# Jak chronić infrastrukturę krytyczną przed desynchronizacją?

**Konflikt między Rosją a Ukrainą zmienił nasze postrzeganie wojny elektronicznej. Wydaje się, że umiejętne zakłócanie sygnałów GPS może być bardzo skuteczną bronią cybernetyczną, ponieważ pozwala blokować podstawowe funkcje PNT (*Positioning, Navigation and Timing*) każdego odbiornika satelitarnego. Umożliwia to skutecznie destabilizowanie infrastruktury krytycznej państwa, bo zależność systemów informatycznych IT i przemysłowych OT od funkcjonalności PNT, a zwłaszcza od systemów GPS, wzrasta.**

Okazuje się, że obecnie łatwiej jest destabilizować pracę całych systemów IT/OT niż włamywać się do dobrze zabezpieczonych i odizolowanych od internetu sieci wewnętrznych. Najważniejsze sieci infrastrukturalne używają precyzyjnego czasu, którym można manipulować.

## Zagrożenia dla infrastruktury krytycznej

Desynchronizacja, czyli rozsynchronizowanie zegarów w rozproszonych systemach, jest w stanie zaburzyć parametry pracy na różnych poziomach sprzętu, oprogramowania systemowego i aplikacji.

> *Desynchronizacja sieci infrastrukturalnych IT/OT, objętych dyrektywą NIS2, może prowadzić do awarii o nieprzewidywalnych konsekwencjach. Coraz częściej pojawiają się ostrzeżenia przed wielką awarią, która może wywołać efekt domina.*

Rozsynchronizowanie czasu w urządzeniach sieciowych prowadzi też do zaburzenia obliczeń opóźnień w przepływie informacji siecią TCP/IP. W przypadku rozproszonej architektury współczesnych systemów IT/OT, oznacza to groźbę użycia zdezaktualizowanych danych i odrzucenia prawidłowych informacji. To determinuje nowy rodzaj zagrożenia i definiuje dwa rodzaje cyberataków destabilizacji, przed którymi chroni firma ELPROMA (www.elpromaelectronics.com) :

- **Time Synchronization Attack** (atak na czas)
- **Time Delay Attack** (atak na opóźnienia w sieci)

Obserwowane na przestrzeni ostatniej dekady awarie zawsze w jakimś stopniu wskazywały na udział desynchronizacji. Wśród wielu możliwości zagrożeń na szczególną uwagę zasługują te dotyczące odbiorników satelitarnych GNSS.

**Istnieją dwie metody zakłócania GPS: zagłuszanie oryginalnego sygnału *jamming* i fałszowanie wskazań odbiorników poprzez podawanie nieprawdziwych danych w depeszach, tzw. *spoofing*. W samej kategorii *jammingu* możemy rozróżnić podgrupy *jammingu PRN, chirp jammingu, coded jammingu* itp. Podobnie w *spoofingu* istnieją podgrupy synchronicznego *spoofingu*, a ostatnio Niemcy opublikowali informację o identyfikacji nowego rodzaju *spoofingu*, który nazwali okrężnym (*circle spoofing*). Rozpoznanie nowych rodzajów zagrożeń atakami RF jest istotne dla stworzenia antidotum i wytworzenia odporności układów odbiorczych GNSS na zagrożenie. Tym właśnie zajmują się eksperci z polskiej firmy ELPROMA.**

## Rosyjska aktywność

Prowadzone od 2016 r. przez niezależne zespoły USNO[1] i C4ADS[2] obserwacje wskazały miejsce źródła zagłuszającego GPS w rejonie Morza Czarnego. Do badań wykorzystano dopplerowskie pomiary sensorem STP-H5[3] zainstalowanym na stacji kosmicznej ISS orbitującej 400 km nad powierzchnią Ziemi. Na co dzień służył on do badań jonosfery, ale „w wolnych chwilach" wykonywał dodatkowe pomiary. Za pomocą wbudowanego w pełni programowalnego odbiornika satelitarnego SDR (Software Defined Radio) rejestrowano sygnały GPS wiązek L1 i L2 z częstotliwością próbkowania 6 Mbps. Niezinterpretowane surowe dane, przekazane na Ziemię specjalnym 60-sekundowym slotem transmisyjnym, zostały poddane rozszerzonej analizie sygnałowej DSP. W analizie wykorzystano sztuczną inteligencję i uczenie maszynowe. Badania skoncentrowano na rejonie Morza Czarnego, gdzie odnotowywane były w połowie poprzedniej dekady interferencje sygnałów GPS, a szczególnie dawał się we znaki *spoofing*. Wiele wcześniejszych raportów żeglujących tam statków handlowych opisywało anomalia pracy odbiorników GPS. Niektórzy kapitanowie twierdzili, że ich statki nawigacja przenosiła o kilkaset kilometrów dalej – do Moskwy.

