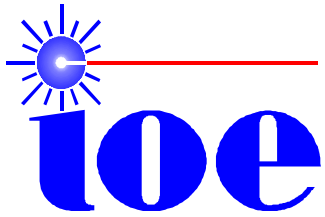


Inteligentne systemy dostawy energii elektrycznej (ISDEE)
Wydział Elektrotechniki, Automatyki, Informatyki i Elektroniki
Akademii Górniczo-Hutniczej

Bezpieczeństwo elektromagnetyczne kraju a inteligentne systemy dostawy energii elektrycznej

Płk rez. dr inż. Maciej MROCZKOWSKI
Email: mmroczkowski@wat.edu.pl

Zakład Systemów Optoelektronicznych
Instytutu Optoelektroniki
Wojskowej Akademii Technicznej

Kraków, 18 listopada 2010 r.

Cykl seminariów:

Inteligentne systemy dostawy energii elektrycznej (ISDEE)

pod patronatem:

Dziekana Wydziału Elektrotechniki, Automatyki, Informatyki i Elektroniki AGH

i

Komisji Elektrotechniki,

Informatyki i Automatyki

POLSKIEJ AKADEMII NAUK

Oddziału w Krakowie

Pojęcie bezpieczeństwa

Pojęcie bezpieczeństwa elektromagnetycznego wymaga wprowadzenia serii określeń przybliżających wyzwania, które stoją przed wielu środowiskami profesjonalistów w naszym kraju. Zrobimy to z perspektywy „bottom-up" – od szczegółu do ogółu, objaśniając pewne pojęcia innymi, łatwiejszymi do opisania.

Bezpieczeństwo.

Poczucie bezpieczeństwa możemy zdefiniować przez pewien stan, stan braku poczucia zagrożenia, ponieważ łatwiej jest nam te zagrożenia wymienić. Bezpieczeństwo może też być definiowane jako stan kontrolowania zidentyfikowanych zagrożeń, w formie ochrony przed pewną klasą zdarzeń lub narażeń, aby osiągnąć akceptowalny poziom ryzyka – czyli miarę zagrożenia – np. wielkości strat w funkcji prawdopodobieństwa zajścia zdarzenia.

Uzyskiwanie poczucia bezpieczeństwa jest raczej procesem ciągłym i długotrwałym, odbywającym się w grze z otoczeniem, w trakcie którego obserwujemy świat zewnętrzny, analizujemy jak on na nas oddziałuje i próbujemy celowo oddziaływać na niego, do tego z pewnym wyprzedzeniem, czyli prognozując stany przyszłe. Analizy prowadzi się wg ustalonych reguł, z systemowego, operacyjnego i technicznego punktu widzenia, tworząc najczęściej trójwymiarowe przestrzennie i zależne od czasu „sceny"…

Indywidualna pierwotna potrzeba bezpieczeństwa

Prowadzenie wspomnianych analiz wymaga posiadania całych rodzin adekwatnych matematyczno-fizycznych modeli rzeczywistości, algorytmów i modeli numerycznych, wreszcie programów, między innymi tzw. hydrokodów i potężnych środków obliczeniowych do symulacji komputerowych oraz systemów wizualizacji i walidacji wyników. Nawet w wirtualnej formie jest to ogromny wysiłek…

Intuicyjnie wiemy, że potrzeba bezpieczeństwa należy do fundamentalnych pragnień człowieka. Za Wikipedią przytoczymy podstawowe sformułowania odnoszące się do wspomnianego problemu. W ramach antropologii, a w szczególności w koncepcji kultury, w obrębie teorii funkcjonalistycznej Bronisław Malinowski sformułował tezy objaśniające motywacje działań ludzkich wynikające z tzw. potrzeb pierwotnych związanych z naturą biologiczną ludzi oraz wtórnych związanych z ich naturą społeczną.
Siedem podstawowych potrzeb wg. Malinowskiego to:
1) metabolizm,
2) reprodukcja
3) odpowiednie warunki fizyczne,
4) bezpieczeństwo,
5) ruchliwość,
6) rozwój
7) zdrowie.

Społeczna natura potrzeby bezpieczeństwa

Wymienionym siedmiu potrzebom ma odpowiadać siedem podstawowych imperatywów kulturowych:
1) zaopatrzenie,
2) małżeństwo i rodzina (system pokrewieństwa),
3) mieszkanie i ubranie,
4) ochrona i obrona,
5) aktywność i komunikacja,
6) przyuczanie i szkolenie,
7) higiena.
Ludzkie potrzeby są zaspokajane przez instytucje, czyli zbiorowości ludzi powiązanych wspólnym zadaniem, wspólnymi regułami i dysponujących wspólnymi urządzeniami technicznymi. Na potrzeby pierwotne odpowiada pierwotna organizacja instytucjonalna:
a) instytucje zaopatrzenia w żywność
b) pokrewieństwa, małżeństwa i reprodukcji
c) ochrony i obrony przed zagrożeniami.
Na potrzeby wtórne odpowiadają instytucje prawne, ekonomiczne, wychowawcze i polityczne. Sens każdej instytucji jest zrozumiały tylko w kontekście całego swoistego systemu, w którym występuje.

Potrzeba bezpieczeństwa w hierarchii potrzeb ludzkich

Możemy tę myśl bliżej sprecyzować i ustalić pozycję potrzeby bezpieczeństwa pośród innych potrzeb, powołując się na znacznie później sformułowaną hierarchię potrzeb ludzkich opracowaną przez współtwórcę tzw. psychologii humanistycznej: Abrahama Maslowa, za którym możemy przytoczyć następujące grupy potrzeb:

- **potrzeby fizjologiczne (głód, pragnienie, seks itd.);**
- **potrzeby bezpieczeństwa (pewności, stałości, porządku, opieki, wolności od strachu, lęku, chaosu, zagrożenia itd.);**
- **potrzeby afiliacji (kontaktów społecznych, miłości, czułości, przynależności);**
- **potrzeby szacunku (osiągnięć, prestiżu, uznania dla samego siebie oraz ze strony innych);**
- **potrzeby samorealizacji (samourzeczywistnienia, tj. zrealizowania swoich pragnień, zainteresowań, wykorzystania posiadanych zdolności, poczucia spełnienia itd.).**

Hierarchię odzwierciedla graficznie tzw. piramida Maslowa, od podstawy w górę.

Piramida Maslowa

Piramida potrzeb ludzkich według A. Maslowa

Kategorie bezpieczeństwa indywidualnego i zbiorowego- bezpieczeństwo elektromagnetyczne

Powszechnie wyróżnia się następujące kategorie bezpieczeństwa:

ze względu na obszar jaki obejmuje – bezpieczeństwo globalne, bezpieczeństwo międzynarodowe, bezpieczeństwo regionalne, bezpieczeństwo narodowe;

ze względu stosunek do obszaru państwa – bezpieczeństwo zewnętrzne i bezpieczeństwo wewnętrzne;

ze względu na dziedzinę w jakiej występuje – bezpieczeństwo militarne, bezpieczeństwo polityczne, bezpieczeństwo energetyczne, bezpieczeństwo elektroenergetyczne, bezpieczeństwo ekologiczne, bezpieczeństwo teleinformatyczne, bezpieczeństwo społeczne, bezpieczeństwo kulturowe; bezpieczeństwo fizyczne i bezpieczeństwo socjalne; bezpieczeństwo strukturalne i bezpieczeństwo personalne.

Naszym celem jest połączenie - ze względu na szczególne cechy – problematyki polityki bezpieczeństwa narodowego z polityką bezpieczeństwa militarnego oraz bezpieczeństwem elektroenergetycznym i teleinformatycznym - aby stworzyć „nową" kategorię:

bezpieczeństwo elektromagnetyczne

Bezpieczeństwo elektromagnetyczne kraju a inteligentne systemy dostawy energii elektrycznej (ISDEE) - sformułowanie problemu

Nasza cywilizacja techniczna, poczynając od wprowadzenia ARPANETU poprzez Internet i jego WWW (World Wide Web) znalazła się w sieciocentrycznym internetowym społeczeństwie ery informacyjnej - epoce wiedzy, technologii mikroelektronicznych i optoelektronicznych, nanotechnologii i informatyki oraz postępującej globalizacji – wielkich szans i „nowych" wielkich zagrożeń, a w tym najwyższego w historii stopnia zależności od środowiska elektromagnetycznego, elektroenergetyki, teleinformatyki – głównie techniki cyfrowej i od narażeń elektromagnetycznych.

W dziedzinie militarnej mamy do czynienia z rewolucją militarną i pojawieniem się sieciocentrycznego pola walki.

W tej sytuacji „zagrożeniem" stała się już nawet niska jakość dostaw energii elektrycznej, na co zareagowano organizowaniem specyficznych systemów elektroenergetycznych tzw. Smart Grids, które nakładają na klasyczne sieci elektroenergetyczne nowe sieci teleinformatyczne, mieszczące w swoich węzłach skomplikowane cyfrowe systemy sensorów, cyfrowych kontrolerów i aktuatorów dających prawie pełną kontrolę nad parametrami przesyłanej energii.

Bezpieczeństwo elektromagnetyczne kraju a inteligentne systemy dostawy energii elektrycznej (ISDEE) - sformułowanie problemu

Niestety „stare” zagrożenia nie zniknęły! Wszystkie militarne środki napadu elektronicznego, czy radioelektronicznego (tak naprawdę elektromagnetycznego), czy też wojny elektronicznej (tak naprawdę elektromagnetycznej) stały się o rzędy groźniejsze. Pojawił się też terroryzm elektromagnetyczny.

Dopiero łączne, nowe podejście do tej problematyki daje szansę na przetrwanie naszej cywilizacji, mogącej być narażoną na zniszczenie w pierwszych mikrosekundach nowego typu konfliktu – wojny elektromagnetycznej.

