszowany, maszyny tracą orientację w przestrzeni.

Samoloty mogą latać bez GPS/GNSS, wykorzystując klasyczne instrumenty i radary. Zakłócenia sygnału wpływają jednak na procedury podejścia do lądowania na niższych wysokościach, co odczuwalnie zwiększa ryzyko operacyjne całego lotu.

Na morzu zniknięcie sygnału oznacza poważne utrudnienia w bezpiecznym prowadzeniu jednostek i utrzymaniu kursu.

Pojazdy bezzałogowe czy zautomatyzowane maszyny rolnicze po utracie nawigacji tracą całkowitą stabilność i precyzję działania.

Wyobraź sobie ruchliwą autostradę w gęstej mgle. Samochody wciąż mają kierownice i hamulce, ale nagle znikają wszystkie białe linie na asfalcie i gasną latarnie. Da się jechać, ale ryzyko karambolu, opóźnień i chaosu wzrasta diametralnie.

Ukryte zagrożenie: czas, który steruje światem

To najmniej znana, ale najbardziej krytyczna funkcja satelitów. GPS/GNSS to nie tylko linijka do mierzenia odległości, to przede wszystkim najdokładniejszy zegar na świecie, który steruje współczesną cywilizacją.

Cały potężny system światowej infrastruktury opiera się na idealnej synchronizacji czasu na poziomie niewyobrażalnych dla człowieka nanosekund. Co się dzieje, gdy tego czasu zabraknie?

Weźmy pod uwagę telekomunikację (np. sieci 5G). Bez precyzyjnych znaczników czasu z kosmosu przestałyby działać stacje bazowe telefonii komórkowej.

Analogia. Sieć komórkowa to bieg sztafetowy. Kiedy jedziesz samochodem i rozmawiasz przez telefon, jedna wieża (biegacz) przekazuje twój sygnał drugiej wieży. Muszą to zrobić w idealnym ułamku sekundy. Bez sygnału z satelity biegacze tracą rytm, pałeczka upada na ziemię, a twoje połączenie zostaje zerwane.

Innym przykładem jest energetyka. Inteligentne sieci energetyczne muszą utrzymać tzw. spójność fazową. Bez sygnału czasu mogą wystąpić katastrofalne awarie i masowe przerwy w dostawach prądu (blackout).

Analogia. Sieć energetyczna to wielka orkiestra symfoniczna. Instrumenty (elektrownie) mogą być świetne, ale jeśli zabierzemy im dyrygenta (czas z GPS/GNSS), zaczną grać poza rytmem. Zamiast muzyki powstanie niszczący hałas, a cały koncert trzeba będzie przerwać.

W przypadku finansów i bankowości każda transakcja giełdowa, przelew lub płatność kartą wymagają precyzyjnego znacznika czasu. Bez tego systemy bankowe nie wiedziałyby, czy najpierw przelałeś pieniądze, czy pobrałeś je z bankomatu, co doprowadziłoby do ich paraliżu.

Efekt domina (awarie kaskadowe)

Największym ryzykiem nie jest awaria pojedynczego elementu, lecz to, co inżynierowie określają mianem awarii kaskadowej. Europa jest tak silnie uzależniona od tej technologii, że zakłócenia działają jak efekt domina. Zablokowany port morski oznacza, że ciężarówki nie odbierają towaru. Spóźnione ciężarówki oznaczają wstrzymanie linii produkcyjnych w fabrykach. Zatrzymane fabryki to straty na giełdzie. Dlatego dzisiaj ochrona sygnałów nawigacyjnych to już nie tylko kwestia wygody, ale absolutny fundament bezpieczeństwa całego państwa.

To nie wina twojego telefonu (analogia z kompasem i magnesem)

Gdy nawigacja zaczyna wariować, pierwszą reakcją większości z nas jest panika. Ludzie wyłączają i włączają telefon, stukają w ekran, reinstalują aplikacje. To nie pomaga.

Co robić? Zrozumieć, że problem leży na zewnątrz.

Analogia. Wyobraź sobie, że masz w ręku tradycyjny kompas, a ktoś złośliwy położył tuż obok potężny magnes. Igła kompasu zacznie szaleć. Potrząsanie nim, uderzanie w szybkę czy zamykanie go w pudełku nic nie da. Kompas jest sprawny, po prostu otoczenie jest „zatrute”.

Praktyczna rada: jeśli zauważysz, że aplikacja mapy pokazuje głupoty, nie trać czasu na restarty telefonu. Wyłącz na chwilę lokalizację w urządzeniu i po prostu spójrz przez okno na fizyczne drogowskazy. Warto też przed dłuższą podróżą pobrać mapy do trybu offline, dzięki temu nawet bez GPS-u wciąż masz w telefonie cyfrową mapę, którą możesz przesuwac palcem.

Dla użytkowników aplikacji transportowych (analogia z rozmytym listem)

Chcesz zamówić taksówkę na aplikację (Uber, Bolt) lub wypożyczyć hulajnogę, a system pokazuje, że stoisz w Morzu Bałtyckim albo na lotnisku oddalonym o 200 kilometrów.