Kiedy ISS przelatywała nad obszarem Morza Czarnego podejrzanym o *spoofing* GPS, wartość depeszy LNAV była odczytywana jako zero na wszystkich dostępnych kanałach odbiornika GPS. Zera znikały po opuszczeniu obszaru zakłóceń. Nie było wątpliwości co do celowego zakłócania GPS, jednak nie pasowało to do klasycznego *jammingu*, ponieważ dekodowana informacja nie była zakłócona losowym szumem częstotliwości nośnej L1. Nie był to też typowy *spoofing* GPS, bo nie wykazano fałszowania telemetrii nawigacyjnej depeszy LNAV, a jedynie jej wyzerowanie. Analiza spektralna w widmie częstotliwości L1 1575,42 MHz potwierdziła obecność sztucznego sygnału zakłócenia. Amerykanie nazwali ten rodzaj zakłócenia *coded jamming*. Dzisiaj uważa się, że jest to forma cyberataku DoS, blokująca funkcjonalność PNT odbiornika GPS z chwilą, gdy musi on wykonać zimny start lub reakwizycję satelitów GPS. Kodowany *jamming* stanowi więc potencjalną i niewidoczną dla odbiornika GPS pułapkę.

W 2018 r. Amerykanie pokusili się o określenie lokalizacji źródła *jammingu*. Pomiar był skomplikowany, zależał od parametrów ruchu stacji ISS po orbicie. Wynik obliczeń wszystkich zaskoczył: źródło *jammingu* GPS „znad Morza Czarnego" znajdowało się o kilkaset kilometrów dalej, w basenie Morza Śródziemnego. Okazało się, że nadajnik zagłuszający umiejscowiony był na terenie rosyjskiej bazy wojskowej w Syrii[4]. Wygląda na to, że zakłócenia GPS na terenie Polski są prawdopodobnie spowodowane podobnym *jammingiem* GPS wywoływanym przez Rosję z jej terytorium.

## PNT w ryzach

Często błędnie zakładamy, że czas i pozycja odbiornika GNSS są przesyłane z kosmosu, a odbiornik satelitarny działa jak karta sieciowa LAN. W rzeczywistości parametry PNT wyznaczane są w odbiornikach GPS na Ziemi i każdy robi to nieco inaczej. W konsekwencji nie ma dwóch bliźniaczych odbiorników wyznaczających jednocześnie te same parametry PNT. Różnica wskazań PNT jest miarą oczekiwanej dokładności i błędu odbiornika. Dzieje się tak, ponieważ odbiornik GPS musi sporo policzyć, a jego przetwarzanie – mimo zgodności sprzętu i *firmware* – jest asynchroniczne.

Problem utrzymania zgodności PNT odbiorników rozproszonych na dużym obszarze kraju czy kontynentu rozwiązuje się za pomocą sztucznej inteligencji (SI), która używając metod statystycznych potrafi zminimalizować niepewność pomiaru (szum) *jitter*. Wbudowana w firmware odbiorników SI dla DSP pozwala rozpoznawać zakłócenia, takie jak odbicia, opóźnienia, zagłuszanie i fałszowanie sygnałów GNSS. W celu zwiększenia cyberodporności na ataki DoS, odbiorniki GPS mogą korzystać z naziemnych poprawek A-GPS (GSM), RTK drogą radiową, a te wyposażone w łączność mobilną 4G/5G mogą otrzymywać wsparcie synchronizacji z wykorzystaniem NTP i PTP IEEE1588. Coraz więcej odbiorników korzysta z telemetrii satelitów LEO i geostacjonarnych stellitów SBAS (EGNOS).

Rozumiejąc niepewność GPS, Amerykanie jako pierwsi zalecili w 2020 r. dywersyfikację ryzyka PNT i używanie naziemnych struktur dystrybucji czasu z NIST (dyrektywa EO13905[5]). W styczniu 2023 r., Komisja Europejska opublikowała zaktualizowaną dyrektywę NIS2, która w ślad za doktryną USA zaleca krajom członkowskim UE tworzenie alternatywnych naziemnych systemów A-PNT (*ang. Assured Piositiong Navigation and Timing*).

