INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY

Zakład Kompatybilności Elektromagnetycznej we Wrocławiu

ul. Swojczycka 38
51-501 Wrocław
tel.: +48 71 36 99 803
faks: +48 71 372 88 78
e-mail: wroclaw@il.wroc.pl
www.il.wroc.pl

National Institute of Telecommunications

ul. Szachowa 1
PL – 04-894 Warszawa
T: [+48 22] 512 81 00
F: [+48 22] 512 86 25
E-mail: info@itl.waw.pl
www.itl.waw.pl

Współistnienie, współzawodnictwo i współpraca w sieciach bezprzewodowych (wybrane zagadnienia)

Raport Z21/1317//09

Współistnienie, współzawodnictwo i współpraca w sieciach bezprzewodowych (wybrane zagadnienia)

WROCŁAW grudzień 2009

Metryka dokumentu

Nr pracy	:	21300019
Nazwa pracy	:	Współistnienie, współzawodnictwo i współpraca w sieciach bezprzewodowych (wybrane zagadnienia)
Zleceniodawca	:	Praca Statutowa
Data rozpoczęcia	:	Styczeń 2009 r.
Data zakończenia	:	Grudzień 2009 r.
Słowa kluczowe	:	
Kierownik pracy	:	prof. dr hab. inż. Ryszard Strużak
Wykonawcy pracy	:	prof. dr hab. inż. Ryszard Strużak

Autor raportu : Ryszard Strużak

Praca wykonana w Zakładzie Kompatybilności Elektromagnetycznej
Instytutu Łączności we Wrocławiu

Kierownik Zakładu: dr inż. Janusz Sobolewski

Streszczenie

Współistnienie, współzawodnictwo, kolaboracja – to pojęcia znane z ekologii i socjologii. Określają one wzajemne oddziaływania i relacje miedzy osobnikami, grupami i gatunkami. Praca niniejsza omawia oddziaływania elektromagnetyczne między urządzeniami – przyjazne i wrogie, celowe i niezamierzone. Rozwój Społeczeństwa Informacyjnego i postępy technologii powodują, że rośnie liczba urządzeń i sieci (zwłaszcza bezprzewodowych), wykorzystujących zjawiska elektromagnetyczne. Eksperci szacują, że do roku 2017 będzie przypadało 1000 urządzeń bezprzewodowych na każdego mieszkańca ziemi. Ich rozpowszechnienie oraz rozwój komputerów i Internetu zmieniają sposób, w jaki nowoczesne społeczeństwo wykorzystuje cyberprzestrzeń – prowadzą do poprawy dotychczasowych usług i powstania nowych usług. Sieci komputerowe są przykładem współpracy najbardziej zaawansowanej.

Ten rozwój spowoduje także większe uzależnienie społeczeństwa od niezawodnego działania takich urządzeń i sieci, co pokazały doświadczenia z sytuacji kryzysowych. Innym oczekiwanym skutkiem będzie wzrost współzawodnictwa, które w skrajnym przypadku przeradza się we wrogie działanie – atak. Należy liczyć się z możliwością terrorystycznych ataków elektromagnetycznych nieniszczących (infiltracja, cyberatak, zagłuszanie) i niszczących infrastrukturę fizyczną lub jej elementy (EMP, NEMP, HPM). Już obecnie, co sześć sekund rejestruje się w Internecie cyberatak i kradzież tożsamości. Z drugiej strony, pojedynczy atak EMP może nieodwracalnie zniszczyć infrastrukturę na terenie całej Polski. Podobne efekty, ale w znacznie mniejszej skali, powodować mogą w szczególnych okolicznościach niezamierzone zakłócenia elektromagnetyczne.

Systematyczne prace nad ochroną fizycznej infrastruktury cywilnej przestrzeni informatycznej przed atakiem elektromagnetycznym nie były dotychczas w Polsce prowadzone. Założenia do Rządowego *„Programu ochrony cyberprzestrzeni RP na lata 2009-2011”* opublikowane w 2009 r. inicjują prace nad spójną strategię ochrony cyberprzestrzeni Polski. Taka ochrona to problem holistyczny, w którym przeplatają się elementy techniczne, organizacyjne, ekonomiczne i socjalne, oraz działania prewencyjne, ochronne, przygotowawcze i naprawcze. Założenia programu rządowego koncentrują się na ochronie przed wrogą modyfikacją programów komputerowych i baz danych. Ochrona cywilnej infrastruktury fizycznej przed narażeniami elektromagnetycznymi nie jest tam uwzględniona. Instytut Łączności, Państwowy Instytut Badawczy, pierwsza i przez długi czas jedyna w Polsce placówka n.-b., wyspecjalizowana w problemach narażeń elektromagnetycznych (EM) i odporności na nie, prowadził z sukcesem prace w odniesieniu do narażeń niezamierzonych. Plany dotyczące rozszerzenia tej działalności na narażenia celowe (atak EM) zostały tam zaniechane w związku z brakiem zainteresowania (finansowania) ze strony przemysłu i ze strony administracji. Wobec zainicjowania prac nad spójną strategię ochrony cyberprzestrzeni Polski zaistniała możliwość publicznej dyskusji w sprawie ochrony przed atakiem elektromagnetycznym. Niniejsze opracowanie stanowi wprowadzenie do takiej dyskusji.

Spis treści

Spis rysunków

1. Wstęp

Współistnienie, współzawodnictwo, kooperacja – to pojęcia znane przede wszystkim z ekologii i socjologii. Określają one wzajemne oddziaływania i relacje miedzy osobnikami, grupami i gatunkami istniejącymi w tym samym czasie i w tym samym środowisku. Jeżeli nie oddziaływają one na siebie, mamy do czynienia z neutralizmem, jeżeli zaś wpływają na siebie, to ich oddziaływania mogą być antagonistyczne, wrogie, albo nieantagonistyczne, przyjazne (np. współpraca). Od kiedy Verhulst,[1] Volterra[2] i Lotka[3] zaproponowali pierwsze modele matematyczne oddziaływań środowiskowych, ich koncepcje inspirowane zachowaniem żywych organizmów znalazły zastosowania w dziedzinach tak odległych od biologii jak telekomunikacja. Telekomunikacja zainteresowana jest głównie oddziaływaniami elektromagnetycznymi, ponieważ wykorzystuje ona fale elektromagnetyczne (kierowanych i niekierowanych) do przetwarzania i przenoszenia informacji na odległość.[4]

Terminy „środowisko elektromagnetyczne”[5] i „sieć inteligentna”[6] „zaawansowana sieć inteligentna”[7] weszły już na stałe do słownictwa telekomunikacyjnego, a urządzeniom i systemom telekomunikacyjnym przypisuje się cechy istot żywych. Mówi się o „inteligencji zbiorowej” (*swarm intelligence*)[8], o zdolności do samoorganizacji, do współpracy, do uczenia się i adaptacji, czy do rozpoznawania otoczenia. Impuls w tym kierunku dał sukces popularnego standardu „Plug-and-Play”, który określa zdolności komputera do pracy z urządzeniami

---

[1] Pierre François Verhulst (1804 – 1849), matematyk belgijski;

[2] Vito Volterra (1860 – 1940), matematyk włoski;

[3] Alfred James Lotka (1880 – 1949); matematyk, fizyk i chemik amerykański (urodzony we Lwowie)

[4] Oddziaływania elektromagnetyczne są jednym z czterech rodzajów oddziaływań podstawowych, jakie wyróżnia fizyka. Pozostałe trzy to oddziaływania grawitacyjne (znane z fizyki klasycznej) oraz oddziaływania słabe i oddziaływania silne (znane z fizyki kwantowej).

[5] Definicja według słownika ATIS Telecom Glossary 2007: Electromagnetic environment (EME): 1. For a telecommunications system, the spatial distribution of electromagnetic fields surrounding a given site. *Note:* The electromagnetic environment may be expressed in terms of the spatial and temporal distribution of electric field strength (volts/meter), irradiance (watts/meter^2), or energy density (joules/meter^3). 2. The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation-static. [ATIS Telecom Glossary 2007];

[6] Definicja według słownika ATIS Telecom Glossary 2007: Intelligent network (IN): 1. A network that allows functionality to be distributed flexibly at a variety of nodes on and off the network and allows the architecture to be modified to control the services. 2. In North America, an advanced network concept that is envisioned to offer such things as (a) distributed call-processing capabilities across multiple network modules, (b) real-time authorization code verification, (c) one-number services, and (d) flexible private network services [including (1) reconfiguration by subscriber, (2) traffic analyses, (3) service restrictions, (4) routing control, and (5) data on call histories]. [ATIS Telecom Glossary 2007];

[7] Definicja według słownika ATIS Telecom Glossary 2007:Advanced intelligent network (AIN): A telecommunications network architecture that uses databases to facilitate call processing, call routing, and network management, allowing carriers to change the routing of both inbound and outbound calls from moment to moment. [FCC-5] 2. A proposed intelligent-network (IN) architecture that includes both IN/1+ and IN/2 concepts. [ATIS Telecom Glossary 2007];

[8] Bonabeau E, Dorigo M, Theraulaz G: Swarm Intelligence. From Natural to Artificial Systems; Oxford University Press, 1999

peryferyjnymi oraz do rozpoznawania otoczenia i zmian w połączeniach (dodanie lub odłączenie urządzenia). Przeglądarka Google wskazała w Internecie 260 000 publikacji na temat „Cognitive Wireless Networks" 61 200 publikacji na temat "Intelligent Wireless Networks"; i 2 200 na temat „Electromagnetic Ecology" (16.08.2009). Przy tak olbrzymiej liczbie publikacji nie jest możliwe szczegółowe omówienie wszystkich istotnych zagadnień w tak ograniczonym opracowaniu.

