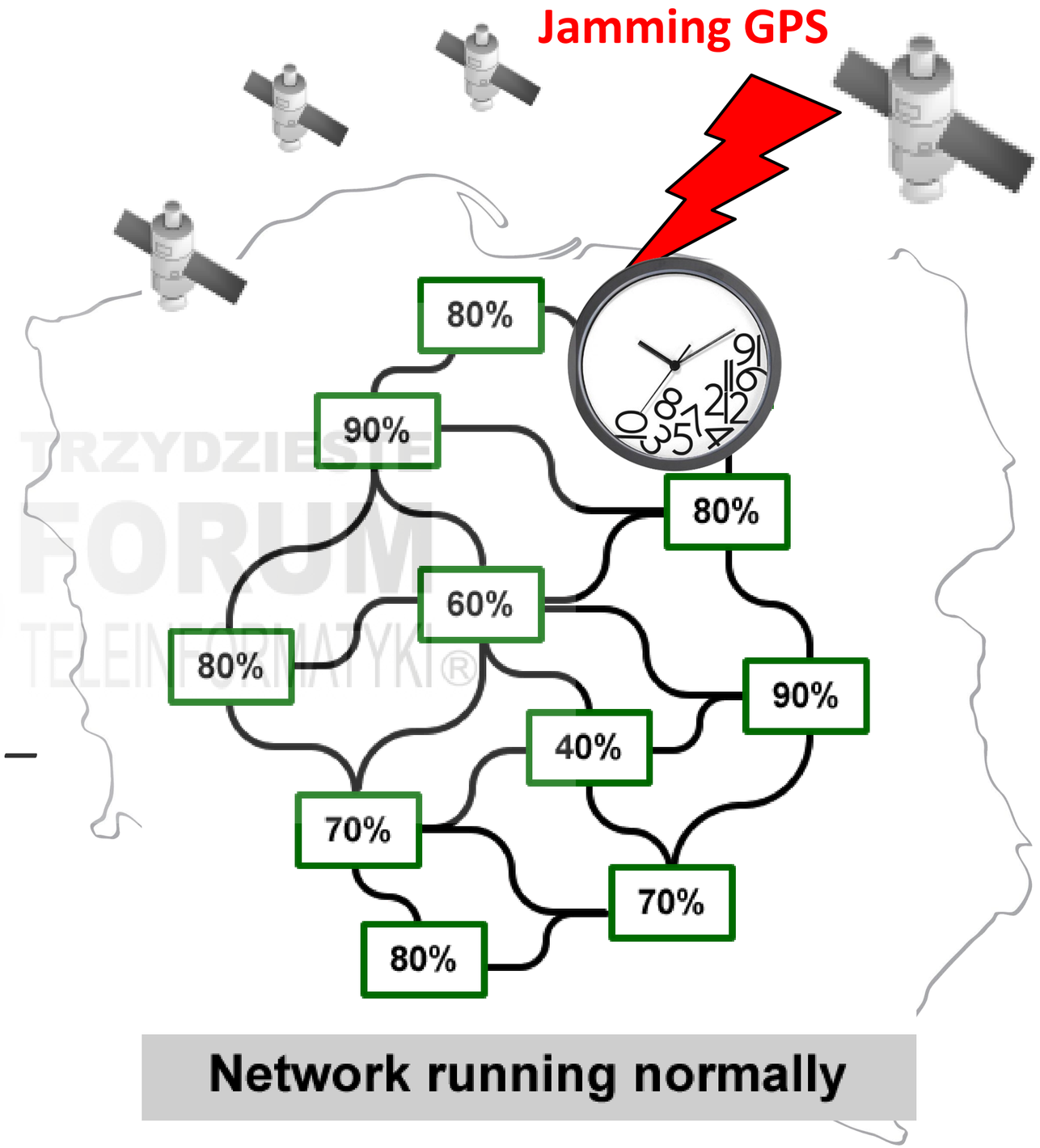
ELPROMA

Tomasz Widomski

Desynchronizacja IT/OT infrastruktury krytycznej państwa z użyciem jammingu i spoofingu GPS – -jak monitorować i zapobiegać".



Desynchronizacja IT/OT...

ELPROMA

1983

COMPUTER SYSTEMS LABORATORY

DEPARTMENTS OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
STANFORD UNIVERSITY · STANFORD, CA 94305

Maintaining the Time in a Distributed System

Keith Marzullo
Susan Owicki

Technical **Report No.** 83-247

August 1983

This research was supported by the National Science Foundation under Contracts NSG MCS M-1536

1992

United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives

February 1992

PATRIOT MISSILE DEFENSE

Software Problem Led to System Failure at Dhahran, Saudi Arabia

RELEASED

RESTRICTED--Not to be released outside the General Accounting Office unless specifically approved by the Office of Congressional Relations.

GAO/IMTEC-92-26

2021

KTH ROYAL INSTITUTE OF TECHNOLOGY

Doctoral Thesis in Electrical Engineering

Security of Time Synchronization for PMU-based Power System State Estimation: Vulnerabilities and Countermeasures

EZZELDIN SHEREEN

Stockholm, Sweden 2021

Desynchronizacja IT/OT...

2023

Rozdział 12

Niedoceniane zagrożenie – źródło i dystrybucja czasu

Wiesław Paluszyński
Polskie Towarzystwo Informatyczne

1. Wstęp

Jest znana anegdota przytaczana przez Marka Abramowicza w latach osiemdziesiątych w Paryskiej Kulturze. Mówi ona o tym jak w 1925 roku Polskie Radio rozpoczęło nadawanie programu i w południe podawało z dokładnością do pół sekundy wzorcowy sygnał czasu z obserwatorium astronomicznego w Krakowie. Tak duża dokładność robiła wielkie wrażenie w kraju i za granicą. Redakcja jednego z dzienników wysłała dziennikarza do profesora Tadeusza Banachiewicza, żeby dowiedzieć się skąd astronomowie wiedzą, kiedy jest południe z tak fantastyczną dokładnością. Profesor Banachiewicz wyjaśnił jak bardzo to jest proste mówiąc: „Reguluję swój zegarek codziennie rano w drodze do pracy, kiedy przechodzę obok witryny sklepu zegarmistrzowskiego, który oferuje szwajcarskie zegarki najlepszych marek. Używając wskazań swojego zegarka uderzam punktualnie w południe w kowadełko i sygnał ten emituje na terenie kraju Polskie Radio."

Dziennikarz udał się do sklepu zegarmistrzowskiego, aby zapytać sprzedawcę skąd ten wie, jak ustawić zegary na witrynie z tak dużą dokładnością i usłyszał odpowiedź:
„Codziennie włączam radio i w południe profesor Banasiewicz podaje mi dokładnie z dokładnością do pół sekundy informacje, kiedy jest południe i ustawiam swoje zegary."

Niezależnie od tego jak śmieszna jest ta anegdota, zawiera ona bardzo głęboką prawdę, że nie ma żadnej innej metody sprawdzania zgodności czasu pokazywanego przez zegary niż porównywanie ich wskazań między sobą[1]. Synchronizacja wymaga więc zawsze zaufanego dokładnego źródła odniesienia, a jego fałszowanie będzie miało daleko idące konsekwencje dla bezpieczeństwa ludzi i maszyn.

