CYBERBEZPIECZEŃSTWO VS. SZTUCZNA INTELIGENCJA

INFORMATYKA – PRAWO – ZARZĄDZANIE

POD REDAKCJĄ NAUKOWĄ

BOLESŁAWA SZAFRAŃSKIEGO

Wojskowa Akademia Techniczna

Cyberbezpieczeństwo vs. Sztuczna Inteligencja
Rozdział XV

Desynchronizacja IT/OT infrastruktury krytycznej – jak monitorować i zapobiegać

Tomasz Widomski
ELPROMA Elektronika Sp. z o.o.
05-152 Czosnów, ul. Duńska 2a

Sztuczna inteligencja (SI) odgrywa coraz istotniejszą rolę w informatyce, również w kontekście badań oryginalności sygnałów satelitarnych GNSS jako źródeł telemetrii PNT do wyznaczania pozycji (P), nawigacji (N) i czasu (T) w odbiornikach pracujących na Ziemi. Wspiera to wykrywanie zagrożeń takich jak jamming i spoofing GPS oraz pomaga lokalizować źródła zakłóceń. Dotychczas obszar ten pozostawał w sferze zainteresowań obronności, ale rosnąca zależność cywilnych systemów informatycznych (IT) i sterowania automatyką w Przemyśle 4.0 (OT) od technik satelitarnych GNSS wymusza redefinicję zagrożeń bezpieczeństwa. Przyjrzymy się, gdzie technologie oparte na SI są wykorzystywane do interpretacji zdarzeń związanych z GNSS, a także jakie wyzwania stawiają zagrożenia związane z jammingiem i spoofingiem GPS w sferze zapewnienia stabilności pracy infrastruktur krytycznych, które opisuje dyrektywa unijna NIS2[1]. Autor zachęca do zapoznania się z pozycją[2] literatury [1] będącej ważnym wstępem do poruszanej tu tematyki. Rozdział zawiera obszerne fragmenty pracy dyplomowej autora studiów MBA Cyberbezpieczeństwo p.t. „Analiza zjawiska desynchronizacji czasu jako nowej cyber-broni destabilizującej infrastruktury krytyczne państwa" (WAT czerwiec 2024) [15].

1. Wstęp

Działania Rosji, polegające na zakłócaniu GPS w Syrii i w Ukrainie, odsłoniły duże możliwości operacyjne Rosji także poza obszarem działań wojennych. Wydaje się, że umiejętne zakłócanie sygnałów GNSS może być skuteczną bronią. Pozwala blokować funkcje PNT każdego odbiornika satelitarnego na Ziemi, a w warunkach działań hybrydowych skutecznie wspierać może destabilizację infrastruktur krytycznych państwa. W przypadku konfliktu, może tym samym wpływać na głębię logistyczną NATO. Stało się to możliwe przez zbyt dużą zależność systemów IT/OT od funkcjonalności PNT, zwłaszcza od satelitarnego systemu GPS, ale i innych systemów rodziny GNSS (rysunki 1 i 2).

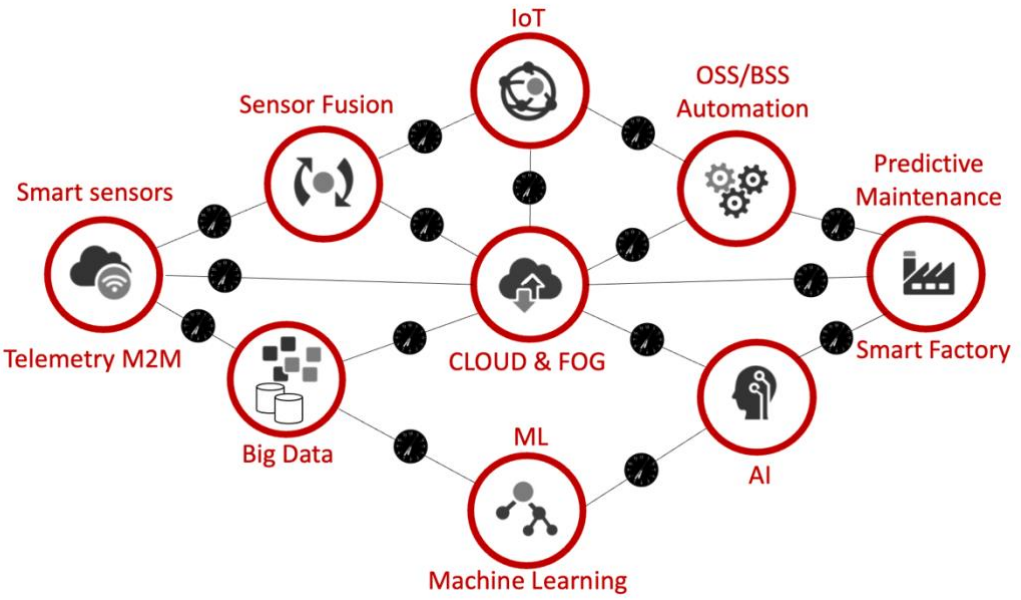
[1] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en.

[2] Paluszyński, „Niedoceniane zagrożenie – źródło i dystrybucja czasu", [w:] B. Szafrański (red.) *Cyberbezpieczeństwo – redefinicja zagrożeń*, s. 177–214, WAT, Warszawa 2023.

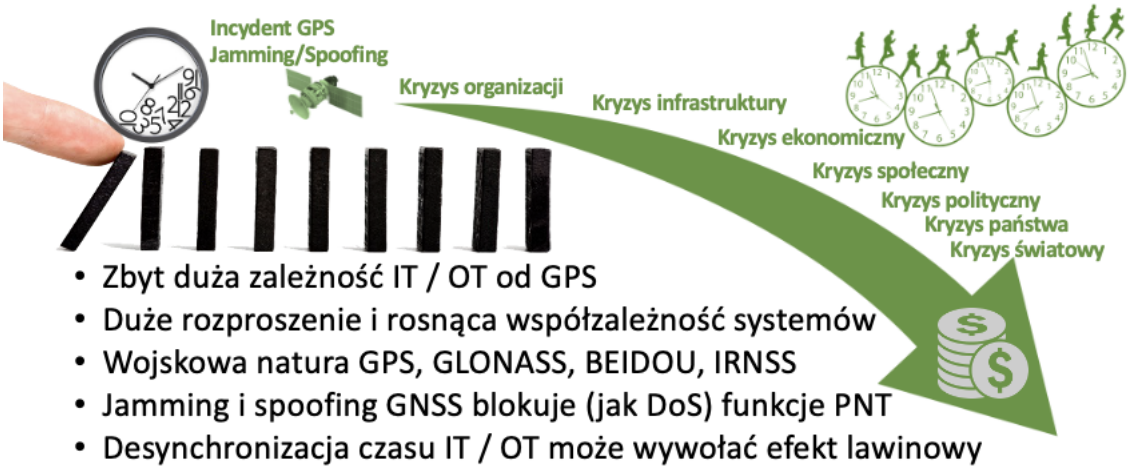
Rys.1. Stabilność głębi logistycznej NATO zależy od systemów kierowania ruchem kolejowym, które ściśle zależą od GPS. Awaria serwerów czasu NTP w dniu 17 marca 2022r, wstrzymała na wiele godzin ruch pociągów we wschodniej Polsce.
Źródło: prezentacja Elproma na V konferencji „Bezpieczeństwo na kolei" (Gdynia, grudzień 2023)

Rys. 2. Stabilna synchronizacja rozproszonych systemów OT jest niezbędna do koordynacji procesów produkcyjnych w przemyśle 4.0, ale używają jej również chroniące ten przemysł systemy obrony przeciwlotniczej. Ma to wpływ na stabilność głębi logistycznej podczas konfliktu zbrojnego.
Źródło: własne (licencja)

Rewolucja przemysłowa 4.0 i trwająca transformacja cyfrowa zwiększa poziom zagrożenia stabilności pracy systemów informatycznych, wprowadzając niewidoczne dla nas silne powiązania poszczególnych grup rozwiązań IT i OT, które wcześniej były od siebie i niezależne (rysunek 3). Scenariusz eskalacji kryzysu opartego o celowe zakłócanie sygnałów GPS, a w konsekwencji desynchronizację coraz większej i bardziej rozpraszającej się architektury informatycznej powinien być dziś brany pod uwagę (rysunek 4).



Rys. 3. Skorelowana w domenie czasu UTC współzależność grup systemów w przemyśle 4.0.
Źródło: własne na konferencji ITSF 2021 Brighton, Wielka Brytania



Rys. 4. Incydent zakłócania GPS wnosi ryzyko efektu lawinowego awarii technicznych w IT i OT wywołujących eskalujący kryzys
Źródło: własne dla MBA Cyberbezpieczeństwo WAT

Okazuje się, że we współczesnej technice prościej jest destabilizować pracę całych systemów IT/OT manipulując czasem (niskopoziomowymi ustawieniami zegarów programowych w systemach operacyjnych i w *firmware* urządzeń), niż włamywać się do dobrze zabezpieczonych, odizolowanych od Internetu sieci wewnętrznych LAN. Najważniejsze sieci infrastrukturalne używają precyzyjnego czasu do synchronizacji swoich zasobów. Zgodny czas, podobnie jak dyrygent orkiestry, koordynuje pracę niezależnych urządzeń komunikujących się. Zapewnienia *funkcjonalność* całego rozwiązania opartego na fuzji poszczególnych elementów sieciowych, *wydajność* (optymalne wykorzystanie zasobów) i *stabilność* odpowiedzialną za bezawaryjność i bezpieczeństwo każdej rozproszonej współczesnej architektury IT/OT. Synchronizacją można stosunkowo prosto manipulować, np. używając jammingu i spoofingu GPS, od którego technika zrobiła się w ostatnich latach zbyt zależna (rysunek 3 i 4). Podatne są wszystkie sektory gospodarki i obsługujące je sieci infrastrukturalne, które opisuje dyrektywa unijna NIS2[1]:

- **energia** (OZE/atom/kopalne/biomasy, smart metering, zarządzanie smart grid),
- **transport** (lotniczy, kolejowy, drogowy, zarządzanie portami morskimi),
- **bankowość** i ubezpieczenia,
- **giełda papierów wartościowych** i giełdy towarowe,
- **zdrowie publiczne**,
- **woda** (produkcja i dystrybucja),
- **ścieki** i zanieczyszczenia (utylizacja),
- **infrastruktura cyfrowa** (serwery DNS, routery, sieci, chmura i centra danych),
- **administracja publiczna** (związek z transformacją cyfrową i odejściem od papieru),
- **obronność** (wojsko, przemysł kosmiczny, nauka),
- **żywność** (produkcja, przetwarzanie i dystrybucja).

Rozsynchronizowanie sieci infrastrukturalnych IT/OT, może już dziś prowadzić do awarii o nieprzewidywalnych konsekwencjach. Coraz częściej ostrzega się przed widmem wielkiej awarii, która może wywołać efekt domina. Dlatego synchronizacja stała się elementem cyberbezpieczeństwa. Ryzyko skutecznego użycia jammingu i spoofingu GPS nie może być pominięte. Rygor utrzymania dyscypliny synchronizacji narzucają rekomendacji ITU, IEEE, ESMA/SEC. Określają parametry czasu i częstotliwości (T&F) i wymogi ich utrzymania w coraz wyższych granicach precyzji. Na przykład w smart grid dokładność czasu (T) określa dokument IEEE C37.238, który wymaga od serwerów czasu dokładności lepszej niż 200 nanosekund (ns). Wewnątrz infrastruktury 5G potrzebna jest dokładność UTC względem GPS większa niż 10 nanosekund po to, aby na dużym obszarze kraju utrzymać poziom synchronizacji urządzeń poniżej 1 mikrosekundy (μs). Parametry dokładności T&F dla telekomunikacji 5G określa grupa robocza ITU o identyfikatorze SG15, a jej prace podlegają pod ITU WP7A odpowiedzialną za skalę czasu UTC. Niespełnienie rekomendacji grozi stabilnością pasm logicznych w światłowodach i radiowych BTS wpływając na wydajności całej sieci 5G. W przypadku telewizji naziemnej DVB-T2 rozsynchronizowane BTS spowoduje automatyczne ich wyłączenie odcinając dostęp do telewizji w regionie. Sektor finansowy podlega dyrektywie ESMA MiFID II. Na giełdach

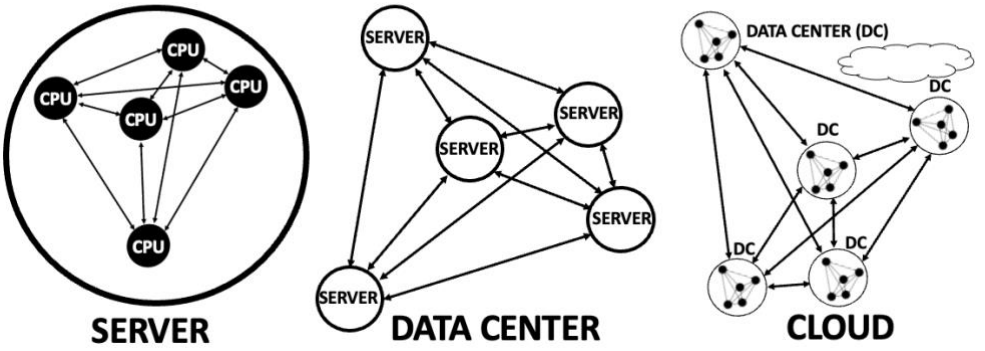
stwierdzenie „czas to pieniądz” ma dosłowne znaczenie i bardzo dużą mierzalną wartość strat. Zautomatyzowane inwestycje HFT (*ang. High Frequency Trading*) objęte są rygorem zapewnienia dokładności 100 μs UTC wszystkich giełd finansowych na świecie. Z tego powodu serwerownie amerykańskiej firmy Equinix są zsynchronizowane z dokładnością aż 1μs. Tyle wynosi maksymalny błąd między wschodnim a zachodnim wybrzeżem serwerowni Equinix w USA. Zestawienie wymaganych dokładności ilustruje tabela (rysunek 5).

Najczęściej jednak bagatelizujemy nie te wielkie, a te z pozoru niewielkie dokładności milisekundowe (ms) rozwiązań pracujących w naszym pobliżu. Zapominamy, że od synchronizacji zależy kompletność kopii zapasowych (backupów) transakcyjnych baz danych SQL. Prawidłowy czas i data używane są certyfikatach uwierzytelniających SSL i szyfrowaniu. Pewnych niewielkich dokładności synchronizacji wymaga nawet *blockchain*. Prawidłowy czas determinuje chronologię zapisu zdarzeń w dziennikach LOG. Brak chronologii w LOG na zawsze uniemożliwia identyfikację przyczyny awarii. Znaczniki czasu są używane w systemie plików systemu operacyjnego oraz w jądrze OS kernel. W większości przypadków niedoceniana rola czasu wynika z ukrytej funkcji jakie wykonuje w tle system operacyjny (np. zarządzanie współbieżnością, porządkowanie zasobów pamięci RAM, defragmentacja plików). Któż z nas pamięta na co dzień, że synchronizacja jest ważna w fazie rozruchowej ładowania oprogramowania w wieloprocesorowym środowisku (CPU).

Sector	Accuracy	Resilience	Threats	Immutability	Scale	Traceability	Intuitive
Power	1μs	★★★	★★★	★	1,000s	★	★
Telecoms	1μs	★★★	★★★	★	10,000s	★	★
Military	10μs	★★★	★★★	★★	10,000s	★	★
Finance	100μs	★★	★★★	★★★	10,000s	★★★	★★
Gambling	1ms	★	★	★★★	10,000s	★★★	★
Real-time bidding	1ms	★	★	★★	10,000s	★★	★
Gaming	1ms	★	★	★★★	10,000s	★★	★
Media	1ms	★★	★★★	★	10,000s	★	★★
GNSS Monitoring	1ms	★★	★★★	★	10,000s	★	★★
Enterprise	1ms	★	★★★	★★	100,000s	★★	★★
Smart factories	1ms	★★★	★★★	★★★	1,000,000s	★	★★
Transport	1ms	★★	★★★	★	1,000,000s	★★	★★★
Digital currencies	1ms	★★	★★	★★★	10,000,000s	★★★	★
Insurance	100ms	★★	★	★★★	10,000,000s	★★★	★
Payments	10ms	★★	★★★	★★★	10,000,000s	★★★	★★★
Health	10ms	★★	★★★	★★★	10,000,000s	★★★	★★★

Rys. 5. Porównanie dokładności protokołów NTP, PTP, PTP+PT*M* i WR.
*Z*estawienie rygoru *wymogu* precyzji czasu segmentami *oraz* pożądan*a* odporności na zagrożenie.
Źródło: Network Time Foundation we współpracy z EUSPA

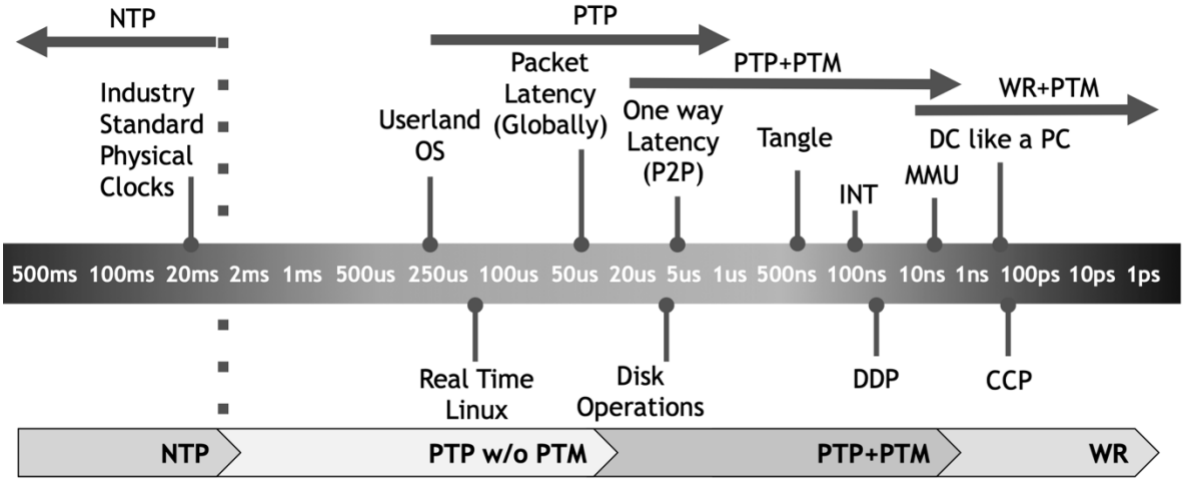
Dzisiaj precyzyjny czas nie jest już tylko kwestią narodowej metrologii (NMI), ale również stanowi istotny czynnik łączący technologie informatyczne IT i OT, wpływając na ich bezpieczeństwo oraz wydajność. Dlatego desynchronizacja jest współczesną cyber-bronią. Stopień zagrożenia jest zróżnicowany. Zależy od złożoności, typu rozproszenia architektury oraz wymaganego prawem nieprzekraczalnego maksymalnego błędu czasu. Im większa żądana dokładność i stabilność synchronizacji, tym rozwiązanie jest podatniejsze na atak desynchronizacji. W większości systemów IT i OT rozproszenie jest rozumiane w sensie zewnętrznej rozległości, ale może również oznaczać wzrost złożoności wewnętrznej w granicy pojedynczego urządzenia lub systemu (rysunek 6).