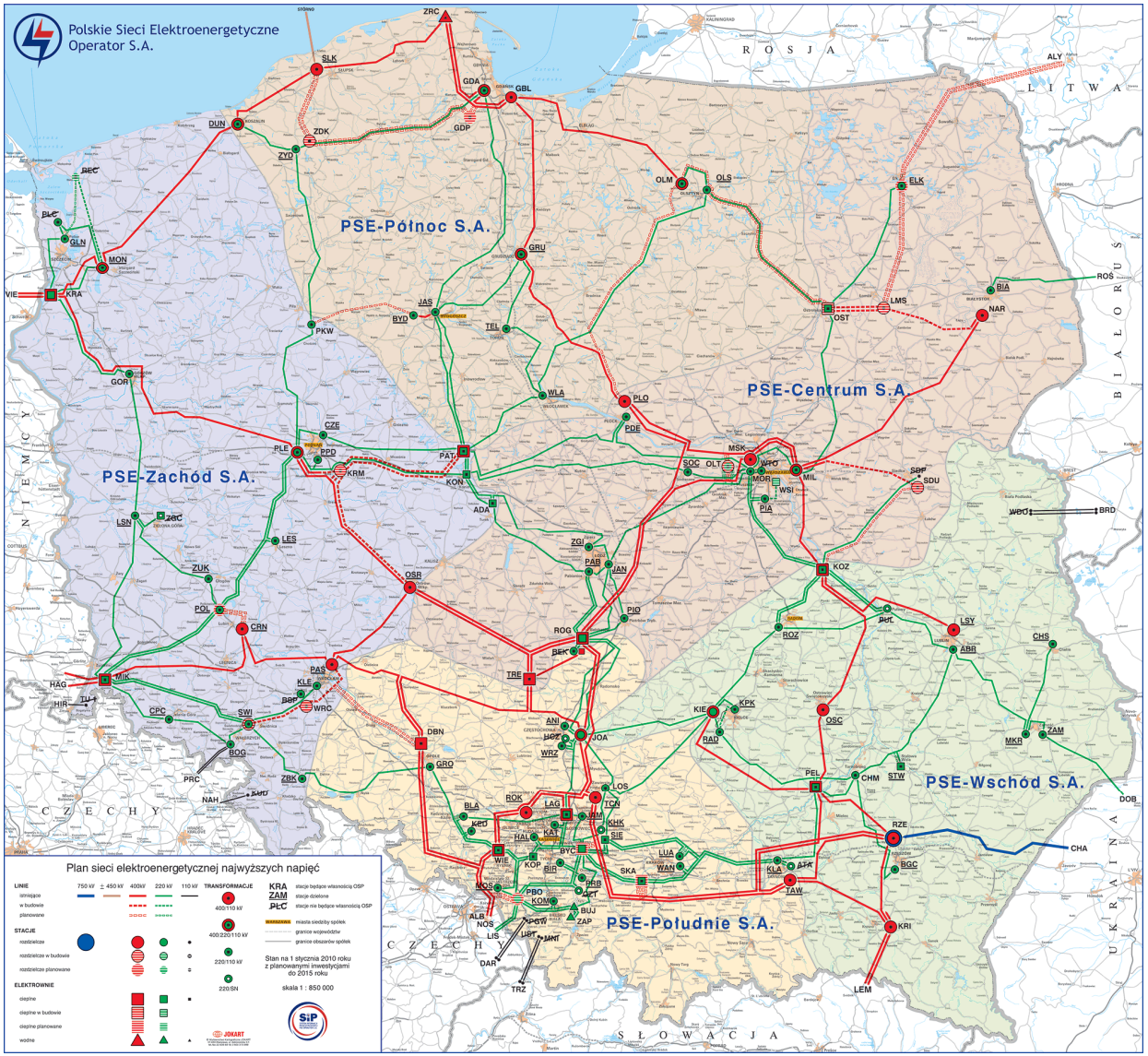
Smart Grids dają nowe szanse na podniesienie przeżywalności systemu dostaw energii elektrycznej, warto jest te szanse pokazać i nadać większy impet działaniom.

Wzrastające zapotrzebowanie na pasma częstotliwości skierowały uwagę środowiska na badania i wykorzystanie pasm w zakresie częstotliwości terahercowych (rzędu 10 do potęgi 12).

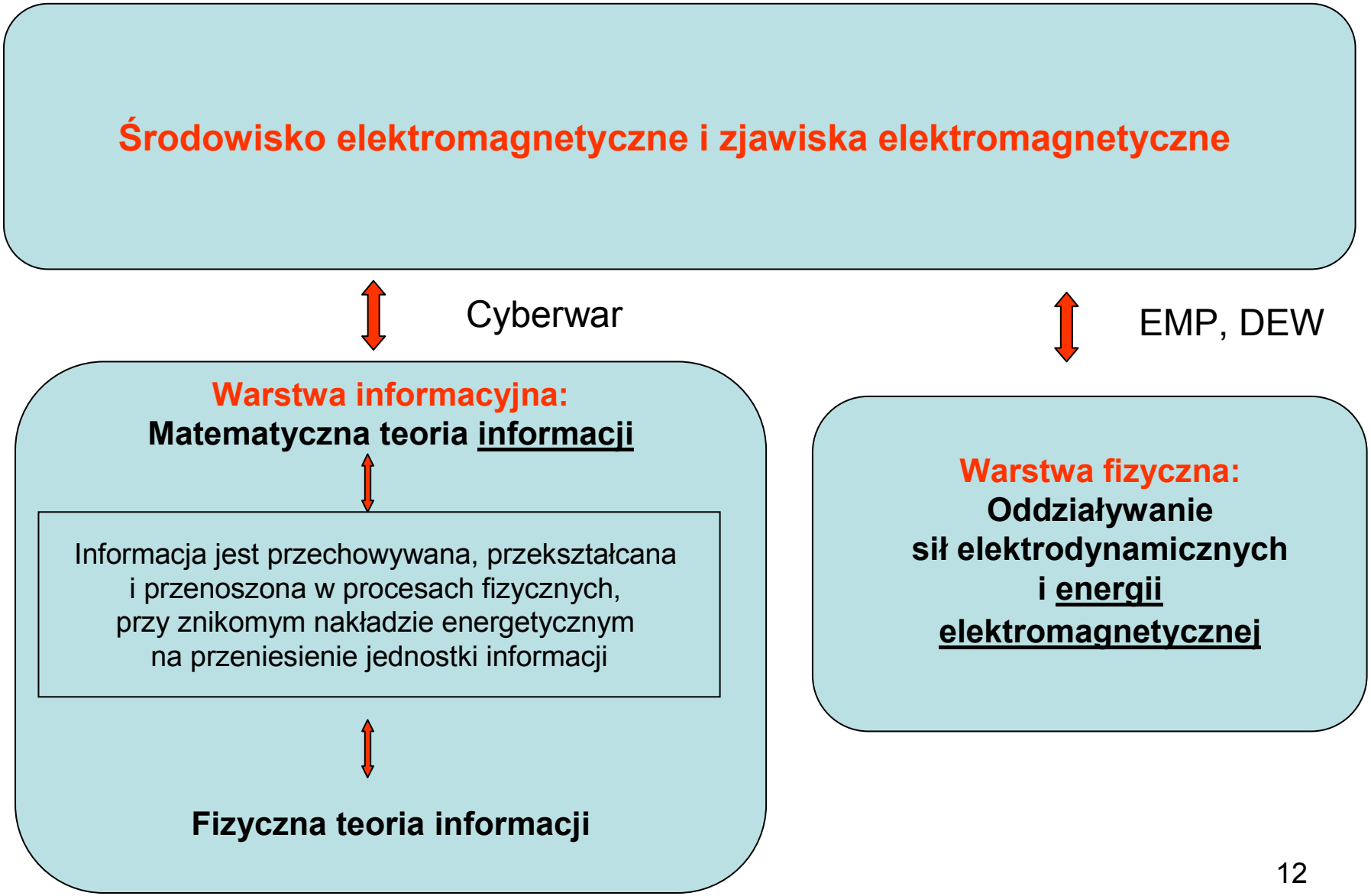
Chcąc czy nie chcąc obsuwamy się w ten nowy obszar zagrożeń!

Nowym niebezpieczeństwom musimy stawić czoła, a nowe szanse wykorzystać!

Bezpieczeństwo elektromagnetyczne kraju a ISDEE - skala problemu



Środowisko elektromagnetyczne



WALKA ELEKTRONICZNA A WOJNA ELEKTROMAGNETYCZNA
Definicje

- **Wiele rozmaitych terminów, akronimów, a także i żargon używany w naukach związanych z walką elektroniczną (EW) łączy się z tymi samymi zjawiskami, problemami i urządzeniami. Zazwyczaj musimy użyć równocześnie leksykonu walki elektronicznej i słownika Departamentu Obrony USA lub NATO albo nazewnictwa społeczności kompatybilności elektromagnetycznej (EMC).**
- **W gruncie rzeczy walka elektroniczna nie jest elektroniczna, tzn. nie jest prowadzona przy pomocy elektronów (co oznacza wiązkę naładowanych cząstek), ale jest elektromagnetyczna (to znaczy wykorzystuje fale elektromagnetyczne albo wiązki fotonów) zajmując jako pole bitwy całe widmo promieniowania elektromagnetycznego.**

WALKA ELEKTRONICZNA A WOJNA ELEKTROMAGNETYCZNA
Definicje i uzasadnienie terminu WEM (EMW)

Bardziej precyzyjnie termin walka elektroniczna znaczy:

- **wg DOD: militarna akcja wymagająca wykorzystania energii elektromagnetycznej do decydowania o korzystaniu, wyzyskaniu dla siebie, obniżeniu wrogiego wykorzystania albo niedopuszczenia do wrogiego wykorzystania widma elektromagnetycznego; jest to akcja, która zachowuje wykorzystanie przez własne jednostki widma elektromagnetycznego**
- **wg NATO: militarna akcja wymagająca wykorzystania energii elektromagnetycznej do decydowania o korzystaniu, wyzyskaniu dla siebie, obniżeniu wrogiego wykorzystania albo niedopuszczenia do wrogiego wykorzystania widma elektromagnetycznego; jest to działanie zachowujące jego skuteczne wykorzystanie przez własne jednostki.**