Neutralizm ma swój odpowiednik w telekomunikacji – kompatybilność elektromagnetyczną.[9] Jest to stan, w którym systemy i urządzenia ani nie zakłócają środowiska (tj. działania innych systemów), ani nie odczuwają oddziaływania środowiska w sposób istotny. Kiedy stan taki nie może być zachowany, występują nadmierne oddziaływania – zakłócenia elektromagnetyczne. Kooperacja jest podstawą działania każdego systemu telekomunikacyjnego. Na przykład w sieciach bezprzewodowych komunikujące się obiekty wykorzystują te same wcześniej uzgodnione częstotliwości radiowe, identyczne modulacje, formaty sygnałów itd. Bez takiej współpracy nawiązanie/ utrzymanie łączności byłoby niemożliwe. Taki rodzaj kooperacji Fitzek i Katz[10] nazywają kooperacją *pasywną* lub *ukrytą* (*passive* or *implicit*), w odróżnieniu od aktywnej lub jawnej (*active* or *explicit*). Współzawodnictwo należy do oddziaływań antagonistycznych, z uwagi na występujący tu konflikt interesów. Klasycznym przykładem współzawodnictwa w ekologii jest rywalizacja o ograniczone zasoby niezbędne do życia, a skrajną jego formą jest drapieżnictwo, które prowadzi do śmierci ofiary. W telekomunikacji bezprzewodowej możemy mówić o współzawodnictwie, kiedy dwa systemy używają tego samego pasma częstotliwości w sposób konfliktowy. Ekstremalnymi przykładami jest celowe zakłócanie lub zagłuszanie transmisji, „włamanie" elektromagnetyczne, „oszustwo" elektroniczne, albo atak elektroniczny. "

1.1 Plan pracy

W następnej części pracy omówione są trendy rozwojowe i ich konsekwencje oraz Programy Rządowe dotyczące rozwoju Społeczeństwa Informacyjnego i Ochrony Cyberprzestrzeni Kraju. Kolejny rozdział stanowi krótki przegląd problemów współpracy urządzeń, systemów i sieci telekomunikacyjnych. Autor nie rozwija tego tematu szerzej, odwołując się do swych oddzielnych opracowań i do innych publikacji. W rozdziale czwartym omówione są zagrożenia w przestrzeni wirtualnej (cyberprzestrzeni) i w przestrzeni fizycznej, na jakie narażone są systemy i sieci teleinformatyczne. Rozdział ten i następne nawiązują bezpośrednio do wspomnianego Programu Ochrony Cyberprzestrzeni Kraju. Problemy ochrony przed takimi zagrożeniami są omawiane w rozdziale piątym. Tutaj wykorzystane zostały materiały specjalnej komisji powołanej przez Kongres Stanów Zjednoczonych AP, opublikowane w 2008 r. W tym rozdziale zostały omówione także wcześniejsze prace i plany Zakładu Kompatybilności Elektromagnetycznej Instytutu Łączności, które wiążą się z tym tematem. Zamieszczone zostały tam także fotografie i szkice stanowisk niezbędnych do badania odporności urządzeń na celowe narażenia elektromagnetyczne. W rozdziale szóstym

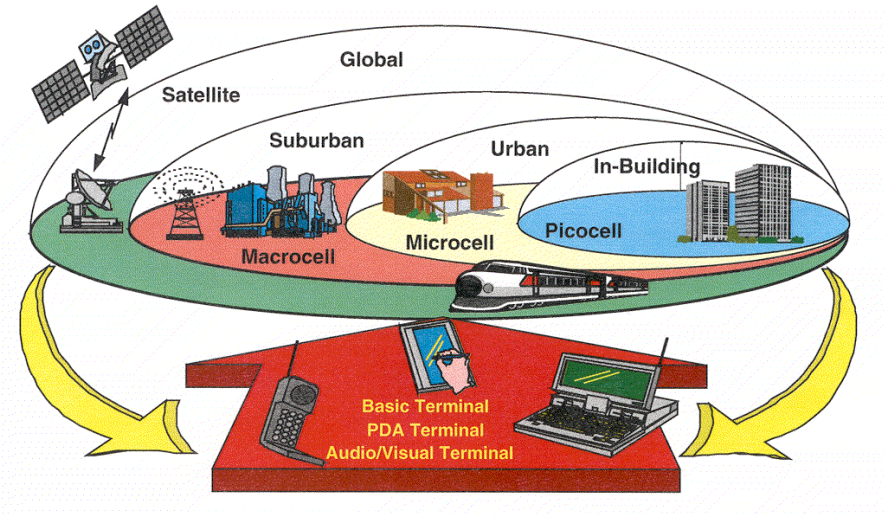
[9] Definicja według słownika ATIS Telecom Glossary 2007: Electromagnetic compatibility (EMC) is the condition which prevails when telecommunications equipment is performing its individually designed function in a common electromagnetic environment without causing or suffering unacceptable degradation due to unintentional electromagnetic interference to or from other equipment in the same environment. [NTIA] 2. The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness. [ATIS Telecom Glossary 2007];

[10] Fitzek F.H.P., Katz M.D.: Cognitive Wireless Networks; ISBN 978-1-4020-5978-0, Springer 2007

podsumowano całe opracowanie i przedstawiono szereg problemów, które zdaniem autora, wymagają rozwiązania w kraju. Z uwagi na brak specjalistycznego słownictwa w języku polskim, w opracowaniu jest często przytaczane słownictwo amerykańskie według najnowszej wersji (2007) oficjalnego słownika ATIS – Alliance for Telecommunication Industry Solutions. Wybór ten jest uzasadniony tym, że w Stanach Zjednoczonych terminologia telekomunikacyjna jest rozwinięta (prawdopodobnie) najlepiej.

2. Trendy i zamierzenia

W miarę rozwoju Społeczeństwa Informacyjnego i w miarę postępów technologii rośnie liczba urządzeń elektronicznych, zwłaszcza komputerów, i sieci bezprzewodowych. Rysunek 1 ilustruje wizję teleinformatyki bez granic – współpracujące ze sobą systemy o zasięgu globalnym, -makro, -mikro, -piko czy jeszcze mniejszym. Jakie będą konsekwencje tego rozwoju? Na to pytanie oczywiście nikt nie jest w stanie udzielić rzetelnej odpowiedzi, ale zakładając ciągłość rozwoju można określić trendy na podstawie dotychczasowych obserwacji.



Rysunek 1. Wizja współpracujących ze sobą systemów o zasięgu globalnym, -makro, -mikro i –piko.

Fitzek i in. podają na przykład (za Wireless World Research Forum, WWRF), że do 2017 roku w użyciu będzie siedem trylionów urządzeń bezprzewodowych, średnio tysiąc (!) urządzeń na osobę.[10] Będą one pracowały w sieciach globalnych, regionalnych i innych, np. w sieciach:

- lokalnych (WLAN, Wireless Local Networks),
- personalnych/ osobistych (WPAN, Wireless Personal Area Networks, WBAN – Wireless Body-area networks, Body-centric wireless communications),
- sensorowych (WSN, Wireless Sensor Networks),
- samochodowych (C2C, Car-to-Car Communication networks),
- identyfikacji radiowej (RFID, Radio Frequency Identification),
- pola bliskiego (NFC, Near-Field Communications),
- kontroli i zbierania danych (SCADA, Supervisory Control And Data Acquisition),
- nadzoru i bezpieczeństwa (Radio Technology for Social Safety and Security),
- innych, które rozwiną się w międzyczasie.

Większość publikacji na temat przyszłych systemów i aplikacji (“Internet of Things”, IOT; “e-commerce”; “e-government”; “e-education”; “e-health”; “Internet of Services, IOS”. „Next Generation Systems”, NGS”; „Long-Term-Evolution Systems, LTE” itp.) koncentruje się na fascynujących możliwościach nowych usług, jakie mogą one oferować. Zagadnienie oddziaływań środowiskowych nie znajduje w nich takiego odzwierciedlenia, na jakie ten problem zasługuje. Tymczasem doświadczenia nabyte do tej pory (z istniejącymi systemami) wskazują, że problemy współistnienia i współzawodnictwa mogą być czynnikiem ograniczającym praktyczne znaczenie nowych rozwiązań. Sprawy te omawiane są poniżej.

2.1 Więcej konfliktów

Wzrasta *liczba* potencjalnych konfliktów elektromagnetycznych miedzy obiektami. Przyczynia się do tego:

- wzrost liczby urządzeń, który prowadzi do zmniejszania odległości miedzy nimi,
- wzrastająca gęstość upakowania elementów tj. miniaturyzacja,
- stosowanie coraz mniejszych mocy i niższych napięć zasilających w urządzeniach elektronicznych (Green Radio Technologies). W rezultacie, nowe układy elektroniczne są ***bardziej wrażliwe*** i nawet słabe pola elektromagnetyczne mogą zakłócać ich działanie, lub powodować ich uszkodzenie.