a b c

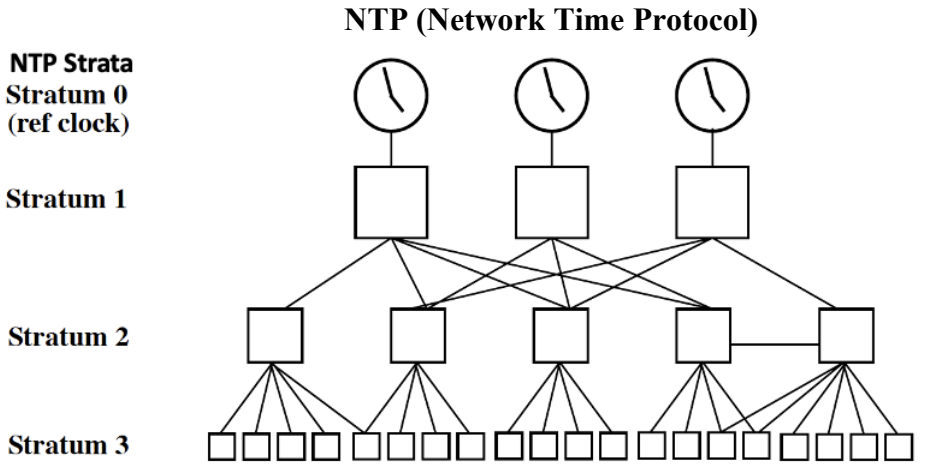
Rys. 6. (a) rozproszenie do wewnątrz (b) rozproszenie w sieci (c) złożony model hybrydowy
Źródło: własne

Prostym przykładem zewnętrznej architektury rozproszonej są klasyczne sieci komputerowe (rysunek 6.b), w których komputery i inne urządzenia są połączone w celu wymiany informacji. Rozproszenie można także rozważać jako cechę wewnętrzną pojedynczego urządzenia. Przykładem są wieloprocesorowe kontrolery macierzy dyskowych, płyty główne i modułowe klastry serwerów (rysunek 6.a). Są również złożone hybrydowe modele rozproszenia, które łączą zarówno elementy zewnętrzne, jak i wewnętrzne w wielopoziomową, często bardzo skomplikowaną strukturę. Przykładem jest chmura (rysunek 6.c). Synchronizacja cloud jest prawdziwym wyzwaniem, ponieważ obejmuje wiele poziomów od nanoskali wieloprocesorowych kontrolerów dyskowych, przez urządzenia sieciowe, po rozproszenie całych serwerowni używających zmiennego w czasie szyfrowania do ochrony kanałów komunikacyjnych. Zapominaną cechą chmury jest równy czas dostępu do danych niezależny od fizycznej lokalizacji użytkownika (punktu dostępu). Z kolei odpowiednie podzielenie danych (rozdrobnienie), kompresja, zwielokrotnienie kopii zapasowych, ich globalne rozproszenie, daje chmurze zdolność odzyskiwania utraconej informacji nawet w przypadku bardzo dużych awarii.

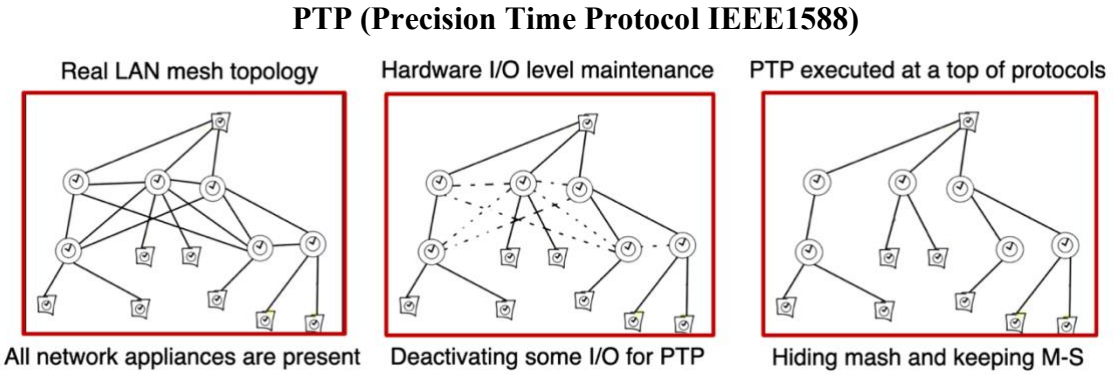


Rys. 7. Porównanie protokołów synchronizacyjnych: NTP, PTP, PTP+PTM i White Rabbit (WR).
Źródło: Facebook - Ahmad Byagowi

Dlatego synchronizacja architektury rozproszonej IT/OT opiera się na modelu hierarchicznym zegarów programowych działających na poziomie systemu operacyjnego. Topologia sieci synchronizacji może się różnić od topologii sieci fizycznej i przepływu danych opartych na TCP/IP, chociaż obie bazują na tej samej fizycznej sieci szkieletowej. Przykładem takiego zróżnicowania jest protokół synchronizacji PTP, który może działać jednocześnie (niezależnie) od protokołu NTP. Oba protokoły wykazują podatność na desynchronizację. Protokół PTP realizuje zapotrzebowanie na duże dokładności, podczas gdy NTP realizuje te mniejsze. Duże nanosekundowe dokładności wymagają używania specjalnych dedykowanych kart sieciowych NIC, łącz i przełączników ETH. W tym celu używa się tzw. znakowanie sprzętowe (*ang. hardware timestamping*). Polega ono na wyliczeniu i korygowaniu opóźnienia jakie wprowadza system operacyjny do chwili wysłania danych siecią LAN (UDP). Konfiguracja PTP zapewnia nanosekundowe (ns) dokładności, a w przypadku WR może osiągać nawet dokładności pikosekundowe (ps). Od roku 2020 wszyscy operatorzy cloud włączając Facebook, Microsoft, Google, AWS itp. rozpoczęli proces wdrażania PTP IEEE1588 zachowując redundantnie NTP w rezerwie.



Rys. 8. Topologia drzewa STRATUM 0-15 synchronizacji NTP
Źródło: własne



Rys. 9. Topologia sieci fizycznej vs. topologia synchronizacji PTP. Przesyłanie zwykłych danych i pakietów synchronizacyjnych PTP odbywać się powinno inną drogą.
Źródło: własne

2. Niedoceniane zagrożenie – źródło i dystrybucja czasu

Desynchronizacja to inaczej mówiąc rozsynchronizowanie zegarów. Wszystkie urządzenia dołączane do sieci komputerowej wyposażone są w zegar. Każdy system operacyjny posiada na poziomie jądra *kernel* zegar programowy wymagający zsynchronizowania do UTC. Według Wiesława Paluszyńskiego[3] z Polskiego Towarzystwa Informatycznego, desynchronizacja stanowi poważne zagrożenie[4] dla współczesnych infrastruktur krytycznych, ponieważ może zaburzyć parametry pracy na różnych poziomach sprzętu, oprogramowania systemowego, komunikacji oraz aplikacji. Można to porównać do arytmii serca dla ludzkiego organizmu. Rozsynchronizowanie w IT i OT wpływa na obniżenia wydajności komunikacji, nieprawidłowości funkcyjnej rozwiązania, a w skrajnych przypadkach do awarii krytycznej *blackout* całego systemu.

Tab. 1. Porównanie wpływu arytmii serca na organizm ludzki i desynchronizacji zakłóceniem GPS

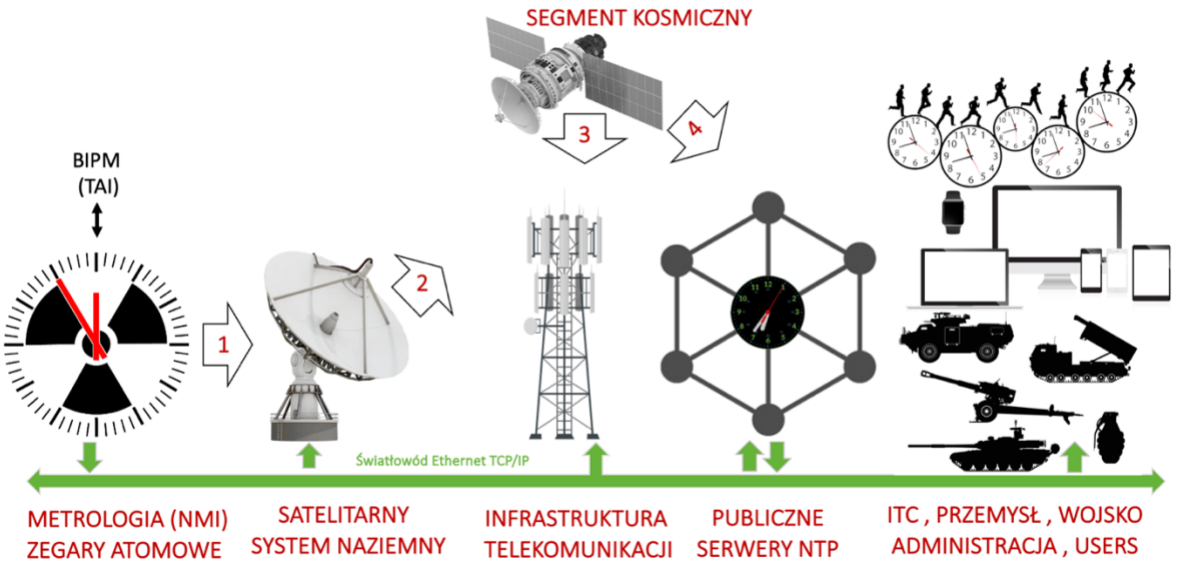
Arytmia serca (organizm ludzki)	**Zakłócenia GPS (infrastruktura krytyczna)**
• niewydolność organizmu, • choroba lub zapaść, • śmierć.	• mniejsza wydajność pracy systemów IT/OT, • incydent lub awaria, • awaria krytyczna - blackout infrastruktury.

Rozsynchronizowanie zegarów w urządzeniach sieciowych podłączonych do sieci prowadzi również pośrednio do zaburzenia prawidłowości obliczeń opóźnień *delay* w przepływie informacji. Przypomina to problem podróży emisariuszy w wielkim imperium mongolskim Dzingis Chana w XIII wieku, gdzie informacje przekazywane do władcy były już przestarzałe z powodu ogromnej odległości do przebycia, a zdobyte tereny mogły być ponownie do tego czasu utracone. W przypadku systemów automatyki przemysłowej OT, może to doprowadzić do użycia zdezaktualizowanych danych i odrzucenia prawidłowych informacji. W konsekwencji sterowane coraz częściej predykcją SI systemy informatyczne mogą podjąć błędną decyzję zarządzającą. Inspiracją do predykcyjnego sterowania były przemysłowe systemy QoS (*ang. Quality of Service*) wykorzystujące uczenie maszynowe. Zamykając analizę odczytanych danych w pętli sprzężenia zwrotnego PLL, stworzono predykcyjny mechanizm sterowania, pozwalający przewidywać stan w kolejnych chwilach i dopasowujący doń precyzyjnie parametry sterujące. Ponadto zaburzenie chronologii zdarzeń zapisanych w dzienniku LOG tworzy paradoks, w którym skutek może wyprzedzić swoją przyczyną. Uniemożliwi to logiczną analizę błędów, a więc ostatecznie również poznanie prawdziwej przyczyny awarii. To determinuje nowy rodzaj zagrożenia i definiuje dwa rodzaje nowych cyberataków:

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

[3] . Paluszyński, „Niedoceniane zagrożenie – źródło i dystrybucja czasu", [w:] B. Szafrański (red.) *Cyberbezpieczeństwo – redefinicja zagrożeń*, s. 177–214, WAT, Warszawa 2023.

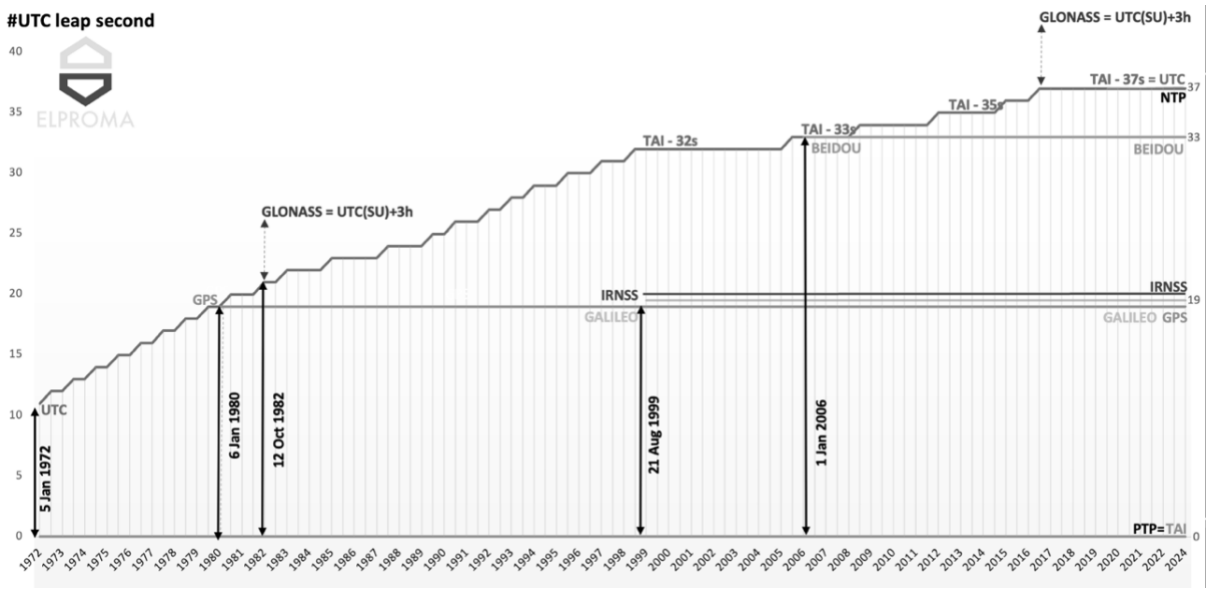
[4] Wywiad z Prezesem PTI, Wiesławem Paluszyńskim dla eCzasPL: https://youtu.be/smRxpEoyEDw.



Rys. 10. Struktura powstawania i dystrybucji czasu UTC w chronologii od lewej do prawej, od powstania w laboratorium narodowej metrologii NMI (w Polsce GUM RP), przez dystrybucję siecią Ethernet i radiowym systemem (np. GPS lub fale długie kHz), do systemów pośredniczących redystrybucją UTC (np. publiczne serwery czasu grupy NTPPOOL), aż do odbiorców końcowych (przemysł, administracja, biznes, infrastruktury krytyczne, wojsko)
Źródło: własne

Technika komputerowa opiera się na tzw. uniwersalnej skali czasu UTC[5]. To nie jedyna skala czasu, ale jest jedną z najważniejszych dla naszej cywilizacji. Jest wykorzystywana w jądrze systemów operacyjnych takich jak Windows, MacOS, Linux, Unix i ich pochodnych. Systemy te automatycznie dostosowują czas na pulpicie do bieżącej strefy czasowej, ale gdzieś w głębi nie rozróżniają swojego położenia geograficznego i używają zgodny czas UTC. Lokalny czas strefowy jest ważny dla nas ludzi i pozostaje on nieistotny dla maszyn. Skala UTC ma nieregularny charakter wynikający ze znanego problemu sekund przestępnych (*ang. leap second*[6]). Jest to dodawana lub odejmowana bardzo nieregularnie jedna sekunda, mająca na celu kompensację różnicy między obserwowalnym czasem astronomicznym, takim jak historyczny GMT[7], a bardzo stabilnym czasem odmierzanym przez zegary atomowe definiujące wzorzec jednej sekundy. Takich sekund jest obecnie 37. Każda kolejna nowa sekunda przestępna, dodatnia lub ujemna, stanowi duże cyber-zagrożenie dla urządzeń sieciowych IT/OT, które nie wiedzą jak obsługując tę jedną sekundę uniknąć desynchronizacji całego systemu informatycznego. Problem jest tak poważny, że stał się przyczyną nieformalnej zmowy milczenia największych graczy z Doliny Krzemowej skupionych przy Open Computing Project (OCP). W grudniu 2015 r., z powodu zbliżającej się sekundy przestępnej firma CISCO wydała komunikat zalecający użytkownikom wyłączenie posiadanych routerów Catalyst na kilka godzin przed północą UTC i ponowne włączenie dopiero następnego dnia.

[5] https://en.wikipedia.org/wiki/Coordinated_Universal_Time.
[6] https://en.wikipedia.org/wiki/Leap_second.
[7] https://en.wikipedia.org/wiki/Greenwich_Mean_Time.