## Czas pod kontrolą

Uznanie synchronizacji za obszar cyberbezpieczeństwa wymaga aktualizacji procedur operacyjnych, zarówno na

1 https://navi.ion.org/content/68/4/673, https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf
2 https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf
3 https://space.skyrocket.de/doc_sdat/stp-h5.htm
4 https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf
5 https://www.govinfo.gov/app/details/DCPD-202000071

szczeblu państwowym, jak i w lokalnych środowiskach pracy. Kluczowym elementem jest edukacja, która podnosi świadomość znaczenia utrzymania stabilnej domeny czasu UTC (uniwersalnego czasu skoordynowanego) dla nowoczesnych technologii informatycznych (IT) i systemów sterowania (OT) zarówno w czasie pokoju, jak i w przypadku konfliktu.

Odbiorniki GNSS (korzystające z GPS) wyprodukowane przed 2022 r. nie są odporne na zakłócenia typu *jamming* i *spoofing*. W Polsce, podobnie jak w innych krajach, funkcjonuje bliżej nieznana duża liczba urządzeń wykorzystujących odbiorniki satelitarne, które pomimo deklaracji producenta, zamiast korzystać z systemów GPS+GALILEO, synchronizują się do rosyjskiego GLONASS i chińskiego BEIDOU.

> *Krajowi posiadacze starszych serwerów NTP, niezależnie od marki, powinni rozważyć wymianę urządzeń.*

Dobrym kandydatem w miejsce starszych urządzeń są krajowe serwery NTP/PTP firmy ELPROMA. Posiadają kodyfikację NATO i certyfikację metrologiczną Głównego Urzędu Miar RP.

Polskie serwery czasu używane w NATO.

## eCzasPL

Polska wcześniej niż USA i Wielka Brytania zauważyła konieczność wyodrębnienia czasu urzędowego i zaczęła go chronić prawnie. Polscy użytkownicy powinni wziąć pod uwagę dołączenie swoich infrastruktur IT/OT do krajowego systemu bezpiecznej synchronizacji eCzasPL[6] Głównego Urzędu Miar RP, który niezależnie od GPS dostarcza uwierzytelniony kryptograficznie polski czas urzędowy UTC(PL) za pomocą sieci Internet i dedykowanych łączy Ethernet. System został oddany do użytku na dwa tygodnie przed pierwszymi zakłóceniami sygnałów GPS nad Polską. Technologia eCzasPL została opracowana w latach 2015–2016 przez inżynierów polskiej firmy ELPROMA[7], którzy uczestniczyli w europejskim projekcie Horizon 2020 o nazwie DEMETRA[8]. Obecnie technologia eCzasPL jest kompletnym rozwiązaniem oferowanym na eksport przez polskie konsorcjum firm ELPROMA i PIK Time[9]. Rozwiązanie to obejmuje również projekt i wyposażenie laboratorium w zegary atomowe.

Polski serwer czasu firmy ELPROMA model NTS-5000 z anty-jammingiem i anty-spoofingiem GPS (LEVEL-1). Takich serwerów dołączonych bezpośrednio do zegarów atomowych używa projekt eCzasPL

Możliwe jest włączenie odizolowanych od Internetu systemów korporacyjnych ICT i sieci infrastrukturalnych OT do eCzasPL. Takie połączenie jest realizowane na poziomie trzecim oznaczonym etykietą LEVEL-3 za pomocą urządzenia GNSS-firewall. Urządzenie to symuluje sygnał satelitarny GNSS na podstawie wzorca UTC(PL) czasu urzędowego określonego w ustawie o czasie urzędowym.

Symulator LEVEL-3 pobiera czasu urzędowy z systemu eCzasPL i konwertuje na sygnał antenowy serwerów ELPROMA NTS-5000, NTS-4000, NTS-3000. W ten sposób tworzy się źródło czasu UTC niezależne od jammingu/spoofingu GPS nad Polską.