Blisko 100 lat później, w XXI wieku znaczenie synchronizacji zaczęło odgrywać szczególną rolę, zmieniając paradygmat cyberbezpieczeństwa zbyt zależnej od GNSS silnie zautomatyzowanej rozproszonej architektury każdej infrastruktury krytycznej. Stało się to na tyle istotnym zagadnieniem stabilności systemów teleinformatycznych w erze przemysłu 4.0, że w lutym 2020 roku prezydent USA Donald Trump podpisał specjalną dyrektywę EO13905[2], rekomendującą uniezależnienie amerykańskich infrastruktur krytycznych od GPS. Okazało się, że zamiast łamać zabezpieczenia chronione matematycznie Infrastrukturą Klucza Publicznego (PKI), znacznie prościej jest destabilizować pracę infrastruktury manipulując czasem pochodzącym z satelitów GNSS

[1] Fragment wystąpienia Stanisława Bajtlika „Co to jest czas", https://youtu.be/BGE_kn1aM80.
[2] US Federal Register – The Daily Journal US Presidential Executive Order EO13905, https://www.govinfo.gov/app/details/DCPD-202000071.

2024

Rozdział XXIX

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]. Rozdział odpowie na pytanie, dlaczego systemy PNT ewoluują do A-PNT, (*ang. A-Assured Positioning, Navigation and Timing*) i w przyszłości zwiększać będą autonomię pracy. Autor zachęca do zapoznania się z pozycją[2] literatury [1] będącej ważnym wstępem do poruszanej tu tematyki.

1. Wstęp

Konflikt między Rosją a Ukrainą zmienił nasze postrzeganie wojny elektronicznej i cyberbezpieczeństwa. 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.

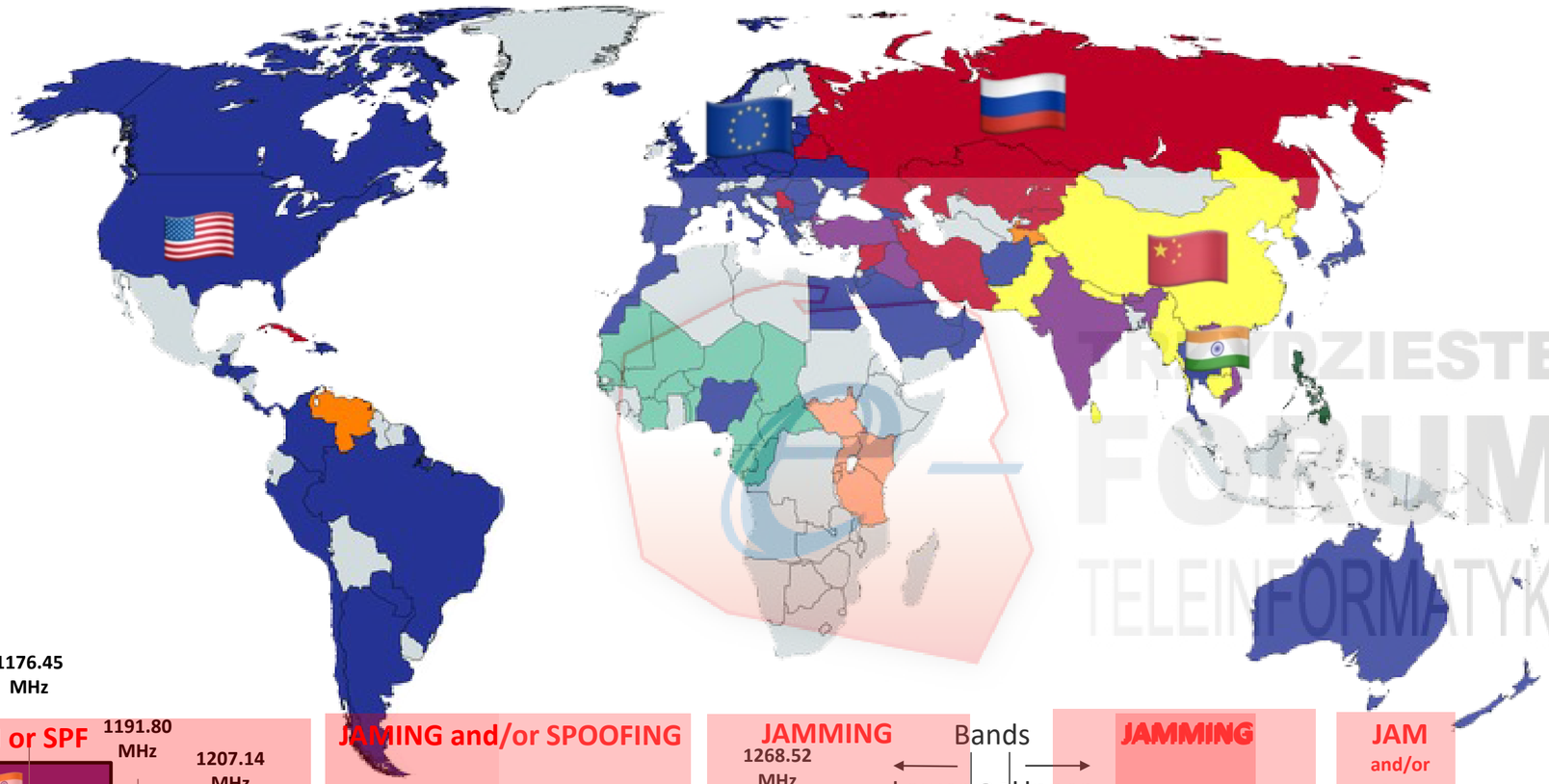
Desynchronizacja IT/OT…

- Desynchronizacją można ***destabilizować*** każdy system IT / OT **NIS2**.
- Manipulując czasem można wywołać ***blackout*** infrastruktury krytycznej.
- Obecny ***jamming GPS*** jest testowaniem Polski i ma uśpić czujność.
- Zasadniczy 2-gi atak ***spoofingiem GNSS*** nastąpi później i będzie skuteczny.

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

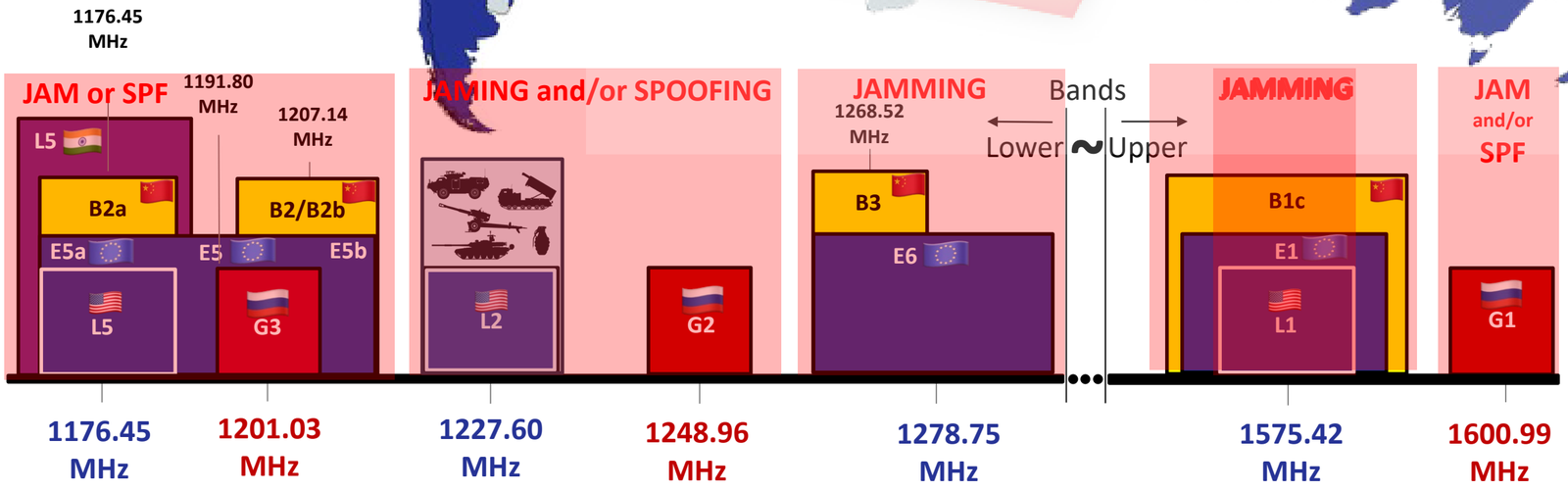
Desynchronizacja IT/OT...