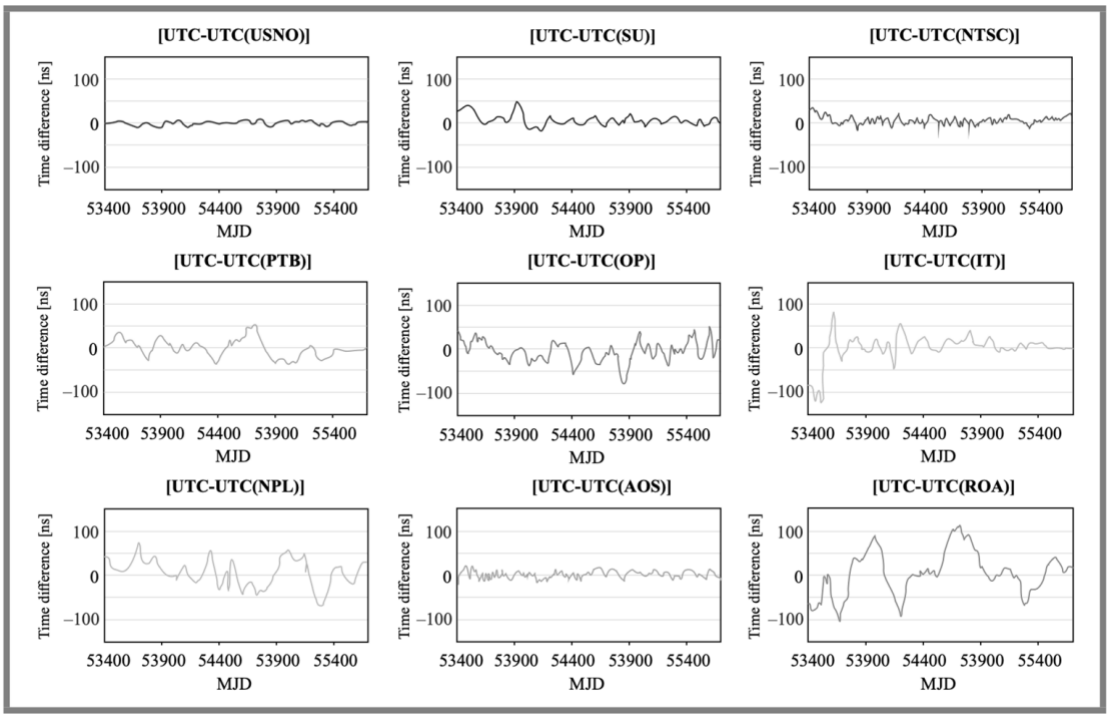
Rys. 11. Porównanie skal czasu UTC, TAI, NTP, PTP i wewnętrzne satelitarne grupy GNSS
Źródło: własne w oparciu o dane z 2024 roku

Skala UTC zawiera „luki czasowe" spowodowane obecnością sekund przestępnych. Są one odpowiedzialne za schodkową, nieciągłą charakterystykę skali UTC (rysunek 11). Brak standardu obsługi sekund przestępnych UTC jest przyczyną rozsynchronizowywania wnętrza infrastruktury IT/OT. Jedne systemy wytracają tę sekundę płynnie, a inne skokowo tworząc max. błąd 1 s. Nieoczekiwane większe niż sekunda błędy wynikają z przepełnień numerycznych w odbiornikach GPS używanych jako źródło UTC w kontrolerach PLC i sieciowych serwerach czasu NTP/PTP. To uprawnia do stawienia pytań o techniczną możliwość pośredniego wpływania desynchronizacją na awarię sprzętu i oprogramowania systemów sterujących w przemyśle podobnych do awarii PKP[8] z dnia 17 marca 2022 roku.

Już podczas samej zapowiedzi sekundy przestępnej za pośrednictwem GPS, jeszcze na wiele tygodni przed jej wprowadzeniem mogą pojawić się niebezpieczne duże skoki liczone w dniach, tygodniach, miesiącach, a nawet latach. Największy udokumentowany błąd synchronizacji wystąpił po dniu 6 kwietnia 2019 i wynosił 19.7 lat. Był związany z przepełnieniem i wyzerowaniem licznika tygodni jakie przekazuje do odbiornika na Ziemi system telemetrii GPS. To dobrze udokumentowany przykład jak dane przesyłane radiem mogą wpłynąć na niestabilność odbiornika satelitarnego. Tak samo manipulując zapowiedzią sekundy przestępnej UTC można być może wpływać na awarię całych systemów IT/OT. To z kolei może powodować eskalację kryzysu, wywołując kolejne awarie zależnych od siebie systemów Przemysłu 4.0. Desynchronizacja może być powodem blokad szyfrowanych kanałów transmisyjnych chmury CLOUD, skutkując odmową dostępu, odrzuceniem prawidłowych certyfikatów SSL. Problem wymaga budowy świadomości administratorów IT oraz utrzymania żelaznej korporacyjnej dyscypliny zarządzania UTC.

[8] Rynek Kolejowy, awaria PKP w dniu 17/03/2022, https://www.rynek-kolejowy.pl/mobile/alstom-nie-bylo-cyberataku-byl-nasz-blad-107195.html.

Skala czasu UTC nie jest jednolita. Współtworzy ją wiele laboratoriów na świecie. Skale UTC(k) poszczególnych państw różnią się nieznacznie na poziomie nanosekund. Z każdą dekadą dokładności te są większe, ponieważ zegary systematycznie „uczą" się wad własnego chodu, porównując go z chodem innych zegarów wzorcowych. Skala UTC dla systemu satelitarnego GPS jest skalą laboratorium USNO w USA i będzie się różnić od skal laboratoriów dostarczających wzorzec do systemów satelitarnych GALILEO, GLONASS, BEIDOU i IRNSS. Wszystkie będą się różnić od polskiej skali czasu urzędowego UTC(PL) jaką wytwarza Główny Urząd Miar RP. Obok GUM RP, drugą niezależną polską skalą czasu jest UTC(AOS) wytwarzaną przez obserwatorium astronomiczne CBK w Borowcu. Dla porównania, Niemcy mają aż cztery niezależne skale UTC, w tym aż dwie należą do Deutsche Telecom T-Mobile. Większa liczba autonomicznych skal czasu w państwie zwiększa bezpieczeństwo przemysłowe tworząc zapasowe, niezależne od GPS źródła czasu.



Rys. 12. Skale UTC poszczególnych państw i laboratoriów różnią się charakterystykami. Źródło: W. Lewandowski, M. Marszalec – Instytut Łączności , Literatura [4]

Jakie znaczenie mają autonomiczne skale czasu UTC dla bezpieczeństwa? Nie zależą od zakłócanego coraz częściej GPS, ani od innych systemów GNSS. Ich bezpośrednie używanie eliminuje ryzyko manipulacji jammingiem i spoofingiem w gospodarce i zapobiega desynchronizacji systemów IT i OT w przemyśle. Autonomiczne skale czasu UTC(k) używane są również do testów bezpieczeństwa odbiorników satelitarnych GNSS. Problem luk bezpieczeństwa w odbiornikach GNSS opisano[9] i w literaturze [1].

Na rynku dostępne są komercyjne odbiorniki GNSS, które nie działają zgodnie z deklaracją producenta. Naszą uwagę zwróciła wiele lat temu firma NVS[10] (rysunek 13).

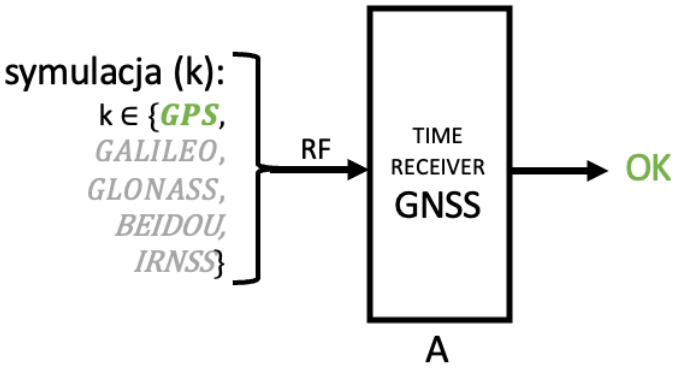
[9] *Cyberbezpieczeństwo redefinicja zagrożeń*, pod redakcją B. Szafrańskiego, rozdział XII „*Niedocenione zagrożenie – źródło i dystrybucja czasu*" – W. Paluszyński (PTI) strony 193-195.

[10] http://www.nvs-gnss.com/products/gnss-receiver.html.

Posiada ona rejestrację zarówno w Szwajcarii jak i w Rosji. Generowany przez odbiornik NV08C wzorzec UTC wykazał w testach cechy koherencji z rosyjską skalą czasu UTC(SU) /SU - Soviet Union/. Jest to wzorzec czasu rosyjskiego wojskowego systemu GLONASS. Mimo widniejącej na etykiecie NV08 nazwy GALILEO układ ten nie obsługuje europejskiego systemu GALILEO, natomiast korzysta z chińskiego systemu BEIDOU.

Rys. 13. Układ odbiornika GNSS „szwajcarskiej" (rosyjskiej) firmy NVS sprzedawany jest globalnie również przez amerykańskich wiodących dystrybutorów podzespołów elektronicznych
Źródło: Internet www.nvs-gnss.com

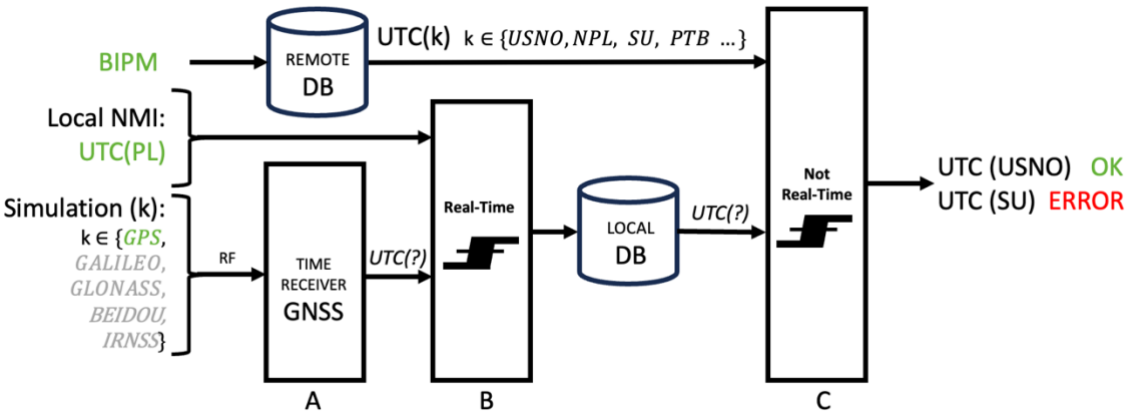
Bardzo trudno jest wykazać, że odbiornik satelitarny GNSS skonfigurowany do odbioru pojedynczego systemu GPS, nie „oszukuje nas" podążając w to miejsce np. za wojskowym rosyjskim systemem GLONASS. Użycie symulatora GNSS ustawionego w tryb pracy GPS powinno dać wiążącą odpowiedź na pytanie o prawdę. Niepowodzenie tej metody (faza A rysunek 14 i 15) należy tłumaczyć tym, że oprogramowanie odbiornika GNSS może rozpoznać symulację GPS i odbiornik będzie się zachowywać w takim teście „grzecznie".



Rys. 14. Zaproponowany w 2024 r. przez EUSPA[11] jednofazowy „A" schemat testowania odbiorników GNSS. Ustawienie symulatora na wybrany pojedynczy system GPS, GALILEO, GLONASS, BEIDOU, IRNSS sprawdza czy jest on obsługiwany przez testowany odbiornik. Taki test nie wykrywa luk bezpieczeństwa odbiornika pozostającego pod „kontrolą" innego niż założenie systemu (np. ustawiony jest GPS, a odbiornika zależy nadal od wojskowego GLONASS).
Źródło: Internet

Prawdziwe intencje odbiornika GNSS odsłoni dopiero rozszerzony test, na którym schemat testowania EUSPA (rysunek 14) stanowi pierwszą fazę „A" trzystopniowej struktury diagnostycznej „A-B-C" (rysunek15). W takim testowaniu pomaga sztuczna inteligencja SI.

[11] https://www.euspa.europa.eu.



Rys. 15. Zaproponowane w 2024 przez Polskę, trójfazowe „A-B-C" badanie laboratoryjne odbiornika jednoznacznie potwierdzi jego ukrytą zależność od niepożądanego systemu GNSS. Źródło: własne dla EUSPA

Rozszerzenie testu o dwie kolejne fazy B i C (rysunek 15) pozwala na analizę sygnału wyjściowego UTC (faza A), jaki „wyprodukuje" odbiornik GNSS w oparciu o wymuszoną na wejściu A konstelację *k* grupy GNSS. Wyjściowy sygnał UTC z fazy A porównywany jest z wzorcem autonomicznej skali czasu urzędowego UTC(PL) Głównego Urzędu Miar.

Faza B pełni rolę testu „przesiewowego" i może być wykonywana na bieżąco w czasie rzeczywistym. Skuteczność rozpoznania luk bezpieczeństwa testowanego odbiornika zależy od algorytmów SI wspieranych uczeniem maszynowym i posiadanej bazy wiedzy korelacji wzorcowego UTC(PL) z innymi skalami czasu zarejestrowanymi w bazach danych BIPM. Pozwala to wstępnie odpowiedzieć na pytanie, czy testowany z pomocą SI odbiornik „udaje" zwierzchność systemu *k* (np. GPS), podczas gdy w rzeczywistości podporządkowany może być „zwierzchności" innego systemu satelitarnego (np. GLONASS). Jednoznaczne potwierdzenie diagnozy możliwe jest w fazie C testów.

Faza C testu jest badaniem „jakościowym" odbiornika opartym o retrospektywną analizę porównawczą badanego UTC-UTC(PL) z archiwum UTC(k) z baz danych BIPM. Jej wynik dostarczany jest z miesięcznym opóźnieniem, ponieważ tyle trwa spływanie danych z laboratoriów narodowej metrologii do BIPM. W analizowanym hipotetycznym przypadku odnalezienie „odcisków palca" koherencji UTC(SU) /SU-Soviet Union/, daje 100% pewność zależności testowanego odbiornika od wojskowego systemu satelitarnego GLONASS. Bardzo ważne jest, aby trójfazowy test A, B i C wykonać z uwzględnieniem zdarzeń:

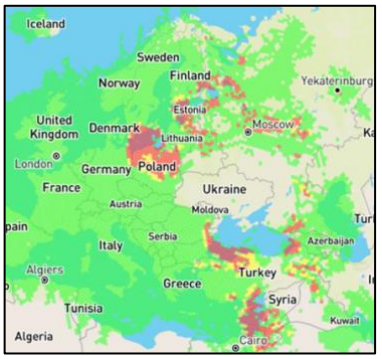
- **zimny start odbiornika GNSS**
- **reakwizycja satelitów przez odbiornik GNSS**

Testy należy prowadzić w środowisku symulacji *sandbox* i z dostępem do fizycznych satelitów. Badać należy wpływ wyłącznie pojedynczych konstelacji GNSS.

3. Jak monitorować i identyfikować źródło jammingu GPS?

W książce pt. *Cyberbezpieczeństwo redefinicja zagrożeń*, pod redakcją B. Szafrańskiego, autor rozdziału XII p.t „*Niedocenione zagrożenie – źródło i dystrybucja czasu*" – W. Paluszyński (PTI) dokonuje przeglądu technik desynchronizacji systemów, obszernie ilustrując przykładami różne rodzaje zagrożeń oraz skutki możliwych ataków na czas (TAS) i opóźnienie (TDA). Zachęcamy do zapoznania się z tą publikacją. która stanowi ważne wprowadzenie do tego akapitu.

Skoncentrujemy się na konkretnym zagrożeniu jakim jest desynchronizacja IT/OT z użyciem techniki zakłócania satelitarnego sygnału GNSS, a dokładniej ujmując systemu GPS. Głównym źródłem informacji o zakłóceniach sygnału GPS stał się od niedawana internetowy serwis *gpsjam.org*, który pokazuje na mapie obszary, gdzie występują nieprawidłowości w odbiorze GPS raportowane przez ruch lotniczy. W dniu 26 grudnia 2023 r. po raz pierwszy na mapie zakłóceń pojawiły się czerwone plamy na terenie Polski. Zakłócenia tego dnia objęły olbrzymi obszar od Danii przez Morze Bałtyckie do praktycznie całego zachodniego wybrzeża morskiego Polski.



23/03/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-03-23
02/03/2024
https://gpsjam.org/?lat=41.49383&lon=44.65934&z=2.1&date=2024-03-02
14/02/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2024-02-14
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
26/12/2024
https://gpsjam.org/?lat=52.29651&lon=19.43511&z=4.2&date=2023-12-26

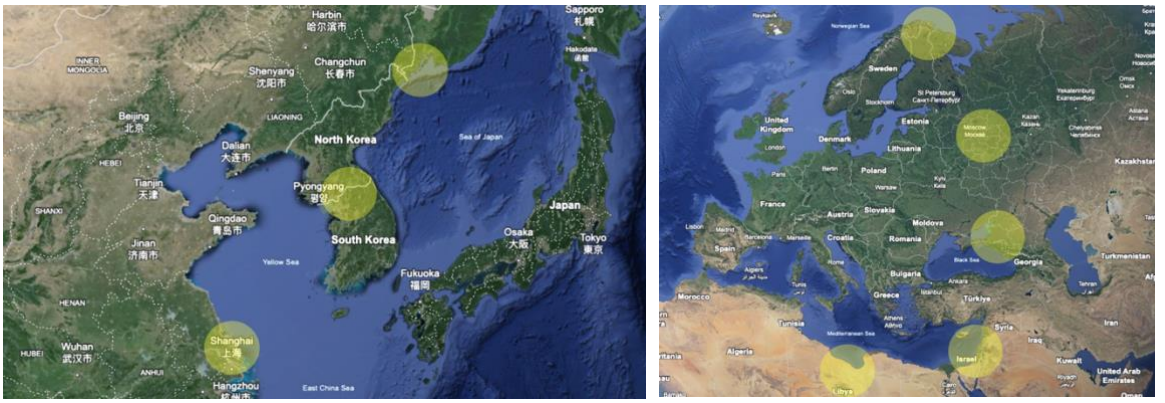
Rys. 16. Pierwsze zakłócenie GPS nad Polską odnotowano w dniu 26/12/2023
Źródło: gpsjam.org

Również służby niemieckie przyznały, że od pewnego czasu w rejonie Morza Bałtyckiego poważnie zakłócany jest sygnał nawigacji GPS. W związku z tym Bundesnetzagentur (Niemiecka Federalna Agencja ds. Sieci), odpowiedzialna m. in. za ochronę elektromagnetyczną, wszczęła dochodzenie w porozumieniu z Bundeswehrą. Niemieckie służby mają zdolność precyzyjnego lokalizowania źródeł zakłóceń, jednak żadne informacje dotyczące wyników badań nie zostały dotychczas udostępnione publicznie. Podobnie jak w przypadku wspomnianych służb szwedzkich i estońskich, podejrzenia Niemców kierują się w stronę rejonu Królewca. Dla rosyjskiej armii zakłócenia GPS nie mają prawdopodobnie znaczenia, gdyż korzysta ona z własnego systemu wojskowej nawigacji satelitarnej GLONASS, wspieranego w zakresie synchronizacji naziemnym radiowym systemem Czajka[12]. Do prowadzenia działań wojskowych, może ona również używać wsparcia dużej liczby rozproszonych w sieci Internet publicznych rosyjskich serwerów czasu

[12] https://en.wikipedia.org/wiki/CHAYKA.

puli NTPPOOL. Mogą one dostarczyć wzorzec UTC ważny podczas zimnego startu odbiornika (ang. *cold start*) i reakwizycji satelitów GNSS.