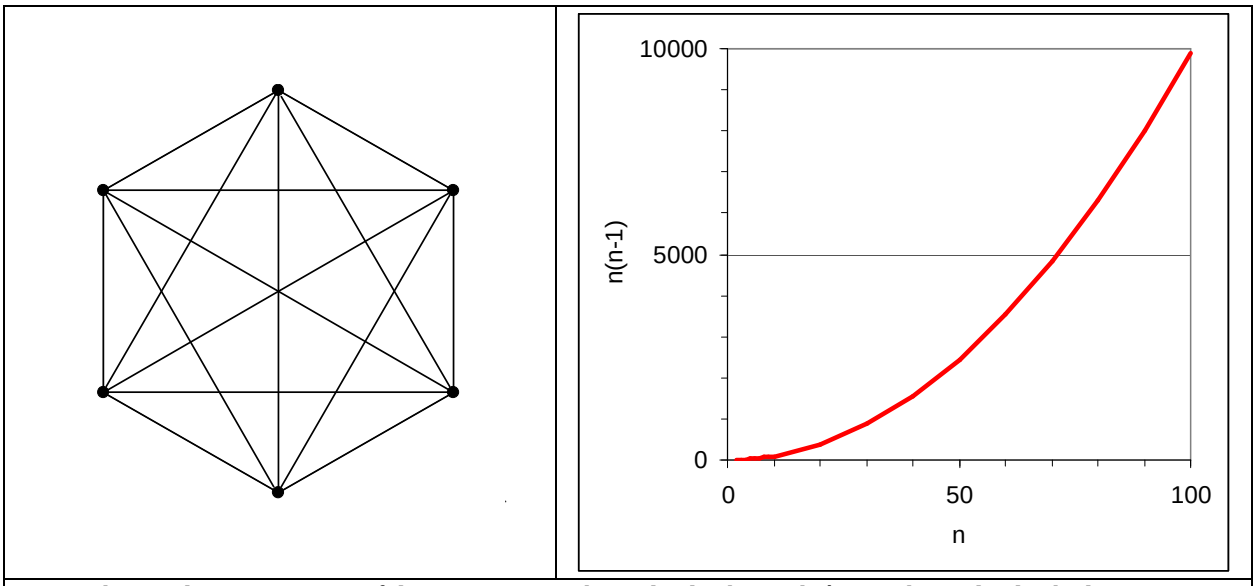
Sprawę ilustruje Rysunek 2. Przedstawia on sześć (n) urządzeń (np. terminali teleinformatycznych), które są reprezentowane przez punkty – wierzchołki grafu. Linie przedstawiają potencjalne oddziaływania miedzy nimi. Każde urządzenie łączy się z co najwyżej pięcioma (n-1) innymi urządzeniami. Ogólnie, potencjalna liczba oddziaływań wynosi co najwyżej n (n – 1). Przy zmniejszaniu siły oddziaływań elektromagnetycznych (sprzężeń i wrażliwości obiektów na te oddziaływania), w skrajnym przypadku część linii w grafie znika. Pozostają w nim jedynie te linie, które reprezentują oddziaływania użyteczne, niezbędne do transmisji informacji.

2.2 Większe uzależnienie

Wzrasta *uzależnienie* społeczeństwa od sprawnego działania urządzeń, systemów i sieci teleinformatycznych. Już obecnie kontrolują one w znacznym stopniu dostawy energii i usług komunikacyjnych, transportowych, finansowych i innych. Przechowują niezbędne informacje osobiste (od metryki urodzenia do aktu zgonu) i publiczne (lokalne, regionalne i krajowe), dokumenty finansowe, akta sądowe itd. Trend ten trafnie scharakteryzowała grupa ekspertów Międzynarodowego Związku Telekomunikacyjnego (International Telecommunication Union, ITU) w specjalnym raporcie „The Internet of Things”, przygotowanym dla konferencji „World Summit on Information Society 2005”. Czytamy w nim m. in.:

> *„Technological advances in „always on” communications promise a world of networked and interconnected devices that will provide relevant content and information to users, wherever they may be located. Machine-to-machine communications and person-to-computer communications will be extended to things, from everyday household objects to sensors monitoring the movement of Golden Gate Bridge or detecting earth tremors. Everything from tires to toothbrushes will fall within communication range, heralding the dawn of a new era, one in which today’s internet (of data and people) gives way to tomorrow’s Internet of Things”.*[11]

[11] ITU Internet Reports: The Internet of Things; Geneva, November 2005,



Rysunek 2. Po lewej stronie: Graf ilustrujący związek miedzy liczbą punktów i maksymalną liczba linii łączących je. Po prawej stronie: Wzrost liczby potencjalnych wzajemnych zakłóceń w zależności od liczby obiektów (n) powodujących zakłócenia i wrażliwych na nie.

2.3 Większa sieć powiązań

Rozwój sieci telekomunikacyjnej przyczynił się do rozwoju powiązań gospodarczych i kulturalnych nazywanych krótko „globalizacja". Globalizacja z kolei jest motorem napędowym dalszego rozwoju sieci teleinformatycznych i dalszego rozwoju sieci rozmaitych powiązań i oddziaływań. Funkcjonowanie rozwiniętego Społeczeństwa Informacyjnego przypomina pracę żywego organizmu, w którym zakłócenie normalnej pracy jednego tylko organu może prowadzić do bardzo poważnych następstw. Sieciowe systemy informatyczne (Networked Information Systems, NISs) integrują działania ludzi z systemami komputerowymi i telekomunikacyjnymi obejmując rożne struktury rozłożone często na wielkich obszarach. Sieci powiązań funkcjonalnych badała ostatnio Komisja Kongresu Stanów Zjednoczonych AP (nazywana dalej Komisją Grahama, od nazwiska przewodniczącego) w aspekcie oceny skutków ewentualnego ataku elektromagnetycznego. W swoim raporcie[12] opublikowanym w 2008 r., komisja wyróżnia dziesięć współzależnych obszarów infrastruktury:

- Elektroenergetyka *(Electric power)*
- Telekomunikacja *(Telecommunications)*
- Bankowość i finanse *(Banking and finance)*
- Paliwa *(Petroleum and natural gas)*
- Transport *Transportation*
- Żywność *(Food)*
- Woda *(Water)*
- Służby pogotowia *(Emergency services)*
- Satelity *(Space)*
- Rząd i samorząd *(Government)*

[12]Graham R et al. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Critical National Infrastructures; April 2008. http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf; http://www.empcommission.org/docs/empc_exec_rpt.pdf.

Rzeczywiste powiązania i zależności funkcjonalne ujawniają się najwyraźniej w sytuacjach krytycznych. Dla przykładu, powódź w Dolinie Odry w 1997 r., która doprowadziła w trzech krajach (Czechy, Polska i Niemcy) do śmierci 114 osób i szkód materialnych około 4,5 miliarda euro[13] wykazała krytyczną rolę niezawodnej telekomunikacji w wydarzeniach o tej skali. W raporcie, dla Komisji Sejmowej, powołanej w sprawie powodzi czytamy:

> *" System ostrzeżeń, informowania i ewakuowania zagrożonej ludności okazał się niesprawny, działał z opóźnieniem, a w pierwszych dniach powodzi - chaotycznie. Szczególnie dotkliwy był brak łączności na terenach zalanych, ponieważ łączność opierała się głównie na sieci telefonów przewodowych, zaś jak wiadomo z doświadczeń poprzednich powodzi, przewody telefoniczne i linie energetyczne jako pierwsze ulegają awarii już na początku wezbrania. W protokołach komisji badających przyczyny i skutki powodzi 1970, 1 972, 1977, 1979, 1980 r. i innych, zawsze, jako najistotniejsze utrudnienie w akcji przeciwpowodziowej wymieniano brak łączności. […]. Brakowało istotnej informacji z powodu zerwanej łączności lub zalania bądź niedostępności na skutek powodzi. Zalana także została siedziba oddziału wrocławskiego IMGW - głównego źródła komunikatów, prognoz i ostrzeżeń, łączność z tym ośrodkiem była zerwana przez kilka dni. […] Ostatnia powódź przekonała […] o wielkiej roli niezawodnej i trafnej informacji na temat aktualnych i prognozowanych zagrożeń. Konieczność rozwoju nowoczesnych, niezawodnych systemów informacji i prognoz dostrzegają wszyscy, rzecz w tym, aby to priorytetowe zadanie zostało szybko zrealizowane.*[14]

Takie same doświadczenia uzyskano w innych krajach a także w różnych organizacjach międzynarodowych. Najlepiej ujmuje te doświadczenia motto raportu dla Biura Koordynacji Akcji Humanitarnych Organizacji Narodów Zjednoczonych[15] (United Nations Office for the Coordination of Humanitarian Affairs)[16]:

> *"In the field, reliable communications is often a matter of life or death."*[17]

