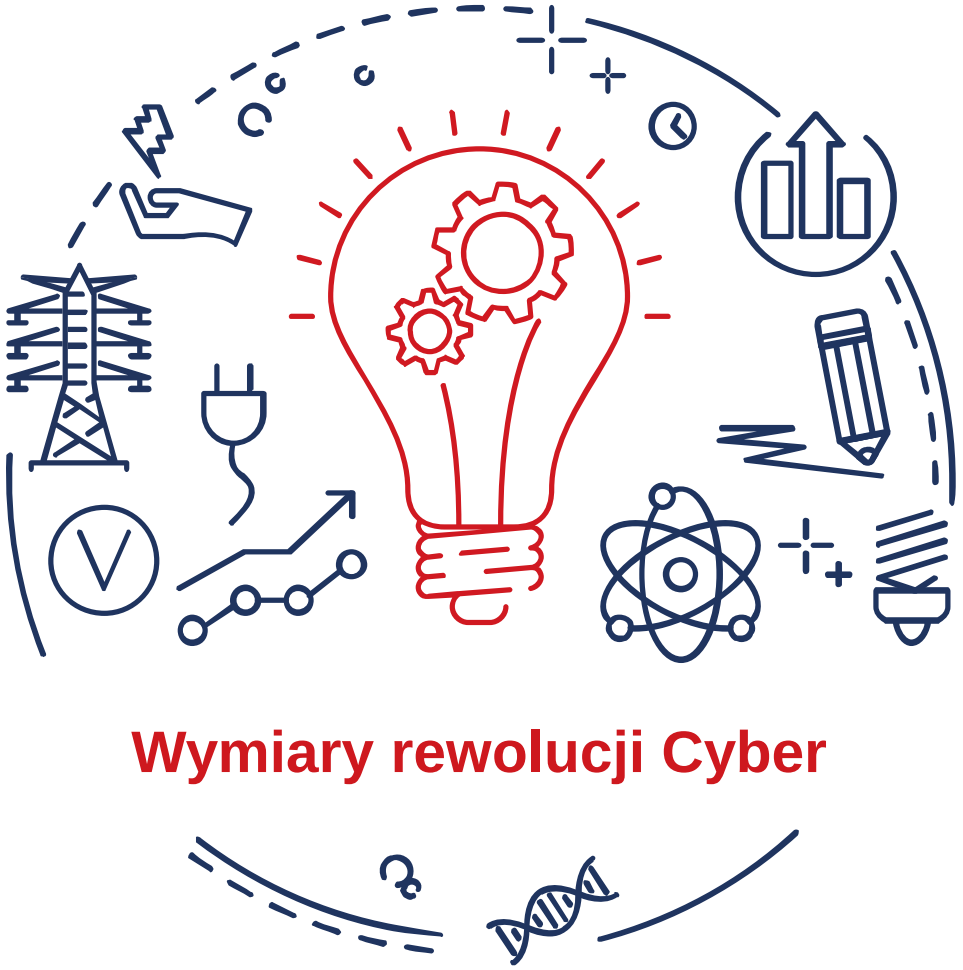
Polskie Sieci Elektroenergetyczne S.A.

Znaczenie cyberbezpieczeństwa dla niezawodności dostaw energii elektrycznej - bieżące i przyszłe wyzwania

Grzegorz Bojar, Jarosław Sordyl, Jeremi Gryka

REE 2018 | Kazimierz Dolny | 25 kwietnia 2018 r.



Wymiary rewolucji Cyber

Cyber-świat na wyciągnięcie ręki

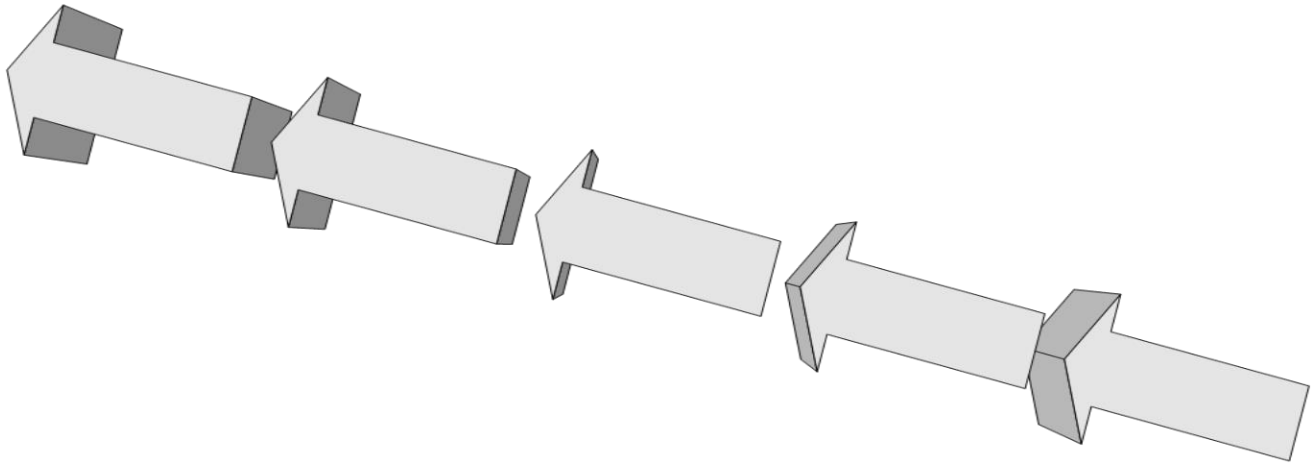
Naukowcy mówią wprost - to co do niedawna znaliśmy z literatury Stanisława Lema, na przestrzeni kilku lat stanie się rzeczywistością.

2016.09.21 / Poznań, Uniwersytet Ekonomiczny, Cybernetyka

Cyberbezpieczeństwo stało się często używanym terminem.

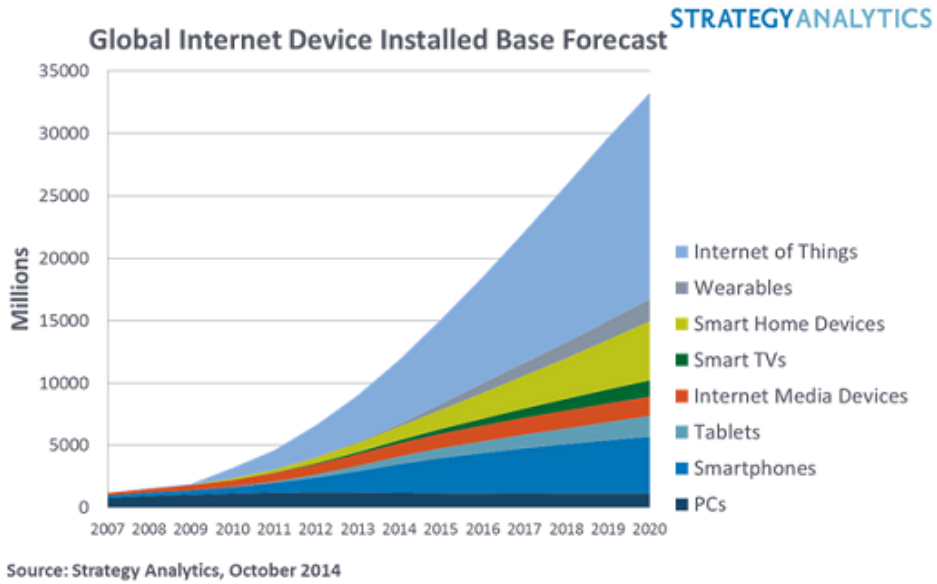
Dotyczy Cyber Świata, czyli wszystkich obszarów działalności organizacji i osób fizycznych, gdzie w jakikolwiek sposób używane są technologie komputerowe.