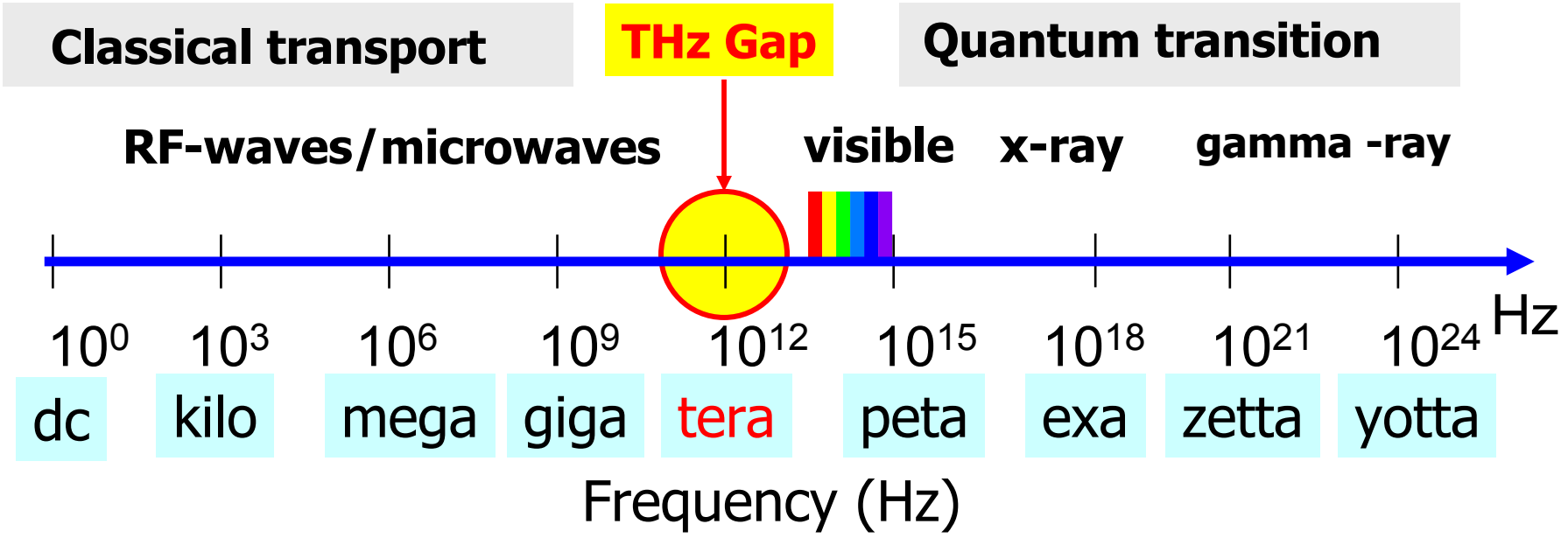
PRZYTOCZONE DEFINICJE Z KOMENTARZAMI WSKAZUJĄ JEDNOZNACZNIE, ŻE TERMIN WALKA (WOJNA) ELEKTRONICZNA (EW) POWINIEN BYĆ ZASTĄPIONY TERMINEM WALKA (WOJNA) ELEKTROMAGNETYCZNA (EMW)

WOJNA ELEKTROMAGNETYCZNA ODBYWA SIĘ Z PRĘDKOŚCIĄ ŚWIATŁA

KLUCZOWYM ELEMENTEM PIERWSZYCH MIKROSEKUND(!) WOJNY ELEKTROMAGNETYCZNEJ MOŻE BYĆ IMPULS ELEKTROMAGNETYCZNY WYSOKIEGO WYBUCHU JĄDROWEGO, STĄD KONIECZNOŚĆ ZABEZPIECZEŃ OBU SFER.

Widmo Elektromagnetyczne

Z fizycznego punktu widzenia wojna elektromagnetyczna (EMW) lub konflikt elektromagnetyczny obejmuje wojnę informacyjną (IW) i dziedzinę historycznie nazywaną dotąd walką elektroniczną (EW) oraz aspekty energetyczne broni skierowanych energii i kwestie użycia EMP oraz HPM.



MHD-EMP, HEMP, HPM, MASER, LASER, X-RAY LASER

RF – Weapons, Directed Energy Weapons - DEW

Graph partially: http://www.rpi.edu/~zhangxc

Przewodnik do zjawisk związanych z EMW (Electromagnetic War)

Nuklearny impuls elektromagnetyczny (środowisko HEMP):

EMP(HEMP)- High Altitude Nuclear Electromagnetic Pulse,
MHD-EMP – Magnetohydrodynamic EMP,

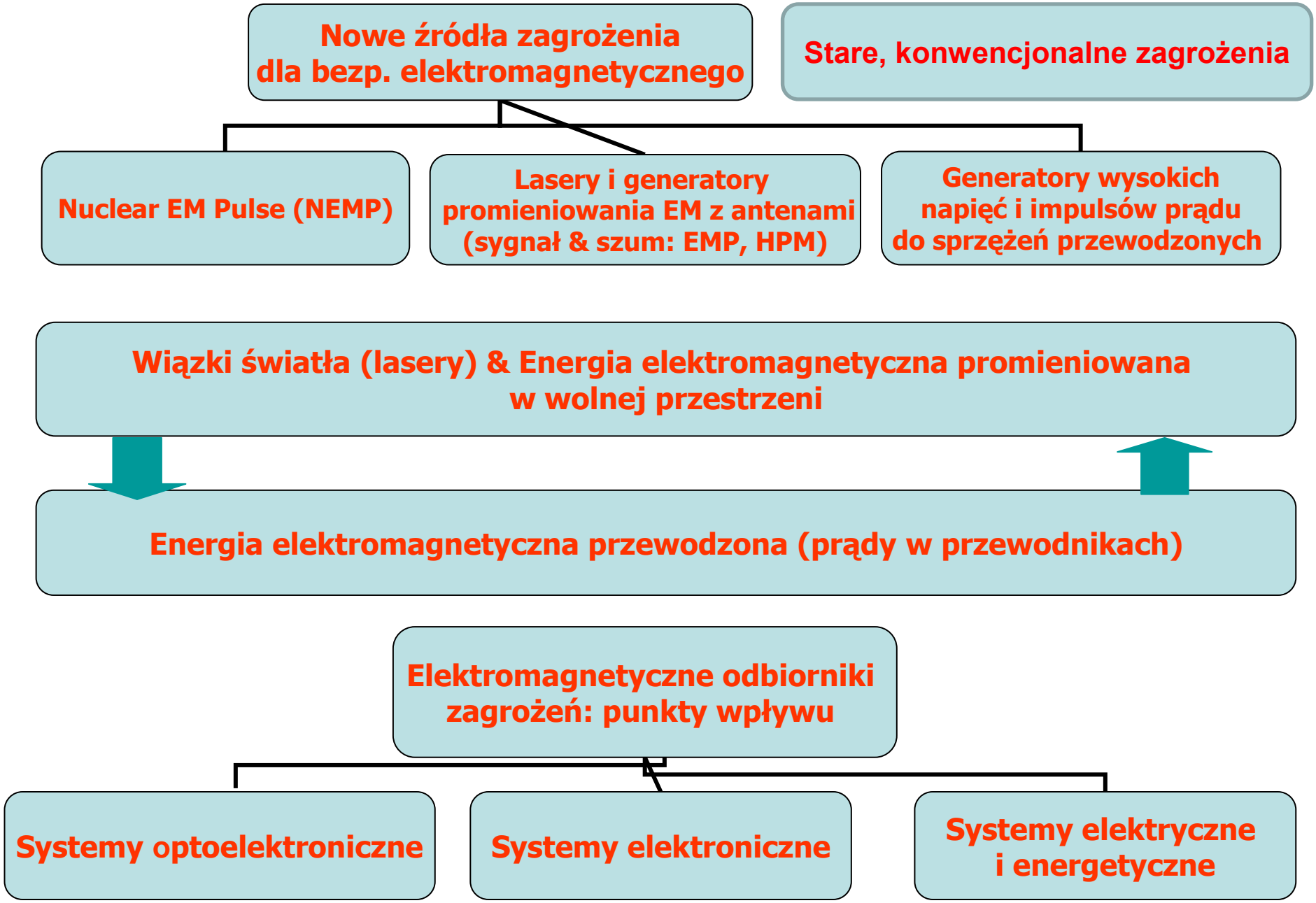
Nienuklearny impuls elektromagnetyczny:

Środowisko: HPEM – High Power Electromagnetics,
RF – Weapons, HPM - High Power Microwave,

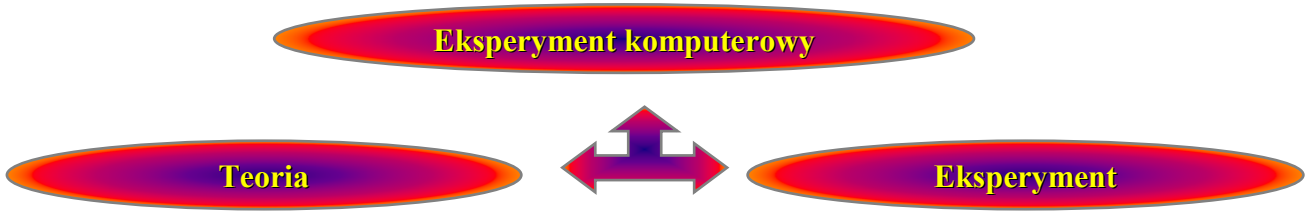
Directed Energy Weapons – DEW

MASER, LASER, X-RAY LASER

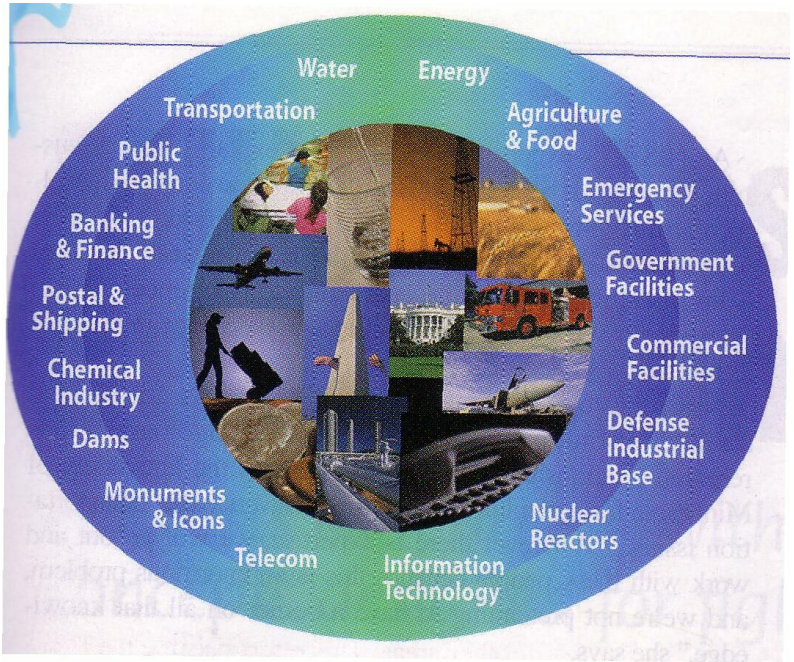
„CYBERWAR"


Nowe źródła zagrożenia dla bezp. elektromagnetycznego
Stare, konwencjonalne zagrożenia
Nuclear EM Pulse (NEMP)
Lasery i generatory promieniowania EM z antenami (sygnał & szum: EMP, HPM)
Generatory wysokich napięć i impulsów prądu do sprzężeń przewodzonych
Wiązki światła (lasery) & Energia elektromagnetyczna promieniowana w wolnej przestrzeni
Energia elektromagnetyczna przewodzona (prądy w przewodnikach)
Elektromagnetyczne odbiorniki zagrożeń: punkty wpływu
Systemy optoelektroniczne
Systemy elektroniczne
Systemy elektryczne i energetyczne

We współczesnych badaniach skomplikowanych oddziaływań systemów na poziomie zarówno operacyjnym jak i fizycznym nieodzowne jest użycie symulacji komputerowych do prowadzenia eksperymentów komputerowych nt. wpływu ataków terrorystycznych, cyberataków itd. na systemy militarne, biznes, łączność, Internet, sieci finansowe itp.