Co robić? Przejmij kontrolę nad danymi.

Zamawianie taksówki przez automatyczną lokalizację GPS/GNSS to jak wysłanie do kierowcy listu z wydrukowanym adresem. Jeśli w wyniku zakłóceń drukarka zwariowała i wydrukowała plamę, kierowca do ciebie nie trafi. Co robisz? Bierzesz długopis i piszesz adres własnoręcznie.

Praktyczna rada: zignoruj niebieską kropkę na mapie. Gdy aplikacja pyta „Skąd cię odebrać?”, nigdy nie klikaj „Użyj mojej lokalizacji”. Wpisz z klawiatury dokładny adres (np. „Świętojańska 15, Gdynia”) lub podaj nazwę charakterystycznego budynku obok.

Dla kierowców na trasie (analogia ze złośliwym drogowskazem)

Co się dzieje? Jedziesz autostradą, a nawigacja nagle każe ci ostro skręcić w pole albo zjechać z wiaduktu.

Co robić? Ufaj oczom, nie ekranom.

Nawigacja samochodowa to twój pilot rajdowy, ale bardzo łatwowierny. Jeśli ktoś na drodze celowo przestawi znaki kierujące na Warszawę tak, by wskazywały na jezioro (to jest właśnie spoofing), twój pilot powie: „Skręć do jeziora”. Ty jednak masz oczy i widzisz, że tam nie ma drogi.

Praktyczna rada: zanim wyruszysz w dłuższą trasę, oddal mapę na ekranie i zobacz „duży obraz” przez jakie większe miasta będziesz przejeżdżać. Jeśli nawigacja nagle zmieni zdanie i wyda absurdalną komendę, zignoruj ją. Trzymaj się głównej drogi i kieruj się tradycyjnymi, blaszanymi znakami drogowymi, aż system znów „złapie” właściwy sygnał.

Dla operatorów dronów – tu ryzyko jest największe (analogia z żeglowaniem we mgle)

Co się dzieje? Twój dron nagle zatrzymuje się w powietrzu, zaczyna szybko dryfować z wiatrem, albo co gorsza, wykonuje gwałtowny manewr ratunkowy i ucieka, bo „myśli”, że wleciał w strefę zakazaną.

Co robić? Lataj w trybie ręcznym.

Można to wytłumaczyć poprzez analogię. Latanie dronem na automatycznym GPS-ie w rejonie zakłóceń jest jak żeglowanie we mgle z zepsutym sterem, gdzie ślepo ufasz maszynie. Musisz mieć w ułamku sekundy chwycić za koło sterowe i przejąć dowodzenie.

Praktyczna rada: obserwuj mapy zakłóceń. Zanim wystartujesz, sprawdź serwisy monitorujące sygnał GNSS (tzw. detektory jammingu).

Naucz się latać bez wspomagaczy. To absolutnie kluczowe. Każdy operator musi umieć przełączyć drona w tryb ATTI, czyli tryb lotu bez wsparcia pozycjonowania GPS, i bezpiecznie nim wylądować, polegając wyłącznie na własnym wzroku i kamerze.

Zrezygnuj z funkcji „Return to Home” (RTH). Jeśli dron straci sygnał wideo, funkcja automatycznego powrotu do miejsca startu na podstawie GPS może go skierować prosto w drzewo lub wywieźć kilkadziesiąt kilometrów dalej. Ustal alternatywne procedury awaryjne.

Takie codzienne uświadamianie to najlepsza tarcza ochronna dla społeczeństwa. Kiedy ludzie wiedzą, jak działają te zakłócenia, przestają być bezradni, a zjawisko traci swój paraliżujący efekt.

Jak „zobaczyć” niewidzialne zakłócenia?

Sygnały satelitarne przemieszczają się w niewidzialnej dla nas przestrzeni elektromagnetycznej. Aby je monitorować, inżynierowie stosują tzw. analizę widmową.

Analogia z akustykiem i koncertem:

Wyobraź sobie, że prawdziwy sygnał z satelity to cicha, piękna melodia grana na flecie. Zagłuszanie (jamming) to sytuacja, w której ktoś włącza obok ryczącą betoniarkę. Z kolei fałszowanie (spoofing) to odtworzenie z ukrytego głośnika innej melodii na flecie, żeby zmylić słuchacza.

Człowiek słyszy tylko hałas. Ale jeśli nagramy ten dźwięk i wrzucimy do specjalnego programu (analizatora widma), zobaczymy na ekranie dokładny, graficzny „odcisk palca” tego dźwięku. Program od razu pokaże cienką linię fletu i wielką, poszarpaną plamę betoniarki. Tak właśnie stacje monitorujące wykrywają ataki na systemy nawigacyjne.

Rola Politechniki Gdańskiej. Mózg zamiast uszu

Aby łowić te zakłócenia na żywo, państwo buduje specjalne systemy nasłuchowe. Politechnika Gdańska nie posiada obecnie własnej operacyjnej sieci takich „mikrofonów” terenowych (jak np. krajowy system rtgms.pl). Brak własnych anten nie wyklucza jednak uczelni z działań w tym obszarze. Wręcz przeciwnie, wyznaczają jej inną, istotną rolę.