ELPROMA



WSZYSTKIE SYSTEMY SĄ WOJSKOWE!

GPS		
BEIDOU		
GLONASS		
IRNSS		
GALILEO		CIVIL



Dwa nowe ataki:

- Time Sync Attack
- Time Delay Attack

Desynchronizacja IT/OT…

Nieprawidłowym (**dezinformacja**) jest zbytnie medialne uogólnienie, że:

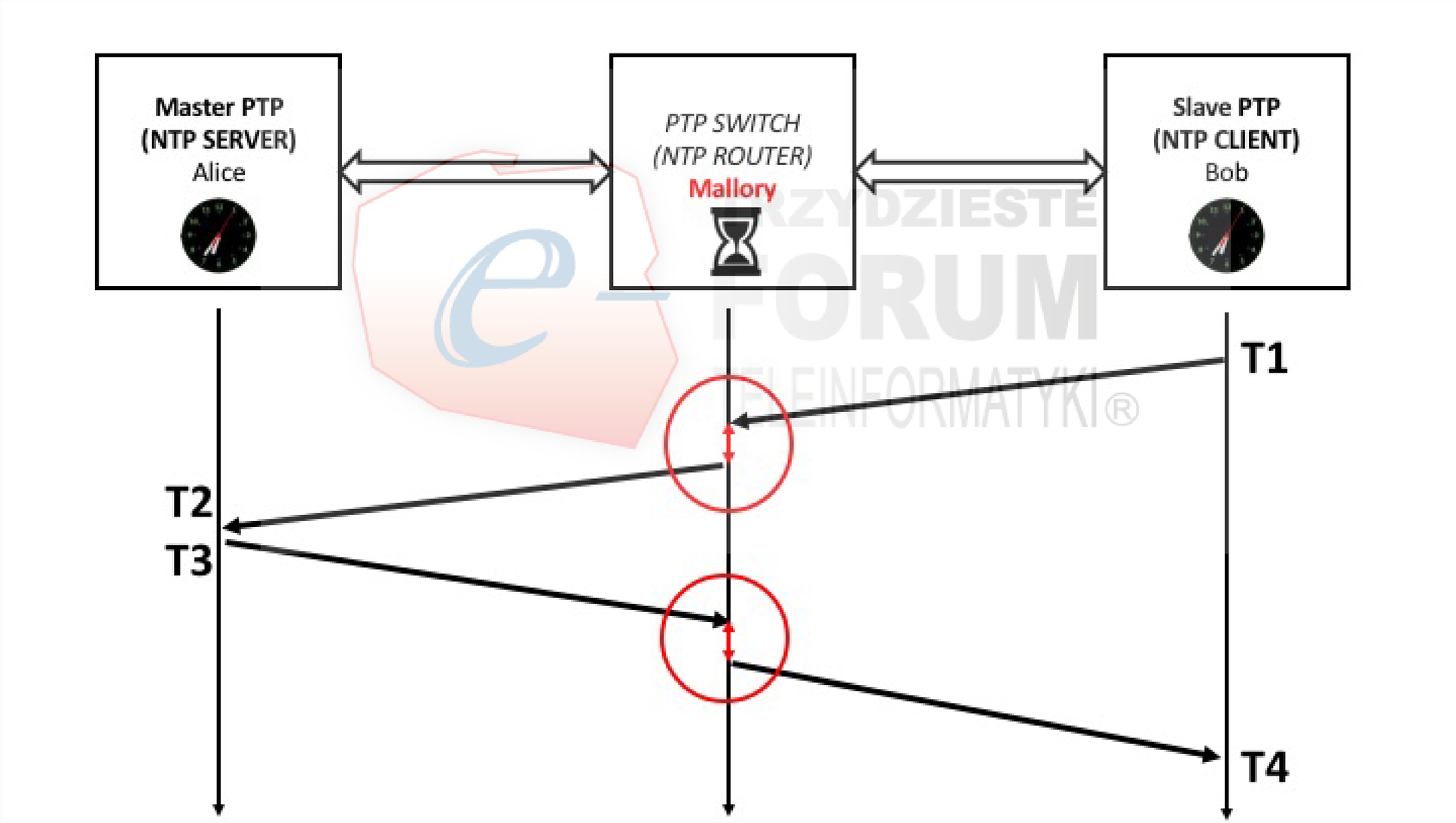
- Jamming i spoofing GPS dotyczy wyłącznie **samolotów** w powietrzu

Uprawnionym (**informacja** poparta testami symulacji) jest że desynchronizacją można ***destabilizować*** każdy system IT / OT określony w dyrektywie **NIS2**:

- Jamming i spoofing GPS dotyczy w szczególności np. **ruchu kolejowego**
- Systemy naziemne **PAŻP**, bankowość, sektor finansowy (**GPW**), systemy **ZUS**, przemysł40 (**automatyka i sterowanie**), medycynę (GPS jest w RM i TK) itp. Manipulując czasem można wywołać ***blackout*** *każdej* infrastruktury IT/OT,
- Obecny ***jamming GPS*** jest wstępem i testowaniem odporności Polski To element współczesnej **wojny elektronicznej** w cyberprzestrzeni.

Desynchronizacja IT/OT...