Cyber Świat jest bardzo złożony i podlega szybkiej ewolucji w wielu wymiarach.



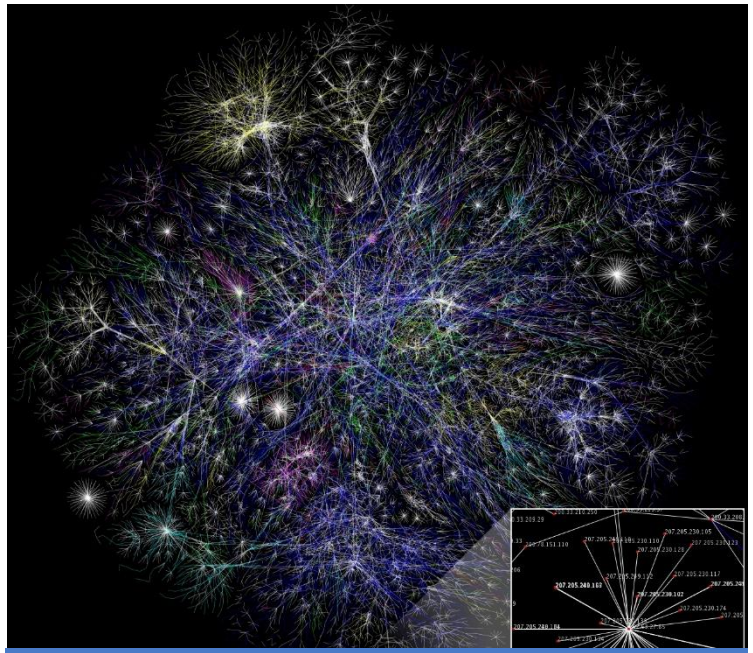
- **Wymiar 1 – ROZWÓJ TECHNOLOGICZNY**
  - **Ciągły rozwój technologiczny w technikach komputerowych**
    - rośnie szybkość przetwarzania
    - postępuje miniaturyzacja
    - powstają nowe funkcjonalności
    - wzrasta niezawodność
  - **Przybywa zastosowań technologii cyfrowych w urządzeniach technicznych**
    - rozwiązania profesjonalne
    - rozwiązania powszechnego użytku

- **Wymiar 2 – PRZYROST WOLUMENU**
  - **Wzrost liczby systemów komputerowych**
    - 100 mln serwerów
    - 2 mld komputerów personalnych
    - 3 mld smartfonów
      – *liczby trudne do potwierdzenia*



Source: Strategy Analytics, October 2014

- **Lawinowy przyrost liczby urządzeń, przedmiotów i organizmów z wbudowanymi „chip'ami"**
  - prognozuje się 30 – 50 mld hostów w 2020 roku



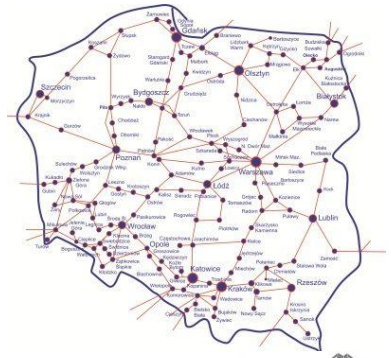
- **Wymiar 3 – SIECI**
  - **Połączone systemy informatyczne**
    - sieci prywatne (technologiczne, Intranet, Extranet)
    - sieci publiczne (Internet)

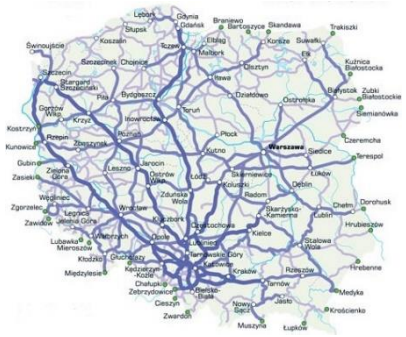
    bardziej połączone, większe, szybsze

  - **Połączone „rzeczy”**

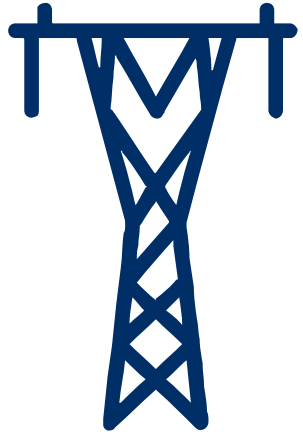
    Internet of Things (IoT)

    w sposób niemal niekontrolowany, powstaje i rozwija się świat połączonych urządzeń, które wykonują różne czynności