Analogia z detektywem:

Sensory w terenie, rozsiane po Polsce, to tylko „oczy i uszy” systemu ostrzegawczego. Zbierają one codziennie gigantyczne ilości danych (terabajty nagrań szumu). Aby z tego szumu wyciągnąć wnioski, potrzebny jest analityczny „detektyw” pracujący w laboratorium. Rolę takiego „detektywa” może pełnić infrastruktura obliczeniowa Politechniki Gdańskiej dostępna w CI TASK.

Co dokładnie robi PG?

Z perspektywy CI TASK Politechniki Gdańskiej kluczowe jest to, że monitorowanie zakłóceń GNSS nie kończy się na samym zarejestrowaniu sygnału. Prawdziwa wartość pojawia się dopiero wtedy, gdy dane z wielu sensorów, stacji referencyjnych i systemów pomocniczych zostaną połączone, oczyszczone i przeanalizowane w dużej skali. Wymaga to odpowiedniej infrastruktury obliczeniowej, pamięci masowej, szybkiej transmisji danych oraz kompetencji w zakresie wysokowydajnych obliczeń (HPC), chmury obliczeniowej, analizy Big Data i sztucznej inteligencji. Takie środowisko umożliwia analizę milionów pomiarów pochodzących z wielu źródeł niemal w czasie rzeczywistym, co jest praktycznie niewykonalne przy wykorzystaniu standardowej infrastruktury informatycznej.

CI TASK stanowi zaplecze obliczeniowo-analityczne dla tego typu zastosowań. Superkomputery i środowiska chmurowe umożliwiają analizę dużych strumieni danych radiowych i nawigacyjnych, trenowanie modeli uczenia maszynowego rozpoznających charakterystyczne wzorce zakłóceń, korelację danych GNSS z innymi źródłami informacji, takimi jak AIS, ADS-B, dane meteorologiczne czy informacje o infrastrukturze krytycznej, a także prowadzenie symulacji wpływu zakłóceń na systemy transportowe, telekomunikacyjne i energetyczne. W efekcie możliwe staje się przejście od prostego wykrywania incydentów do budowy systemów wczesnego ostrzegania, prognozowania oraz wspomagania decyzji.

W praktyce oznacza to możliwość budowy zaawansowanych platform analitycznych, które integrują dane z wielu źródeł, przetwarzają je w czasie zbliżonym do rzeczywistego, automatycznie wykrywają anomalie, klasyfikują rodzaje zakłóceń i wspierają ocenę ryzyka dla infrastruktury krytycznej. Takie podejście ma szczególne znaczenie na Pomorzu, gdzie koncentrują się kluczowe elementy infrastruktury morskiej, lotniczej, energetycznej, telekomunikacyjnej i naukowej, a uwarunkowania geopolityczne powodują podwyższone ryzyko występowania zakłóceń sygnałów satelitarnych.

Kto za to odpowiada? Współpraca z Ministerstwem Cyfryzacji i IŁ-PIB

Zakłócenia sygnałów GPS nie są wyłącznie „problemem technicznym”. To twardy atak na krajową infrastrukturę krytyczną, a przestrzeń fal radiowych jest dziś traktowana jako kluczowy element cyberprzestrzeni.

Jak to wygląda od strony formalnej?

Ministerstwo Cyfryzacji (MC) jest resortem odpowiedzialnym w Polsce za szeroko rozumiane cyberbezpieczeństwo cywilne oraz spójność infrastruktury telekomunikacyjnej. Ministerstwo ma za zadanie dbać o to, by usługi cyfrowe, od których zależy państwo, działały bez zakłóceń.

Instytut Łączności – Państwowy Instytut Badawczy (IŁ-PIB), działający z ramienia Ministerstwa Cyfryzacji, odpowiada za bezpośrednią osłonę tej części cyberprzestrzeni. To IŁ-PIB buduje i rozwija wspomniany wcześniej, działający w czasie rzeczywistym system RTGMS, będący fundamentem monitorowania celowych incydentów w Polsce.

Synergia państwa i nauki

Politechnika Gdańska może stanowić w tym obszarze istotne zaplecze naukowe i technologiczne. IŁ-PIB z ramienia MC dysponuje siecią nasłuchową i dostarcza surowe dane operacyjne, chroniąc cyberprzestrzeń na pierwszej linii. Z kolei infrastruktura superkomputerowa, środowiska chmurowe oraz kompetencje w zakresie sztucznej inteligencji dostępne w CI TASK PG mogą te dane błyskawicznie przetwarzać, zasilając państwo gotowymi, zautomatyzowanymi modelami wykrywania zagrożeń. To układanka, w której zaawansowana nauka bezpośrednio wzmacnia odporność państwa na zakłócenia systemów PNT oraz innych elementów infrastruktury krytycznej.

Autorzy opracowania:

Jerzy Proficz, Centrum Informatyczne TASK Politechniki Gdańskiej

prof. Mariusz Figurski, Politechnika Gdańska / Instytut Łączności – Państwowy Instytut Badawczy

ppłk Wojciech Żurawski, Ministerstwo Obrony Narodowej