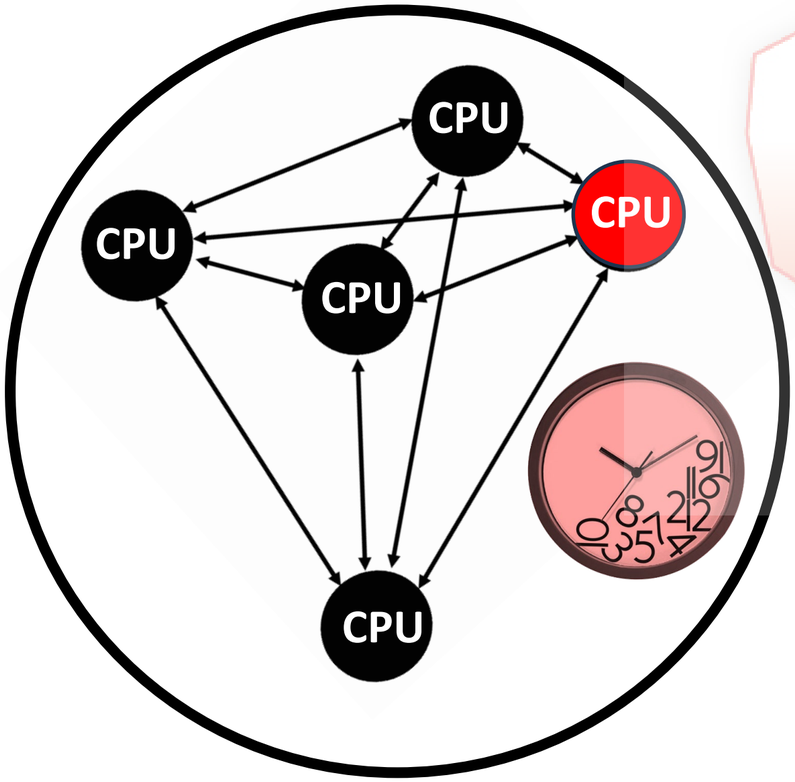
Atak na opóźnienie dotyczy komunikacji sieciowej TCP/IP i protokołów NTP/PTP



Desynchronizacja IT/OT...

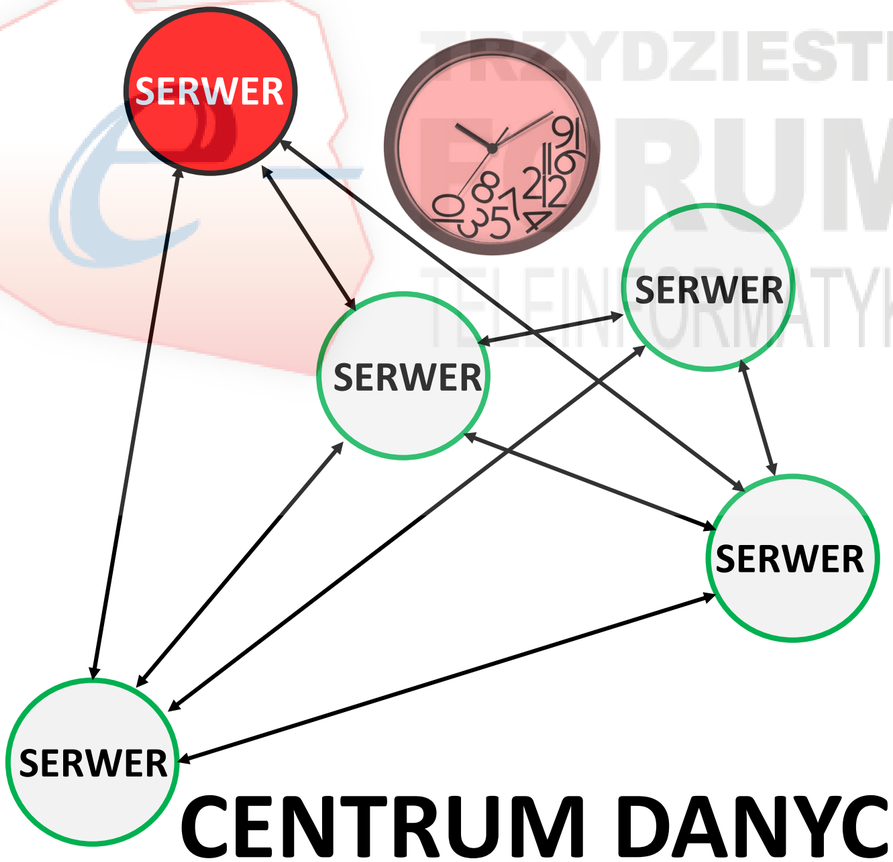
Desynchronizacją jest zagrożona każda **rozproszona architektura** IT i OT, zarówna ta rozproszona do **wewnątrz** jak i na **zewnątrz**, oraz te **hybrydowe**.