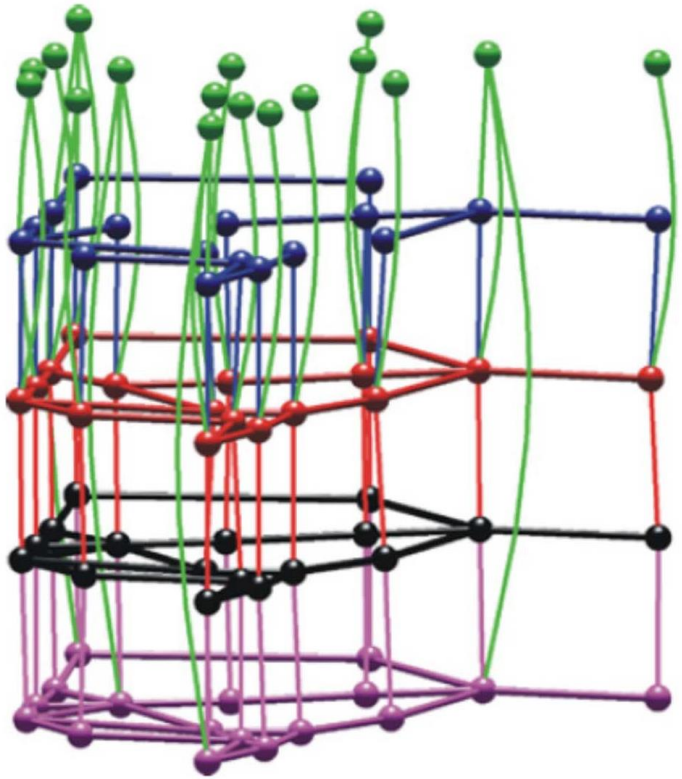


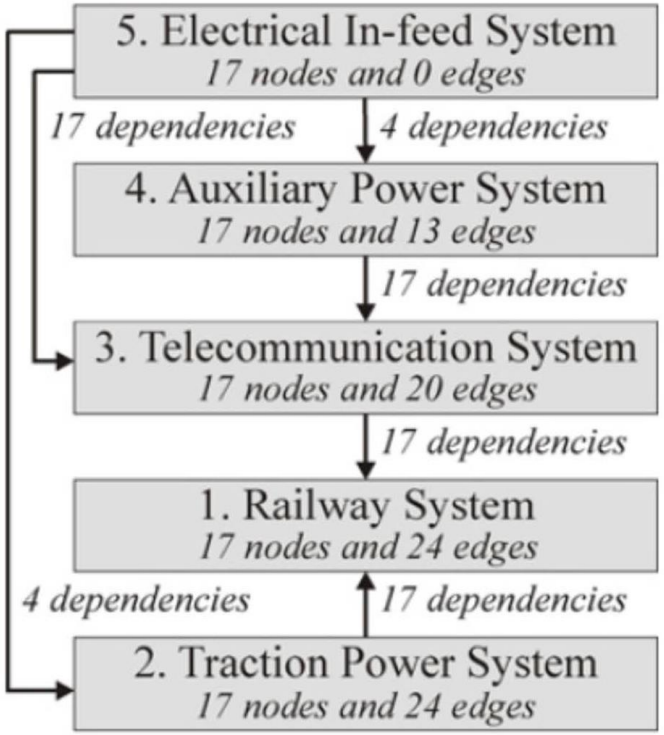
- **Wymiar 3 – SIECI = SYSTEMY**
  - **Telekomunikacyjne**
    - sieci naziemne
    - GSM
  - **Energetyczne**
    - elektroenergetyczne
    - gazowe
    - paliw płynnych
  - **Transportowe**
    - lotnicze
    - kolejowe
    - drogowe
    - wodne
  - **…**



- **Wymiar 4 – WSPÓŁZALEŻNOŚCI**
  - **Różne sieci / systemy mają na siebie wpływ, czyli w rzeczywistości są połączone**

National level interdependencies





Johansson and Hassel 2010

- **Sieci są GLOBALNE**

Różne sieci / systemy są połączone międzynarodowo i mają na siebie wpływ pomiędzy krajami, czyli wzajemny wpływ może być propagowany w regionie, kontynentalnie, a nawet globalnie

- **Wymiar 4 – WSPÓŁZALEŻNOŚCI**

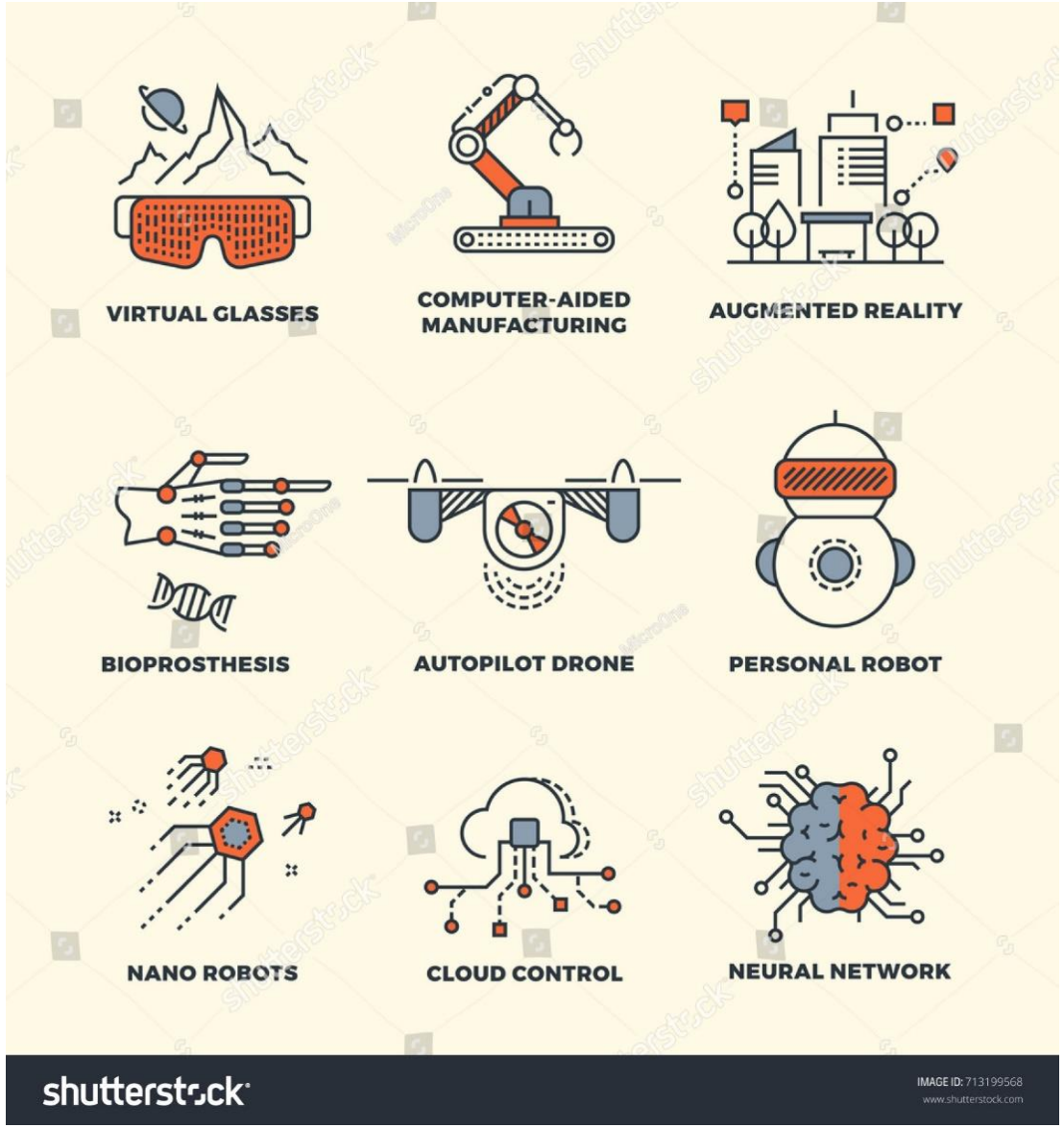
Sieć elektroenergetyczna w porównaniu z innymi sieciami energetycznymi charakteryzuje się:

- zdecydowanie większą liczbą węzłów,
- dużo większą złożonością,
- bliskim wzajemnym wpływem połączonych systemów różnych krajów,
- bardzo krótkim czasem propagacji wpływu zdarzeń sieciowych.

Na samodzielne działanie sieci elektroenergetycznej składa się działanie dwóch nakładających się sieci wewnętrznych: sieci elektrycznej oraz sieci teleinformatycznej. Silna współzależność działania tych dwóch sieci jest dwukierunkowa i w sposób oczywisty:

- bez zasilania nie działa sieć teleinformatyczna,
- bez sieci teleinformatycznej brakuje narzędzi sterowania i komunikacji w zakresie utrzymania sieci elektrycznej.