Udokumentowana historia zakłóceń GPS, ma swój początek w 2011 roku na Półwyspie Koreańskim. Kolejne przypadki odnotowano w rejonie Szanghaju w Chinach i na wschodnim wybrzeżu Rosji. Eskalacja zjawiska objęła rejon Zatoki Perskiej i niektóre kraje Europy. Zakłócenia GPS zaczęto odnotowywać na północy Norwegii w części graniczącej z Rosją, w basenie Morza Czarnego między Krymem a Soczi, a co ciekawe również w Moskwie[13], Libii i Syrii, gdzie od pewnego czasu Rosja posiadała swoje bazy wojskowe. Zaczęto budować stopniową narrację medialną, że świat musi mieć do czynienia z celowym zakłócaniem systemu GPS. W Polsce zakłócenia pojawiły się 26 grudnia 2023 r.



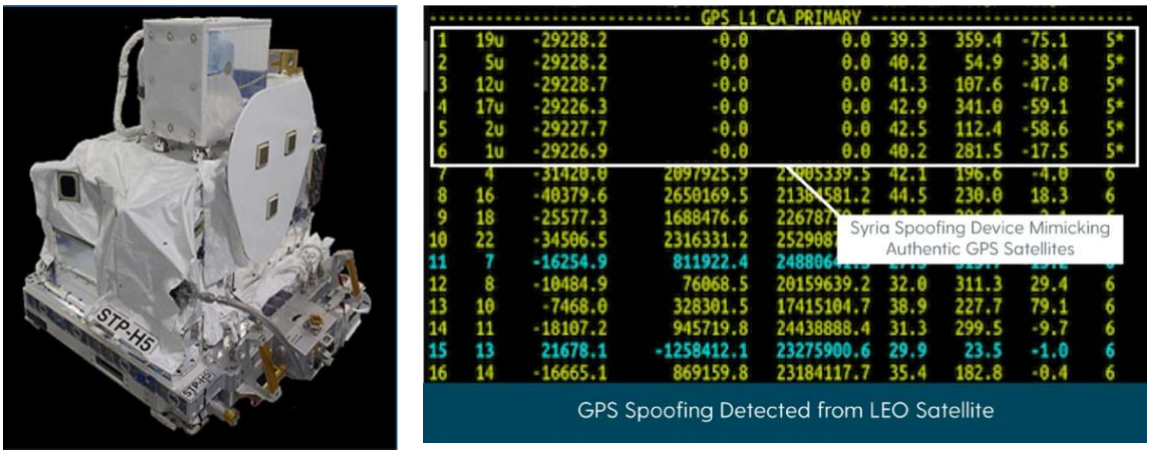
Rys. 17. Pierwsze zakłócenie GPS odnotowano w 2011 r. na Półwyspie Koreańskim. Później pojawiło się na wybrzeżu Chin i Rosji.
W kolejnych latach w Norwegii, Izraelu, Syrii, a po 2014 r. w regionie Morza Czarnego, co zaskakujące również w Moskwie
Źródło: [3], CNN[14]

Choć istnieje wiele teorii i prób wytłumaczenia domniemanego postępowania Rosji, to w rzeczywistości oficjalnie nie znamy nawet rodzaju jammingu, który wystąpił na naszym terenie. Ogólnie wiemy, że istnieją dwie metody zakłócania GPS: zagłuszanie oryginalnego sygnału (GPS jamming) i fałszowanie (GPS spoofing) odbioru poprzez podawanie nieprawdziwych danych pokrywających te oryginalne. W grupie tej używana jest też technika retransmisji radiowej Meaconing[15].

W samej kategorii jammingu GPS możemy rozróżnić podgrupy jammingu PRN, CHIRP jammingu, CODED jammingu. Podobnie w przypadku spoofingu istnieją podgrupy SYNCHRONOUS (synchronicznego), CIRCLE (okrężnego), z retransmisją sygnału MEACONING. Na tym etapie, zwrócimy uwagę na mało znany medialnie fakt – słaby jamming może wywołać efekt spoofingu. Każdy odbiornik reaguje też inaczej na zagrożenie. Prowadzone od 2016 r. przez niezależne zespoły USNO[16] i C4ADS[17,] badania wskazały

[13] CNN, https://www.youtube.com/watch?v=sBYGHkx8yas.
[14] CNN, mirror: https://youtu.be/wM5LVpH1eNo.
[15] https://en.wikipedia.org/wiki/Meaconing.
[16] https://navi.ion.org/content/68/4/673.
https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf.
[17] https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf.

lokalizację źródła zagłuszającego odpowiedzialnego za jamming i spoofing GPS w rejonie Morza Czarnego. Do badań wykorzystano dopplerowskie pomiary sensorem STP-H5 i zainstalowanym na stacji kosmicznej ISS orbitującej 400 km nad powierzchnią Ziemi. Na co dzień STP-H520 służył do badań jonosfery, ale „w wolnych chwilach" mógł wykonać dodatkowe pomiary dla USA. Przy pomocy wbudowanego w pełni programowalnego odbiornika satelitarnego SDR (ang. *Software Defined Radio*) zarejestrowano sygnały GPS dwóch wiązek L1[18] i L2[19] z częstotliwością próbkowania 6 Mbps. Niezinterpretowane „surowe" dane *„raw data"* przesłano na Ziemię specjalnym sześćdziesięciosekundowym wolnym slotem transmisyjnym ISS. Dane poddano rozszerzonej analizie sygnałowej DSP. Pomiar zakłóconego GPS odbywał się w nietypowej konfiguracji GPS-Ziemia-ISS. Odbiornik STP-H5 był skierowany w dół w stronę Ziemi, patrząc w kierunku „za siebie" w stosunku do kierunku lotu stacji kosmicznej ISS. W analizie danych na Ziemi wykorzystano SI do obrazowania rodzaju i miejsca powstawania zakłóceń CODED jammingu GPS (rysunek 19).



Rys. 18. Użyty sensor STP-H5, zainstalowany na stacji ISS (orbita 400km nad Ziemią) wyposażony w odbiornik GPS służący do badań jonosfery. Zdekodowane dane wykazały w polach LNAV wartość 0, tzw. „coded jamming"
Źródło: [3]

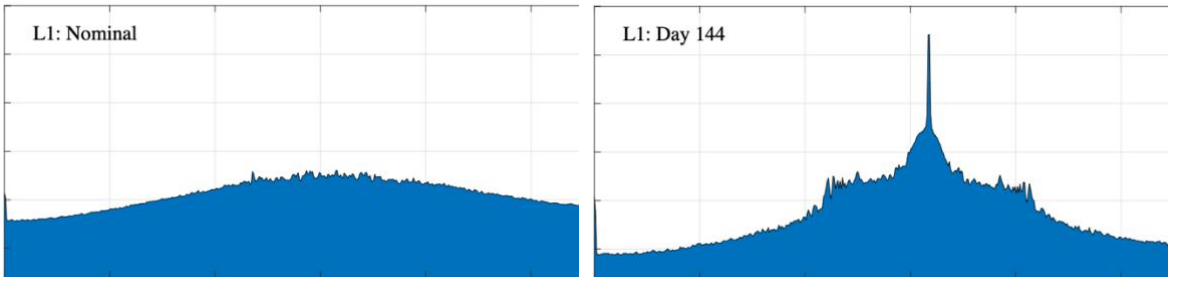
Rys. 19. Rejestracja zakłócanego w rejonie Morza Czarnego sygnału GPS wykonana w roku 2017 z poziomu stacji kosmiczne ISS za pomocą sensora STP-H5
Źródło: [3]

[18] GPS wiązka cywilna L1 o częstotliwości 1575.42 MHz. Obecnie jest również wiązka L5 1176 MHz.
[19] GPS wiązka wojskowa L2 o częstotliwości 1227.60 MHz.

Badania skoncentrowano na rejonie Morza Czarnego, gdzie odnotowano od 2014 roku silne interferencje zakłócające GPS. Wiele wcześniejszych raportów żeglujących statków handlowych raportowało tam anomalia pracy GPS. Niektórzy kapitanowie twierdzili, że ich statki nawigacja przenosiła wirtualnie o kilkaset kilometrów dalej na lotnisko do Moskwy.

Podczas dekodowania ramek depesz C/A GPS L1 na Ziemi, stwierdzono, że mają one poprawny format, ale pojawiła się dziwna obserwacja (anomalia). Kiedy satelita przelatywał nad obszarem Morza Czarnego podejrzanym o spoofing GPS, wartość depeszy LNAV była odczytywana z wartościami zero na wszystkich dostępnych zarejestrowanych kanałach. Zera znikały po opuszczeniu regionu zakłóceń (rysunek 19). Nie było wątpliwości co do celowego zakłócania GPS, jednak nie pasowało to do klasycznego jammingu GPS, ponieważ dekodowana informacja nie była zakłócona losowym szumem 1575.42 MHz (L1). Takie same obserwacje dotyczyły wiązki wojskowej L2. Oznaczało to, że nie był to typowy spoofing GPS, ponieważ nie wykazano fałszowania danych telemetrii nawigacyjnej LNAV, a jedynie ją skutecznie zerowano. Analiza spektralna potwierdzała obecność sztucznego sygnału zakłócenia L1 i L2. Dlatego Amerykanie nazwali ten rodzaj zakłócenia "coded jamming GPS". Dzisiaj uprawnieni jesteśmy do stwierdzenia, że jest to forma cyber-ataku DoS, blokująca funkcje PNT odbiornika GPS szczególnie w chwili, gdy musi on wykonać zimny start lub reakwizycję satelitów. Kodowany jamming stanowi więc potencjalną niewidoczną dla odbiornika pułapkę, w którą o ile wpadnie to może w niej pozostać. Podejrzewa się, że szczególnie niebezpieczny jest wymuszony restart odbiornika z resetem danych o położeniu satelitów względem Ziemi (tzw. almanach). Efekt taki, być może można aktywować zdalnie np. silnym impulsem elektromagnetycznym.

Dlatego uprawnionym staje się założenie, że być może w obecnej chwili doświadczamy w Polsce pewnego rodzaju „przyzwyczajania nas” do obecności sygnału zakłócającego GPS, wyłącznie po to, abyśmy nie zbudowali odporności naziemnych systemów informatycznych IT/OT na zagrożenie, które dopiero może nadejść w przyszłości.



a b

Rys. 20. (a) Analiza widma częstotliwość niezakłócanego GPS L1 1575.42 MHz
(b) Widoczna w środkowej części interferencja zakłóceń L1
Źródło: [3]

Zdecydowanie najciekawszym wyzwaniem okazała się próba określenia lokalizacji miejsca emisji zakłóceń GPS. Amerykanie przypomnieli sobie historię z rosyjskim Sputnikiem 1, z 1957 roku. Emitował on sygnał w paśmie fal radiowych o częstotliwości około 20,005 MHz i 40,002 MHz. Ten prosty sygnał miał charakterystyczną sekwencję „beep-beep-beep”, która była słyszalna na całym świecie i stała się symbolem początku ery kosmicznej eksploracji. Właśnie ten sygnał nasłuchiwali Amerykanie, uważani za twórców

pomysłu systemu GPS[20], William Guier i George Weiffenbach. Podobnie jak wielu ich kolegów, śledzili oni każdy przelot rosyjskiego Sputnika-1 i obliczali, jak daleko znajduje się on od nich. Wykorzystywali do pomiaru niewielkie mierzalne zmiany częstotliwości spowodowane efektem Dopplera, tym samym, który zmienia dźwięk ambulansu medycznego, gdy mija nas jadąc na sygnale. Fizycy skoncentrowali się na analizie „przesunięcia Dopplera" stawiając sobie ambitny cel, jakim było wydedukowanie całej trajektorii orbity rosyjskiego satelity oraz przewidzenie jego dokładnej pozycji w dowolnym momencie.

W 2018 roku Amerykanie użyli tego samego pomysłu co w 1957 roku, w celu określenia lokalizacji źródła jammingu GPS w rejonie Morza Czarnego. Założyli, że jeżeli przedmiotowe źródło zakłóceń GPS bazuje na stabilnym oscylatorze TCXO lub OCXO, to być może można będzie policzyć w oparciu o zarejestrowaną z poziomu ISS „historię dopplerowską", dokładną pozycję szukanego nadajnika zakłócającego. Naukowcy ocenili w oparciu o tzw. dewiacje Allana (ADEV), że dla przeciętnego oscylatora TCXO błąd lokalizacji źródła wyniósłby max. 7km, a dla dobrej jakości oscylatora OCXO błąd wynosiłby jedynie 70 m. W obu przypadkach rokowania identyfikacji miejsca nadajnika były zadowalające. Obliczenia były wprawdzie skomplikowane, zależały od parametrów ruchu stacji ISS po orbicie względem Ziemi, ale możliwy. Wynik obliczeń zaskoczył wszystkich, ponieważ wskazał, że 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[21].

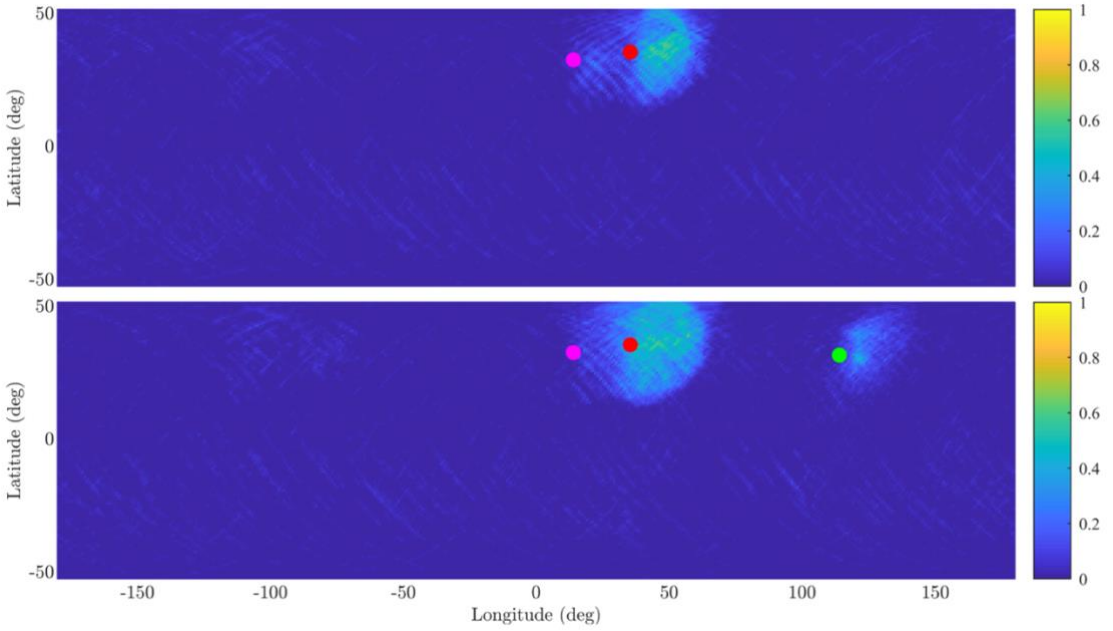
Rys. 21. Obliczenia oparte o historię dopplerowską wskazały, że za zakłócenia GPS w rejonie morza Czarnego odpowiadał nadajnik w rosyjskiej bazie wojskowej w Syrii
Źródło: [3]

Wygląda na to, że zakłócenia GPS na terenie Polski mogą być spowodowane podobnym jammingiem GPS. Po kilku miesiącach zdążyliśmy się już do niego przyzwyczaić, ponieważ dotychczas nie doszło do żadnych spektakularnych awarii. Brakuje sensacji, wielkich incydentów awarii, chociaż czasami Polska pojawia się na pierwszych stronach światowych mediów, np. gdy jamming zmusił brytyjskie służby i RAF

[20] https://www.bbvaopenmind.com/en/technology/visionaries/the-birth-of-gps-an-unexpected-child-of-the-space-race/.
[21] https://radionavlab.ae.utexas.edu/images/stories/files/papers/leo_int_mon.pdf.

do uruchomienia specjalnych procedur na pokładzie samolotu przewożącego Ministra Obrony Wielkiej Brytanii Granta Shappsa[22, 23, 24, 25] podczas przelotu z Polski na Litwę.

Badania przeprowadzone z użyciem sensora PHOTON STP-H5 na stacji ISS umożliwiły standaryzację metody identyfikacji źródeł zakłóceń GPS na całej kuli ziemskiej. Automatyzacja procesu identyfikacji jammingu i spoofingu GPS oparta została na metodzie statystycznego testowania hipotez (ang. *Hypothesis Testing Problem*). Problem testowania hipotez polega na formułowaniu hipotez dotyczących parametrów populacji na podstawie pewnej próby danych oraz na przeprowadzeniu odpowiednich testów statystycznych, aby ocenić, czy dane dostarczają wystarczających dowodów na poparcie lub odrzucenie tych hipotez. Na rysunku 22 jednolity kolor ilustruje „czystą" częstotliwość, z jaką hipoteza się nie potwierdza – to przelot stacji ISS nad niezakłóconymi obszarami oceanów. W efekcie ekspozycji ulega stosunek liczby zarejestrowanych potencjalnych zdarzeń zakłócających GPS L1 (górny panel) i L2 (dolny panel) do całkowitej liczby przeprowadzonych testów hipotez, w każdej lokalizacji na mapie współrzędnych.