W efekcie nowe środowisko elektromagnetyczne wspólne dla systemów militarnych, logistycznych i cywilnych wymusza zupełnie inne podejście do identyfikacji potencjalnych celów.



Skutkiem tej sytuacji jest przytoczona obok lista narzędzi modelowania komputerowego rozwijanych w NISAC (National Infrastructure Simulation and Analysis Center) z wykorzystaniem możliwości laboratoriów narodowych USA: Los Alamos i Sandia.

Zależności są sieciowe, z fizycznym dostępem każdego, zatem zależności stają się „poziome".

Jest to modelowa ilustracja sytuacji, w której mamy do czynienia ze złamaniem tradycyjnej hierarchii zarówno w dowodzeniu jak i w zarządzaniu.

Stare konwencjonalne zagrożenia dla Smart Grids pozostały bez zmian - są tylko precyzyjniejsze

Filmy komputerowe

„Know-what” przed „Know-how”: rewolucja militarna (RMA) i sieciocentryczne pole walki (NCW)- sieci walczące

Co to dla nas oznacza? Odpowiedź zawiera się w wyborze odpowiednich dziedzin badań i wdrożeń, czyli w planowanym wzroście wiedzy i nowych technologii, które właściwie zareagują na zmianę natury i celów współczesnych konfliktów konwencjonalnych wymuszonych (tu nie ma dowolności!) przez:

a)wyzwania międzynarodowego terroryzmu, b) rozwój międzynarodowych praw wojny, c) koncepcję utrzymania pokoju i koncepcję uderzenia prewencyjnego, d) wynikającą z nich koncepcję broni obezwładniających, e) potencjalną asymetryczność konfliktu

b)Filozofia NCW dotyczy wszystkich sieci cywilnych i wojskowych, czyli całej cyberprzestrzeni.

Reguły dla sieci wojskowych są mniej znane, ale podobne do reguł NCW dla sieci komercyjnych (w tym Smart Grids): mało – bardzo drogie zamienia się na dużo - bardzo tanie (COTS) wbudowane w niezawodne i odporne sieci ze zminiaturyzowanych (!) węzłów.– np. dla wojska są to: a) sieci rozpoznania, b) sieci dowodzenia i łączności (C4ISR), c) sieci precyzyjnego ataku (C4ISTAR), budowane dla mobilnych lekkich komponentów wojsk, żołnierzy przyszłości (Future Soldiers) i mobilnych stanowisk dowodzenia oraz d) sieci nadzoru przestrzeni powietrznej.

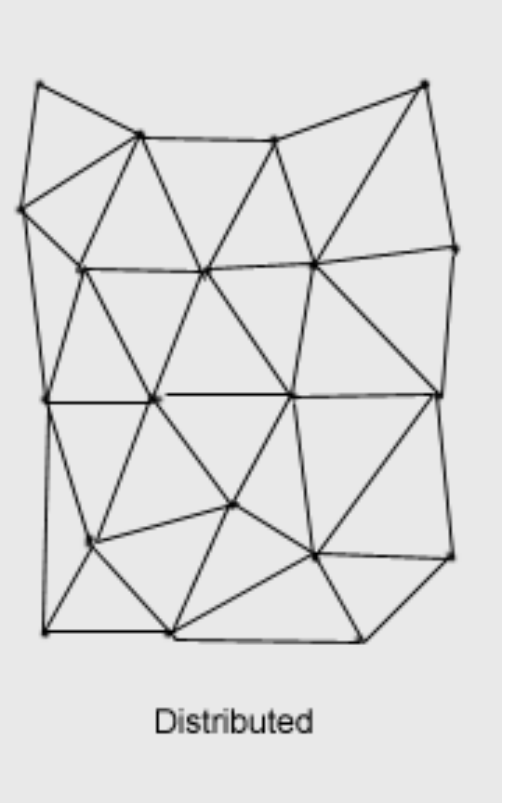
Co to jest sieciocentryczność?

Chcąc przybliżyć ideę systemu sieciocentrycznego możemy powiedzieć potocznie co znaczy pojęcie - być sieciocentrycznym (NCOW):

NCOW oznacza być ucyfrowionym, mieć zdolności obliczeniowe i symulacyjne – być jednocześnie swoim własnym symulatorem (CPU z GPGPU, pamięć, I/O, oprogramowanie, DB bazy danych oparte na relacjach),

NCOW oznacza być w połączonym w sieci (szerokopasmowy cyfrowy nadajnik/odbiornik Software Defined Radio - SDR na bardzo wysokich częstotliwościach, używający np. protokołu IP v.6 Mobile), trzeba być też kompletnie zorientowanym (GPS/INS)

NCOW oznacza mieć węzły-routery i znać precyzyjnie wszystkich najbliższych sąsiadów



NCW znaczy:

a) być w sieci,
b) być ucyfrowionym,
c) wiedzieć to co wie sieć ("common operational or tactical picture„) i mieć węzły pamiętające to.

Nieklasyczne pole walki – obejmujące widmo częstotliwości (elektromagnetyczne)
HEMP, HPM, DEW – Broń elektromagnetyczna

Cel: osiągnięcie przewagi i dominacja na elektromagnetycznym polu walki, którego najważniejszą częścią w czasie konwencjonalnego „pokoju” jest cyberprzestrzeń

„Klasyczne” pole walki
NF – Networked fires – prowadzić precyzyjny ogień, atakować i walczyć w sieci. Sieć w tym przypadku to może być tzw. taktyczny internet.

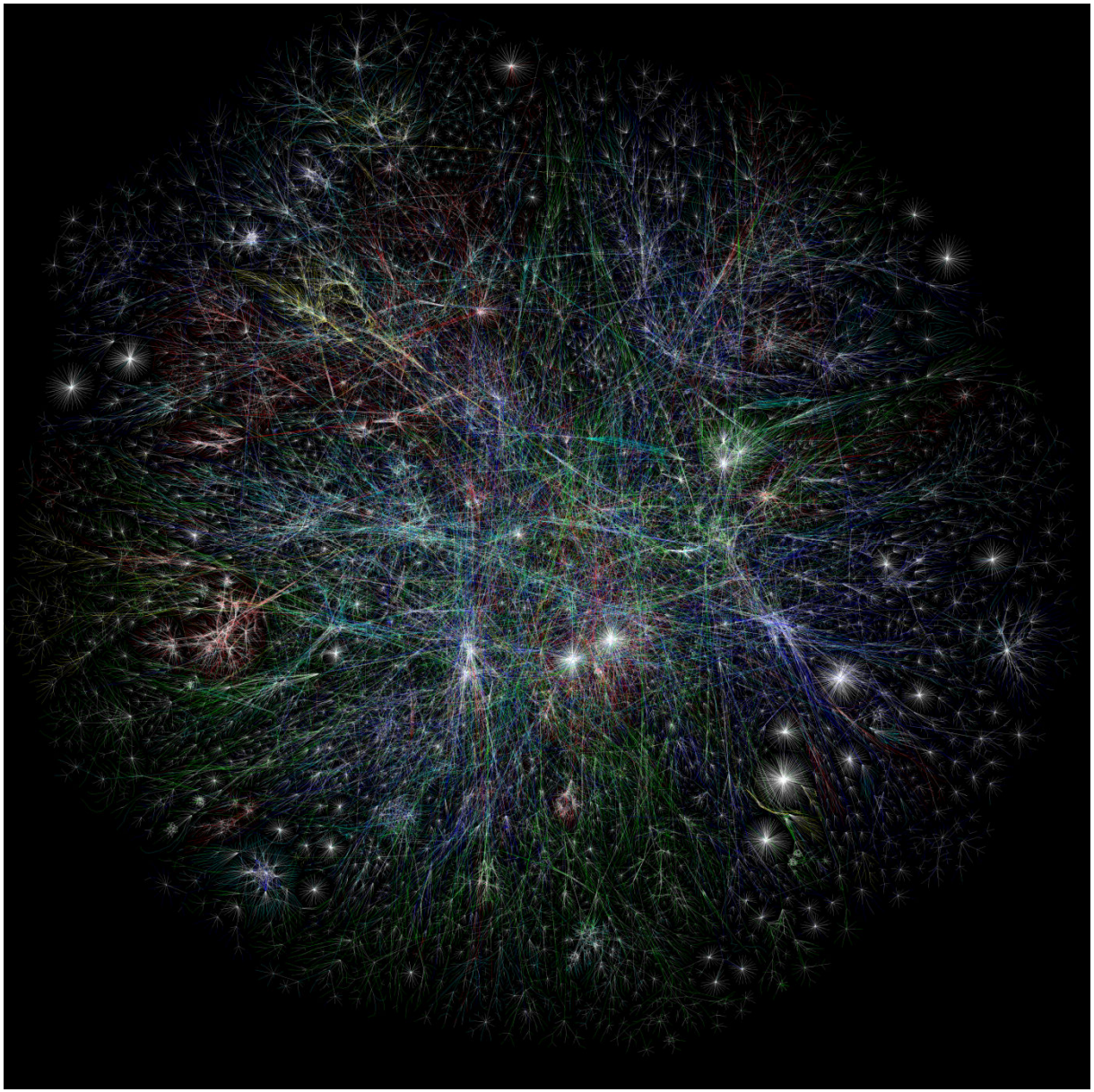
Cel: „klasyczne” cele wojny– dotychczas wymieniane w geopolityce, geostrategii, geoekonomii oraz podręcznikach sztuki wojennej, które pozostają bez zmiany.

Termin "cyberprzestrzeń" został użyty po raz pierwszy w 1984 roku przez Williama Gibsona w powieści Burning Chrome. Wygenerowany przez komputer świat immersyjnej, wirtualnej rzeczywistości (VR), którą amerykański klasyk cyberpunkowych powieści nazywał też matrycą (matrix).

Cyberprzestrzeń jest jednak w rzeczywistości domeną fizyczną będącą wynikiem utworzenia systemów informacyjnych i sieci, które umożliwiają wzajemne oddziaływania drogą elektroniczną, szerzej: elektromagnetyczną, czyli wykorzystującą jako nośniki zarówno elektrony jak i fotony.