rozproszenie do wewnątrz



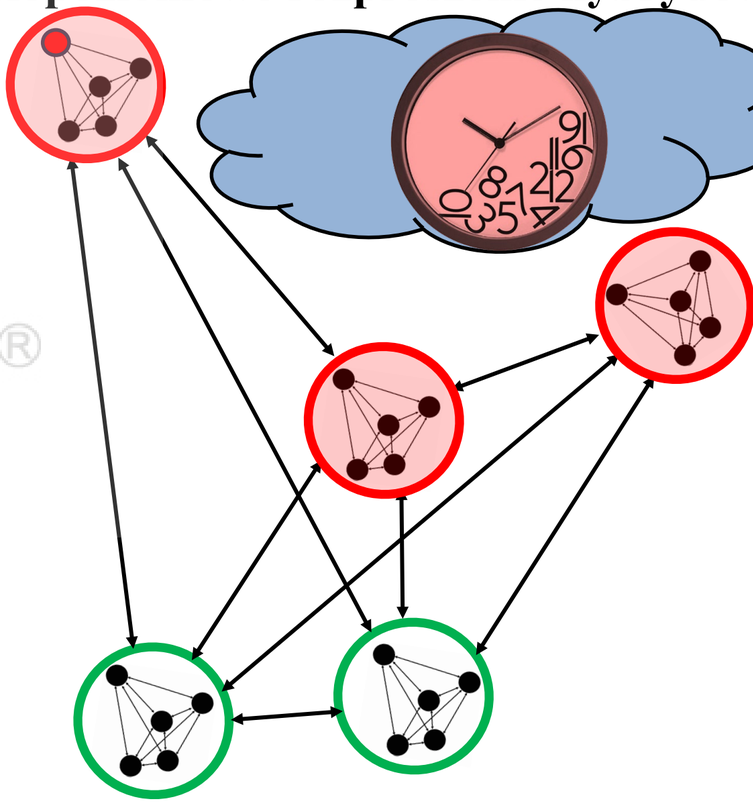
SERWER

rozproszenie na zewnątrz



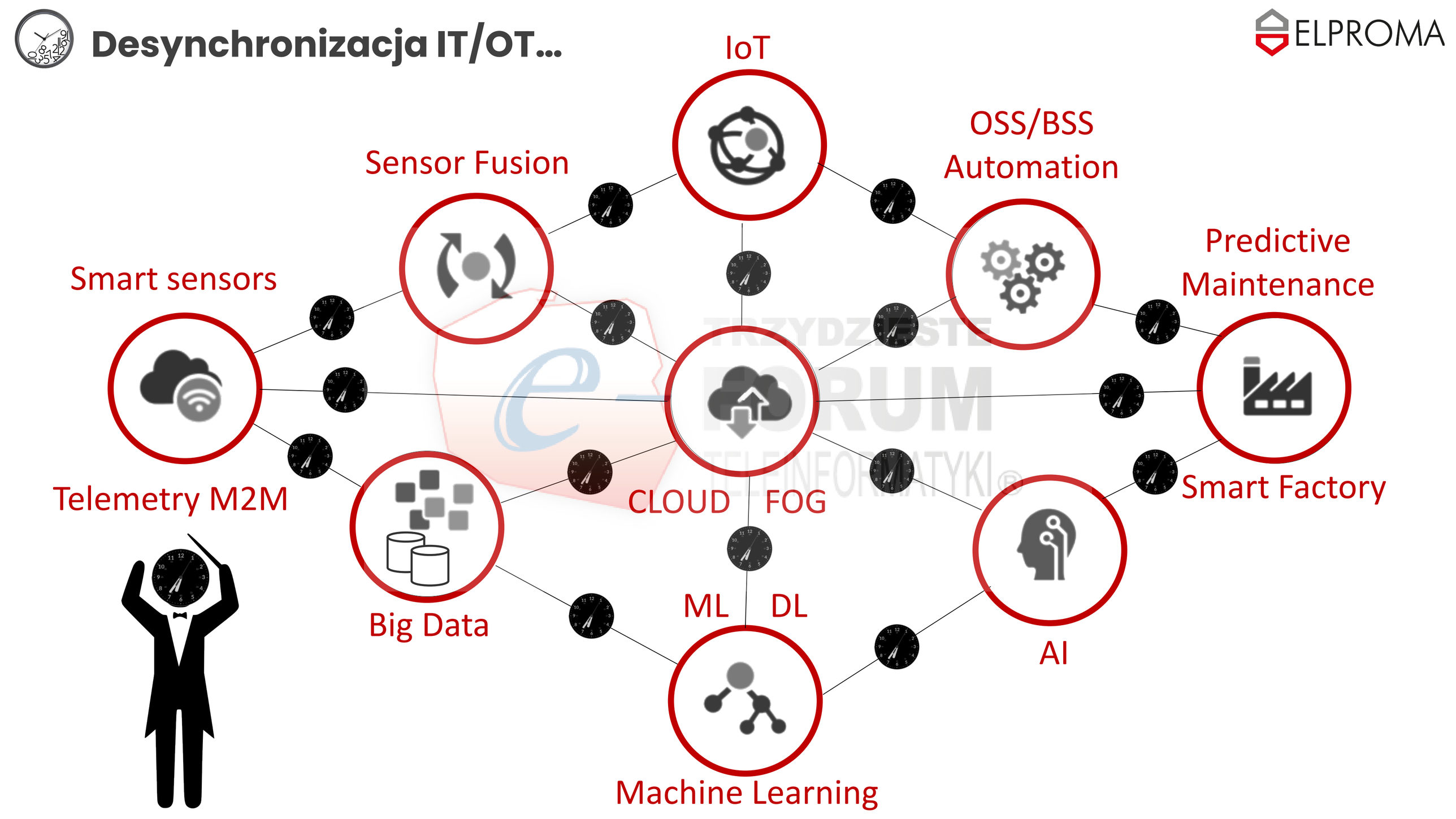
CENTRUM DANYCH

wielopoziomowe rozproszenie hybrydowe



CHMURA

Desynchronizacja IT/OT...



Desynchronizacja IT/OT…

ELPROMA

Desynchronizacją rozproszonej architektury IT / OT infrastruktury krytycznej można doprowadzić do kryzysu

Incydent GPS
Jamming/Spoofing

Kryzys organizacji

Kryzys infrastruktury

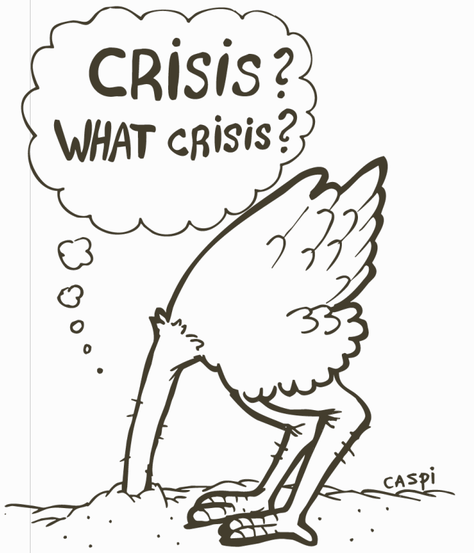
Kryzys ekonomiczny

Kryzys społeczny

Kryzys polityczny

Kryzys państwa

Kryzys światowy



- **Zbyt duża zależność** IT / OT od GPS
- **Wojskowa natura** systemów GPS, GLONASS, BEIDOU, IRNSS
- Duże rozproszenie i **rosnąca wzajemna współzależność** systemów
- **Jamming i spoofing GPS blokuje** pracę odbiorników i systemów IT / OT
- **Nieświadomość** używania rosyjskiego GLONASS
- Desynchronizacja **może wywołać efekt lawinowy**

Desynchronizacja IT/OT…

ELPROMA

Destabilizacja wspólnej domeny czasu UTC to skuteczne narzędzie CYBERATAKU na każde państwo

PRZYKŁADOWE CELE

- 5G – MIN. WYDAJNOŚĆ + AWARIASYSTEMU
- DVB-T2 – BRAK CYFROWEJ TELEWIZJI/RADIA
- ENERGETYKA – PRZERWY W DOSTAWACH
- PKP - WSTRZYMANIE RUCHU KOLEJOWEGO
- PAŻP - DESTABILIZACJA RUCHU LOTNICZEGO
- 112 – AWARIA KRYTYCZNA SYSTEMU
- SMART CITY - PARALIŻ
- BANKI - ZAKŁÓCENIA TRANSAKCJI
- GPW – WSTZRYMANIE OPERACJI FINANS.
- CLOUD - BLOKADA KANAŁÓW SZYFROWANCH
- NIEKOMPLETNE ARCHIWIZACJE DATA CENTER
- ROZSTROJENIE INDEKSÓW SQL I BACKUPÓW
- FAŁSZOWANIE DATY I MIEJSCA TRANZAKCJI ELEKTRONICZNYCH, LICYTACJI, LOTERII
- DESTRUKCYJNY WPŁYW NA SYSTEMY AUTOMATYKI PRZEMYSŁOWEJ

JAK?

1. ZAGŁUSZANIE/FAŁSZOWANIE GPS (GNSS)
2. ZAKŁÓCENIE SATBILNOŚCI DOMENY CZASU UTC
3. WPROWADZANIE SZTUCZNYCH OPÓŹNIEŃ LAN
4. ATAKI HAKERSKIE DDOS GENERUJĄ SZUM DELAY LAN

PRZYKŁADOWE EFEKTY

- DESTABILZACJA PAŃSTWA
- GŁĘBI LOGISTYCZNEJ NATO
- WYWOŁYWANIE KRYZYSÓW
- W KONSEKWENCJI SPADEK PKB
- WYWOŁANIE PANIKI SPOŁECZNEJ
- SPADEK WARTOŚCI WALUTY PLN
- FLUKTUACJE W KLUCZOWYCH SEKTORACH GOSPODARKI I INFRASTRUKTURZE KRYTYCZNEJ
- UTRATA I WYCIEK DANYCH IT
- ZAGROŻENIE BEZPIECZEŃSTWA NARODOWEGO

Bo okazuje się, że prościej jest destabilizować niż hakować

Desynchronizacja IT/OT…

ELPROMA

Jamming i spoofing GPS wnoszą również ryzyko desynchronizacji rozproszonej architektury IBCS

Desynchronizacja IT/OT...