Rys. 22. Graficzna wizualizacja zakłóceń GPS oparta na statystycznym testowaniu hipotez. Źródło: [3]

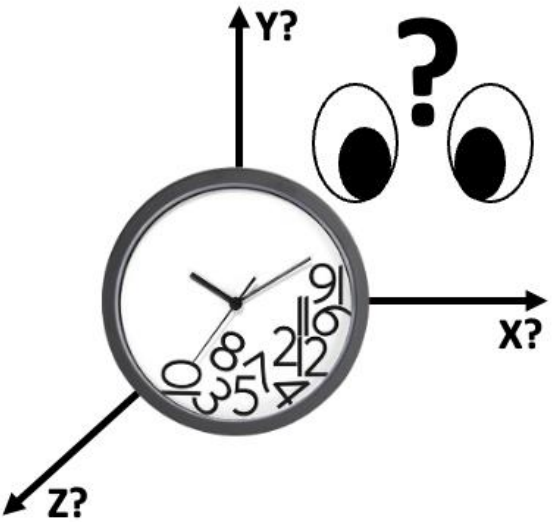
Czerwone kropki wskazują szacowane pochodzenie zakłóceń z obszaru Syrii. Kolejny obszar zakłóceń można zauważyć na zachód od lokalizacji w Syrii. Fioletowe kropki oznaczają przybliżoną lokalizację raportów o zakłóceniach GPS w regionie Libii. Oprócz zakłóceń w obszarach Syrii i Libii zaobserwowano również silną interferencję na częstotliwości L2 w Chinach kontynentalnych. Zielona kropka w punkcie (32◦ N, 114◦ E) wskazuje hipotetyczną lokalizację źródła zakłóceń na podstawie kształtu i lokalizacji obserwowanego hotspotu. Wykorzystywana do graficznej wizualizacji technika pomiaru z

[22] https://www.theguardian.com/politics/2024/mar/14/russia-suspected-of-jamming-gps-signal-on-aircraft-carrying-grant-shapps
[23] https://www.thetimes.co.uk/article/russia-electronic-attack-grant-shapps-plane-qltjc6gqg
[24] https://www.bbc.com/news/uk-68569676
[25] https://www.telegraph.co.uk/news/2024/03/14/grant-shapps-gps-jammed-aircraft-trip-poland-troops/

poziomu niskich orbit satelitarnych LEO jest technologią wschodzącą i oferuje obiecujące perspektywy serializacji takich badań. Z dużym prawdopodobieństwem pozwala ona określić dokładne położenie, a co za tym idzie również źródło i przynależność wojskową zakłóceń. Metoda oraz matematyczny opis przedstawiono w pracach [2][3]. Polecamy również uwadze czytelnika webinar omawiający realizację pomiarów z poziomu ISS dostępny na YouTube[26].

Ważnym wnioskiem wynikającym z powyższego przykładu jest stwierdzenie, że kodowany jamming GPS wydaje się być atakiem porównywanym do DoS (ang. *Denial of Service*), blokującym funkcjonalność wyznaczania PNT (ang. *Positioning, Navigation and Timing*) przez odbiornik GPS, zwłaszcza podczas początkowej fazy rozruchowej zimnego startu (ang. cold start) i reakwizycji dostępnych satelitów. Aby lepiej zrozumieć to zagrożenie przybliżymy zasadę wyznaczania PNT przez każdy odbiornik satelitarny GPS. Dla uproszczenia założymy, że system GPS działa bez uwzględnienia Ziemi, czyli tak jakby nasza planeta nie istniała. Założymy też, że przestrzeń jest próżnią (brak opóźnień jonosfery), oraz czas biegnie tak samo wszędzie (brak relatywistycznej dylatacji czasu). Uproszczony algorytm wyznaczania PNT przez odbiornik satelitarny GPS:

1. **Inicjalizacja**. Po włączeniu zasilania odbiornik GPS rozpoczyna pracę. Dostraja swoje radio do pracy w paśmie częstotliwości 1575.42 MHz. Wyszukuje sygnały docierające z satelitów GPS znajdujących się na orbitach. Identyfikuje je i przydziela indywidualne kanały (ang. *GPS channel*) do obsługi dekodowanych danych. W tej fazie pracy odbiornik nie ma jeszcze orientacji o położeniu w czasie ani przestrzeni (rysunek 23).



Rys. 23. Odbiornik GPS po włączeniu zasilania (zimny-start) i podczas reakwizycji satelitów, nie ma orientacji w czasie ani przestrzeni. To najlepszy moment do jego blokady jammingiem GPS. Źródło: własne

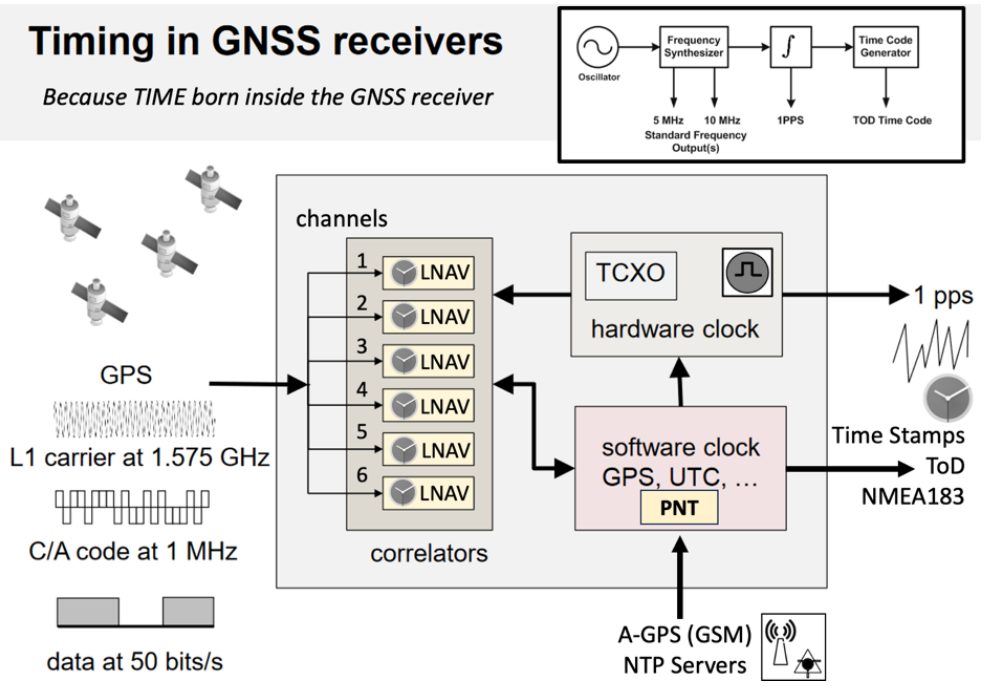
2. **Synchronizacja czasu (T)**. Gdy odbiornik odbiera sygnały z satelitów GPS, to dekoduje zawarte w nich informacje zawierające znacznik czasu. Uśrednia odczyty i synchronizuje swój wewnętrzny zegar. Uzyskuje w ten sposób słabą, milisekundową dokładność. Zagłuszenie GPS, a w szczególności wyzerowanie odbieranej informacji z pola znaczników czasu skutecznie blokuje odbiornik.

[26] https://www.youtube.com/watch?v=XDbn85IBIus.

3. **Obliczanie odległości od satelitów**. Zsynchronizowany zegar odbiornika, pozwala zmierzyć czas podróży sygnału z satelity GPS. Tak można obliczyć odległość odbiornika od satelity, która jest równa różnicy czasu wskazań zegara odbiornika, pomniejszonej o odczyt znacznika czasu sygnału jaki dotarł za pośrednictwem satelity GPS i pomnożonej przez prędkość światła c (rozchodzenia się sygnału w przestrzeni).
4. **Wyznaczanie pozycji (P)**. Znając odległość odbiornika GPS od co najmniej 4 satelitów, może on sam obliczyć swoją pozycję względem tych satelitów używając techniki trilateracji. Polega ona na wyznaczeniu współrzędnej pozycji w oparciu o reprezentację długości odcinków dzielących odbiornik od nadających sygnał satelitów.
5. **Cykliczna aktualizacja (P) i (T)** na bieżąco powoduje, że odbiornik GPS regularnie powtarza obliczenia. Im dłużej pracuje, tym kolejne odczyty pozwalają poprawić precyzję określania czasu (T) i pozycji (P) zwiększając dokładność odbiornika.
6. **Nawigacja (N)**. Aktualizacja PT w czasie rzeczywistym sprawia, że odbiornik może wyznaczać zmianę swojego położenia względem systemu GPS, a więc również kierunek swojego ruchu, a pośrednio również zmianę kąta, prędkość i przyspieszenie.

Działanie odbiornika GPS jest w uproszczeniu niczym innym jak porównaniem wskazań zegarów. Dokładność wyliczanych w odbiorniku GPS parametrów PNT zależy od algorytmu TRAIM oraz stabilności wbudowanego oscylatora częstotliwości TCXO. Na jakość wpływa też czułości odbiornika radiowego, rozdzielczości użytych układów DAC, mocy obliczeniowej procesora CPU, dostępnej pamięci RAM i liczby kanałów *channels*.

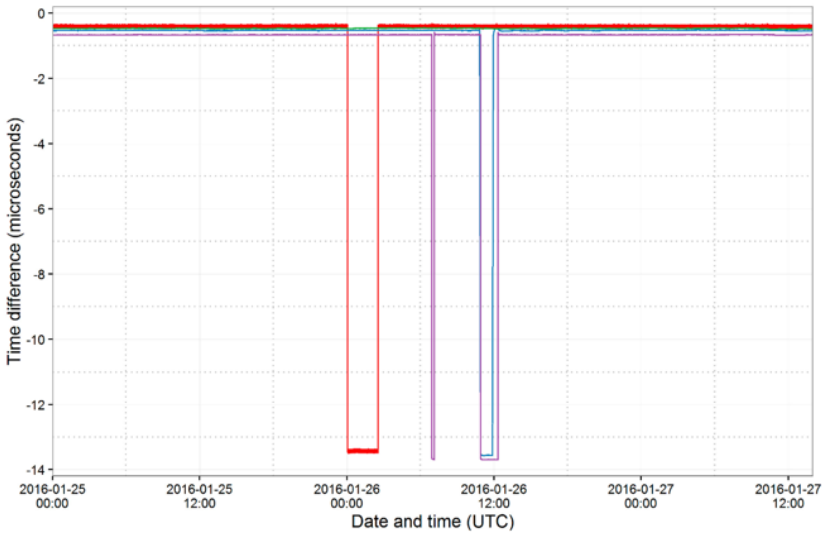
Odbiorniki czasowe UTC. Uproszczony ogólny schemat blokowy 6 kanałowego odbiornika czasowego GPS pokazano na rysunku 24. W szczególności, odbiornik czasowy GPS wyróżnia wysoka jakość generowanego w nim czasu UTC składającego się z wzorca częstotliwości 1PPS (ang. *Pulse Per Second*) i informacji o fazie skali czasu UTC dostarczanej łączem rs232 w formacie ramki NMEA183. Zawiera ona czas i datę (kalendarz).



Rys. 24. Uproszczony schemat blokowy odbiornika GPS używanego do synchronizacji UTC
Źródło: własne

Odbiorniki RTK. Odbiornik satelitarny Real-Time Kinematic (RTK) wykonuje kilka dodatkowych kroków w porównaniu do std. odbiorników GPS, aby zapewnić wysoką dokładność i pozycjonowanie w czasie rzeczywistym (RT). Oto niektóre: jednoczesny odbiór sygnału wielu częstotliwości i konstelacji GNSS, precyzyjne pomiary fazy nośnej z każdego satelity, poprawki różnicowe z odniesienia naziemnego BTS, parametry opóźnień w jonosferze. Istnieje również wiele naukowych odbiorników GPS oferujących najlepszą dokładność, jednak są one bardzo drogie.

Podsumowując, najczęściej błędnie interpretujemy, że czas i pozycja odbiornika GPS są przesyłane do nas z kosmosu, a odbiornik satelitarny działa jak karta sieciowa LAN. W konsekwencji błędnie wierzymy w bezpieczeństwo naszych rozwiązań opartych na GPS. W rzeczywistości parametry PNT wyznaczane są w odbiorniku GPS na Ziemi i każdy robi to nieco inaczej. W konsekwencji nie ma dwóch bliźniaczych odbiorników wyznaczających jednocześnie te same parametry PNT. Różnica PNT jest miarą dokładności obliczeń odbiornika oraz faktu, że ich praca przebiega wzajemnie niezależnie (asynchronicznie). Odbiornik GPS musi sporo policzyć. W obliczeniach uwzględnia między innymi poprawki opóźnienia sygnału w jonosferze i efekty relatywistyczne dylatacji czasu wynikające z dwóch teorii względności Einsteina: szczególnej i ogólnej. Pierwsza dzienna korekta dylatacji czasu GPS wynosi jedynie 7 mikrosekund i wynika z prędkości 14 tys. km/h, z jaką poruszają się satelity GPS po swoich orbitach wokół Ziemi. Druga to wewnętrzna systemowa poprawka 42 mikrosekund na dobę. Wynika ona z ogólnej teorii względności Einsteina wpływu grawitacji na zjawisko dylatacji czasu. Na Ziemi czas płynie wolniej niż w kosmosie, gdzie krążą satelity. Obie te wielkości mają przeciwstawne znaki, więc codzienna korekta czasu, jaką musi przeprowadzić każdy odbiornik dla systemu GPS, wynosi aż 35 mikrosekund na dobę. To bardzo dużo, zwłaszcza biorąc pod uwagę, że np. współczesna telekomunikacja 5G dopuszcza maksymalny błąd synchronizacji na poziomie pojedynczych nanosekund. Sytuacja się komplikuje, gdy odbiornik używa wielu systemów satelitarnych z grupy GNSS jednocześnie. Musi wtenczas niezależnie przeliczyć dylatację czasu dla każdej konstelacji GPS, GALIELO, GLONASS, BEIDOU, IRNSS oddzielnie. To zwiększają podatność odbiornika GNSS na błędy przepełnień numerycznych. Wykorzystuje to strona atakująca.



Rys. 25. Niejednoczesna reakcja 5 serwerów czasu na błąd 13.5 µs satelity GPS o numerze SVN23. Źródło: Metrologia Fińska (https://aaltodoc.aalto.fi/handle/123456789/19833).

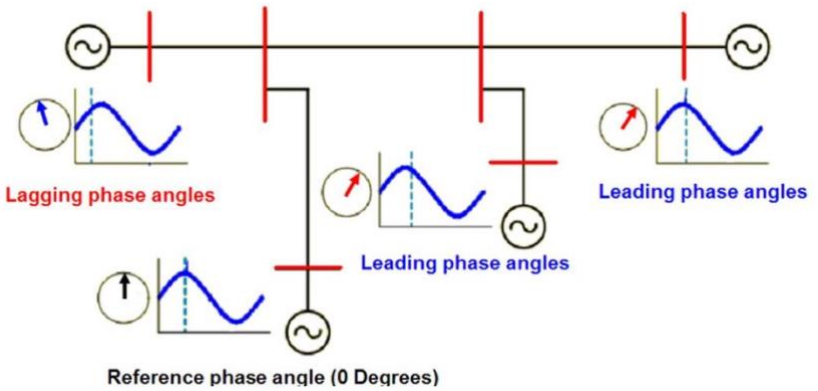
Dziś wiemy, że odbiorniki różnych producentów różnie reagują na sytuacje wyjątkowe i prowadzi to do desynchronizacji. Bardzo dobrze wykazał to incydent błędu wewnętrznego systemu GPS, znany jako błąd satelity SVN23, który miał miejsce 26 stycznia 2016 r. Spowodował on rozsynchronizowanie o 13.5 μs satelity 5 różnych testowanych w tym dniu odbiorników GPS używanych w serwerach czasu NTP/PTP (rysunek 25).

AIR FORCE OFFICIAL PRESS RELEASE - GPS GROUND SYSTEM ANOMALY

JAN 27, 2016

On 26 January at 12:49 a.m. MST, the 2nd Space Operations Squadron at the 50th Space Wing, Schriever Air Force Base, Colo., verified users were experiencing GPS timing issues. Further investigation revealed an issue in the Global Positioning System ground software which only affected the time on legacy L-band signals. This change occurred when the oldest vehicle, SVN 23, was removed from the constellation. While the core navigation systems were working normally, the coordinated universal time timing signal was off by 13 microseconds which exceeded the design specifications. The issue was resolved at 6:10 a.m. MST, however global users may have experienced GPS timing issues for several hours. U.S. Strategic Command's Commercial Integration Cell, operating out of the Joint Space Operations Center, effectively served as the portal to determine the scope of commercial user impacts. Additionally, the Joint Space Operations Center at Vandenberg AFB has not received any reports of issues with GPS-aided munitions, and has determined that the timing error is not attributable to any type of outside interference such as jamming or spoofing. Operator procedures were modified to preclude a repeat of this issue until the ground system software is corrected, and the 50th Space Wing will conduct an Operational Review Board to review procedures and impacts on users. Commercial and civil users who experienced impacts can contact the U.S. Coast Guard Navigation Center at (703) 313-5900.

Rys. 26. Oficjalny komunikat prasowy sił zbrojnych USA dotyczący błędu GPS SVN23.
Źródło: Własne (informacja jawna)



Rys. 27. Błąd 13.5 μs GPS SVN23 mógłby wywołać awarię w sektorze energetycznym *smart grid.* Max. błąd rozsynchronizowania PMU w smart grid wg. IEC C37.238 nie może przekraczać 1 μs.
Źródło: Własne

Rozumiejąc jak dużą niepewność dla bezpieczeństwa infrastruktur krytycznych USA wprowadza używanie wyprodukowanych w latach 1990-2020 odbiorników satelitarnych GPS, Amerykanie jako pierwsi zalecili dywersyfikację ryzyka wprowadzając prezydencką dyrektywę EO13905[27]. Przepisy wykonawcze w obszarze funkcjonalności naziemnych dostaw wzorcowego czasu UTC opisał NIST w dokumencie NIST.TN.2187[28]. W oddzielnym dokumencie NIST.TN.2189[29] opisano zależności przemysłu USA od GPS.