Cyberprzestrzeń jest globalna domeną w środowisku informacyjnym złożonym z niezależnych sieci infrastruktury technologii informacyjnej (węzłów i połączeń między nimi) obejmująca Internet, sieci telekomunikacyjne, systemy komputerowe oraz wbudowane w różne urządzenia procesory i kontrolery cyfrowe.

Cyberprzestrzeń jest to przestrzeń informacji, którą tworzą łącznie wszystkie sieci komputerowe, pokazuje się ją w reprezentacji grafów.



Galaktyka internetu

Barrett Lyon z amerykańskiej firmy komputerowej Network Presence napisał program śledzący trasy, jakie pakiety danych przebywają pomiędzy serwerami. Ilustracja pokazuje, jak podróżują dane pomiędzy kontynentami.
Każdy z kolorów oznacza inny region geograficzny:
Ameryka Północna jest zaznaczona na niebiesko,
region Europa, Bliski Wschód, Centralna Azja i Afryka – na zielono,
Ameryka Łacińska na żółto,
Azja Południowo-Wschodnia, Australia i Oceania – na czerwono,
niezidentyfikowane – na biało.
Szczegóły na stronie www.opte.org

Niektóre właściwości broni elektromagnetycznej

Porównywalna do broni masowego rażenia, jest obecnie bronią przełomowej technologii (Revolution in Military Affairs) przy czym może być bronią obezwładniającą:

WMD – Weapon Mass Destruction

WMD - Weapon Mass Disruption.

Bardzo przydatna do użycia w działaniach asymetrycznych, pozwola dostosować skalę użycia do skali zagrożenia (od obezwładniania do śmiercionośności).

Trudna do zlokalizowania

Bardzo tania

Czas działania liczy się nie w godzinach a w mikrosekundach.

Stosuje się ją zarówno w ataku jak i obronie

Obejmuje wykradanie chronionych informacji i nawet wiedzy - przyspieszając proces dyfuzji szczególnie wrażliwej wiedzy

Wymusza dynamiczne i permanentne zmiany w doktrynach, strategiach militarnych, w działaniach bojowych, sporządzaniu list celów itd.

Działa z prędkością światła oddziałując na systemy dowodzenia i sterowania (D^5), nawet w warunkach gwałtownych zmian głównych kierunków uderzenia.

Bardzo skuteczna: Estonia, Gruzja itd.

Skutki działania, ze względu na efekty ciągnione, kaskadowe są trudne do przewidzenia i do wyobrażenia.

Ma zdolność modyfikacji nie tylko środowiska informacyjnego, środowiska pola walki, ale też środowiska naturalnego (HAARP).

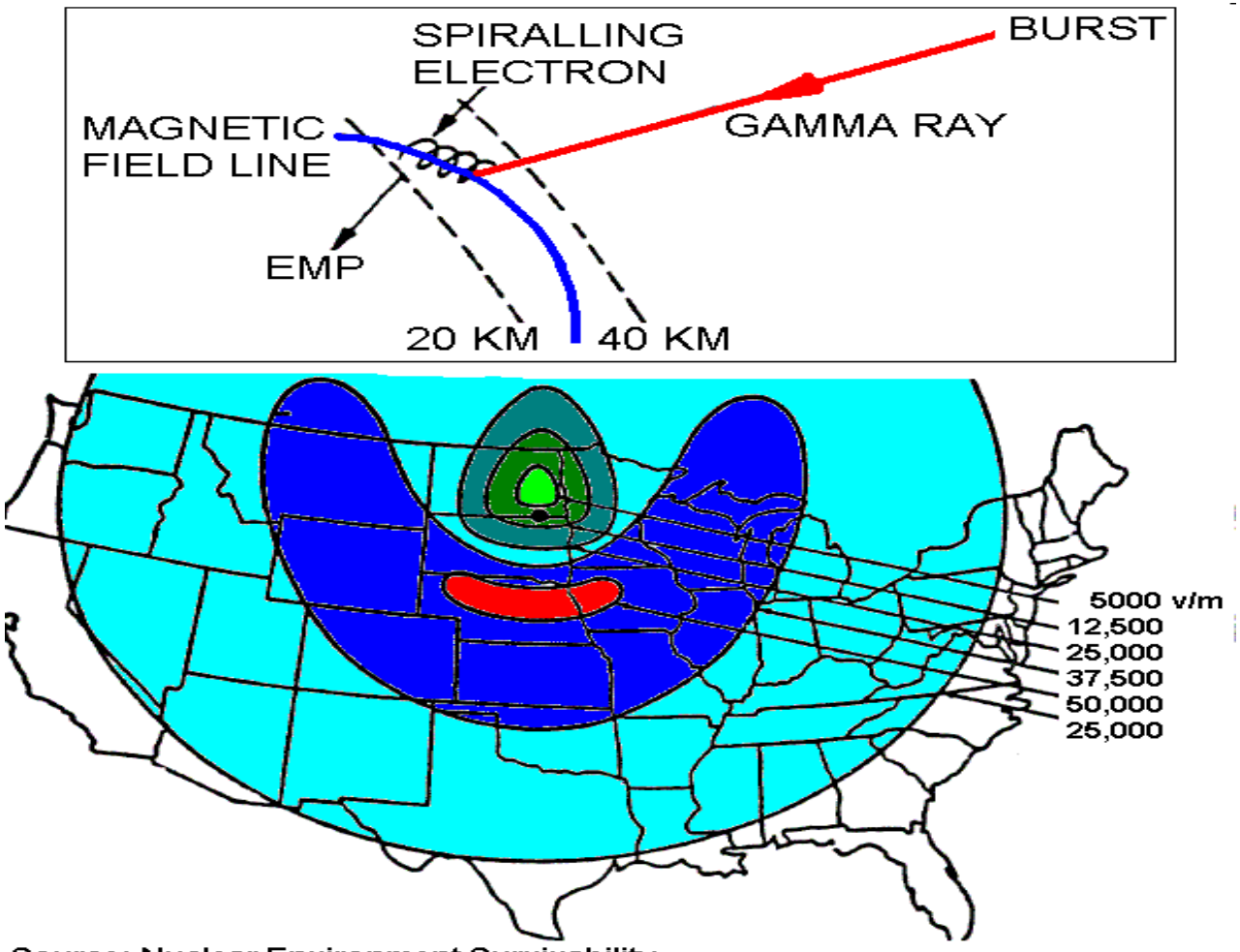
Niektóre właściwości broni elektromagnetycznej c.d.

Będziemy omawiać cztery charakterystyczne rodzaje działań w środowisku elektromagnetycznym:

- **„Cyberwar in Cyberspace" dotyczy problematyki C2 (Communications and Control), a sięga nawet C4 poprzez użycie komputerów w sieci do paraliżu dowodzenia, wg poglądów amerykańskich**
- **walka o dominację nad widmem elektromagnetycznym (Electromagnetic Dominance),**
- **HEMP – Impuls elektromagnetyczny wysokiego wybuchu jądrowego.**
- **broń skierowanej energii (Directed Energy Weapons (DEW): HPM, Masery, lasery).**

Zagrożenia i analiza podatności oraz przeciwdziałanie i uzyskanie odporności leży w obszarze zainteresowania kompatybilności elektromagnetycznej (EMC).

ŚRODOWISKO EMP - MECHANIZM GENERACJI HEMP
HIGH ALTITUTUDE NUCLEAR ELECTROMAGNETIC PULSE



Source: Nuclear Environment Survivability,
U. S. Army, report AD-A278230 (1994)

Jak definiujemy cyberprzestrzeń (Cyberspace) w piątym wymiarze środowiska pola walki?

Cytując:

„Cyberprzestrzeń jest jednak w rzeczywistości *domeną fizyczną* będącą wynikiem utworzenia systemów informacyjnych i sieci, które umożliwiają wzajemne oddziaływania drogą elektroniczną [uwaga redakcyjna - szerzej: elektromagnetyczną, czyli wykorzystującą jako nośniki zarówno elektrony jak i fotony]. Zera i jedynki bitów mają swoje odpowiedniki fizyczne w postaci stanu elektronów w bramkach półprzewodnikowych lub fal światła transmitowanego kablem światłowodowym. Działalność człowieka w tym środowisku wymaga świadomego sterowania przepływem energii. Do przesyłania obrazów komputerowych poprzez Internet potrzeba jedynie niewielkiej energii w porównaniu z przelotem samolotu do określonego miejsca przeznaczenia. Obydwa te działania wymagają jednak utworzenia materialnego pakietu, aby podjąć podróż: zrozumienia sposobu podróżowania w określonym środowisku, protokołów i przepisów ustanowionych w odniesieniu do takiej podróży oraz sposobu współdziałania z innymi systemami po przybyciu na miejsce. Ci, którzy prowadzą wojnę informacyjną, muszą polegać na znajomości zasad fizycznych i systemów rządzących środowiskiem informacyjnym, podobnie jak tradycyjni żołnierze, marynarze i lotnicy muszą rozumieć środowisko w którym prowadzą wojnę".

[„Strategic Warfare in Cyberspace", G.J.Rattray, MIT, 2001]

Wojnę w cyberprzestrzeni prowadzą dowódcy wojskowi wszystkich szczebli jako część działań bojowych. To nie jest wojna informatyków między sobą.

„Cyberwar in Cyberspace”,

Wg poglądów amerykańskich nowe zdolności na polu walki są ściśle związane i uzależnione od:

- operacji sieciowych (network operations),

- operacji w widmie elektromagnetycznym (electromagnetic spectrum operations),

- walki elektronicznej (electronic warfare)

- operacji sieciowych z użyciem komputerów: atak, obrona, ukrywanie, wykradanie, fałszowanie informacji i wiedzy, dezinformowanie (computer network operations: attack, defense, exploitation)

Całkiem nowa sytuacja dotyczy zagrożeń: wspólne użycie tej samej fizycznie i protokolarnie sieci powoduje, że zagrożenia wewnętrzne dla systemów w cyberprzestrzeni są równie znaczące i ważne jak zagrożenia zewnętrzne.

Konieczność posiadania systemów I/O otwiera ścieżki potencjalnego dostępu do wnętrza sieci. Wiąże się to z rozpoznaniem cyberprzestrzeni i wcześniejszym wykrywaniem podatności sieci i komputerów na późniejsze ataki, czyli Computer network operations służą do rozpoznania i identyfikacji słabych punktów systemu i przygotowania metod i narzędzi również do wcześniejszych ataków (preemptive attacks) rozpoczynających nową wojnę.