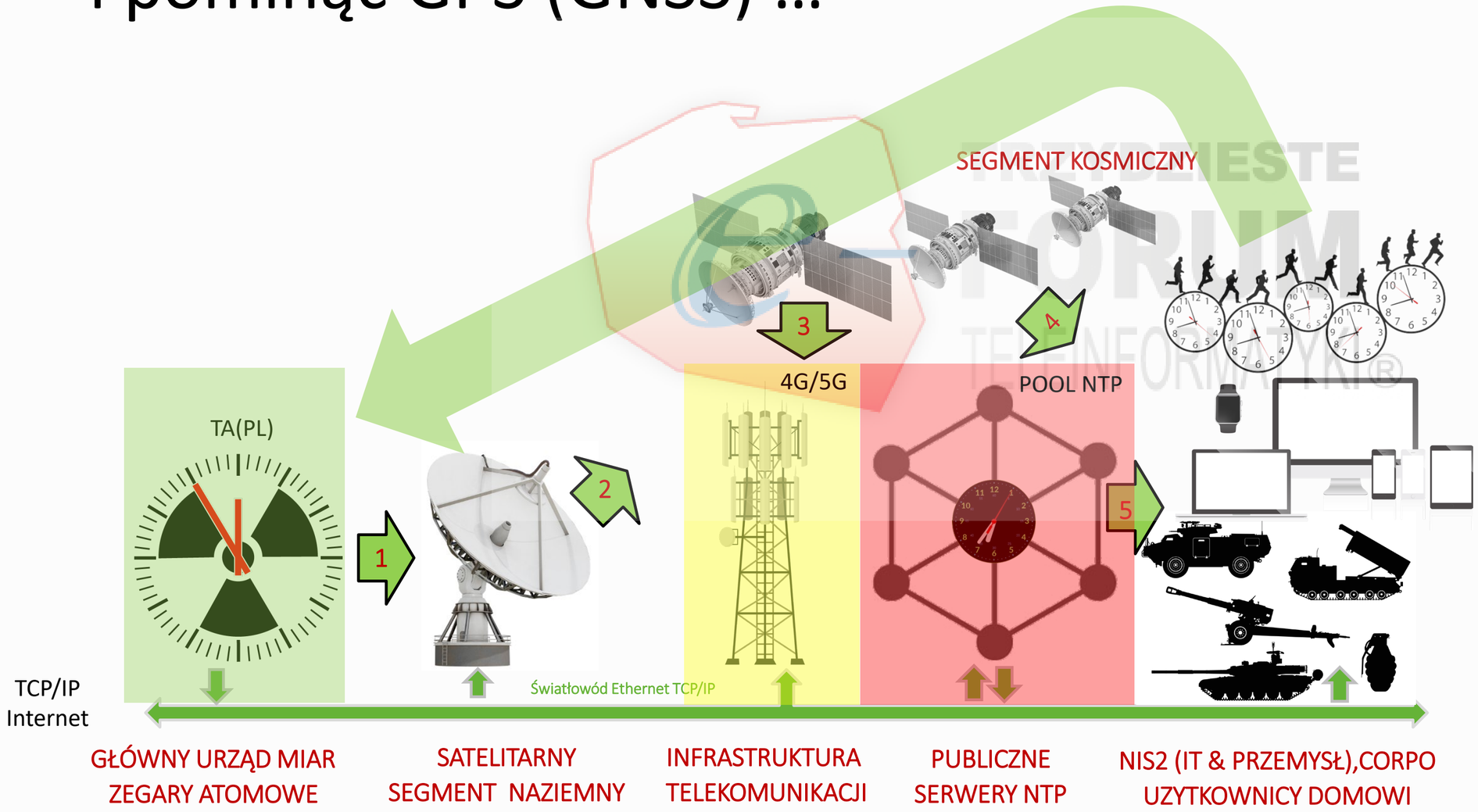
Desynchronizacją rozproszonej architektury IT / OT infrastruktury krytycznej można doprowadzić do kryzysu

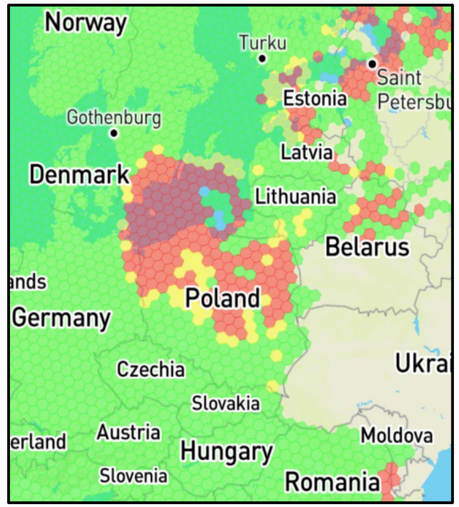
Sector	Accuracy	Resilience	Threats	Immutability	Scale	Traceability	Intuitive
Power	1µs	★★★	★★★	★	1,000s	★	★
Telecoms	1µs	★★★	★★★	★	10,000s	★	★
Military	10µs	★★★	★★★	★★	10,000s	★	★
Finance	100µs	★★	★★★	★★★	10,000s	★★★	★★
Gambling	1ms	★	★	★★★	10,000s	★★★	★
Real-time bidding	1ms	★	★	★★	10,000s	★★	★
Gaming	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	★★★	★★★