- **Jeszcze więcej:**
  - Technologii
  - Funkcjonalności
  - Zastosowań
  - Połączeń
  - Powiązań
  - Zależności
- **Sztuczna Inteligencja**
- **Mniej:**
  - Bezpośredniego wpływu na projekt

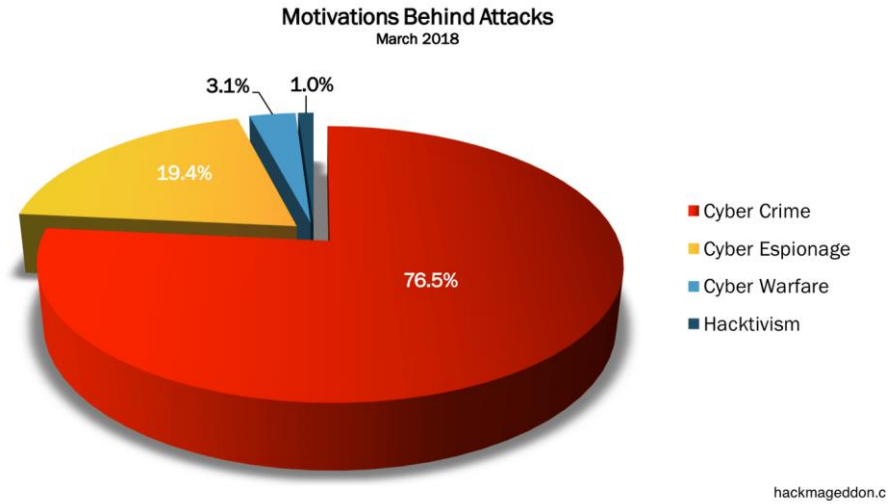


• Wymiar 5 – BEZPIECZEŃSTWO

Szybki, wieloletni rozwój Cyber świata we wszystkich wymienionych wcześniej wymiarach stworzył i w dalszym ciągu rozszerza pole możliwości intencjonalnego zakłócania działania systemów.

Kierunki rozwoju cyberprzestępczości:

- wzrasta liczba przeprowadzanych ataków, zwłaszcza dedykowanych, ukierunkowanych na uzyskanie konkretnych efektów,
- rośnie liczba indywidualnych i zorganizowanych grup hackerskich,
- rozwijane są nowe techniki prowadzenia ataków,
- tworzone są nowe narzędzia wspomagające cyberataki, lub nawet wykonujące je samodzielnie,
- spodziewane jest wykorzystywanie przez hackerów najbardziej rozwiniętych technologii informatycznych, włączając w to zastosowanie „sztucznej inteligencji”.

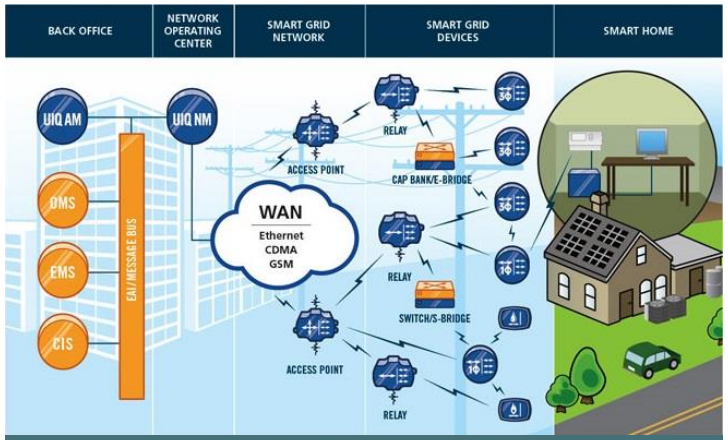


Wymiar 5 – BEZPIECZEŃSTWO

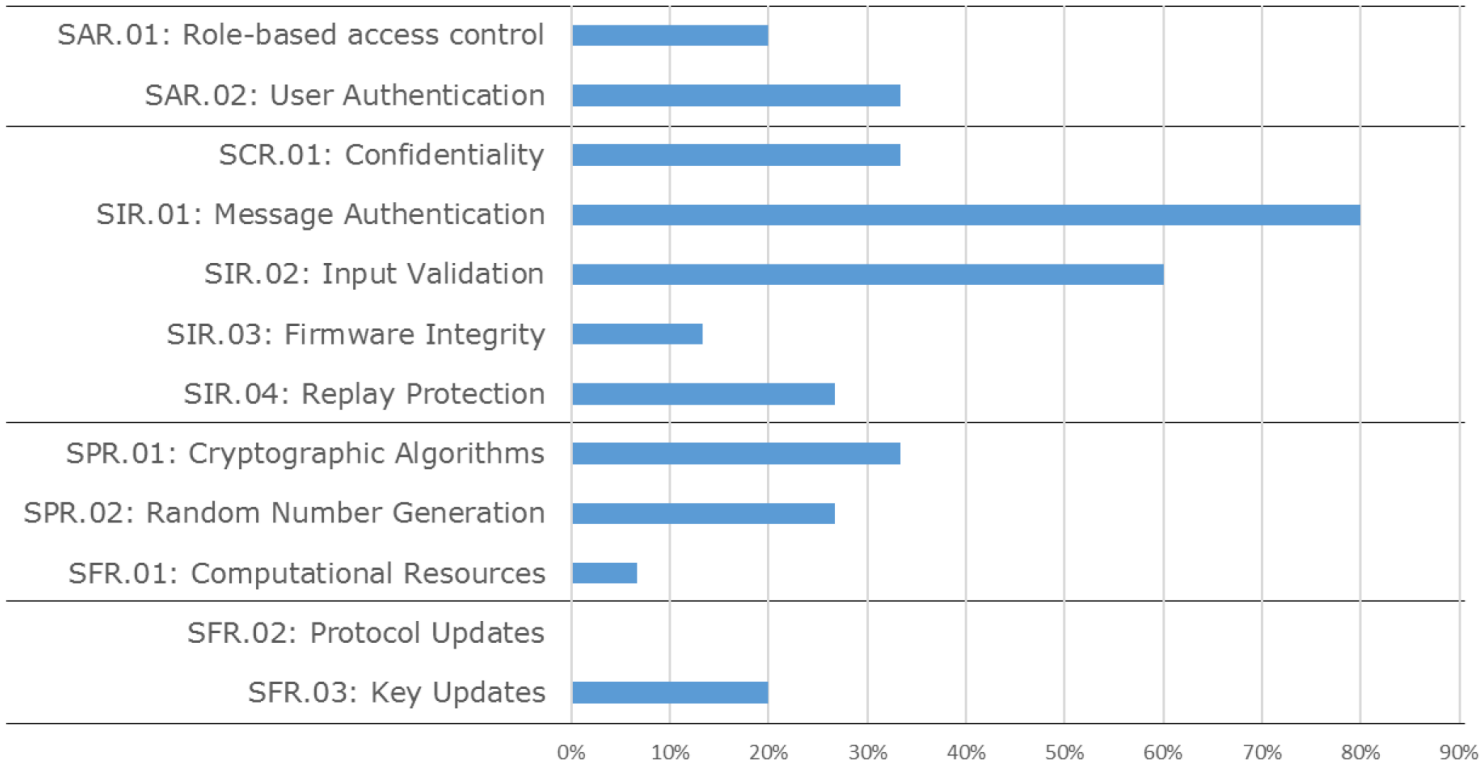
będzie więcej:

- Organizacji
- Przepisów prawa i regulacji
- Standardów i rekomendacji
- Ukierunkowanych, dedykowanych ataków
- Aktywnych atakujących aktorów (hacker'ów i zorganizowanych grup)
- Zautomatyzowanych ataków, nawet z użyciem sztucznej inteligencji

Cyberbezpieczeństwo IoT

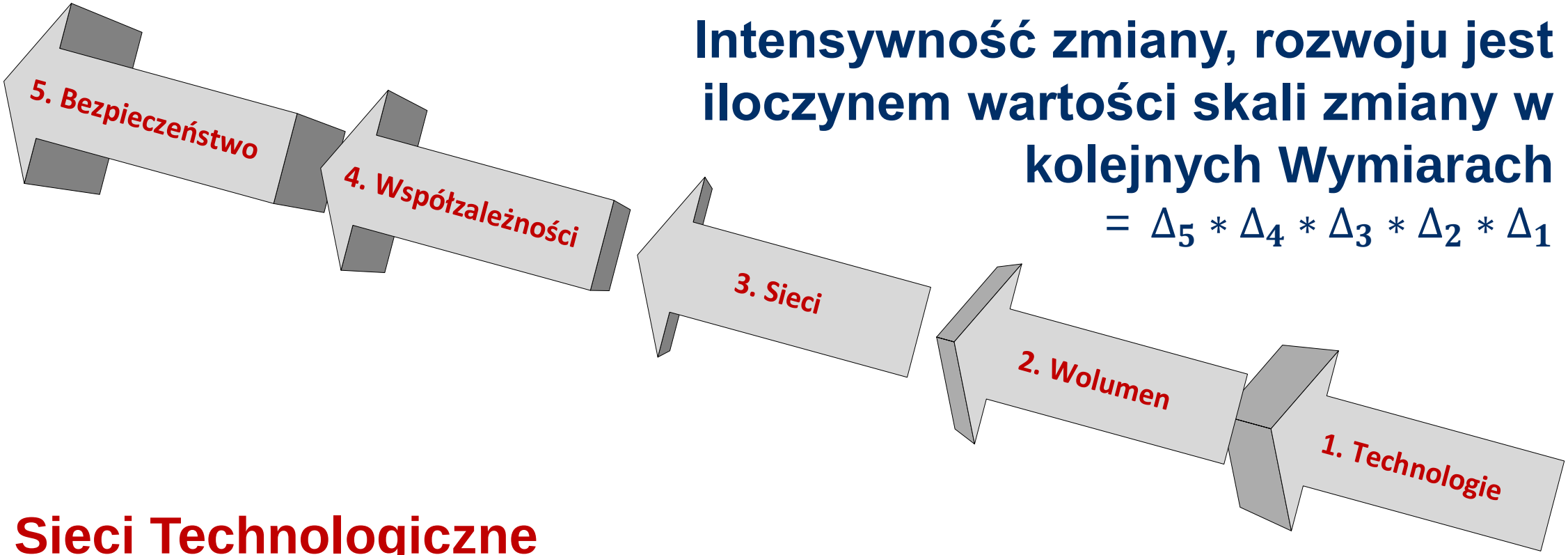


Podsumowanie testów bezpieczeństwa w przeprowadzonych w 25-ciu różnych systemach Smart Metering w EU



Procent systemów, które nie spełniają wymienionego wymagania bezpieczeństwa

Źródło: ENCS (European Network for Cyber Security)



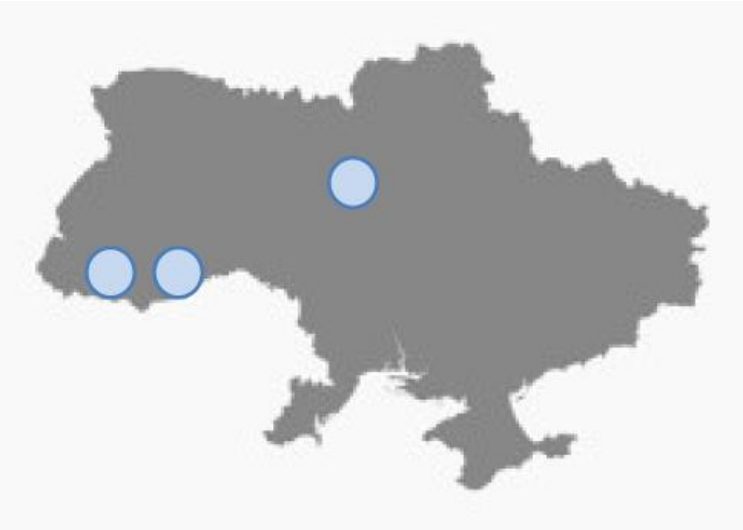
Intensywność zmiany, rozwoju jest iloczynem wartości skali zmiany w kolejnych Wymiarach

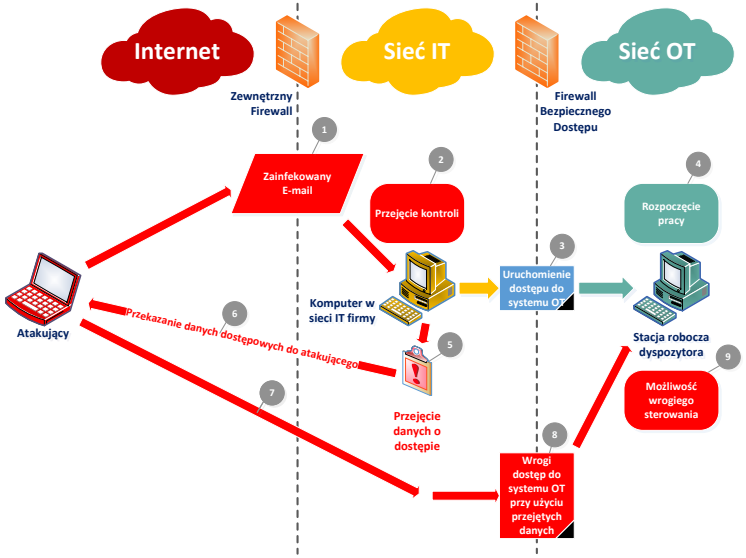
$$= \Delta_5 * \Delta_4 * \Delta_3 * \Delta_2 * \Delta_1$$

Sieci Technologiczne
muszą być całkowicie odizolowane i
inaczej traktowane niż publiczne i trudne
w zabezpieczeniu systemy Świata Cyber, czy też IoT

Déjà vu

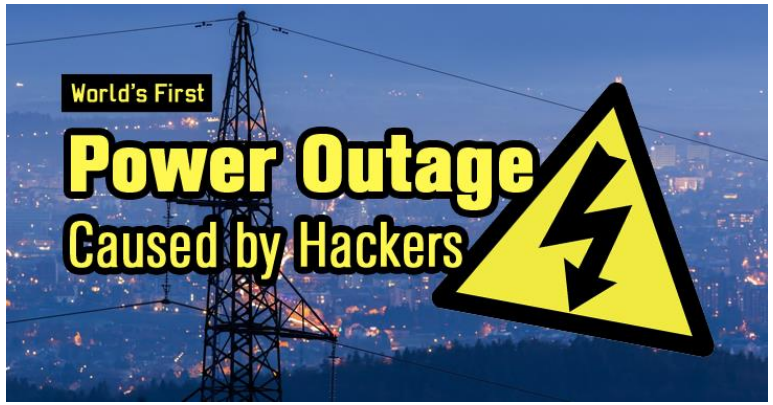
2015-12-23 - Atak na 3 OSD na Ukrainie





Skoordynowany atak na:

- 3 lokalizacje dystrybucyjne,
- Call-Center



- Uruchomienie dostaw energii po ok. 6h odbyło się całkowicie ręcznie, bez systemów sterowania
- Przez 9 miesięcy nie przywrócono pełnego zakresu sterowania sprzed ataku

Hackers did indeed cause Ukrainian power outage, US report concludes

DHS officials say well-coordinated hack cut power to 225,000 people.