Tak długo, jak rozproszone systemy informatyczne mają dostęp do Internetu, zasoby te mogą korzystać z systemu eCzasPL. Należy się jednak liczyć z zagrożeniem, że zcentralizowana struktura informatyczna GUM RP może ulec ograniczeniom funkcjonalności wywołanym hybrydowym atakiem DoS/DDoS na krajową metrologię. Dlatego tak ważne jest posiadanie systemu monitorowania sygnałów GNSS, który wysyłając alarmy, pozwoli na czas uruchomić awaryj-

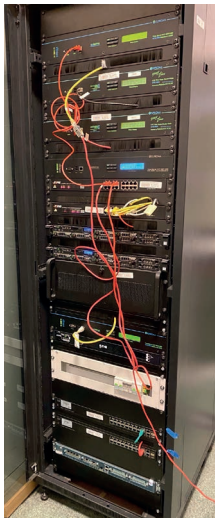
6 https://www.gum.gov.pl/pl/projekty-eu/e-czaspl/3632,e-CzasPL.html.

7 www.elpromaelectronics.com

8 https://www.ion.org/publications/abstract.cfm?articleID=14982

9 https://www.piktime.com

ne procedury postępowania, a w szczególności – w razie konfliktu zbrojnego – mobilne wzorce UTC, tzw. defibrylatory UTC (urządzenia klasy TIME LOADER).



Polski „defibrylator UTC" firmy ELPROMA.

Węzeł autonomicznej synchronizacji UTC w Polskiej Agencji Żeglugi Powietrznej.

Wyposazony jest w zegary atomowe podtrzymujące czas przy braku GPS.

## Czas na wojnie

Wojsko musi zapewnić zgodną domenę czasu dla systemów i składowych OT nie tylko podczas pokoju, ale również podczas konfliktu zbrojnego. Z pomocą przychodzą przenośne systemy podtrzymania czasu UTC z wbudowanym akumulatorem i z wysokiej klasy oscylatorami kwarcowymi lub rubidowymi o dobrej stabilności długoterminowej. Urządzenia takie są już na wyposażeniu taktycznego działania armii w Izraelu. Wspierają pracę systemów autonomicznych UAV, radarów/EO, systemów obrony przeciwrakietowej i dowolnych innych systemów naziemnych, morskich i powietrzno-desantowych, wymagających zewnętrznej synchronizacji ToD/1PPS w czasie rzeczywistym w zabronionych środowiskach dostępności GPS (GNSS).

Innym alternatywnym źródłem UTC dla wojska może być sieć publicznych serwerów NTP dostępnych w Internecie, NTPPOOL[10]. Niestety, korzystanie z tych serwerów wiąże się z ryzykiem, ponieważ nie zawsze wiadomo, kto nimi zarządza i skąd pochodzi źródło czasu UTC. Od czasu wybuchu wojny na Ukrainie liczba publicznych serwerów NTPPOOL w Rosji[11] wzrosła o około 20 proc. – do 200 szt. Istnieje techniczna możliwość utrzymywania przez Rosję serwerów NTP również poza granicami kraju[12].

Dla porównania, od czasu wybuchu wojny w Ukrainie w 2022 r. aspirująca do wejścia do NATO Szwecja zwiększyła liczbę swoich publicznych serwerów NTP aż dwukrotnie. Dwa lata wcześniej wzrost odnotowała Finlandia. Niemcy zwiększyły liczbę publicznych serwerów NTP skokowo w roku aneksji Krymu (2014). Obecnie łączna liczba publicznych serwerów w Niemczech wynosi aż 900.

Przy budowie wewnętrznego korporacyjnego systemu zarządzania czasem trzeba mieć na uwadze, że bezpieczna synchronizacja nie może się bazować na pojedynczym serwerze NTP/PTP. Jako niezbędne minimum uważa się użycie w pojedynczym węźle co najmniej kilku serwerów czasu skonfigurowanych do pracy w układzie redundancji i zapewniających również agregację (bezwładność pracy bez GPS) swoich zegarów. **Firma ELPROMA wspiera w tym zakresie krajowy przemysł i biznes. Prowadzi doradztwo i nieodpłatne konsultacje, jak włączyć wewnętrzne sieci informatyczne do państwowego systemu wiarygodnej synchronizacji czasem urzędowym UTC(PL) – eCzasPL Głównego Urzędu Miar RP.** Używanie eCzasPL jest bezpłatne dla użytkowników krajowych i podmiotów zarejestrowanych w Polsce.



10 https://www.ntppool.org/en/

11 https://www.ntppool.org/zone/ru

12 https://gist.github.com/mutin-sa/eea1c396b1e610a2da1e5550d94b0453