Desynchronizacja IT/OT…

ELPROMA

Chodzi o to aby skrócić drogę synchronizacji i pominąć GPS (GNSS) …



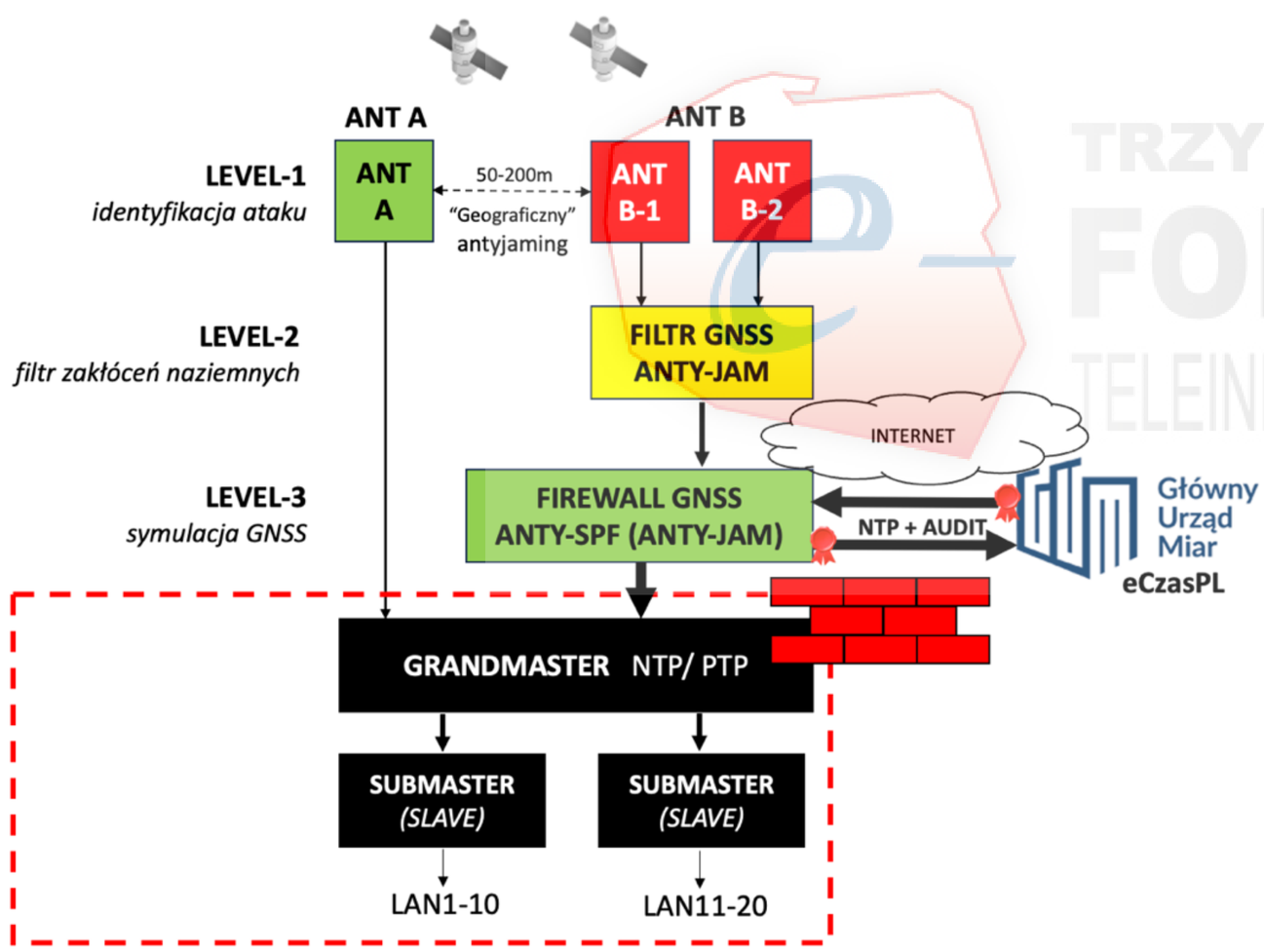


- **Energia**
- **5G/6G**
- **Transport (PKP, PAŻP)**
- **Bankowość i giełda GPW**
- **Zdrowie publiczne**
- **Woda i ścieki**
- **Żywność i odpady**
- **Infrastruktura cyfrowa**
- **Administracja publiczna**
- **Obronność , służby**
- **Nauka**

Desynchronizacja IT/OT…

ELPROMA

Polska może bronić się przed jammingiem GPS
Dołączać IT / OT do czasu urzędowego GUM (eCzasPL)



Konwergencja (teraz):

- Centralizacja (eCzasPL)
- Decentralizacja (Galileo)

Konflikt kinetyczny (później)

- wzmocnić ***pl.ntp.pool.org***
- Uchwała #2 RdC KPRM (z dnia 20/02/2022)

ELPROMA

Problematyczny GPS jamming ? ARGOS to rozwiązanie!

- Systemy IT i OT mogą się chronić przed jammingiem GPS, ale musza o nim wiedzieć (*być zaalarmowane odpowiednio wcześnie po to aby przestać używać GPS*)

- NIS2 definiuje 11 infrastruktur krytycznych wymagających szczególnej uwagi w zapewnieniu cyber-bezpieczeństwa. Wszystkie używają GPS, o czym nie wiemy

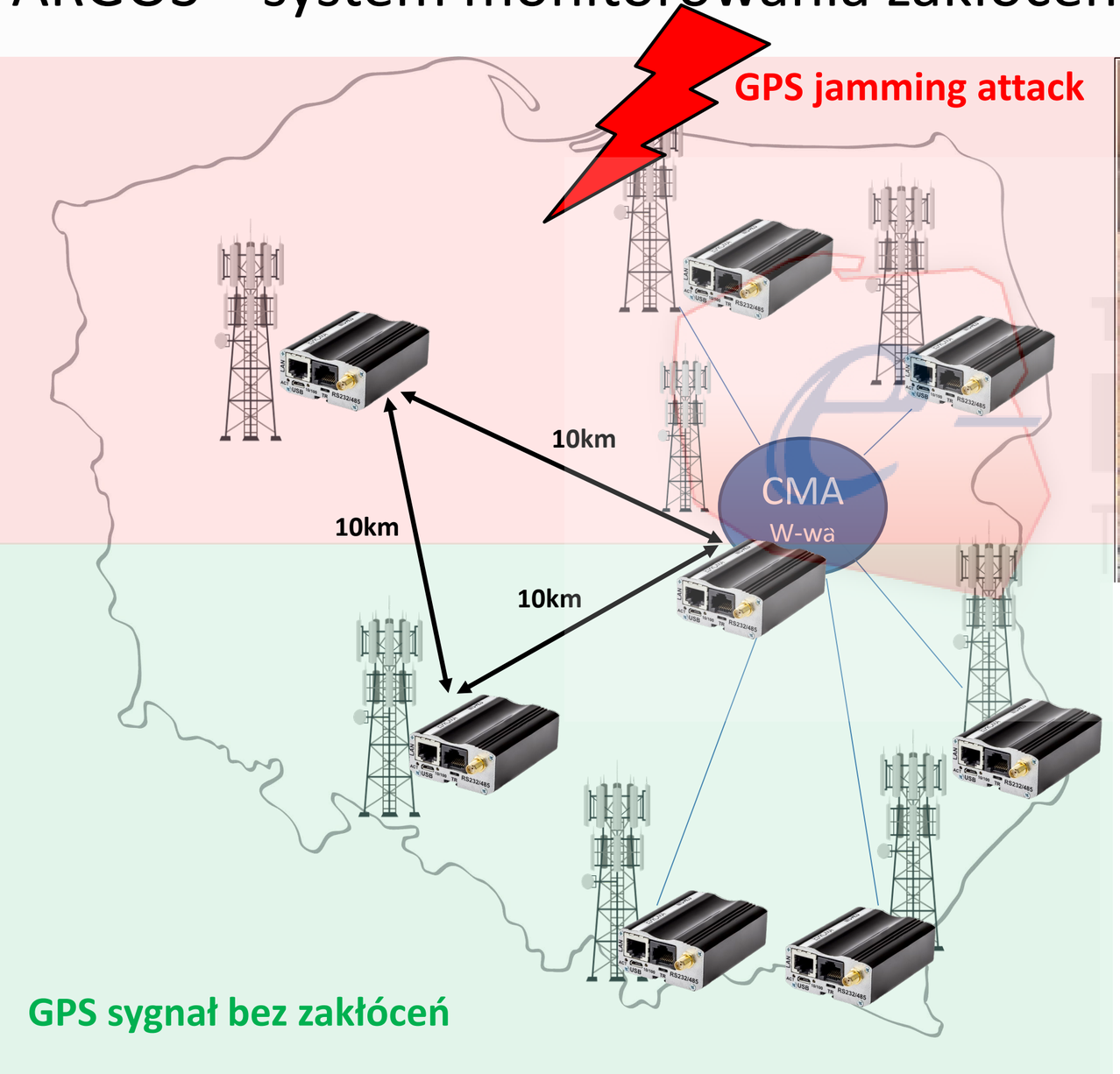
- ARGOS pozwala zapobiegać awariom. i jest narzędziem rozpoznania ataku na GPS na Polskę. Pozwala się przygotować.