W różnych fazach katastrof ujawniają się różne elementy krytyczne. Huragan Katrina, (sierpień 2005) jeden z największych w Stanach Zjednoczonych, może tu służyć za przykład. Na skutek pierwotnego uszkodzenia sieci telekomunikacyjnej, powstała seria kolejnych, powiązanych ze sobą zdarzeń, które doprowadziły do śmierci 1464 osób i do wielkich strat materialnych. Policja, pogotowie ratunkowe zostały sparaliżowane natychmiast. Natomiast skutki uszkodzenia sieci elektroenergetycznej ujawniły się później. Nieczynne elektryczne pompy stacji paliw unieruchomiły transport, co uniemożliwiło ewakuacje ludzi, dostawy wody, żywności i sprzętu. Stan taki trwał tygodniami i miesiącami (zależnie od rejonu), i nawet trzy lata później Nowy Orlean i okolice nie doszedł w pełni do normalnego stanu, czytamy w raporcie

---

[13] http://pl.wikipedia.org/wiki/Powódź_tysiąclecia

[14] Bobiński E, Żelaziński J: Ocena przyczyn lipcowej powodzi. Wnioski do programu ochrony przeciwpowodziowej w przyszłości na Odrze *Ekspertyza opracowana dla Sejmowej Komisji Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa; 15.09.1997;* http://www.odra.pl/pl/dokumenty/962585850.shtml

[15] UN OCHA http://ochaonline.un.org/AboutOCHA/tabid/1076/Default.aspx; http://www.reliefweb.int/telecoms/

[16] Struzak R: Emergency Telecommunications with and in the Field: Evaluation Report; United Nations New York and Geneva, July 2000; http://www.reliefweb.int/telecoms/evalu/evaluation.html

[17] http://www.reliefweb.int/telecoms/evalu/OCHA_1_5.html

wspomnianej komisji Kongresu. Należy podkreślić, iż miało to miejsce w jednym z najbogatszych, najbardziej rozwiniętych i najlepiej zorganizowanych krajów świata.

Dysfunkcja jednego systemu może prowadzić uszkodzenia pozostałych, podobnie jak pojedyncza kula śnieżna może spowodować lawinę. Wśród wszystkich systemów, system energetyczny, system teleinformatyczny i system bankowy mają, zdaniem Komisji, podstawowe znaczenie. Rysunek 3, zaczerpnięty z raportu wspomnianej Komisji ilustruje główne związki funkcjonalne, w których mają one udział.

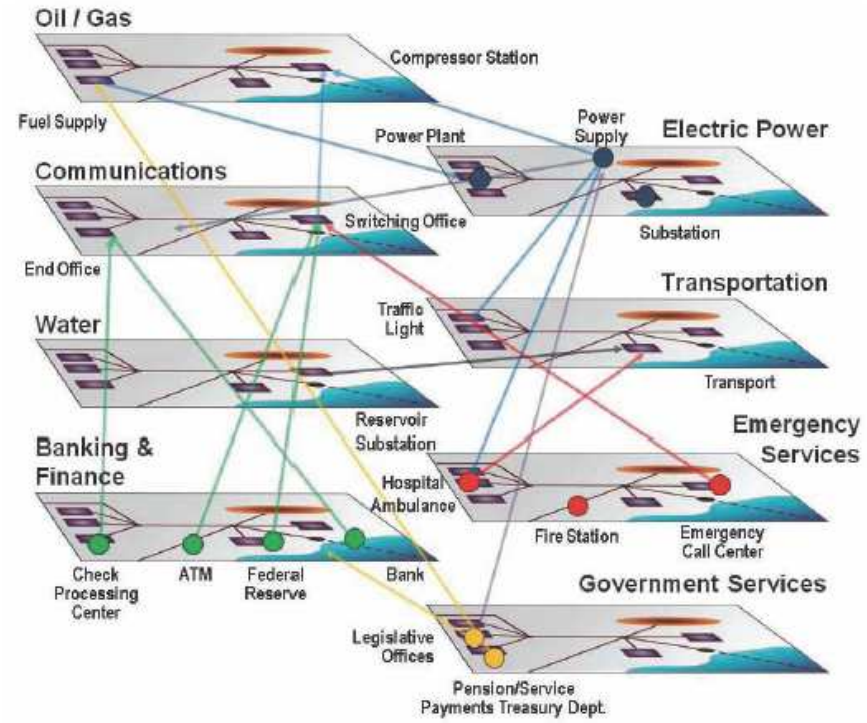


Figure 1-7. A Conceptual Illustration of the Interconnectedness of Elements Contained Within Each Critical Infrastructure. *Some connections are not shown (diagram provided courtesy of Sandia National Laboratory).*

Rysunek 3. Sektory infrastruktury państwa, których działanie może być zakłócone elektromagnetycznie i ich współzależność. Rysunek zaczerpnięty z publikacji: Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.

Niektóre związki są tak złożone, że są trudne do identyfikacji:

"We have produced designs so complicated that we cannot possibly anticipate all the possible interactions of the inevitable failures; we add safety devices that are deceived or avoided or defeated by hidden paths in the systems." [18]

Jednoczesna dysfunkcja większej liczby elementów prowadzić może do ogólnej katastrofy. Komisja podkreśla przy tym, że rozdzielanie tych obszarów i rozpatrywanie ich w oderwaniu od pozostałych utrudnia lub uniemożliwia ocenę rzeczywistej ich współzależności. Charles Perrow scharakteryzował ten fakt następująco:

[18] Perrow C: Normal Accidents: Living with High-Risk Technologies Basic Books, NY, 1984 (cytowane za Raportem Komisji Grahama…).

2.4 Więcej zagrożeń

Co sześć sekund rejestruje się kradzież tożsamości w sieci i ponad 35 tysięcy ataków wirusowych, a „cybercrime" – przestępstwa dokonane za pośrednictwem sieci teleinformatycznej dają łup przewyższający dochody z nielegalnego handlu narkotykami[19] i straty dla legalnego biznesu szacowane na 1 trylion dolarów US[20]. Mniej znane są celowe ataki i niezamierzone oddziaływania elektromagnetyczne, które dają podobne efekty.

Sieci teleinformatyczne są centralnym nerwem infrastruktury kraju. Duże i małe przedsiębiorstwa i organizacje polegają na komputerowych listach plac, księgowości, ewidencji zasobów itd. Dystrybucja energii, żywności i innych dóbr, od producenta do konsumenta, w każdej fazie, jest kontrolowana i sterowana przez skomputeryzowane sieci sensorów i sterowników. Nowe, „inteligentne" systemy teleinformatyczne oferują nowe i/lub lepsze usługi kosztem większej złożoności i często większej wrażliwości na zakłócenia przypadkowe i celowe. Cyberatak, tak jak i oddziaływania elektromagnetyczne mogą czasowo zablokować sieć teleinformatyczną, albo zniszczyć trwale zawartość baz danych lub elementy fizyczne.

Szczególnie wrażliwe są rozległe systemy sensorowe, alarmowe, nadzoru i zbierania danych SCADA (Supervisory Control And Data Acquisition)[21] oraz takie, których funkcje można zmieniać na odległość w czasie normalnej pracy. Podobnie wrażliwe są rozległe sieci gromadzenia danych osobowych (włącznie zdanymi o stanie zdrowia), danych finansowych, aktów prawnych (np. prawa własności). Obecne systemy i ich elementy nie były projektowane z myślą o możliwych atakach elektromagnetycznych. Dotyczy to zwłaszcza systemów bezprzewodowych, których popularność ciągle rośnie. Większość jest nieodporna na ataki elektromagnetyczne, także ze względów ekonomicznych. Szkody spowodowane atakiem "miękkim" mogą być niezauważone natychmiast i pozostać niezauważone w ciągu długiego okresu czasu, albo też zauważone szkody mogą nie być kojarzone z takim atakiem.

Sprawę ilustruje przykład z życia. Amerykański oddział koncernu "Nissan" ostrzegał w 2007 r. swoich klientów, aby nie trzymali określonej serii elektronicznych kluczyków od samochodów blisko telefonów komórkowych. Inaczej silniki mogą nie zapalić. Problem dotyczył specjalnych kluczyków, komunikujących się z samochodem za pośrednictwem pola elektromagnetycznego. Sygnały telefonu komórkowego wymieniane automatycznie ze stacją bazową zmieniały w sposób nieodwracalny kod zapisany w kluczyku[22]. Przyczyna tkwi w układzie scalonym nazbyt wrażliwym na pole elektromagnetyczne telefonu. Takie i podobne układy scalone są używane masowo w wielu urządzeniach.

Trend w kierunku liberalizacji i prywatyzacji zaostrza konkurencję i presję na obniżanie kosztów, co odbija się niekorzystnie na odporności sieci na takie ataki i narażenia. Obniżanie kosztów uzyskuje się zwykle przez stosowanie rozwiązań najtańszych, eliminowanie funkcji

---

[19] Informacja zaczerpnięta z opisu programu "Norton antivirus"

[20] Dane według ITU News, October 2009, str. 10

[21] SCADA are electronic control systems that may be used for data acquisition and control over large and geographically distributed infrastructure systems. They find extensive use in critical infrastructure applications such as electrical transmission and distribution, water management, and oil and gas pipelines. SCADA technology has benefited from several decades of development. It has its genesis in the telemetry systems used by the railroad and aviation industries.

[22] Źródło: Gazeta Wyborcza, 11 czerwca 2007

rzadko używanych, redukcję rezerw itd. Dla zapewnienia rynku, stosuje się rozwiązania firmowe niestandardowe i niekompatybilne z innymi i nadużywa pojęcia „trade secret" lub „intellectual property rights" co powoduje dodatkowe trudności w zapewnieniu niezawodnej i bezpiecznej współpracy urządzeń, systemów i usług oferowanych przez różnych producentów lub dostawców.