Będzie to integralna część działań na szczeblu strategicznym, operacyjnym i taktycznym.

Preemptive attacks mogą spowodować przejęcie kontroli nie tylko nad systemami łączności i zarządzania cywilnymi i wojskowymi, ale także nad sprzętem bojowym, co wymusza postawienie kolejnego pytania: do jakiego momentu nasza broń będzie nasza?

Skuteczne preemptive attacks mogą doprowadzić do skutków porównywalnych z efektem użycia broni masowego rażenia.

„Cyberwar in Cyberspace” c.d.,

Wagę tej problematyki doceniają w czołowych państwach świata. Sztandarowym przykładem są Chiny, które w swej doktrynie porównują właśnie cyberwojnę do użycia broni masowego rażenia, skuteczną i bardzo ważną również w konflikcie asymetrycznym.

W Chinach wdrożono zasadę wykorzystania computer network operations w czasie pierwszego uderzenia.

Powołano jednostki do tych działań od szczebla taktycznego do strategicznego.

Powołano grupy hackerów dla każdej prowincji (ich liczebność ocenia się od 6 tys. do 60 tys. wg. różnych źródeł)

W chińskim ministerstwie, Sztabie Generalnym i Dowództwie Okręgu pekińskiego powołano specjalne komórki i nawiązano ścisłą współpracę z laboratoriami badawczymi uczelni cywilnych i wojskowych.

Chiny traktują computer network operations jako krytyczne dla osiągnięcia przewagi w środowisku elektromagnetycznym we wczesnej fazie konfliktu.

Przykłady zagrożeń wewnętrznych i przykłady zagrożeń zewnętrznych zostaną omówione w trakcie prezentacji.

„Cyberwar in Cyberspace” c.d.

Co ciekawe zaciera się różnica między militarnymi i niemilitarnymi metodami ataku w cyberprzestrzeni, do których równo dla obu sfer zaliczają się m.in.:

Malware – np. Viruses and worms
Hacking
Botnets
Keystroke loggers
Denial of service attacks
Phishing and spoofing.

W.w. metody rozwijają się niezwykle dynamicznie i prowadzą do praktycznej realizacji zdolności D5 będących celem walki elektronicznej (poprawnie elektromagnetycznej):

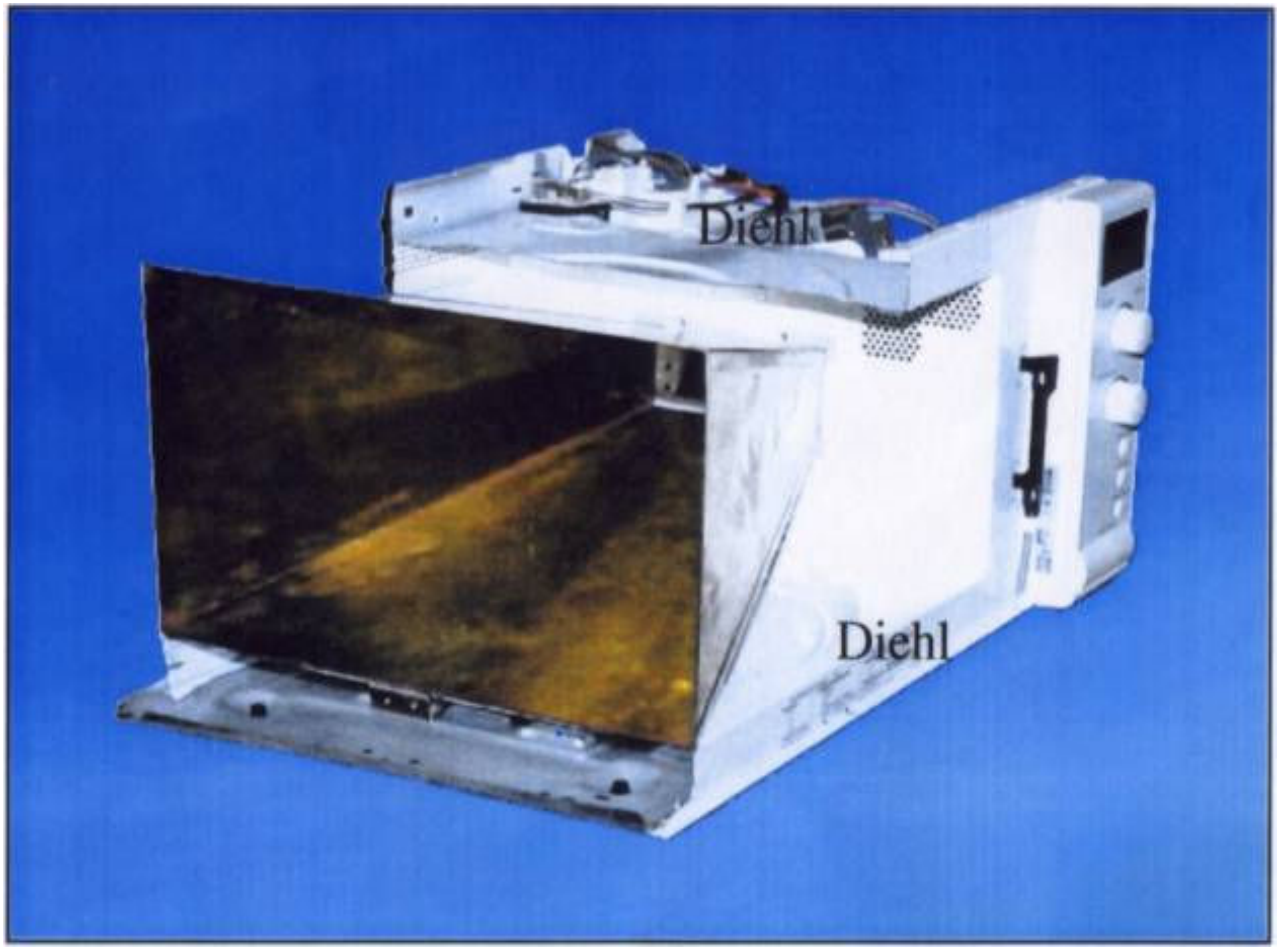
1) deceive,
2) deny,
3) disrupt,
4) degrade,
5) destroy

Pojęcie terroryzmu elektromagnetycznego (Electromagnetic Terrorism - EM Terrorism) i intencjonalnych zakłóceń elektromagnetycznych(Intentional Electromagnetic Interference – IEMI):

Gen.mjr Prof. Loborev podczas wykładu na sesji plenarnej „The Modern Research Problems" na konferencji AMEREM w Albuquerque w 1996 r. ukuł frazę "Terroryzm elektromagnetyczny " jako komentarz do wykorzystania technik elektromagnetycznych EM do zwalczania systemów alarmowych i łączności. Środowisko kompatybilności elektromagnetycznej- Electromagnetic Compatibility (EMC), przyjęło jako nadrzędny termin terroryzmu elektromagnetycznego następującą definicję intencjonalnych zakłóceń elektromagnetycznych (IEMI): jest to celowe i agresywne generowanie energii elektromagnetycznej, dla wprowadzania szumów lub sygnałów do systemów elektrycznych i elektronicznych, aby zakłócić, zmylić lub zniszczyć te systemów do celów terrorystycznych i przestępczych (kryminalnych).

Jest to ważny obszar zainteresowania Międzynarodowej Komisji Elektrotechnicznej -International Electrotechnical Commision (IEC) w zakresie Kompatybilności elektromagnetycznej - Electromagnetic Compatibility (EMC), w szczególności Podkomitetu IEC/SC/77C (EMC)

Terroryzm elektromagnetyczny oraz
kryminalny terroryzm elektromagnetyczny
Prymitywny terrorystyczny wariant broni HPM



Adaptacja kuchenki mikrofalowej na improwizowaną broń HPM

Terroryzm elektromagnetyczny oraz
kryminalny terroryzm elektromagnetyczny
Prymitywny terrorystyczny wariant broni HPM

Przykład zastosowania generatora HPM z adaptowanej kuchenki mikrofalowej przeciwko ludziom lub przeciwko elektronice

Terroryzm elektromagnetyczny oraz kryminalny terroryzm elektromagnetyczny

Instrukcja adaptacji kuchenki mikrofalowej

Terroryzm elektromagnetyczny oraz
kryminalny terroryzm elektromagnetyczny
Potencjalne narzędzia kontroli i wsparcia, zakłócanie GSM

Skaner

Terroryzm elektromagnetyczny oraz kryminalny terroryzm elektromagnetyczny Potencjalne narzędzia kontroli i wsparcia, zakłócanie GSM

Zagłuszacz telefonów GSM

Wykorzystanie widma elektromagnetycznego a deficyt pasm częstotliwości

Wojna elektromagnetyczna odbywa się w środowisku, które wydawałoby się dobrze znamy.

Rozpocznijmy od analizy wykorzystania radiowego pasma częstotliwości przeprowadzonych w USA i obejmujących lata 1990-2011:

Zgodnie z analizą, stwierdzono, że do 2011 roku do jednoczesnego przeprowadzenia dwóch dużych operacji potrzebne będzie pasmo dla środków mobilnych o przepustowości rzędu 16 Gb/s. To spojrzenie okazało się być przesadnie optymistycznym. Zapotrzebowanie lawinowo wzrastało:

1991 Operacja Desert Storm: 540 tys żołnierzy - 10 Mb/s

2002 Operacja Iraqi Freedom: 350 tys. żołnierzy - 4.2 Gb/s, co oznacza, że przy obniżeniu liczby żołnierzy o 40%, zapotrzebowanie na pasmo wzrosło ponad 40 razy(!).

Obecnie, dla jednej operacji, przy liczbie żołnierzy sięgającej tylko 160 tys., minimalne zapotrzebowanie na pasmo przekracza 7,7 Gb/s.

Wykorzystanie widma elektromagnetycznego a deficyt pasm częstotliwości c.d.

Warunkiem powodzenia współczesnych operacji wojskowych jest dostępność pasma elektromagnetycznego dla mobilnych środków łączności i transmisji danych o przepustowości tego rzędu. Przeciwnik ze wszystkich swoich sił będzie temu przeciwdziałał. Jak zdobyć wymaganą przewagę w środowisku elektromagnetycznym?

Musimy iść w wykorzystanie pasma na coraz wyższych częstotliwościach, nawet fizycznie niedostępnych dla potencjalnego przeciwnika np. w terahercach(!!).