W styczniu 2023 r., Komisja Europejska opublikowała zaktualizowaną dyrektywę NIS2[30], która w ślad za doktryną USA zaleca krajom członkowskim UE tworzenie alternatywnych do GNSS systemów A-PNT (ang. *Assured PNT)*.

Jak do tej pory Polska bardzo dobrze wypada na tle innych państw członkowskich UE i NATO. Nowy krajowy system dystrybucji czasu urzędowego eCzasPL[31] [32] został oddany w dniu 10 grudnia 2023 roku, a więc na dwa tygodnie przed pierwszymi zakłóceniami GPS nad Polską. Uruchomienie w Głównym Urzędzie Miar RP systemu eCzasPL miało miejsce równo w dwudziestą rocznicę publikacji ustawy o czasie urzędowym UTC(PL) /Dz.U. Nr 16 z dnia 10 grudnia 2003 roku[33]/. Z kolei w dniu 22 kwietnia 2004 roku, minęło dwadzieścia lat od czasu wejścia w życie rozporządzenia /Dz.U. Nr 56 POZ. 548 z dnia 19 marca 2024[34]/ wskazujące serwery czasu NTP o nazwie *tempus1.gum.gov.pl* i *tempus2.gum.gov.pl* jako oficjalne źródła czasu urzędowego UTC(PL) Głównego urzędu Miar RP (polski odpowiednik amerykańskiego NIST). Tym samym Polska, obok USA, Wielkiej Brytanii i Francji weszła w posiadanie własnej naziemnej infrastruktury dystrybucji czasu urzędowego UTC(PL) niezależnego od wojskowych systemów satelitarnych grupy GNSS, Nasz kraj wyprzedził inne państwa UE oraz kraje takie jak Indie, Japonię, Korę Południową i Izrael. Nad podobną naziemną infrastrukturą dystrybucji czasu UTC nadal pracują Chiny[35] i wiele innych państw. Polski system eCzasPL GUM RP posiada unikatową, mało znaną funkcjonalność. Pozwala Głównemu Urzędowi Miar na zdalną kontrolę UTC na odległych serwerach czasu NTP/PTP pracujących w przemyśle, również tych działających w wewnętrznych sieciach infrastrukturalnych odizolowanych od Internetu. To bardzo ważne, ponieważ najczęściej nie pamiętamy, że protokoły NTP i PTP (IEE1588) nie dają gwarancji synchronizacji po stronie odbiorczej. Dopiero opracowany w projekcie DEMETRA[36] Horizon 2020, przez polskich inżynierów z firmy ELPROMA system audytu pozwolił badać zdalnie na dużą odległość i certyfikować serwery czasu.

[27] https://www.govinfo.gov/app/details/DCPD-202000071.

[28] https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2187.pdf.

[29] https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2189.pdf.

[30] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en.

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

[32] Oficjalny film eCzasPL: https://www.youtube.com/watch?v=rawcGu65OaE.

[33] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20040160144.

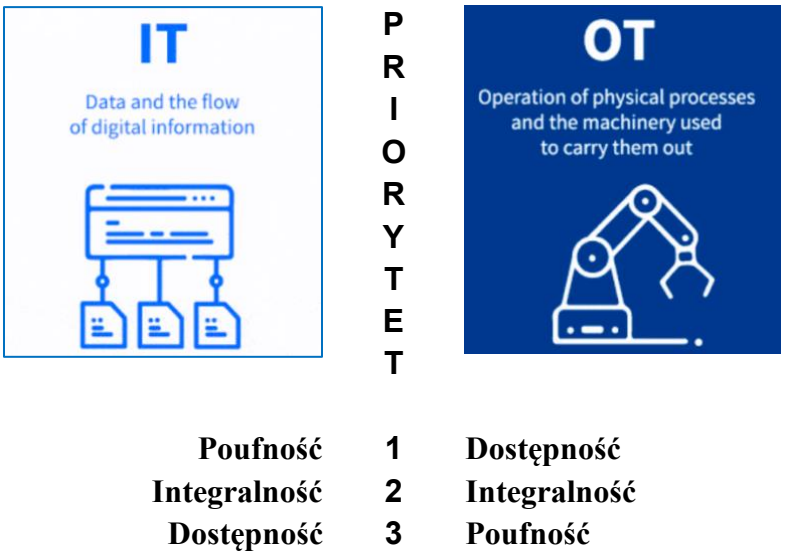
[34] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20040560548.

[35] https://www-thepaper-cn.translate.goog/newsDetail_forward_23171179?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp&_x_tr_hist=true.

[36] https://doi.org/10.33012/2017.14982.

4. Jak zapobiegać desynchronizacji infrastruktur krytycznych

Uznanie synchronizacji za obszar cyberbezpieczeństwa wymaga aktualizacji procedur operacyjnych, zarówno na szczeblu państwowym, jak i w lokalnych środowiskach pracy. Kluczowym elementem jest edukacja społeczeństwa, która podnosi świadomość znaczenia utrzymania stabilnej domeny czasu UTC w czasie pokoju, jak i w przypadku konfliktu zbrojnego. Poprawna synchronizacja UTC jest niezbędna do sprawnego działania wszystkich nowoczesnych technologii informatycznych (IT) i systemów sterowania (OT). W przypadku konfliktu kinetycznego (konflikt zbrojny) waga synchronizacji pozostaje niezmienna, ale obniżany jest rygor dokładności oraz zmienia się sposób realizacji technicznej dystrybucji czasu UTC, wynikający ze zamiany priorytetów użyteczności danych IT vs. OT. Zrozumienie w/w jest ważne wobec faktu trwającego zagłuszania sygnałów GPS nad Polską.



Rys. 28. Zamiana priorytetów IT i OT wynikająca ze zmiany użyteczności danych.
Źródło: gen bryg. M. Chmielewski dla MBA Cyberbezpieczeństwo WAT

Zacząć należy od oceny bieżącej sytuacji (*status quo).* Audytor powinien np. z użyciem dronów lub dokonując osobiście inspekcji, sprawdzić stan anten zainstalowanych na dachu, a następnie zadać administratorowi budynku oraz systemów informatycznych pytania:

- *Czy czas i data są ważne dla systemów IT / OT w organizacji?*
- *Czy desynchronizacja IT / OT może wpłynąć na operacyjność przedsiębiorstwa?*
- *Czy przedsiębiorstwo używana systemów o rozproszonej architekturze IT lub OT?*
- *Czy organizacja używa rozwiązań wieloserwerowych lub o architekturze modułowej?*

Pozytywna odpowiedź na jedno z w/w pytań oznacza, że synchronizacja jest dla organizacji ważna. Uzupełniającym może być wstępne badanie w rozmowie dające audytorowi odpowiedź na pytanie, czy badana organizacja jest przygotowana na wyłącznie lub brak GPS.

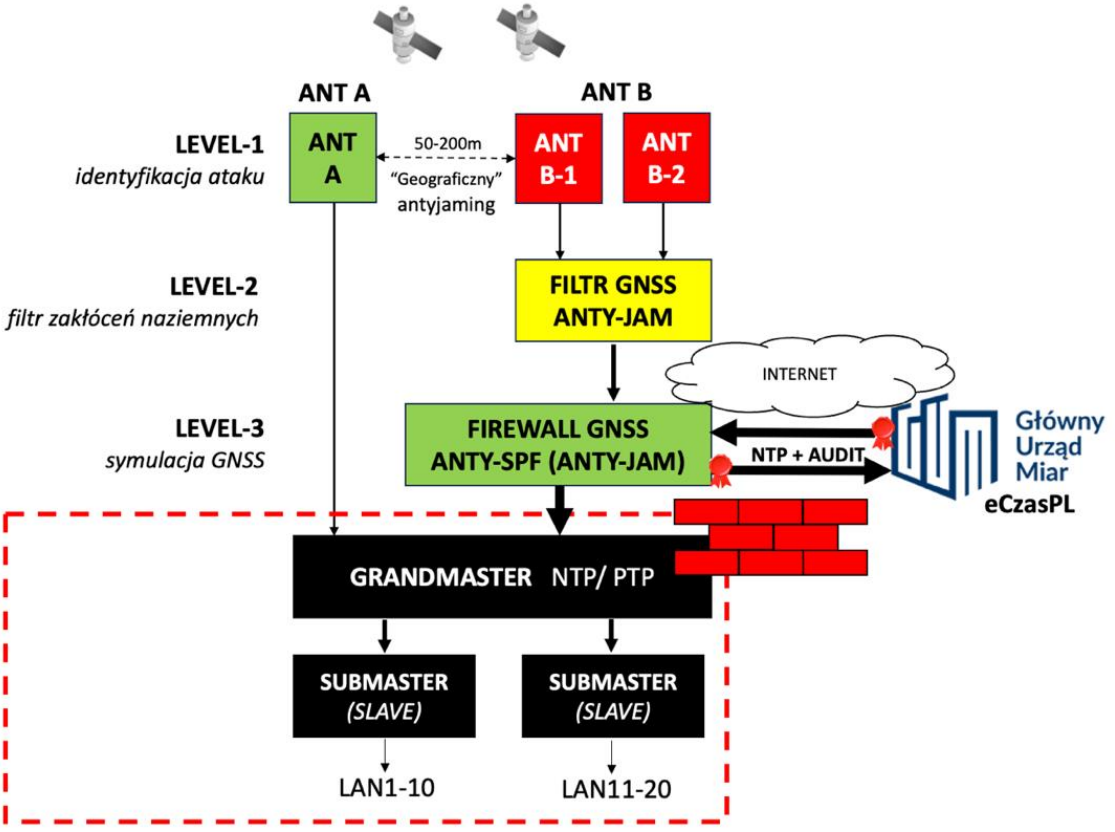
Rys. 29. Widok anten GNSS zamontowanych na dachu budynku infrastruktury krytycznej. Inspekcja dostarcza informacji o ilości systemów zależnych od GPS i jakości instalacji oraz daje pogląd w sprawie okresu pochodzenia poszczególnych rozwiązań zależnych od GPS.
Źródło: własne

Odbiorniki GPS wyprodukowane przed 2022 rokiem nie są odporne na zakłócenia typu jamming i spoofing GPS. W Polsce, podobnie jak w innych krajach, funkcjonuje bliżej nieznana duża liczba urządzeń wykorzystujących odbiorniki satelitarne dostarczonych jako element składowy dużych systemów IT i OT, które pomimo deklaracji producenta, zamiast korzystać np. z systemów GPS i GALILEO, mogą korzystać z GLONASS lub BEIDOU.

Krajowi posiadacze urządzeń do synchronizacji, w tym w szczególności starszych serwerów NTP/PTP używających GPS (GNSS) niezależnie od marki, powinni rozważyć wymianę urządzeń na nowsze modele wyprodukowane już po roku 2022. Dobrym kandydatem dla Polski są krajowe serwery NTP/PTP posiadające kodyfikację NATO i certyfikację metrologiczną Głównego Urzędu Miar RP. Polskie produkty są dziś bardzo cenione na świecie, który zaczyna dostrzegać walor cyberbezpieczeństwa synchronizacji.

Rys. 30. Polskie urządzenia do synchronizacji NTP/PTP używane w NATO i w projekcie eCzasPL
Źródło: Elproma, PIK Time Systems

Krajowy przemysł i użytkownicy powinni rozważyć zmianę i włączenie posiadanych struktur informatycznych do niezależnego od GPS systemu synchronizacji eCzasPL[31] GUM. Noty aplikacyjne ze schematami konfiguracji podłączeń odizolowanych od Internetu wewnętrznych sieci infrastrukturalnych do atomowych wzorców czasu urzędowego UTC(PL) omówione zostały obszernie na stronach 210-212 w literaturze [1].



Rys. 31. Model bezpiecznej synchronizacji eCzasPL, 100% odpornej na jamming i spoofing GPS. Źródło: eCzasPL (Główny Urząd Miar RP)

Kluczowymi elementami bezpieczeństwa struktury przedstawionej na rysunku 31 są:

1. **Wielośródłowość UTC**. Referencyjny czas pobierany z wielu miejsc jednocześnie, takich jak GNSS, odległe zegary atomowych Głównego Urzędu Miar RP (eCzasPL), lokalne oscylatory holdover Rubidowe i OCXO wbudowane w serwer czasu NTP/PTP.
2. **Geopolityka GNSS**. Polska powinna skupić się na wiodącej roli europejskiego systemu GALILEO jako źródło wzorca czasu UTC, wspierane amerykańskim systemem GPS. Rola systemów wojskowych takich jak rosyjski GLONASS, chiński BEIDOU i indyjski IRNSS, powinna być ograniczona wyłącznie do funkcji porównań i analiz. Tor ANT-A powinien być ustawiony wyłącznie na pracę GALILO, a tor ANT-B na GPS.
3. **Redundancja UTC o cechach asymetrii** w torze połączeń anten A i B LEVEL-1. Zhakowanie, zagłuszenie, spoofowanie toru anteny ANT-A nie ma wpływu na bezpieczeństwo toru ANT-B, w której występują dodatkowe zabezpieczenia filtrujące LEVEL-2 i symulacja GNSS LEVEL-3. Dobrą praktyką jest stosowanie dwóch odbiorników GNSS, pochodzących od różnych producentów, dla toru ANT-A i ANT-B.

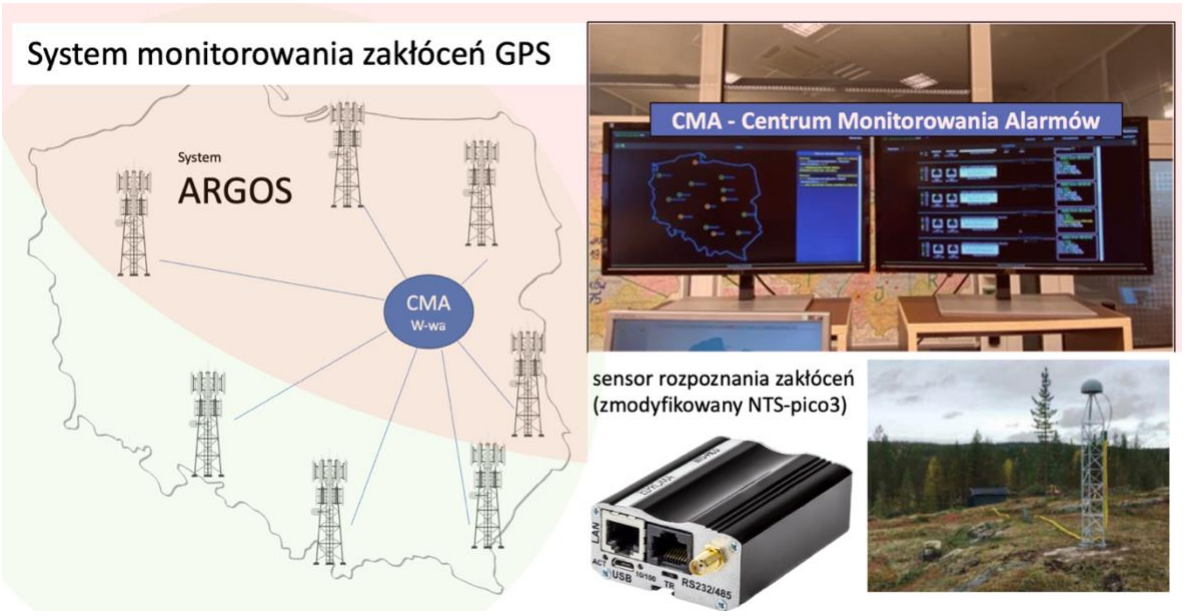
4. **Odporność na amatorskie zakłócenia GPS**. W celu ograniczenia wpływu lokalnych działań dywersyjnych lub sabotażowych, minimalna odległość między ANT-A i ANT-B powinna wynosić 50-200 metrów. Jest to tzw. naturalny „geograficzny anty-jamming", bardzo skuteczny w przypadku mobilnych urządzeń zakłócających sygnały GNSS.
5. **Model bezpieczeństwa o cechach konwergencji**. Pozwala synchronizować centralnie do niezależnego od GNSS naziemnego systemu czasu urzędowego eCzasPL, a w przypadku utraty połączenia TCP/IP z GUM RP, synchronizacja automatycznie decentralizuje się kontynuując pracę korzystając z GALILEO (ANT-A) i GPS (ANT-B).
6. **Autonomia UTC** zapewnia kontynuacje pracy zarówno przy braku sygnałów GNSS jak i w przypadku utraty linku do eCzasPL Głównego Urzędu Miar RP. Rozwiązanie pobiera czas z zagregowanych zegarów Rubidowych (Rb) i OCXO wbudowanych w sprzęt pracujący wewnątrz infrastruktury krytycznej (poziom LEVEL 1-3 i GRANDMASTER).
7. **LEVEL 1-2-3**, **hierarchia zarządzania** bezpieczeństwem synchronizacji w sieci NIS2:

   LEVEL-1. Anteny i odbiorniki. Konfiguracja GNSS realizuje stawiane założenia odzwierciedlające cele bezpieczeństwa związane z geopolityką państwa i regionu. Np. krajowe infrastruktury UE i USA nie powinny zależeć od rosyjskiego systemu GLONASS i chińskiego BEIDOU, ale i v-ce versa trudno sobie wyobrazić, że rosyjskie i chińskie infrastruktury krytyczne będą zależeć do wojskowego GPS. Minimalna odległość anten torów ANT-A i ANT-B 50-200 metrów zmniejsza podatność rozwiązania na wpływ amatorskich jammerów GPS o małej mocy.

   LEVEL-2. Poziom aktywnej filtracji zakłóceń jamming i spoofing GNSS. Urządzenia pracujące na tym poziomie używają techniki NULL STEERING rozpoznania i odrzucenia fałszywego sygnału emitowanego z ziemi. W tym celu używają pomiarów różnicowych, a więc muszą być wyposażone w kilka anten. Przeciętna liczba używanych anten to 3. Zdarzają się rozwiązania 2 i 6 antenowe.