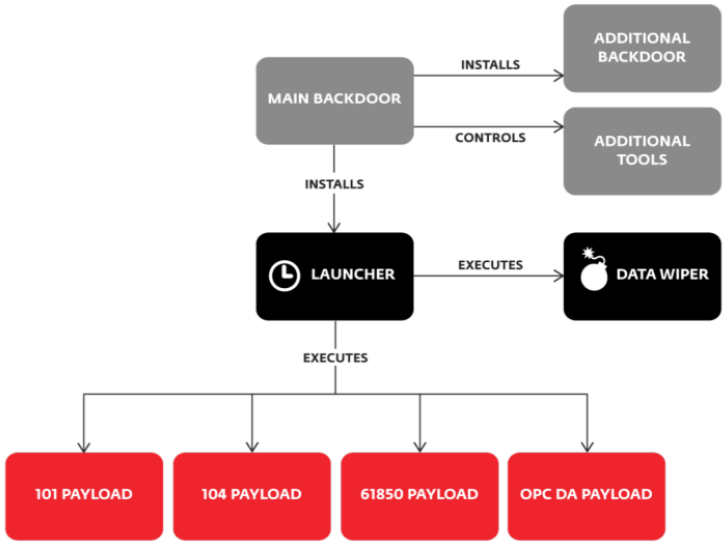
by Dan Goodin - Feb 26, 2016 8:14pm CET

32

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

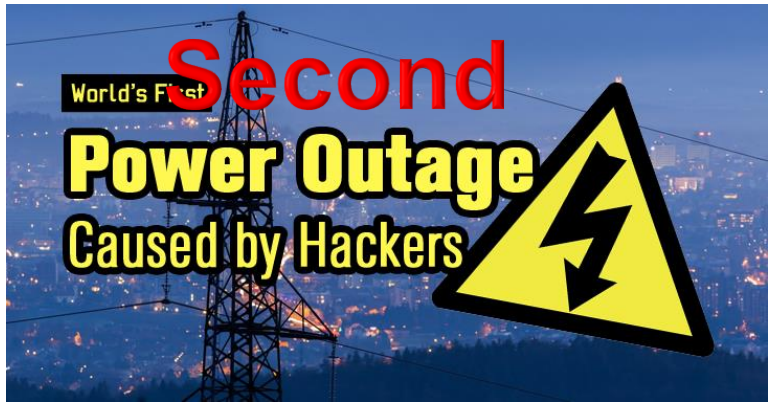
Déjà vu - 2016-12-17 - Atak na ukraińskiego OSP



Źródło: WIN32/INDUSTROYER, ESET

Atak na UkrEnergo:

- 1 SE na północ od Kijowa
- 1/3 miasta odłączona



- Malware w e-mailu pozwolił na kradzież haseł systemów
- Uruchomienie dostaw energii po ok. 75 min
- Prawdopodobne powiązania z innymi, wcześniejszymi atakami na Ukrainie

Energy firm points to hackers after Kiev power outage

Erm, it was hovering between -9˚C and -1˚C that day

21 Dec 2016 at 10:58, John Leyden

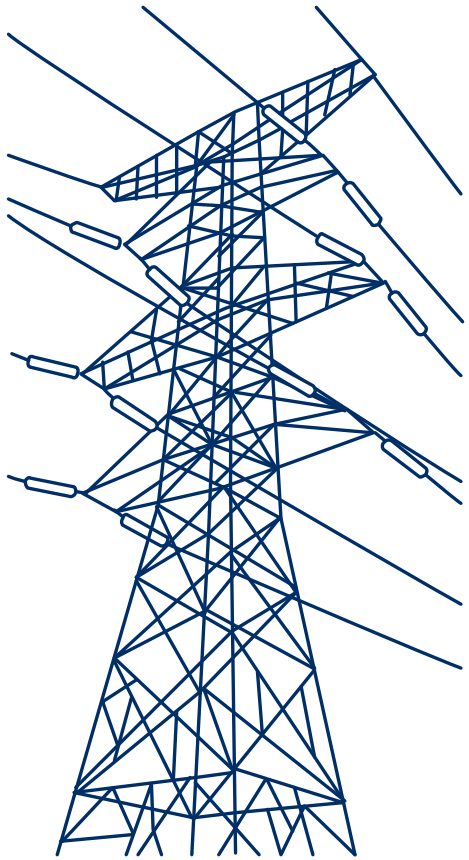
A cyber attack is suspected in connection with an outage of the Ukrainian power grid that affected homes around Kiev last weekend.

INDUSTROYER

Ten wirus może atakować elektrownie i wodociągi – jest tak samo groźny jak Stuxnet

Źródło: 2017-06-12 WIN32/INDUSTROYER, ESET

Wnioski po 2 atakach na Ukrainie



2 ataki na infrastrukturę elektroenergetyczną na Ukranie:

- **były w pewnych aspektach podobne do siebie –**
  - w zakresie ogólnej organizacji ataku i schematu działania
  - użycia metod i narzędzi (phishing, przejęcie haseł, niszczenie danych)
- **różniły się istotnie –**
  - pierwszy atak był prowadzony ręcznie
  - drugi przeprowadzono z użyciem nowego narzędzia: INDUSTROYER, czyli półautomatycznie