Infrastruktura informatyczna, jej elementy "twarde" (hardware) i "miękkie" (software & data) mogą same być celem ataku terrorystycznego, lub mogą służyć jako narzędzie do ataku na inne cele (np. system elektroenergetyczny). Olbrzymia większość elementów cywilnej sieci telekomunikacyjnej jest celem względnie łatwym. Na szczęście, przy braku rozległych uszkodzeń fizycznych usługi sieciowe mogą być często przywrócone w ciągu godzin. W tym czasie jednak powstać może chaos i ogólna panika, której skutki mogą przynieść nieobliczalne straty. Nieodwracalna utrata lub wrogie zafałszowanie krytycznych danych przechowywanych w formie elektronicznej może powodować podobne straty i mieć trwałe skutki dla społeczeństwa.

2.5 Program rządowy

Unia Europejska planuje upowszechnienie Internetu i tzw. „e-usług", publicznych i komercyjnych. Wobec wrażliwości tych usług na narażenia, Rada Europejska przyjęła w 2003 roku *Europejską Strategię Bezpieczeństwa* i program *"Zapobieganie, gotowość i zarządzanie skutkami aktów terroryzmu"* w ramach ogólnego programu *"Bezpieczeństwo i ochrona wolności"* na lata 2007-2013. W skali ogólnoświatowej, szereg organizacji prowadzi prace zmierzające do ograniczenia takich ataków, m.in. Międzynarodowy Związek Telekomunikacyjny ITU, Międzynarodowa Unia Nauk Radiowych URSI[23], Międzynarodowa Komisja Elektrotechniczna IEC [[24]].

Zamierzenia Polski w zakresie upowszechnienia *e-usług* przedstawione w 2008 r. dokumencie rządowym „Strategia Rozwoju Społeczeństwa Informacyjnego w Polsce do roku 2013"[25] są imponujące, ale podobnie jak plany europejskie wymagają odpowiednich działań wspomagających w zakresie ochrony infrastruktury informatycznej. Takie działania zawierają Założenia do Rządowego *„Programu ochrony cyberprzestrzeni RP na lata 2009-2011"* [26] opublikowane w marcu 2009 r. Przez „cyberprzestrzeń" rozumie się ogólnie media cyfrowe wszelkiego rodzaju od telefonii komórkowej do usług Internetowych. (stąd alternatywna nazwa – Przestrzeń Informatyczna). Dokument rządowy Zawiera on założenia działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania cyberterroryzmu oraz innych zagrożeń dla bezpieczeństwa państwa pochodzących z publicznych sieci teleinformatycznych. Przewiduje w przyszłości utworzenie

[23] Wik M: URSI statement - Nuclear electromagnetic pulse [EMP] and associated effects; Antennas and Propagation Society Newsletter, IEEE, Jun 1987, Vol. 29/3, pp 19- 23

[24] IEC 61000-2-9 – Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance. Basic EMC publication, ; http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=cat-det.p&wartnum=020728

[25] Strategia Rozwoju Społeczeństwa Informacyjnego w Polsce do roku 2013, Projekt wersja 3.00 (październik 2008); http://www.mswia.gov.pl/strategia/

[26] Założenia do Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011 (Data publikacji : dn.11 marca 2009) http://www.mswia.gov.pl/portal/pl/2/6966/Zalozenia_do_Rzadowego_programu_ochrony_cyberprzestrzeni_RP_na_lata_20092011.html

kompleksowego Narodowego Programu Ochrony Infrastruktury Krytycznej. Działania techniczne wyszczególnione w Programie obejmują osiem elementów:

a) rozbudowę zespołu reagowania na incydenty komputerowe,

b) rozbudowę systemu wczesnego ostrzegania przez atakami sieciowymi,

c) wdrażanie dodatkowych rozwiązań prewencyjnych,

d) zarządzanie ćwiczeń obejmujących badanie odporności krytycznej infrastruktury teleinformatycznej na kontrolowane cyberataki,

e) szczególną ochronę kluczowych systemów informatycznych,

f) wdrażanie rozwiązań zapasowych, które mogą przejąć realizację procesu w sytuacji uszkodzenia, zniszczenia lub niedostępności systemów i sieci zaliczonych do krytycznej infrastruktury teleinformatycznej,

g) rozwój witryny www.cert.gov.pl jako podstawowego źródła informacji o metodach przeciwdziałania, podatnościach i atakach z cyberprzestrzeni,

h) konsolidację dostępu do usług publicznych.

Miarą skuteczności tych działań będzie ocena stworzonych regulacji, instytucji i relacji. Cały program rządowy koncentruje się na ochronie przed wrogą modyfikacją programów komputerowych i baz danych („miękkiej” infrastruktury). Założenia nie wspominają o narażeniach elektromagnetycznych ani o przedsięwzięciach zmierzających do oceny stopnia wrażliwości fizycznej infrastruktury państwa („twardej” infrastruktury) na takie narażenia i ewentualnej potrzebie jej zmniejszenia. W szczególności pomijają one milczeniem problem środków na inwestycje niezbędne do uodpornienia infrastruktury teleinformatycznej na takie narażenia i na prace badawczo-projektowe wymagane do właściwego przygotowania takich inwestycji. Takie przygotowanie powinno obejmować rozpoznanie istniejącego stanu odporności fizycznej infrastruktury państwa na narażenia elektromagnetyczne, na zidentyfikowania elementów wymagających poprawy oraz zaproponowanie sposobów ich wzmocnienia ze wskazaniem i uzasadnieniem sugerowanego rozwiązania. Nie jest określona w programie rola państwowych placówek badawczych, które zostały powołane do wspierania decyzji administracji państwowej i samorządowej niezbędnymi analizami i badaniami, do rozwiązywania problemów ważnych dla państwa, takich jak np. poruszany w niniejszej pracy.

3. Współpraca

Zalety kooperacji są znane z socjologii, biologii, i teorii gier. Na korzyści ich wykorzystania w sieciach telekomunikacji bezprzewodowej wskazywano już wcześniej. W ostatnim okresie możliwości te są przedmiotem intensywnych badan w wielu ośrodkach za granicą.

3.1 Odbiorniki

Współpraca stacji odbiorczych oferuje dodatkowe właściwości, jakich nie dają odbiorniki działające oddzielnie. Przykładem służyć może radio interferometr, prekursor systemów typu SIMO – Single-Input-Multiple-Output. Jego twórcy, M. Ryle i D. Vonberg, w 1946 r. użyli dwu odbiorników radiowych do precyzyjnego określenia kierunku nadejścia fali elektromagnetycznej emitowanej przez odległe źródła w kosmosie. Radio interferometr pozwala uzyskać precyzję pomiaru nieosiągalną innymi metodami. Jego zasada sprowadza się do pomiaru względnego opóźnienia (różnicy faz) fali z docierającej do każdego z odbiorników. Precyzja pomiaru zależy m.in. od bazy pomiarowej – odległości miedzy odbiornikami. Radioastronomowie wykorzystują bazy o wielkich rozmiarach. Na przykład w europejskiej sieci EVN, European Very Long Baseline Interferometry Network (do której należy m.in. obserwatorium w Piwnicach k. Torunia) baza pomiarowa może wynosić tysiące kilometrów, co zapewnia rozdzielczość kątową rzędu 1 milisekundy.[27] Taka precyzja pozwala np. mierzyć ruchy kontynentów z dokładnością do milimetrów. W ramach programu SVLBI - Space Very Long Baseline Interferometry, osiąga się jeszcze większą dokładność, dzięki umieszczeniu w 1997 r. jednego z odbiorników na sztucznym satelicie Ziemi. W ten sposób uzyskuje się bazę, przekraczającą kuli ziemskiej.

Inny przykład to radar pasywny. Wykorzystuje on zespół odbiorników wspólnie analizujących fale elektromagnetyczne odbite od śledzonego obiektu. Fale te mogą pochodzić od istniejących postronnych(niewspółpracujących ze sobą) nadajników radiowych, telewizyjnych, stacji bazowych sieci komórkowych itd. Radar pasywny lokalizuje obiekty nie emitując energii elektromagnetycznej. W odróżnieniu od radaru impulsowego, radar taki jest więc "niewykrywalny", nie wymaga dużych mocy zasilających i może pracować na różnych częstotliwościach, nawet nieprzeznaczonych dla radiolokacji, nie wymagając zgody na emisję. Zasięg i precyzja radaru pasywnego są tym większe im więcej wykorzystuje on odbiorników i nadajników. Może on służyć za przykład implementacji koncepcji MIMO – Multiple Input Multiple Output.