Obecnie w amerykańskich Siłach Zbrojnych weszły nowe systemy łączności satelitarnej AEHF (Advanced Extremely High Frequency System), oparte o technologie, które możemy nazwać przełomowymi, zapewniającymi tzw. bezpieczną łączność na szczeblu strategicznym. Duży stopień wyprzedzenia technologicznego gwarantuje małe prawdopodobieństwo wykrycia, zakłócenia i przechwytu transmisji. AEHF zapewni łączność w całym spektrum misji, w tym na obszarach lądowych, w powietrzu na morzu, dla operacji specjalnych; strategicznych działań nuklearnych; strategicznej obrony; obrony rakietowej teatru działań i miejsc operacji wywiadowczych.

Przedstawione zmiany są nieuchronne i nieodwracalne i dotyczą zarówno naszych Sił Zbrojnych jaki sojuszników. Nasze Państwo jeśli chce zwycięsko rozstrzygać konflikty w operacjach krajowych i ekspedycyjnych, samodzielnie lub w ramach oddziałów sojuszniczych musi zapewnić naszym wojskom przewagę, co wiąże się przede wszystkim z wprowadzeniem (co jest możliwe) nowej architektury systemów C4ISR/ C4ISTAR.

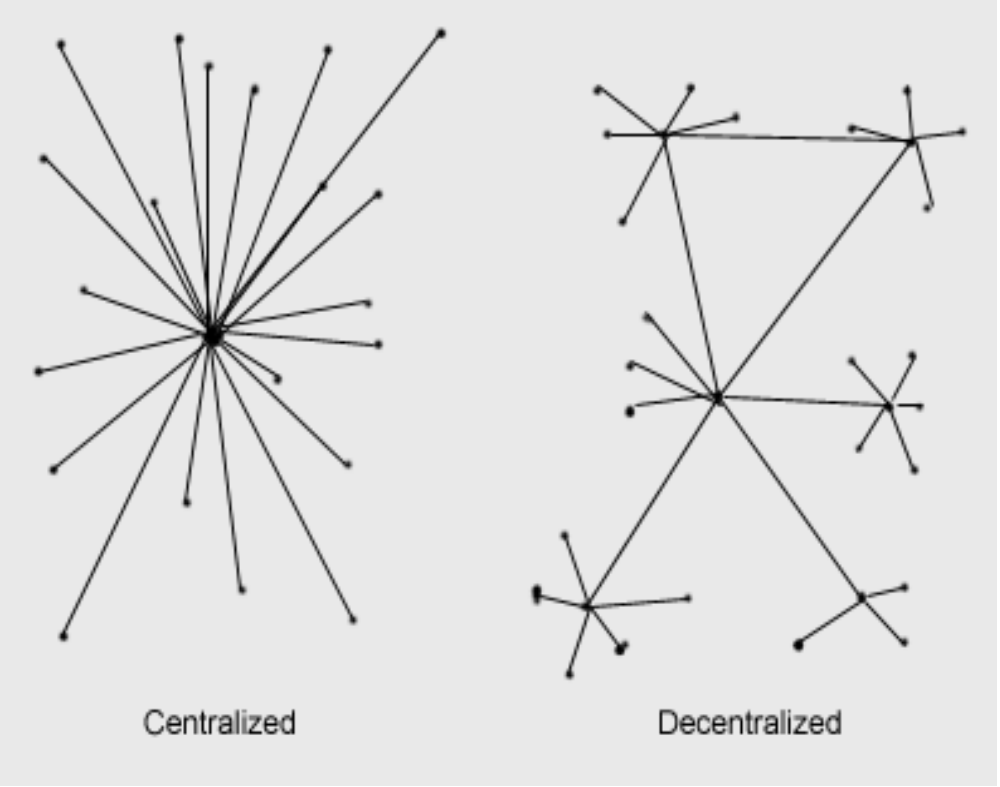
Tak naprawdę trendy w tym zakresie zostały wyznaczone 30-40 lat temu m.in. przez Paula Barana współtwórcy Internetu,, który urodził się w Toruniu.

Poprzednicy nowego systemu

„Stare” systemy łączności i dowodzenia też były sieciowe, ale o zupełnie innej strukturze – klasycznej, ściśle hierarchicznej. Tak zorganizowane systemy będą musiały odejść do lamusa.

Typy sieci zcentralizowanej i zdecentralizowanej:

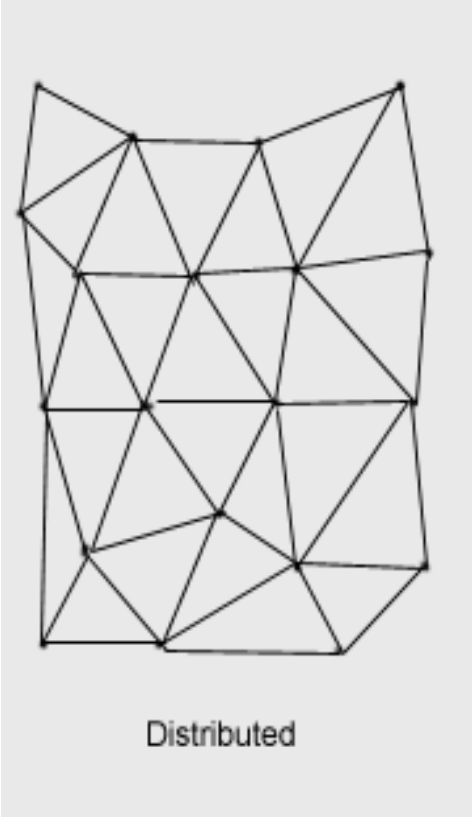
- **dla łączności,**
- **dla dowodzenia,**
- **do dozoru przestrzeni powietrznej i terenu,**
- **do rozpoznania**
- **do walki.**



Nowy typ systemu wojskowego:
C4ISR
i C4ISTAR dla Smart Grids?

Budowa nadmiarowego
niezawodnego systemu nowego typu w postaci
autonomicznej sieci rozłożonej:

- **dla łączności,**
- **dowodzenia,**
- **zarządzania**
- **szeroko rozumianego rozpoznania**
- **oraz naprowadzania na cele i do ataku**



1) Węzeł: sensor i aktuator
pod kontrolą komputera:
procesor i pamięć oraz funkcja
routera -
2) Połączenie – łączność szerokopasmowa
To te trendy zostały wyznaczone ponad 40 lat temu
(Paul Baran: ARPANET - Internet z pakietową transmisją danych)

Directed Energy Weapon

Broń skierowanej energii (DEW) jest typem broni emitującym energię w kierunku celu, rażąc cel odpowiednią porcją energii dla uzyskania pożądanego efektu.

Energia może być emitowana w formie:

Wiązki promieniowania elektromagnetycznego (zazwyczaj z laserów lub maserów).

Wiązki cząstek o skończonej masie (broń z wiązką cząstek).

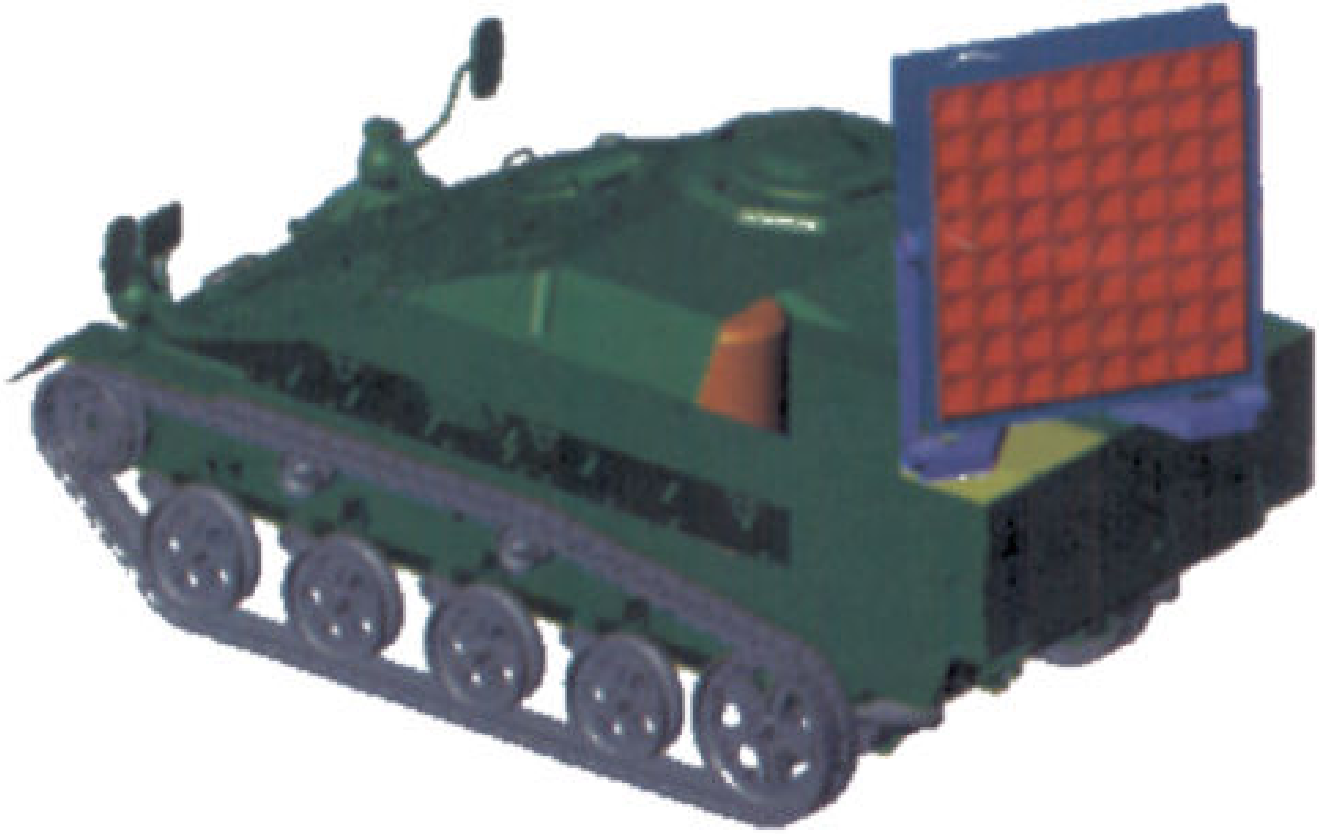
Dźwięku (broń z wiązką dźwiękową)

Directed Energy Weapon

Przykład amerykańskiego modelu 100 kW systemu laserowego na pojeździe Humvee (LLNL,GA,IDT,B.F. Goodrich)