INDUSTROYER to nowe, poważne zagrożenie dla systemów technologicznych

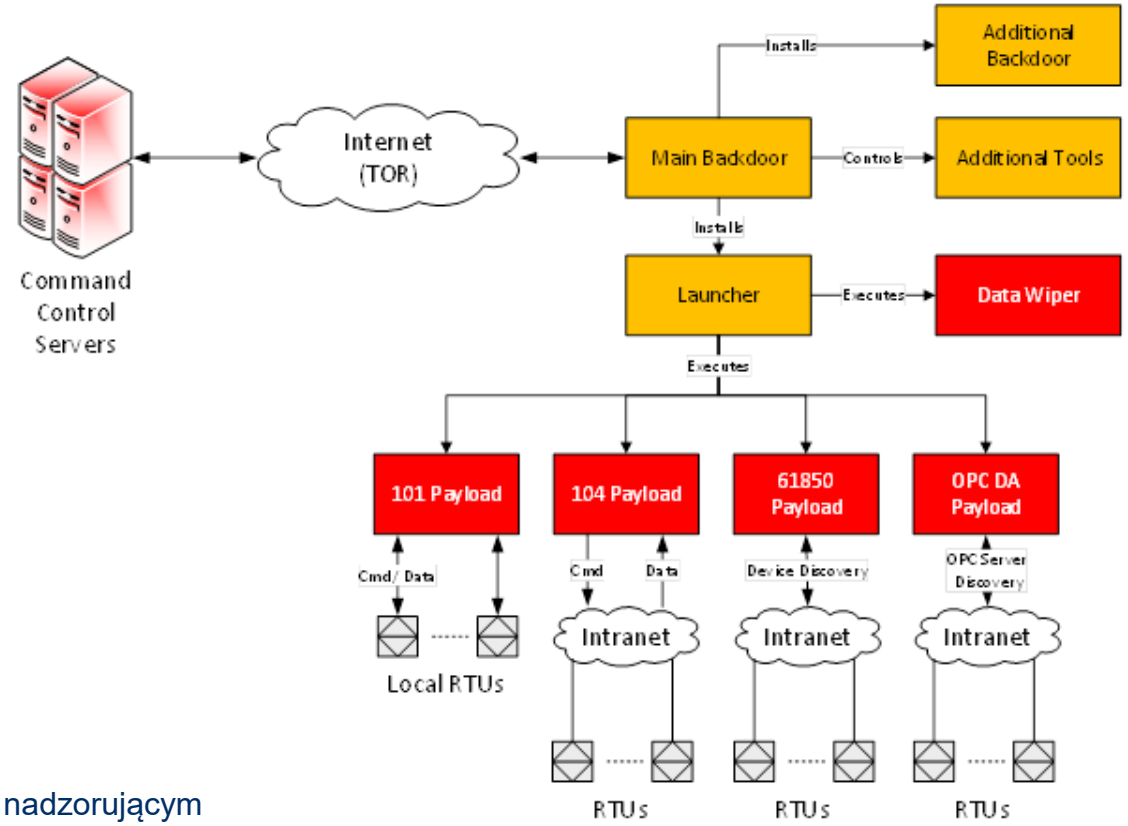
W obu atakach ochrona systemów zawiodła w wielu miejscach, najbardziej:

- **w dziedzinie Separacji Sieci**
  można było dostać się do systemów technologicznych z sieci podstawowej
- **na styku HMI (Human Machine Interface)**
  błędy użytkowników w połączeniu z za słabą ochroną stacji roboczych umożliwiły wejście do sieci podstawowej

Industroyer / CrashOverride

Charakterystyka –

- **Pierwszy na świecie framework opracowany specjalnie do atakowania środowisk przemysłowego sterowania (ICS)**
- **Nie skupia się na konkretnych produktach i może być łatwo dostosowany do atakowania różnych instalacji przemysłowych**
- **Nie posiada funkcji służących do wykradania danych, służy wyłącznie do zakłócania infrastruktury technologicznej**



Command Control Servers - serwery zdalnie zarządzające atakiem
Internet (Tor) - szyfrowana droga, którą Industroyer komunikuje się z serwerem nadzorującym
Main Backdoor - główna tylna furtka - moduł, który odpowiada za dostęp zdalny i sterowanie pozostałymi modułami
Additional Backdoor - dodatkowa tylna furtka - moduł utrzymujący złośliwe oprogramowanie w systemie w przypadku próby jego usunięcia
Additional Tools - dodatkowe narzędzia, np. poszukiwania odpowiednich celów w sieci
Data Wiper - moduł kasowania ważnych danych w systemach w celu ich trwałego uszkodzenia
Payload - ładunek - moduł wykonujący konkretne zadanie w Industroyerze, np. sterowanie urządzeniami IED
RTU - Remote Terminal Unit - zdalna jednostka, która łączy system SCADA z fizycznym urządzeniem
IED - Intelligent Electronic Device - Inteligentne Urządzenie Elektroniczne - urządzenie z mikroprocesorem, które kontroluje sprzęt technologiczny. Jednym z takich urządzeń jest RTU

Industroyer / CrashOverride

Charakterystyka –

- **Zbudowany w architekturze modułowej i posiadał następujące moduły:**
  - Backdoor / Remote Administration Tool – główne moduły zarządzania
  - Launcher (np. do uruchamiania funkcji Wiper)
  - Data Wiper – niszczenie danych celem unieruchomienia sterowania
  - IEC 104 – służy do sterowania RTU
  - IEC 101 – służy do sterowania po łączach szeregowych
  - IEC 61850 – wyszukiwanie i sterowanie urządzeniami
  - OPC DA – wyszukiwanie i przekazywanie komunikatów MicroSCADA
  - SIPROTEC DoS – blokowanie cyfrowych zabezpieczeń nadprądowych
- **Może być stosowany do ataków z następującymi scenariuszami:**
  - Odcięcie Stacji od pradu - wywoływanie w petli komendy otwarcia na RTU
  - Wywołania efektu wyspy - szybkie przełączanie odłączników w celu wywołania reakcji automatyki zabezpieczającej linie
  - Wpływ na system [illegible] przez fałszowanie danych w OPC DA
  - Atak na zabezpieczenia SIPROTEC z wykorzystaniem podatności CVE-2015-5374
- **Dwa ostatnie scenariusze mają za zadanie pogłębić efekt wyspy.**

Podstawy ochrony –

- **Separacja systemów przemysłowych od pozostałych sieci**
- **Wyłączenie zbędnych usług i portów w systemach**
- **Ciągłe monitorowanie systemów i sieci (24/7) w celu wychwytywania anomalii**
- **Wykorzystanie whitelistingu aplikacji, dopuszczaniu tylko tych które są konieczne do pracy (stworzenie golden image wraz z listą haszy programów)**
- **Bezpieczne zarządzanie aktualizacjami firmware'ów**

SHA-1 hashes:

8E39ECA1E48240C01EE570631AE8F0C9A9637187
2CB8230281B86FA944D3043AE906016C8B5984D9
79CA89711CDAEDB16B0CC[illegible]FDCEBD[illegible]AA7E57120A
[illegible]8F24[illegible]2D[illegible]3D4D4C
[illegible]AFE[illegible]A3BFF04
B92149F046F00BB69DE329B8457D32C24726EE00
B335163E6EB854DF5E08E85026B2C3518891EDA8