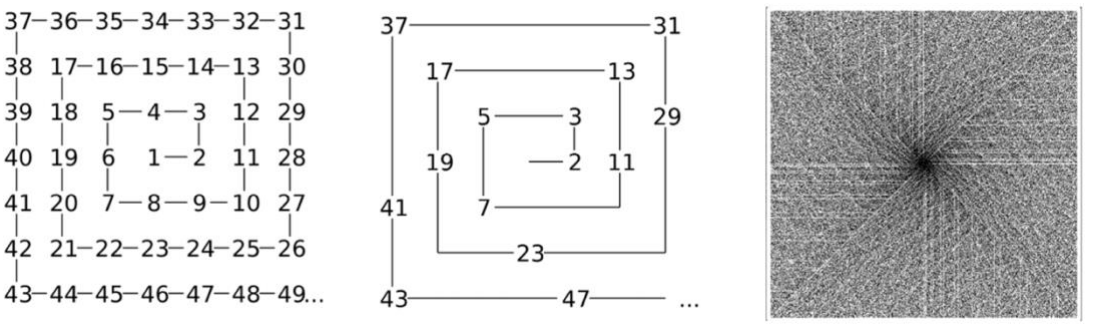
   LEVEL-3. To poziom fizycznej izolacji wewnętrznej infrastruktury od GNSS. Często jest określany terminem GPS-firewall. Urządzenie pracujące na tym poziomie posiada funkcjonalność symulacji sygnału GPS L1 1575.42 MHz lub generuje gotową do użycia zdekodowaną z GPS ramkę w formacie NMEA183. Symulowany system GNSS (w przypadku Polski GALILEO wspierany GPS) przekazywany jest „pomostowo" z pominięciem sieciowego firewall i podawany jest bezpośrednio na wejście serwera czasu GRANDMASTER, pracującego wewnątrz odizolowanej od Internetu sieci infrastrukturalnej NIS2. Połączenie takie jest bezpieczne ponieważ nie używa sieciowego protokołu TCP/IP, jest transmisją elektryczną rs232 lub radiową L1 1575.42 MHz, zabezpieczoną jednokierunkową „diodą" transmisji informacji. W chwili ataku radiowego jamming lub spoofing LEVEL-3 odcina dostęp sieci infrastrukturalnej od fizycznych satelitów GNSS, ale pozostaje w trybie ich monitorowania *(sandbox)* do czasu zakończenia ataku radiowego. To samo urządzenie LEVEL-3 może zdalnie kontrolować i raportować w celu certyfikacji zgodność używanego UTC z czasem urzędowym UTC(PL).

Polska doświadczana jest ostatnio coraz intensywniejszymi atakami zagłuszania GPS. Dlatego ważnym wsparciem proponowanej struktury bezpiecznej synchronizacji eCzasPL jest system monitorowania zakłóceń GPS z powiadamianiem o zdarzeniach rozpoczęcia i oceny końca ataku radiowego na nasz kraj. Takim systemem jest ARGOS firmy ELPROMA.



Rys. 32. Stacjonarny system ARGOS gęstego mapowania sensorami wykrywa zakłócenia GPS.
Źródło: własne

ARGOS to polski stacjonarny system monitorowania sygnałów GNSS o tzw. gęstym mapowaniu sensorami telemetrycznymi badającymi jakość odbieranych sygnałów satelitarnych w poszczególnych podgrupach. Oparty jest na produkowanym w kraju od roku 2017 miniaturowym serwerze czasu Elproma NTS-pico3, który od roku 2017 aktywnie testowany jest przez firmy w Izraelu, USA i Niemczech jako kandydat koordynatora synchronizującego fuzję sensorów i ich danych w autonomicznych pojazdach oraz robotach. Wersja ARGOS sensora NTS-pico3 jest znacząco rozszerzona względem standardowej wersji produktu dostępnego w regularnej sprzedaży. Szczegóły nie są znane, ale producent deklaruje, że sensor może być wyposażony w dwuzakresowy odbiornik satelitarny GNSS, pozwalający śledzić indywidualnie jak i grupami wszystkie dostępne konstelacje GPS, GALILEO, GLONASS, BEIDOU, IRNSS oraz co najważniejsze opcjonalnie może posiadać wbudowany analizator widma częstotliwości. Gęste mapowanie za pomocą sensorów ARGOS pozwala na bardziej szerokie zgłębienie problematyki zakłóceń sygnałów satelitarnych GNSS. Dane mogą być przedstawiane w formie prostej jako jednokolorowa np. czarno-biała bitmapa pikselowa (1- jest zakłócenie, 0-brak) lub z użyciem kolorów.



Rys. 33. Pierwsze 49 liczb spirali Ulama. Wyłuskane liczby pierwsze. Widok dużej populacji liczb pierwszych. Alegorię należy traktować obrazowo, a nie dosłownie.
Źródło: Wikipedia

Podkreślając unikatowe podejście użycia techniki z gęstym mapowaniem, polski producent systemu ARGOS odwołuje się do alegorii poszukiwaniem liczb pierwszych w oparciu o tzw. spiralę Ulama (polski matematyk przedwojennej tzw. Szkoły Lwowskiej, uczestnik projektu Manhattan USA). Patrząc na spiralę Ulama dla dużych statystyk liczb pierwszych (rysunek 33), trudno się nie zgodzić, że obserwujemy graficznie pewną prawidłowość ich położenia w zbiorze liczb naturalnych. Tymczasem zagadnienie poszukiwania liczb pierwszych pozostaje nierozwiązanym problemem milenijnym, znanym jako Hipoteza Riemanna. Ta alegoria ma zachęcić do współpracy również inne podmioty.

Z kolei przyporządkowując paletę kolorów stanom pośrednim 0-1, reprezentującym płynnie poziom zakłóceń, system ARGOS otwiera nowe możliwości badawcze, ważne dla oceny wpływu innych czynników na zakłócenia GPS. Warunki pogodowe, silne zanieczyszczenia atmosferyczne ze strony przemysłu, pole elektromagnetyczne wytwarzane przez energetykę, a nawet fakt przesterowania sygnału źródłowego są interesujące do poznania zjawiska będącego wschodzącą dziedziną cyberbezpieczeństwa cywilnego.

Taki rodzaj badań nawiązuje wprost do koncepcji amerykańskiej omówionej wcześniej w tym rozdziale (rysunek 22), dotyczącej kwestii tzw. graficznej wizualizacji opartej na *statystycznym testowaniu hipotez,* wykorzystującej zarówno uczenie maszynowe jak i sztuczną inteligencję w określeniu miejsca oraz identyfikacji rodzaju zakłóceń GPS.

Być może okażę się w przyszłości, że w uzasadnianych przypadkach niezbędne będzie wzmocnienie wrogiego zagłuszania GPS, własnym silniejszym zagłuszaniem (rysunek 34), tylko po to, aby krajowe systemy przemysłowe zareagowały prawidłowo „immunologicznie" odrzucając GPS jako źródło czasu UTC, zastępując alternatywnym systemem naziemnym eCzasPL z GUM RP. Jest tak ponieważ, dotychczasowe badania wykazują, że w wielu przypadkach słaby jamming GPS może się zachowywać tak samo jak spoofing GPS i konieczna okazać się może „sztuczna pomoc" w wymuszaniu stabilnego stanu poziomu zagłuszania GPS, taka która uruchomi automatyczne procedury przełączania systemów.

Rys. 34. Mobilny jammer GPS produkcji chińskiej (na lewo).
Polskiej produkcji PIAP iTTi/Łuksiewicz profesjonalny programowalny jammer (prawa część), model ZKR-1 o mocy 150W i paśmie 25-5800 MHz, generujący ciągły i responsywny
Źródło: iTTi / Łukasiewicz

Bitmapa wskazań zakłóceń ARGOS jest istotna, ponieważ umożliwia identyfikację również pojedynczych ataków, spowodowanych działaniami dywersyjnymi lub sabotażowymi z użyciem przenośnych jammerów GPS (rysunek 34, lewa strona).

System ARGOS reaguje w czasie rzeczywistym na każdy rodzaj zakłócenia. Generuje alarmy, o rozpoczęciu ataku radiowego, monitoruje poziom zakłóceń podczas przebiegu oraz wysyła informacje o zakończeniu. Sam system jest odporny na jamming i spoofing GPS. Chroni się dzięki rozproszonej strukturze sensorów zarządzanych centralnie programem EDMS wspieranym SI. Włączony do krajowego systemu synchronizacji czasem urzędowym UTC(PL), otrzymuje za pośrednictwem eCzasPL skuteczne narzędzie rozruchowe w przypadku konieczności restartu ARGOS w warunkach silnego zakłócania GPS i GNSS nad Polską.

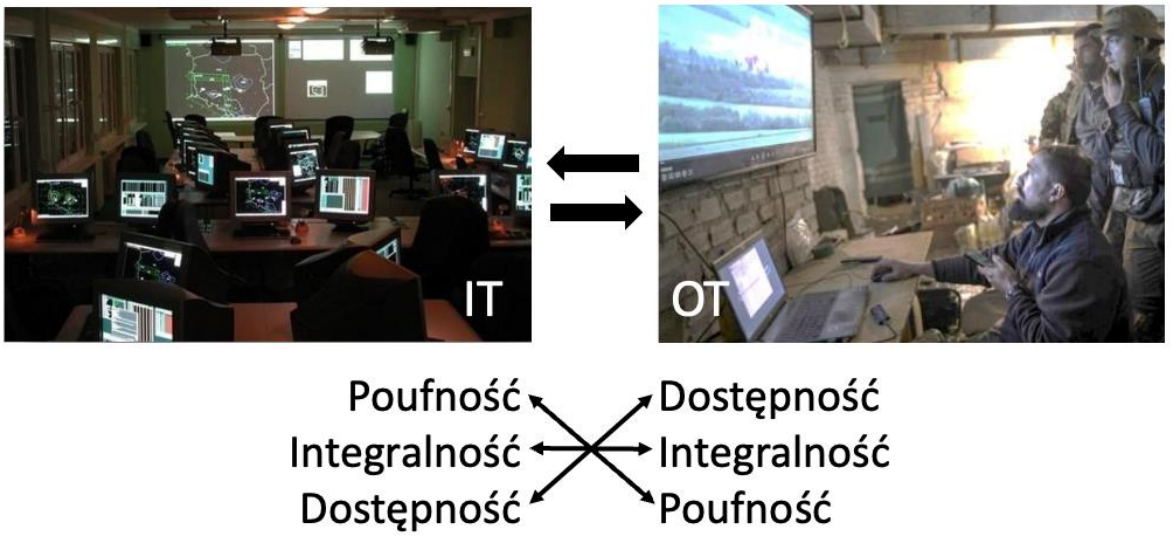
Informacje (alarmy) z ARGOS powinny być przekazywane bezpośrednio do kluczowych infrastruktur krytycznych kraju. Wczesne ostrzeżenie o jammingu GPS jest dzisiaj kluczowym elementem bezpieczeństwa. Pozwala zareagować na atak we wczesnej jego fazie. Już samo wyłączenie odbiornika GPS chroni systemy IT / OT przed skutkami niedeterministycznego zachowania, ale dopiero korzystanie z alternatywnych naziemnych rozwiązań PNT, takich jak eCzasPL, daje 100% odporność i bezpieczeństwo.

Bieżące zakłócenia GPS nad Polską wykazują cechy ataku typu DoS, który blokuje funkcje PNT odbiorników w określonych przypadkach, takich jak uruchamianie (ang. *cold-start*), ponowna reakwizycja sygnałów satelitarnych. Nie można wykluczyć scenariusza, że obecne działanie ma na celu przyzwyczajenie Polski do problemu i zaniedbanie tego ważnego dla bezpieczeństwa problemu.

Dlatego obok statystycznej oceny *ilościowej* konieczne jest dokładne *jakościowe* badanie zakłóceń GNSS za pomocą różnych, niezależnych od siebie metod pomiarowych. Instytut Łączności również prowadzi takie badania. Korzystając z świetnie wyposażonych mobilnych stanowisk laboratoryjnych może on prowadzić zarówno ocenę jakości odbieranych sygnałów GNSS jak i realizować zagłuszanie GNSS w regionie (rysunek 35).

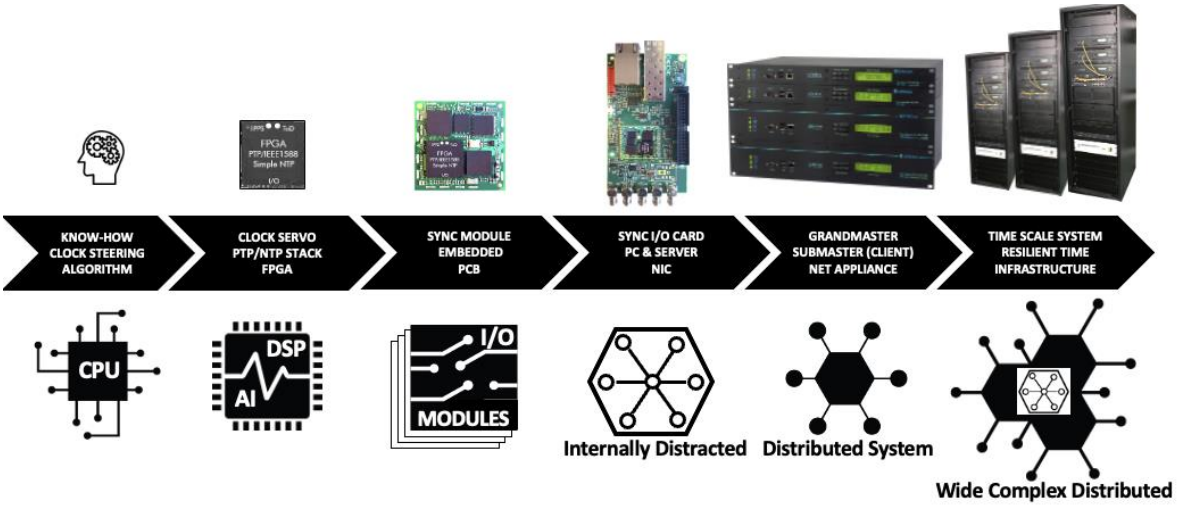
Wśród cywilnych producentów systemów zagłuszania sygnałów radiowych należy zwrócić uwagę na rozwiązanie iTTi / Łuksiewicz (PIAP). Urządzenie ZKR-1 to profesjonalny programowalny jammer o mocy 150W operujący w paśmie 25-5800 MHz. Może on generować zakłócenie jamming ciągły i responsywny (rysunek 34).

Rys. 35. Mobilne stanowisko pomiarowe do badania jakości i zakłócania sygnałów GNSS
Źródło: Instytut Łączności



Rys 36. Zmiana IT w OT i ich priorytetów w obliczu zagrożenia kinetycznym konfliktem. System dowodzenia NATO (lewa strona), operacyjny punkt dowodzenia w Ukrainie (prawa strona). Źródło: gen bryg. M. Chmielewski dla MBA Cyberbezpieczeństwo WAT

W momencie zagrożenia kinetycznego, priorytety ulegają zmianie. Część funkcjonalności stacjonarnych systemów informatycznych IT przenosi się do mobilnych systemów OT, co zwiększa zdolność do przemieszczania się i rozpraszania, ważną dla współczesnego teatru działań wojennych. Transformacja IT-OT nie zmniejsza potrzeby synchronizacji, ale zamienia priorytet stosowania protokołów PTP (IEEE1588) i NTP. Zmniejsza zapotrzebowanie na użycie protokołu najnowszej, precyzyjnej, nierutowalnej synchronizacji PTP i znacznie zwiększa starszego, routowanego w sieci Internet protokołu NTP. Skala transformacji obejmuje wielopoziomową strukturę sprzętu IT/OT (rysunek 37).



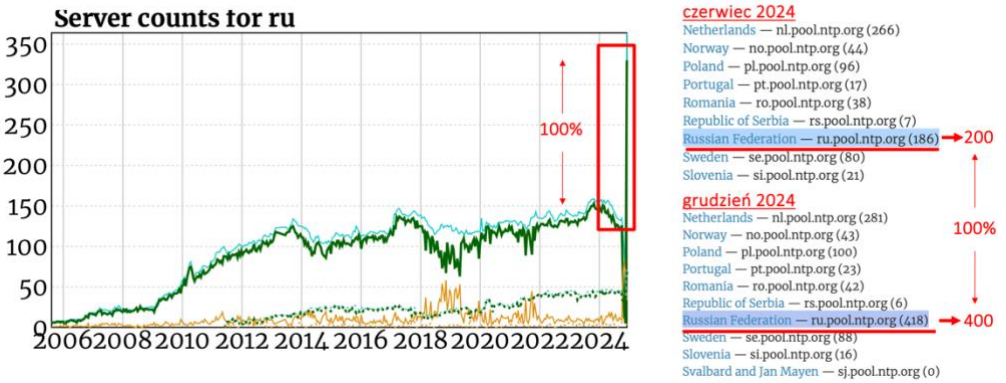
Rys. 37. Ewolucja (grupy) składowych elementów synchronizacji wykorzystywana w IT/OT, od najmniejszej do największej. Każdy kolejny na prawo element zawiera w sobie poprzednik. Źródło: własne

Tak długo jak rozproszone systemy informatyczne mają dostęp do Internetu, ich zasoby mogą korzystać z centralnego systemu synchronizacji eCzasPL[31] [32], dostarczającego czas

urzędowy[33] [34] UTC(PL) nadawany z Głównego Urzędu Miar RP (rysunek 10). Należy jednak wziąć pod uwagę, że w przypadku cyberzagrożenia scentralizowana struktura GUM, pod wpływem cyberataków typu DoS, może ulec ograniczeniom w dostępności. Dlatego już teraz istotne jest planowanie konwergencji oraz umiejętne połączenie cech obecnej centralizacji (eCzasPL, odporna na zakłócenia typu jamming i spoofing GPS) z jednoczesną decentralizacją źródeł synchronizacji. W takim przypadku wzrasta rola do zaufanych, publicznie dostępnych w Internecie serwerów czasu NTP z grupy NTPPOOL[37] (rysunek 10). Niestety, korzystanie z NTPPOOL wiąże się z pewnym ryzykiem, ponieważ nie zawsze wiadomo, kto nimi zarządza i skąd pochodzi źródło czasu UTC. W publicznej puli serwerów czasu POOLNTP odnaleźć można również „podstawione" serwery, które podczas kryzysu mogą celowo zachowywać się niestabilnie dostarczając użytkownikom nieprawidłowy UTC. Dlatego budowanie zaufania do serwerów publicznych NTP wymaga specjalnego statystycznego podejścia ilościowego w narodowej grupie NTPPOOL. Im bardziej liczebna jest grupa publicznych serwerów NTP w państwie (takich, których czas pozostaje pod kontrolą np. narodowej metrologii NMI), tym mniejsza pozostaje zdolność do zewnętrznego wpływania na desynchronizację systemów IT/OT wynikającą z użycia takiej krajowej puli.