3.2 Nadajniki

Zasada współpracy nadajników jest również znana od lat 40-tych ubiegłego stulecia, kiedy wprowadzono system nawigacyjny LORAN – Long RAnge Navigation. Ten system (typu MISO – Multiple Input- Single Output) wykorzystywał kilka współpracujących ze sobą nadajników o znanej lokalizacji do określenia położenia i prędkości odbiornika na podstawie analizy charakterystyk czasowych odbieranych fal. Popularny dziś system GPS – Global Positioning System, uruchomiony w 1995 r., tak jak i planowany system Galileo oparte są na tej samej zasadzie, z tym, że nadajniki (w liczbie 25 do 30), umieszczone są na sztucznych satelitach Ziemi, na wysokości około 20 tysięcy kilometrów.[28] Inny przykład, to zespół nadajników, które

[27] The European VLBI Network; http://www.evlbi.org

[28] Julien O, Macabiau C, Issler J-L: Strukture and Performance of the Future Galileo Civil Signals; Radio Science Bulletin No 330, Sept.2009 p. 31-50

promieniują fale elektromagnetyczne w taki sposób, że w wybranym punkcie przestrzeni wszystkie promieniowane przez nie fale mają zgodną polaryzację i fazę i sumują się. Przy N identycznych nadajnikach (i tłumieniach fal składowych), fala wypadkowa ma amplitudę N-krotnie większą niż każda fala składowa, tj. moc N^2 razy większą. Ta właściwość może być przydatna np. w rozproszonych bezprzewodowych sieciach sensorowych, w których indywidualne nadajniki są za słabe, aby bezpośrednio przekazać informacje do stacji docelowej – centralnego kolektora danych.

3.3 Sieci

Sieci komputerowe są przykładem współpracy najbardziej zaawansowanej. Rozpowszechnienie komputerów i szerokopasmowego Internetu, w powiązaniu z zasadą współpracy, zmieniają sposób, w jaki nowoczesne społeczeństwo wykorzystuje cyberprzestrzeń. Jej zasoby mogą być łączone w wirtualne organizacje, które z kolei mogą łączyć się z innymi organizacjami. Centra danych i sieci komputerowe rozmieszczone w odległych miejscach są coraz częściej łączone ze sobą (np. światłowodami lub bezprzewodowymi łączami satelitarnymi i naziemnymi) tworząc jedną rozległą sieć, która rozciąga się nie tylko wokół ziemi, ale także poza nią, w przestrzeni kosmicznej. Pojawiają się ciągle nowe możliwości, nowe koncepcje i nowe terminy (nie zawsze precyzyjnie zdefiniowane), np.: “Grid computing”, „Computing-on-demand”, “Edge computing”, „Cloud computing”, “Utility computing”, “Software as a Service (SaaS)” itp. Wszystkie one opierają się na zasadzie współpracy i współużytkowania zasobów fizycznych i wirtualnych, takich jak niżej:

Zasoby fizyczne	Zasoby wirtualne
• Moc obliczeniowa komputera • Pojemność urządzeń magazynujących informacje • Pojemność kanału telekomunikacyjnego	o Systemy operacyjne o Oprogramowanie (software), licencje o Zadania / aplikacje o Usługi

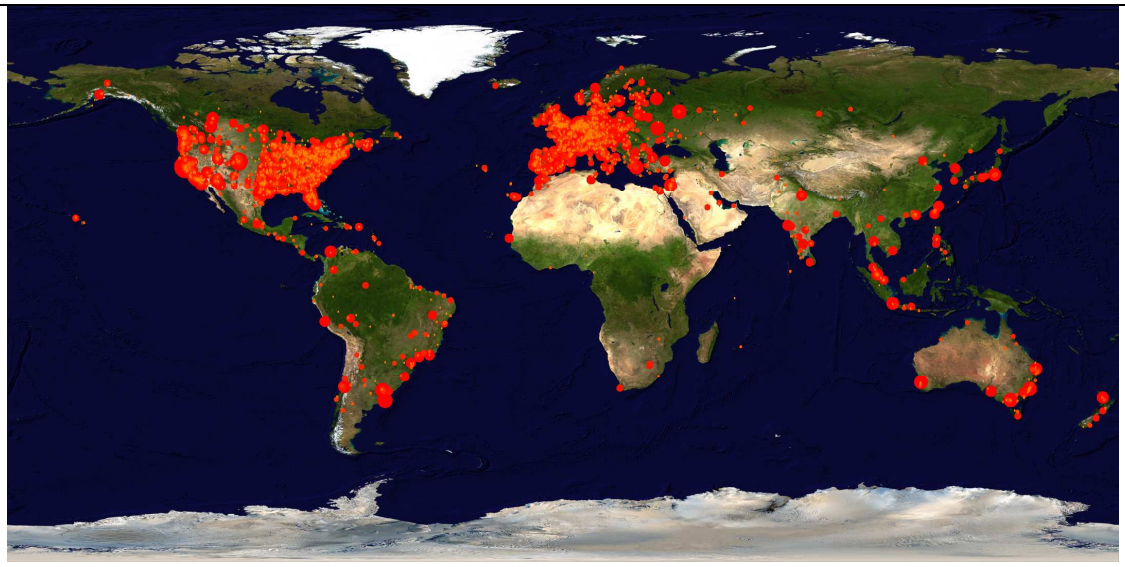
“Grid computing” umożliwia współużytkowanie, wybór i agregację zasobów i procesów. Przykładem może służyć europejska sieć EDGEE (Enabling Grids for E-sciencE), jedna z największych tego rodzaju: łączy ona ze sobą 80 tysięcy procesorów, 140 instytucji, 50 krajów, i 10 tysięcy użytkowników w 300 lokalizacjach[29]. CERN (European Organization for Nuclear Research) wykonuje w niej średnio 150 tysięcy zadań (jobs) dziennie. Koncepcja współpracy staje się coraz bardziej popularna w społeczeństwie i wiele osób prywatnych udostępnia bezpłatnie niewykorzytywane zasoby swoich komputerów osobistych do wykorzystania w rozmaitych programach badawczych. Program „fold@home”[30] może służyć za przykład. Ponad 400 tysięcy konsol Sony PlayStation3 oraz komputerów osobistych z całego świata łączy się przez Internet z serwerami znajdującymi się na Stanford University, skąd pobierane są dane do obliczeń i dokąd odsyłane są wyniki (Rysunek 5). Łącznie oferują one sumaryczną moc obliczeniowa rzędu 4.5 PetaFLOPS (FLOPS to skrót od „**FL**oating point **O**perations **P**er **S**econd; Peta = 10^{15})[31].

[29] http://public.eu-egee.org/

[30] http://folding.stanford.edu/

[31] Distributed Computing: Utilities, Grids & Clouds; ITU-T Technology Watch Report 9, May 2009

Technologia ta jest także wykorzystywana – na mniejsza niż CERN skale – w innych organizacjach. W ITU np. komputery personelu są wykorzystywane poza godzinami pracy, w nocy, do czasochłonnych rutynowych obliczeń i analiz. Grid Computing przenika szybko z zastosowań naukowych i "not-for-profit", do zastosowań komercyjnych. „Utility computing" polega na korzystaniu z cudzych usług komputerowych, oferowanych w formie „wirtualnego" komputera, płacąc tylko za użyty sprzęt, oprogramowania i zasoby pamięci. Taki wirtualny komputer jest implementacja programową życzeń użytkownika w zakresie mocy obliczeniowej, pojemności pamięci, systemy operacyjnego itp.



Rysunek 5. Sieć współpracy w ramach programu Folding@home. Czerwone punkty na mapie świata reprezentują współpracujące (indywidualne) komputery Źródło: http://folding.stanford.edu/

3.4 Wykorzystanie zasobów

Wyższy poziom kooperacji to kooperacja międzysieciowa / międzysystemowa, która w sposób naturalny wiąże się w pewnym stopniu ze współpracą administracyjną międzyrządową i międzynarodową. Zagadnienia współpracy na takim poziomie są przedmiotem studiów technicznych (i negocjacji) w ramach, m.in. Międzynarodowego Związku Telekomunikacyjnego ITU – International Telecommunication Union. Wybrane aspekty takiej kooperacji zostały przedstawione m.in. we wcześniejszych publikacjach autora [32], [33]. Współpraca otwiera tu perspektywy lepszego wykorzystania zasobów częstotliwości radiowych, zwłaszcza w sieciach sensorowych i dostępowych nowej generacji. Zasoby radiowe mają wiele punktów wspólnych z innymi dobrami współużytkowanymi (Public Goods, Common-Pool Resource -CPR, Common Property Resource): tak samo grozi im przeciążenie (congestion), zanieczyszczenie (pollution), nadmierna eksploatacja (overuse), lub zniszczenie. Dobra tego rodzaju mogą być deklarowane jako własność wspólnoty, reprezentowanej przez rząd krajowy, regionalny, lub lokalny, albo własność prywatna poszczególnych osób lub przedsiębiorstw. Kiedy nikt nie zgłasza praw własności, są one zasobami „open access".

[32] Kirby R , Struzak R: On Radio Spectrum, Competition and Collaboration; (Invited Paper), Proceedings of the 17-th General Assembly of the URSI, Tel-Aviv, Israel, 24 September - 2 Oct. 1987

[33] Radicella S (ed.)/ Struzak R: Introduction to International Radio Regulations; International Centre for Theoretical Physics, ISBN 92-95003-23-3 (2003). Dostępna wersja elektroniczna: http://publications.ictp.it/lns/vol16.html.