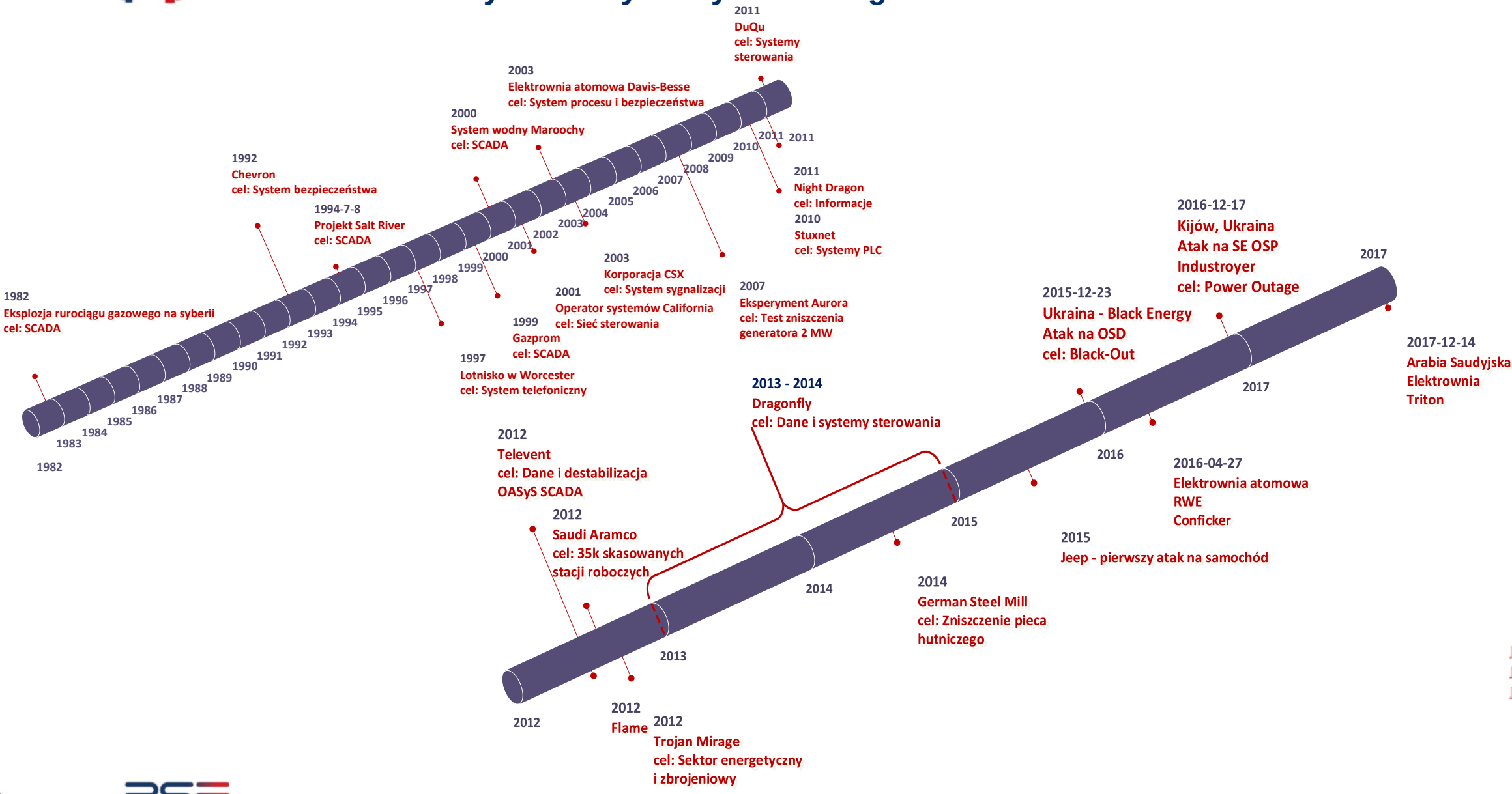
IP addresses of C&C servers:

195.16.88[.]6
46.28.200[.]132
188.42.253[.]43
5.39.218[.]152
93.115.27[.]57

Uwaga: INDUSTROYER może ewoluować

Będą powstawać nowe moduły

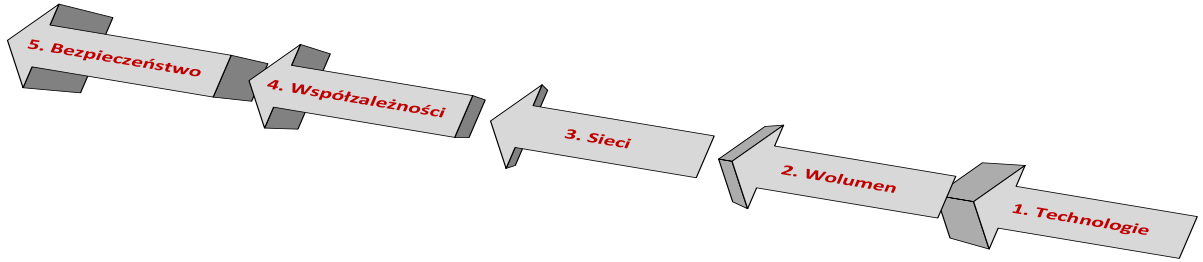
Udane ataki Cyber na systemy technologiczne



Przyszłość cyberbezpieczeństwa w EE

Wnioski

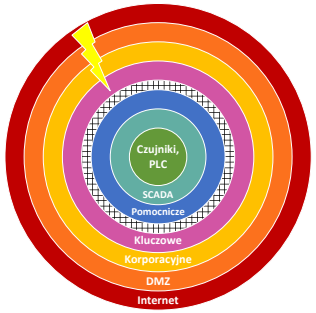
- **Kluczowe wyzwanie - Nowy świat Cyber, w 5 wymiarach:**
  - Rozwój technologiczny
  - Przyrost wolumenu
  - Sieci
  - Współzależności
  - Bezpieczeństwo – musi adresować efekty zmiany wprowadzanych przez ww. wymiary



- **Cyberbezpieczeństwo ma wpływ na niezawodność działania systemu elektroenergetycznego:**
  - bezpośredni – jak pokazały doświadczenia Ukrainy
  - pośredni – jako konsekwencja następującej rewolucji Cyber
- **Tradycyjne podeście do zapewnienia cyberbezpieczeństwa nie wystarczy ze względu na:**
  - presję czasu: zmiany legislacyjne, rynkowe, etc.
  - ograniczone zasoby: ludzie, wiedza, umiejętności
  - przyzwyczajenia i uprzedzenia: bezpieczeństwo na końcu łańcucha, postrzegane jako kula u nogi

Podejście do cyberbezpieczeństwa w nowym Cyber świecie

- **Potrzebna rewolucja? Niekoniecznie!**
- **Standardy, podejście i procesy cyberbezpieczeństwa istnieją i były doskonalone przez lata**
  - znane są i stosowane z nastawieniem na ochronę informacji, danych osobowych, własności intelektualnej i finansów
  - niezbędne jest rygorystyczne stosowanie w elektroenergetyce do ochrony „usług kluczowych” i „systemów krytycznych”
- **Nowe wymagania funkcjonalne doprowadziły do kompromisów w architekturze IT/OT z zaniedbaniem zasady „Security by Design”**
- **Fundamentami cyberbezpieczeństwa w elektroenergetyce pozostają:**
  - **Ostra separacja pomiędzy OT, IoT i IT**
    z precyzyjnie kontrolowaną łącznością, gdy jest konieczna
  - **Bezwzględna ochrona każdego miejsca interakcji użytkownika z systemem**
    stacja robocza, urządzenie mobilne, HMI
  - **Zabezpieczenie każdego perymetru**
    czyli punktów styku między segmentami sieci
  - **Kontrola każdego oprogramowania na każdym etapie jego życia**
    bezpieczny SDLC
  - **Aktywna obrona**
    monitorowanie, wykrywanie anomalii, rejestracja zdarzeń, reagowanie



Polskie Sieci Elektroenergetyczne S.A.

Grzegorz Bojar | grzegorz.bojar@pse.pl | 503 322 007 | Departament Teleinformatyki