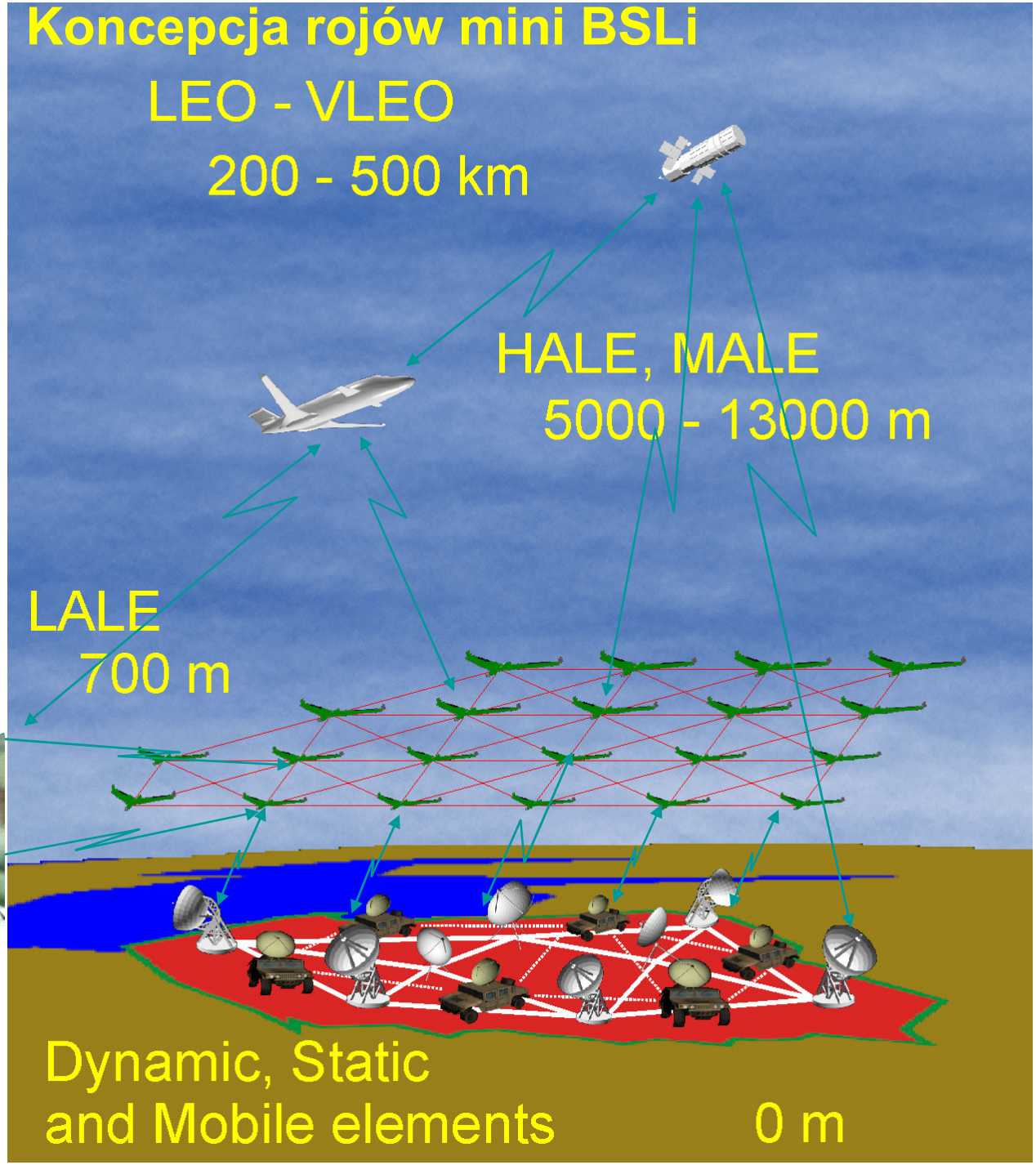
Przykład amerykańskiego systemu HPM ciągłego działania na wozie Hummvee

Przykład systemu HPM ciągłego działania firmy Rheinmetall na wozie Wiesel



Koncepcja uniwersalnych miniaturowych BSLi przewiduje:
Niski koszt 10-20k$
Niska masa<25kg
Ład. użyt. 10-15kg
Długi czas lotu
Duży promień działań

Bardzo duża liczba MINI BSL-R I MINI BSL-A (w rojach)

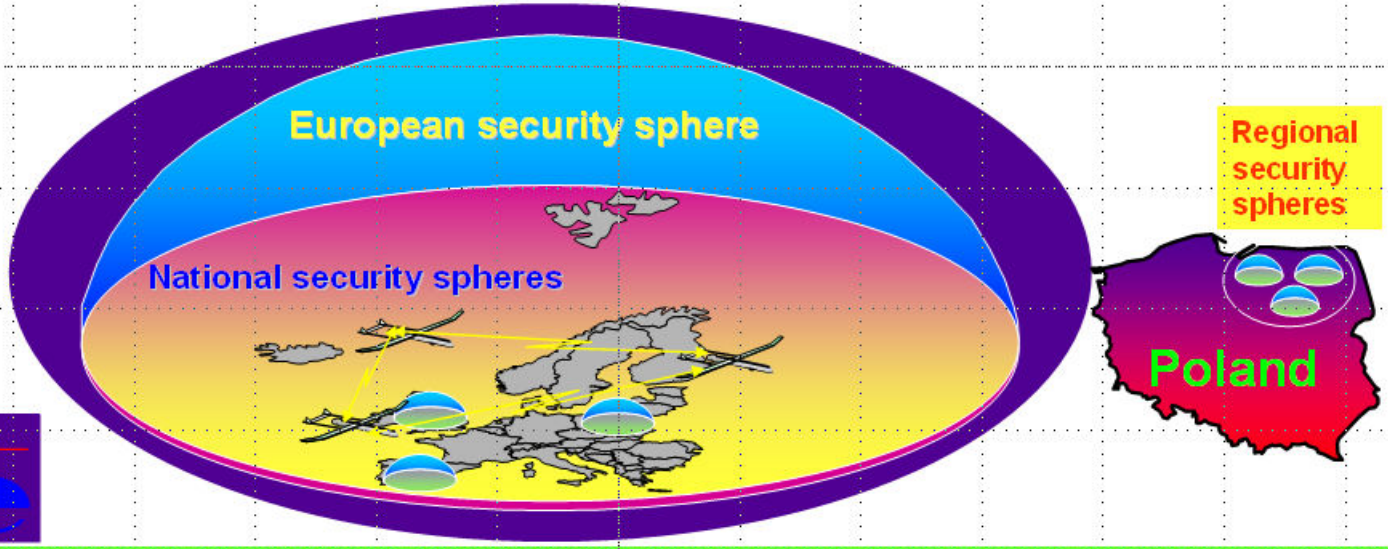


RESEARCH

Security Research

WAT - Military University of Technology
Institute of Optoelectronics
General Police Headquarters of Poland BOA - Office of Antiterrorist Operation
National Civil Defence Headquarters of Poland
The National Headquarters of the State Fire Service
The National Centre for Co-ordination of Rescue and Protection of Population

Three Level Secure Antiterrorist Air-Mobile miniUASs Low Cost Wide Area Power Grid Protection System - Level 1



Authors: Col. Maciej MROCZKOWSKI, Ph.D. Eng. 48 22 6839285; email: mmroczkowski@wat.edu.pl
Col. Ret. Lech SURAŻYŃSKI Ph.D. Eng. 48 22 6839726; email: lsurazynski@wat.edu.pl

Authors: Col. Ret. Maciej MROCZKOWSKI, Ph.D. Eng. 48 22 6839285; email: mmroczkowski@wat.edu.pl
Col. Ret. Lech SURAŻYŃSKI Ph.D. Eng. 48 22 6839726; email: lsurazynski@wat.edu.pl

OGÓLNE WYMAGANIA DLA SYMULATORA DYNAMICZNEJ STRUKTURY SIECIOCENTRYCZNEJ:

Procesor wielordzeniowy + multi-GPU
Pamięć, I/O – moc oblicz. multi-Tflop
Zintegrowane oprogramowanie:
bazy danych, GIS & symulacja systemu „prognoza stanów w czasie krótszym niż rzeczywisty", rozpoznawanie i porównywanie obrazów, itd...

Nosiciele:
male roje
miniBSL

Ladunek użyteczny-sensory:
miniSAR
miniMTI
kamery EO, IR,
sensory UV, CBRNE
LASERY

Szerokopasmowa bezp. cyfr. transmisja
SoftwareRadio&SoftwareRADAR, LASER

Adaptacyjne anteny (smart antenna array)

Ladunek użyteczny-środki obezwladniające:
precyzyjne glowice hukowe, gazy lzawiące, znaczniki widoczne w UV i inne środki obezwladniajace (HPM)

Propagacja fal EM (w perspektywie THz):
np. równanie Friisa:
$P_R = P_T G_T G_R \lambda^{**}2/(4\pi r)^{**}2;$
Równanie radarowe (bistatyczne):
$P_R = P_T G_T A_T \sigma/(4\pi)^{**}2 (r_T)^{**}2 (r_R)^{**}2;$
$A = \lambda^{**}2G/4\pi;$
szum, rozpraszanie, wielodrogowość, efekt Dopplera, wys. anten, EMC

Fizyczne parametry symulacji – punkty materialne x,y,z,t,m,u,v,w, Fx,Fy,Fz
Propagacja fal EM: $P_R = P_T G_T G_R \lambda^{**}2/(4\pi r)^{**}2;$
$P_R = P_T G_T A_T \sigma/(4\pi)^{**}2 (r_T)^{**}2 (r_R)^{**}2;$ $A = \lambda^{**}2G/4\pi;$

PODSUMOWANIE

W Polsce jest możliwe opracowanie i skompletowanie, wdrożenie i dostarczenie do dyspozycji odpowiednich służb i przedsiębiorstw o strategicznym znaczeniu (PSE, PKP, lokalnych dystrybutorów energii elektrycznej:

- **tanich systemów łączności i zarządzania bezpieczeństwem (włączając mobilne sieci autonomicznych miniBSL);**
- **systemów „dziennego i nocnego widzenia” (EO, IR) i miniaturowych systemów radiolokacyjnych MTI do pracy w sieci;**
- **Środków nagłego reagowania na atak, w tym obezwładniających, lokowanych na miniBSL;**
- **tanich elementów dodatkowego wyposażenia oddziałów antyterro-rystycznych, policji, straży pożarnej, SOK, służb energetycznych i innych.**
- **Posłuzy to podniesieniu bezpieczeństwa, w szegółności elektromagnetycznego Smart Grids**

DZIĘKUJĘ ZA UWAGĘ