Zarządzanie zasobami radiowymi różni się znacznie od zarządzania innymi zasobami. Dotychczas odbywało się ono metodą prób i błędów, oparte było na doświadczeniach praktycznych i skupiało się ona na aspektach technicznych i organizacyjnych. Od szeregu lat pojawiają się propozycje zmiany tego podejścia. Wychodząc z przesłanek teoretycznych tzw. Chicago School of Economics, proponuje się prywatyzację zasobów radiowych i ograniczenie roli regulacyjnej państwa i organizacji międzynarodowych takich jak ITU; wykorzystaniem zasobów ma rządzić „niewidzialna ręka rynku", tj. prawa własności, podaży, popytu, ceny i zysku. Idea ta, początkowo niepopularna, zyskiwała coraz więcej zwolenników, aż do czasu obecnego światowego kryzysu ekonomicznego, który obnażył po raz kolejny słabości zasady wolnego rynku. Problem zasobów współużytkowanych budzi coraz większe zainteresowanie i nabiera coraz większego znaczenia. Ekonomiczna Nagroda Nobla w 2009 r. przyznana została Elinor Ostrom za prace dotyczące zarządzaniem takich dóbr w zastosowaniu do problemów ochrony środowiska. Jej obserwacje zaprzeczają tezie, że dobra współużytkowane powinny być sprywatyzowane, bowiem w przeciwnym razie staja się one nieprzydatne, ale pogląd ten nie jest przyjmowany powszechnie i bez zastrzeżeń. W jakim zakresie te wnioski odnoszą się do zasobów radiowych pozostaje do wykazania. Dyskusja tego problemu wykracza jednak poza ramy niniejszego raportu i wymaga oddzielnego opracowania. Problemy wykorzystania zasobów radiowych omówione są miedzy innymi w publikacjach,[34], [35], [36], oraz w oddzielnym opracowaniu autora[37]. Zagadnienia te nie są bliżej rozpatrywane w tym opracowaniu.

[34] Fitzek F.H.P., Katz M.D: Cooperation in Wireless Networks: Principles and Applications; Springer 2006, ISBN 10-1-4020-4710-X (640 p.)

[35] Struzak R: Improved utilization of the radio spectrum respecting physical laws; (Invited paper), Proceedings of the URSI General Assembly, Chicago, Illinois, USA, 9-16 August 2008

[36] Leese R, Hurley S (eds.): Methods and Algorithms for Radio Channel Assignment; (Struzak R: Introduction to Spectrum Management; p. 7 -21); Oxford University Press 2002, ISBN

[37] Struzak R: Trends in Use of RF Spectrum; 2009, Preprint 2009

4. Zagrożenia

4.1 Cyberatak

Popularyzacja sieci komputerowych i „inteligentnych" systemów telekomunikacyjnych i innych nie tylko otwiera możliwości usprawnienia wielu funkcji i usług, ale stwarza także nowe możliwości nieprzyjaznych działań, w formie „cyberataku". Cyberatak polega na skrytej modyfikacji programów lub danych komputerowych w celu przejęcia kontroli nad nimi. Najbardziej znanym agentem w tej wojnie są wirusy, znane dobrze każdemu użytkownikowi komputera. Ta nazwa, zapożyczona z biologii, oznacza wrogi program, który, bez wiedzy użytkownika, dołącza się do innego programu („żywiciela"), lub go zamienia, w celu reprodukcji samego siebie i innych akcji. Taka wroga akcja może prowadzić do przejściowych zakłóceń, lub do trwałych szkód. Computer Science and Telecommunications Board (Division on Engineering and Physical Sciences), National Research Council ujmuje to następująco:

> "*The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. To date, we have been remarkably lucky. Yes, there has been theft of money and information, although how much has been stolen is impossible to know. Yes, lives have been lost because of computer errors. Yes, computer failures have disrupted communication and financial systems. But, as far as we can tell, there has been no successful systematic attempt to subvert any of our critical computing systems. Unfortunately, there is reason to believe that our luck will soon run out. Thus far we have relied on the absence of malicious people who are both capable and motivated. In the United States, information system vulnerabilities, from the standpoint of both operations and technology, are growing faster than the country's ability (and willingness) to respond* [38].

W wielu państwach od dawna prowadzi się zorganizowane przeciwdziałania – prawdziwą „wojnę w cyberprzestrzeni"[39]. „Cyberprzestrzeń" lub „przestrzeń informacyjna" to nie tylko sieci komputerowe, ale wszelkie media cyfrowe takie jak np. Internet, telefonia komórkowa, usługi elektroniczne itd. Wojna ta obejmuje m.in. badania i analizy wrażliwości infrastruktury i eliminację słabych w niej ogniw. W porównaniu z nimi Polska jest opóźniona. Jak wspominano w rozdziale 2, założenia do pierwszego programu rządowego w tej dziedzinie opublikowano dopiero w 2009 r.

4.2 Atak EM

Cyberatak wymaga od atakującego mistrzowskiego opanowania tajników programowania komputerów, sieci teleinformatycznych, systemów operacyjnych, itd. Takie same efekty można uzyskać w sposób bardziej prymitywny, stosując atak elektromagnetyczny (EM). Cyberatak porównać można do operacji neurochirurgicznej na otwartym mózgu. Wymaga on najwyższych kwalifikacji i precyzyjnych narzędzi. Atak elektromagnetyczny jest w porównaniu z nim prymitywny i brutalny. Niszczy on komórki „mózgu" bez wnikania w tajniki techniki komputerowej i nie tracąc czasu na subtelności łamania haseł i omijanie barier softwarowych.

---

[38] Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, National Academy Press, Washington, D.C., 2002., str. 18

[39] D E Denning: Information Warfare and Security; Addison Wesley, 1999

Infiltracja

Infiltracja stwarza warunki fizyczne dla cyberataku. Amerykański słownik terminów telekomunikacyjnych określa go następująco:

"Electromagnetic intrusion: The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion." [40].

Tradycje takiego wrogiego/ kryminalnego działania sięgają początków telekomunikacji. W 1867 r. zanotowano, że gracz na giełdzie Wall Street, wspólnie z pracownikiem operatora Western Union przechwytywał telegramy wysyłane z Zachodu Stanów Zjednoczonych do gazet publikowanych na Wschodzie i zmieniał ich treść informując czytelników o rzekomych bankructwach i innych finansowych problemach tamtejszych firm.. Kiedy w wyniku takich wiadomości kursy akcji tych firm spadały, skupywał je za bezcen [41]. Dzisiaj, przestępca internetowy najczęściej dokonuje podobnych fałszerstw samodzielnie. Infiltracja teleinformatycznych sieci bezprzewodowych jest znacznie łatwiejsza niż sieci przewodowych, można jej bowiem dokonać na odległość. Rysunek 4 ilustruje takie działanie. Pokazana jest na nim stacja bazowa i terminal (komputer). Rozróżnia się na nim penetrację przez anteny i sensory („Front-Door Coupling") oraz przez przewody zasilania, otwory i nieszczelności ekranów urządzeń („Back-Door Coupling"). Potrzebna do tego aparatura ukryta jest w samochodzie ciężarowym zaparkowanym na ulicy. Mogą tam być generatory fałszywych sygnałów lub urządzenia podsłuchu elektronicznego (ang. „intelligence") w rozmaitych jego odmianach.[42], [43], [44], [45]

[40] Definicja według slownika ATIS Telecom Glossary 2007: Electronic deception: The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronics-dependent weapons. *Note:* Among the types of electronic deception are: (a) manipulative electronic deception--Actions to eliminate revealing or convey misleading, telltale indicators that may be used by hostile forces; (b) simulative electronic deception--Actions to represent friendly notional or actual capabilities to mislead hostile forces; (c) imitative electronic deception--The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. 2.Deliberate activity designed to mislead an enemy in the interpretation or use of information received by his electronic systems. ATIS Telecom Glossary 2007

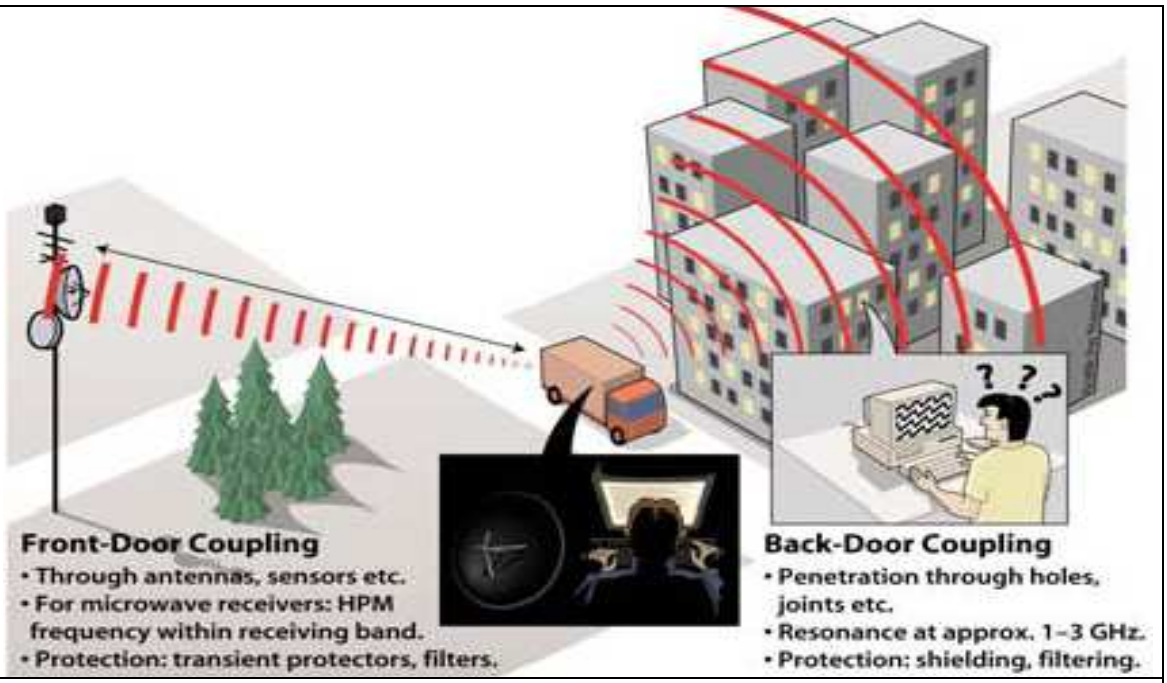
[41] Technical Aspects of Lawful Interception; ITU-T Technology Watch Report 6, May 2008