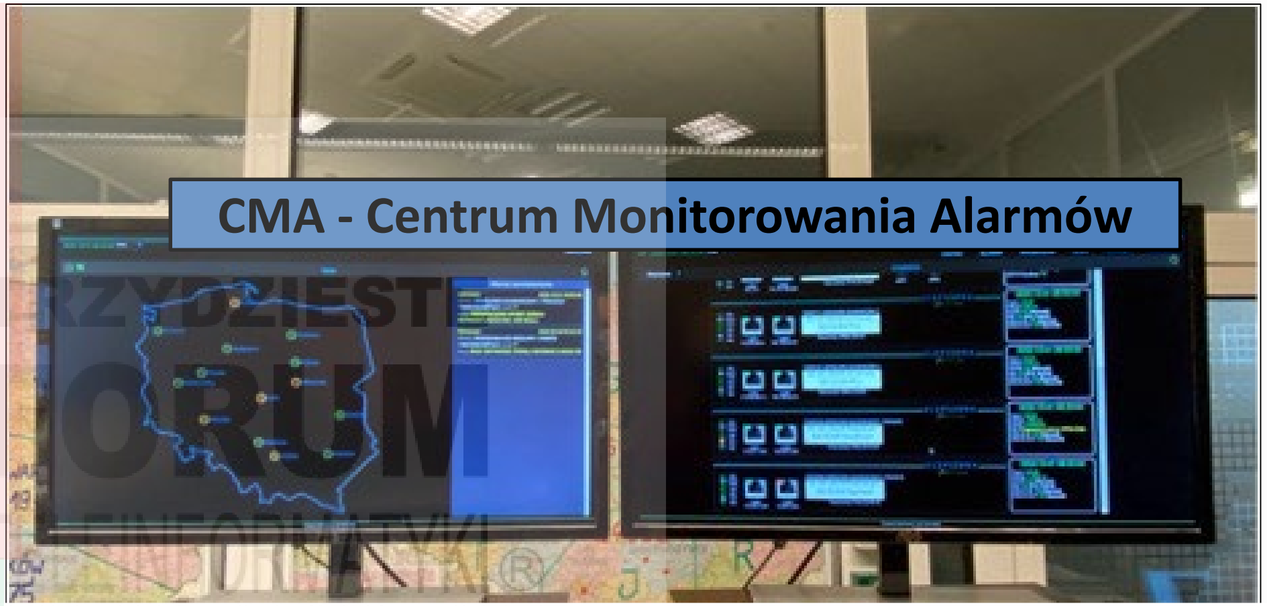
Synchronizacja zależna od GPS używana jest przez IT, automatykę w przemyśle OT oraz systemu obrony przeciwlotniczej

Desynchronizacja IT/OT...

ELPROMA

ARGOS – system monitorowania zakłóceń GPS jamming/spoofing z powiadamianiem





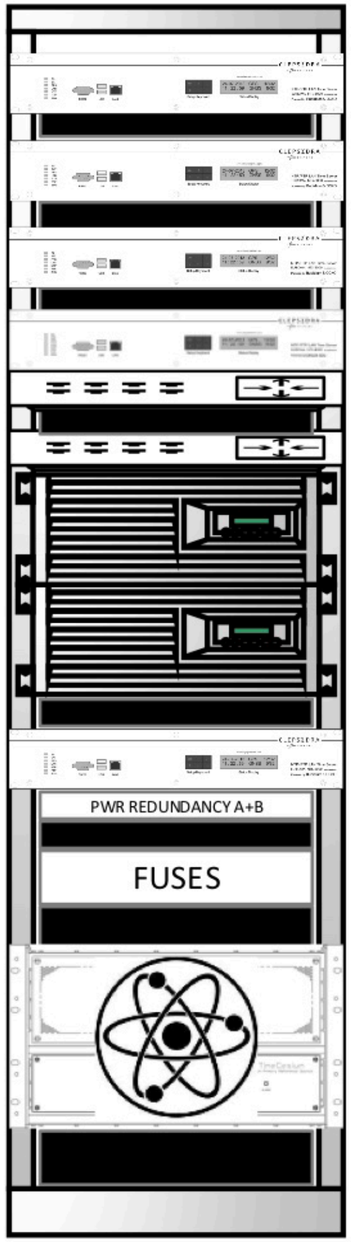
Funkcje

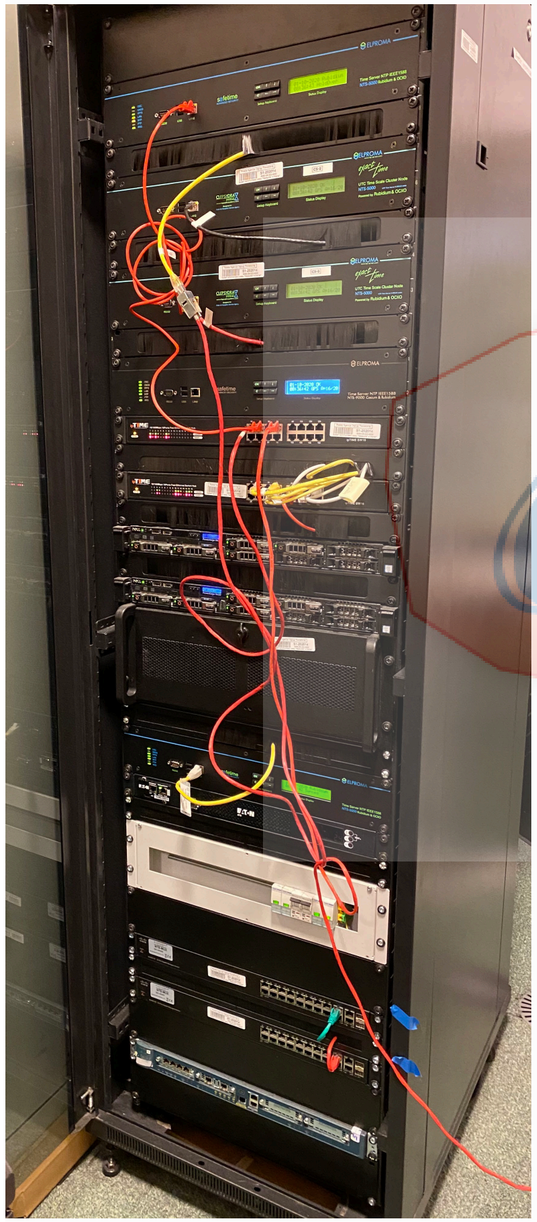
- Wykrywa ataki jamming GPS
- Wykrywa ataki spoofing GPS
- Alarmuje służby, przemysł i IT
- Pozwala zapobiegać awariom

Desynchronizacja IT/OT...

Desynchronizacja IT/OT…

ELPROMA





Oferta:

- Serwery czasu NTP i PTP IEEE1588
- Serwery znakowania czasem TSA (rfc3161)
- Filtry anty-jammingowe GPS
- Time-firewalle izolujące Twoje IT od GPS
- Systemy autonomicznych skal czasu UTC
- Włączamy IT do eCzasPL GUM RP
- Projektujemy laboratoria UTC dla IT
- Wdrażamy i szkolimy bezpieczeństwo IT w obszarze zagrożeń desynchronizacją…

www.elpromaelectronics.com

ELPROMA

Dziękuję za uwagę

Tomasz Widomski
t.widomski@elpromaelectronics.com