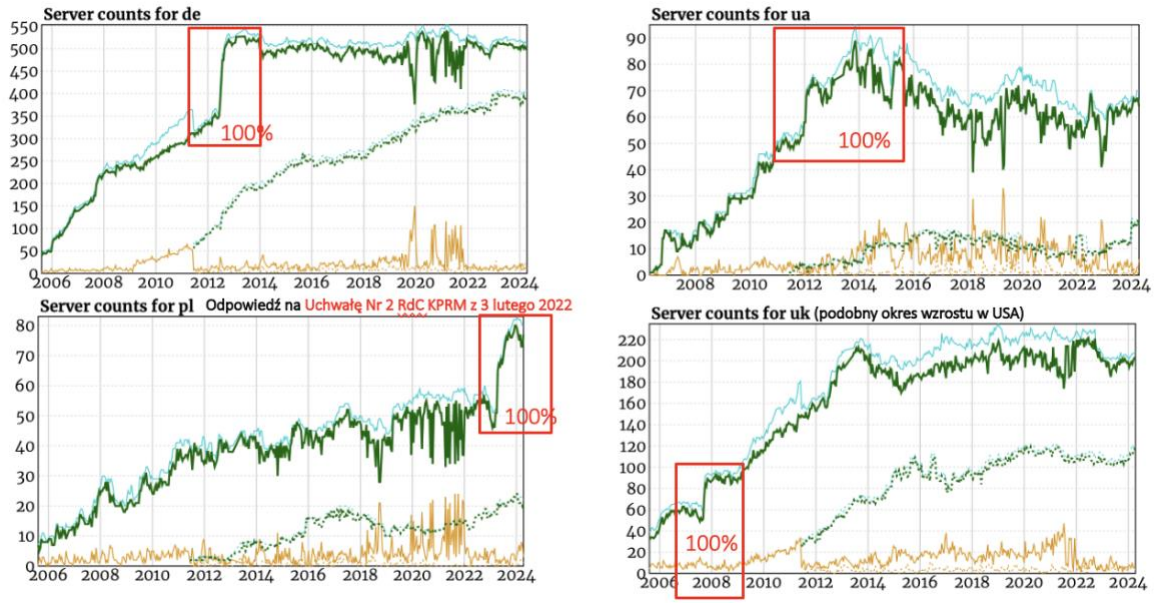
Od czasu wybuchu wojny na Ukrainie, liczba publicznych serwerów NTPPOOL[37] w Rosji[38] wzrosła o około 20%, osiągając w 2023 roku rekordową ilość 200 szt. Od w krótkim okresie 6 miesięcy, tzn. czerwca 2024 do grudnia 2024 liczba publicznych serwerów NTP w Rosji podwoiła się i przekroczyła poziom 400szt. Polska liczba serwerów wzrosła o 100% w 2023 roku. Bez odpowiedzi pozostaje pytanie czy taki wzrost to działanie defensywne Polski, czy ofensywne ze strony obcego państwa (zmanipulowane serwery).

Ponadto istnieje techniczna możliwość, utrzymywania serwerów NTP poza granicami własnego kraju[39]. Dla porównania, od czasu wybuchu wojny w Ukrainie w 2022 r., Szwecja aspirująca do wejścia do NATO, zwiększyła populację własnych publicznych serwerów NTP aż dwukrotnie. Dwa lata wcześniej znaczący wzrost serwerów odnotowała Finlandia. Niemcy rekordowo zwiększyły do 900 szt. liczbę publicznych serwerów NTP w roku 2014, a więc w roku aneksji Krymu.



Rys. 38. Od wybuchu wojny Rosja zwiększa znacząco liczbę publicznych serwerów NTP. W grudniu liczba ta przekroczyła 400szt. Typowe zmiany % w POOL.NTP to pojedyncze %. Źródło: https://www.ntppool.org/zone/ru [38]

[37] https://www.ntppool.org.
[38] https://www.ntppool.org/zone/ru.
[39] https://gist.github.com/mutin-sa/eea1c396b1e610a2da1e5550d94b0453.



Rys. 39*a*. Wzrosty 100% ilości serwerów korelują z latami kryzysu ekonomicznego i politycznego

Precyzyjna SI analiza charakterystyk dostępnych za pośrednictwem NTPPOOL prawdopodobnie wskaże wiele ciekawych związków między liczbą publicznych serwerów NTP kraju, a wydarzeniami ekonomiczno- politycznymi w regionie. Charakterystyki Stanów Zjednoczonych i Wielkiej Brytanii (rys 38a) sugerują skojarzenie 100% wzrostu liczby publicznych serwerów z światowym kryzysem finansowym 2008. Czy to zbieg okoliczności, że dwa wiodące w sektorze finansowym państwa zwiększają aż tak bardzo liczbę swoich publicznych serwerów jednocześnie? Wydaje się, że krajowa grupa NTPPOOL jest poważnym kandydatem źródła synchronizacji w przypadku kryzysów gospodarczych, które mogą wywołać niepokoje społeczne, lub gdy istnieje ryzyko konfliktu kinetycznego w danym państwie.

Interesujący opis znajduje się w uzasadnieniu Uchwały[40] Nr 2 Rady ds. Cyfryzacji przy Ministerstwie Cyfryzacji z dnia 3 lutego 2022. Rekomenduje ona Kancelarii Prezesa Rady Ministrów (KPRM) zwiększenie liczby polskich publicznych serwerów NTP krajowej puli. Działanie takie ma charakter prewencyjny. Z jednej strony, ma na celu zmniejszenie statystycznego osłabienia wpływu „złych", celowo podstawionych do domeny *pl.poo.ntp.org* serwerów NTP wprowadzających błędny wzorzec czasu UTC. Z drugiej strony, zapewni to statystycznie bardziej prawdopodobny dostęp do tych „dobrych" zaufanych serwerów NTP.

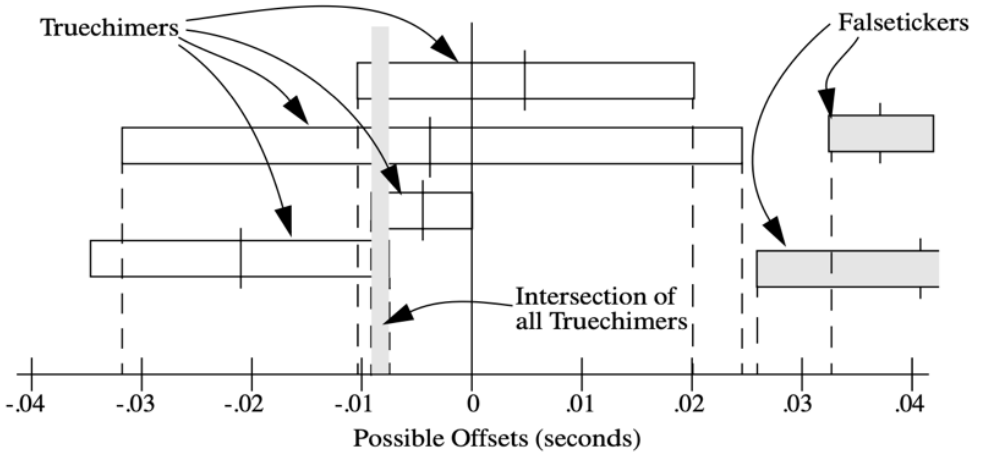
Aby prewencja[40] odniosła skutek niezbędna jest specjalna konfiguracja NTP. Jeżeli zdecydujemy się używać grupę NTPPOOL to powinniśmy używać wyłącznie oprogramowanie źródłowe NTP dostępne do pobrania na stronie *www.ntp.org*. Oprogramowanie to można samodzielnie skompilować ze źródeł C/C++ do wersji binarnej działającej jako usługa na wszystkich wersjach systemu operacyjnego Microsoft Windows. Należy wtenczas zawsze zastosować wiele źródeł NTP wpisanych do pliku *ntp.conf:*

[40] https://www.gov.pl/attachment/a748fde4-8912-4412-b8b2-0718e4e27e0b.

server 0.pl.pool.ntp.org
server 1.pl.pool.ntp.org
server 2.pl.pool.ntp.org
server 3.pl.pool.ntp.org

a następnie uzupełnić:

server tempus1.gum.gov.pl
server tempus2.gum.gov.pl
server tempus3.gum.gov.pl



Rys. 40. Ref. UTC to najmniejszy wspólny przedział, największej grupy „truechimers”
Źródło: D.Deeths, G.Brunette (Sun Microsystems Blueprints 2001)

Używanie wielu źródeł czasu UTC jednocześnie uruchamia wbudowany w NTP mechanizm automatycznego antyspoofingu chroniący przed desynchronizacją. Inaczej mówiąc, używając wielu serwerów NTP jednocześnie, protokół sam potrafi wybrać te „dobre” (ang. *truechimers*) i odrzucić „złe” (ang. *falsetickers*). Mechanizm oparty jest na algorytmie Marzullo[41]. Zaprojektowany został jeszcze w pierwszej połowie lat 80 i służył do ochrony przed desynchronizacją amerykańskich wojskowych systemów obronnych. Jest potwierdzonym doświadczalnie algorytmem decyzyjnym wyboru najlepszego z dostępnych źródeł czasu. Środkowa część prostokąta reprezentuje wskazanie UTC na odległym serwerze NTP. Prawa i lewa strona prostokąta (wielkość obszaru) reprezentuje maksymalny błąd UTC widziany przez klienta NTP. Każdy klient widzi ten sam błąd inaczej, ponieważ zależy to od położenia w sieci, natężenia ruchu, trasy routingu, asymetrii łącz itp. To tak samo jak w relatywistyce Einsteinowskiej – czas jest inny dla każdego obserwatora.

W miejscach, gdzie wojskowe systemy rozproszone OT nie mają dostępu do Internetu i nie mogą skorzystać z eCzasPL, ani z NTPPOOL, wszędzie tam, gdzie praca systemów wymaga zewnętrznej synchronizacji w zabronionych środowiskach dostępności GPS i GNSS, pomocne mogą okazać się mobilne urządzenia synchronizacyjne *Time Loader*. Służą do przenoszenia wzorca UTC, między referencyjną stacją laboratoryjną, a docelowym synchronizowanym systemem obronnym. Wyposażone są w bardzo wysokiej klasy oscylatory podtrzymywania czasu (OCXO lub rubidowe) i zasilanie z akumulatorów. Wspierają pracę wojskowych systemów autonomicznych UAV, Radarów/EO, systemów obrony przeciwrakietowej i dowolnych innych systemów naziemnych, morskich, powietrzno-desantowych, które wymagają zewnętrznej synchronizacji UTC (rysunek 41).

[41] https://en.wikipedia.org/wiki/Marzullo%27s_algorithm.

Rys. 41. Polski przenośny „defibrylator” UTC ELPROMA, po prawej izraelski „Time Loader”. Wielkość urządzenia determinuje czas podtrzymania UTC i zależy od pojemności akumulatorów. Źródło: własne

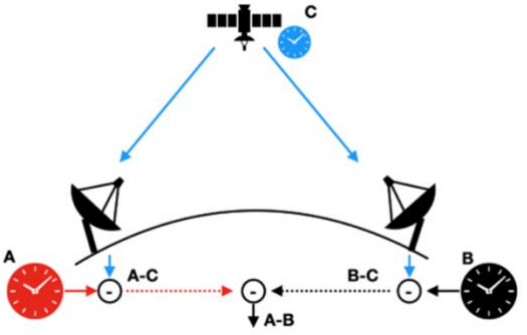
Rys 41a. Reklama izraelskiego mobilnego „defibrylatora” czasu (źródło: Focus Telecom)

5. Ewolucja do systemów autonomicznych skal czasu UTC

Ryzyko skutecznego zakłócania systemów satelitarnych grupy GNSS sprawia, że technika obrała jedyny pozostały kierunek rozwiązania problemu - rozwój autonomicznych skal czasu UTC. Chodzi o zegary *ePRTC* sterowane SI nowej generacji, które zagregowane do pracy w grupach, tworzą koherentne sieci zegarów *cnPRTC*. Pełna autonomia źródła czasu wymaga w pierwszym kroku likwidacji sekund przestępnych UTC *leap second*. Dlatego ITU[42] pilnie dąży do zlikwidowania tej niebezpiecznej dla techniki komputerowej jednej sekundy (źródło [6]). Polska delegacja[43] wniosła tu znaczący wkład do przełamania trwającego od 20 lat impasu negocjacji z Rosją. Okazuje się, że bez ciągłej skali czasu UTC nie może istnieć na dużą skalę autonomia urządzeń, robotów ani samochodów.

Autonomiczne systemy skal czasu UTC to rozwiązania sieciowe. Wyposażone w zegary programowe, które z pomocą SI uczą się charakterystyki atomowych zegarów cezowych. Po kilkunastu tygodniach nauki z użyciem uczenia maszynowego, zegary ePRTC uzyskują zdolność krótko i średnioterminowej predykcji skali czasu UTC. Połączone odpowiednio w grupy (agregacja zegarów) tworzą sieci cnPRTC, które potrafią lepiej przewidzieć przyszłość i zachować zgodność długoterminową względem skali UTC BIPM.

Oczywiście nawet najbardziej inteligentny autonomiczny system skali czasu UTC wymaga okresowej kalibracji zapewniającej poprawność wskazań generowanych wzorców czasu i częstotliwości. Używa się w tym celu techniki *Common View* (CV) obserwacji wspólnych widocznych satelitów (rysunek 42). Zaletą tej metody jest pośrednie wykorzystanie satelity C używane do bezpośredniego porównania wskazań zegarów A i B między sobą.



Rys. 42. Metoda Common View służy do bezpośredniego porównywania wskazań zegarów A i B. Źródło: NIST

Przyszłość autonomicznych skal UTC znacząco wykracza poza zastosowania na Ziemi. Obecnie już trwają w BIPM[44] zaawansowane prace nad księżycową skalą czasu, a w kolejności czeka Mars. Kosmos zmienia się na naszych oczach i staje się miejscem poszukiwań cennych zasobów naturalnych, jakie chcemy importować na Ziemię. To także miejsce rywalizacji o wpływy mocarstw takich jak: USA, Chiny, EU, Rosja i Indie.

[42] https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf.
[43] https://www.gov.pl/web/instytut-lacznosci/polski-sukces-na-konferencji-itu.
[44] https://www.bipm.org/en/-/2023-05-22-moon-time.

Autor dziękuje **Waldemarowi Sielskiemu, Adamowi Widomskiemu, Leszkowi Widomskiemu, Krzysztofowi Borgulskiemu, Mikołajowi Wojciechowskiemu za** uwagi.

Literatura

[1] B. Szafrański, praca zbiorowa „*Cyberbezpieczeństwo redefinicja zagrożeń",* Rozdział XII, W. Paluszyński „*Niedocenione zagrożenie – źródło i dystrybucja czasu*", str.177-214, Wojskowa Akademia Techniczna (2023).

[2] C4ADS Innovation for Peace "*Above us only stars – Exposing GPS spoofing in Russia and Syria*" (2019).

[3] M. J. Murrian, L. Narula, P.A. Iannucci, S. Budzien, B.W. O'Hanlon, M. Psiaki "*First results from 3 years of GNSS Interference Monitoring from Low Earth Orbit*" Aerospace and Ocean Engineering, Virginia Tech, ION, Researchgate (2021).

[4] W. Lewandowski, M. Marszalec "*A Brief History of UTC Leap Second*", JTIT Journal of Telecommunications and Information Technology, No 4 (2023).

[5] M. Smache, A. Olivereau, T. Franco-Rondisson, "*Time Synchronization Attack Scenarios and Analysis of Effective Self-Detection Parameters in a Distributed Industrial Wireless Sensor Network*", in 17th International Conference on Privacy, Security and Trust PST, IEEE (2019).

[6] P. Tavella, T. Widomski (Elproma) "The impact of UTC on Industry 4.0" „*The Future of Coordinated Universal Time*" ITU-News No 02 page 28 (2023)

[7] T. Widomski "*Synchronization security at Smart Gird*", DG-Energy (2017).

[8] P. Tavella, J.X. Mitrovica "*Melting ice solves leap-second problem – for now*", Nature "News & Views Forum", No March 27th (2024).

[9] Praca doktorska "*Security of Time Synchronization for PMU-based Power System State Estimation: Vulnerabilities and Countermeasures*", E. Shereen's Doctoral Thesis in Electrical Engineering, KTH Sweden Royal Institute of Technology (2021).

[10] Zbiorowa praca M. Han, P.A. Crossley, "*Vulnerability of IEEE 1588 under Time Synchronization Attacks*", IEEE Power & Energy Society General Meeting (2019).

[11] Zbiorowa praca W. Alghamdi, M. Schukat i inni, "*Precision time protocol attack strategies and their resistance to existing security*", Cybersecurity, No 4 (2021).

[12] Zbiorowa praca W. Gao, Hong Li, J. Li, M. Lu, "*GNSS Time Synchronization Attack Detection and Discrimination Based on Correlations of Calculated Clock Drift Time Differences*", w: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), September 2020.

[13] Zbiorowa praca T. Widomski, J. Użycki, K. Borgulski i inni, "*Trusted Time Distribution with Auditing and Verification Facilities Project TSI#2*", Conference Precise Time and Time Interval Meeting, ION/PTTI Monterey, California (2016).

[14] Zbiorowa praca Z. Guo, Y. Ni i inni W. S. Wong, L. Shi, "*Time Synchronization Attack and Countermeasure for Multi-System Scheduling in Remote Estimation*", Cornell University (2019).

[14] Zbiorowa praca A. Mujunen, J. Atrokoski, M. Tornikoski, J. Tammi "*GPS Time Disruptions on 26-Jan-2016*" Metsähovin Metsähovi Radio Obserwatory (2016).

[15] T. Widomski, „Analiza zjawiska desynchronizacji czasu jako nowej cyber-broni destabilizującej infrastruktury krytyczne państwa" Praca Dyplomowa MBA Cyberbezpieczeństwo WAT (czerwiec 2024)