[42] Definicja według słownika ATIS Telecom Glossary 2007: Signals intelligence (SIGINT): 1. A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02] 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. [ATIS 2007]

[43] Definicja według slownika ATIS Telecom Glossary 2007: Communications intelligence (COMINT): Technical and intelligence information derived from foreign communications by other than the intended recipients. [JP 1-02]

[44] Definicja według slownika ATIS Telecom Glossary 2007: Electronics intelligence (ELINT): Technical and geolocation intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. [JP 1-02]

[45] Definicja według slownika ATIS Telecom Glossary 2007: Foreign instrumentation signals intelligence (FISINT): Intelligence information derived from electromagnetic emissions associated with the testing and operational deployment of foreign aerospace, surface, and subsurface systems. 2. Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients. Foreign instrumentation signals intelligence is a category of signals intelligence. *Note:*Foreign instrumentation signals include but are not limited to signals from telemetry, beaconry, electronic interrogators, tracking/fusing/ arming/firing command systems, and video data links. [JP 1-02]



Rysunek 4: Sprzężenia elektromagnetyczne, które mogą być wykorzystane do penetracji (podsłuchu albo ataku) elektromagnetycznego. (Zaczerpnięty z pracy: Mats Bäckström: The Threat From Intentional Emi Against yhe Civil Technical Infrastructure; *Reprint from ESW2006, 3rd European Survivability Workshop, 16 – 19 May 2006, Toulouse, France.*

Atak nieniszczący

Podobna do infiltracji jest bardziej prymitywna forma ataku elektromagnetycznego, a mianowicie zagłuszanie (zakłócanie, oślepianie). Zagłuszanie polega na użyciu energii elektromagnetycznej w celu zmiany treści przekazywanej informacji tak, aby stała się ona bezużyteczna. Fizyczna infrastruktura zagłuszanego systemu nie ulega przy tym uszkodzeniu – po wyłączeniu zagłuszania działa on nadal, jak poprzednio.[46], [47]. Zagłuszanie jest stosowane przede wszystkim na polu walki[48], ale może być stosowane także w ataku terrorystycznym lub kryminalnym, na przykład do unieruchomienia bezprzewodowego systemu alarmowego w banku. W ubiegłym stuleciu, czasie tzw. „Zimnej Wojny" zagłuszanie audycji „Glos Ameryki", „Wolna Europa" czy „BBC" było stosowane na szeroką skalę w Europie w krajach „budujących socjalizm" z powodów politycznych. Podstawowym jego celem było blokowanie informacji przekazywanych w formie audycji radiowych. Obecnie, przy wymianie informacji bezpośrednio miedzy zautomatyzowanymi systemami skutki zakłócania mogą być groźniejsze. Dzieje się tak,

[46] Definicja według słownika ATIS Telecom Glossary 2007: Jamming: The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices, equipment, or systems. [ATIS Telecom Glossary 2007]

[47] Definicja według słownika ATIS Telecom Glossary 2007: Electromagnetic interference (EMI): Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics/electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. **2.** An engineering term used to designate interference in a piece of electronic equipment caused by another piece of electronic or other equipment. EMI sometimes refers to interference caused by nuclear explosion. ATIS Telecom Glossary 2007

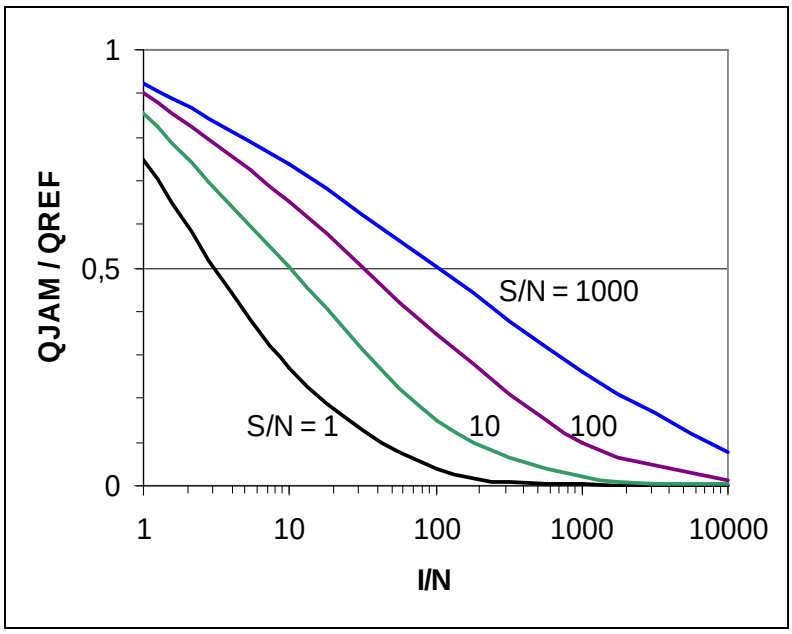
[48] Definicja według słownika ATIS Telecom Glossary 2007: Electronic warfare (EW): Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. ATIS Telecom Glossary 2007

ponieważ – w porównaniu z ludźmi – urządzenia techniczne mają znacznie bardziej ograniczone możliwości rozróżniania sygnału użytecznego od zakłócenia. W warunkach pokojowych celowe lub niezamierzone powodowanie nadmiernych zakłóceń w transmisji telekomunikacyjnej pochodzącej z innego państwa jest nielegalne. Takie działania stanowią pogwałcenie międzynarodowego traktatu „International Telecommunication Convention". Regulacje krajowe również zabraniają powodowania nadmiernych zakłóceń. Konwencje te i regulacje mogą być jednak gwałcone przez organizacje terrorystyczne i kryminalne.

W teleinformatyce, do przenoszenia informacji wykorzystuje się energię odpowiednio zmodulowanych fal elektromagnetycznych. Zakłócanie polega na celowym wprowadzeniu do kanału telekomunikacyjnego sygnału zakłócającego o odpowiednio dużej energii. Transmisję informacji w tych warunkach opisuje klasyczna zależność teoretyczna:

$$Max\_Ilosc\_Informacji = \Delta T \bullet \Delta B \bullet \log_2\left(\frac{S+N+I}{N+I}\right) \qquad (1)$$

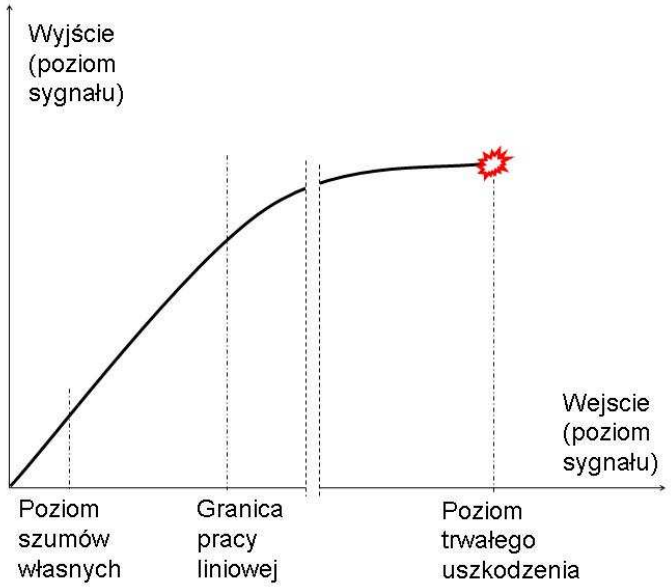
Mówi ona, że maksymalna ilość informacji, jaką może przenieść kanał telekomunikacyjny o szerokości pasma ΔB w czasie ΔT rośnie wraz z mocą sygnału użytecznego (niosącego informację) S oraz maleje wraz z mocą szumów własnych N i sumaryczną mocą sygnałów zakłócających I (wszystkie moce są odniesione do wejścia odbiornika informacji). Przy ograniczonym czasie (ΔT) i paśmie (ΔB) oraz ograniczonej mocy sygnału (S) i mocy szumów (N), wyrażenie w nawiasach dąży do jedności ze wzrostem mocy zakłócenia (I). Funkcja logarytmiczna dąży wówczas do zera, a wraz z nią ilość przekazanej informacji. Rysunek 6 ilustruje ten efekt. Oś pozioma reprezentuje moc zakłóceń (I) odniesioną do mocy szumów (N) a oś pionowa – ilość informacji przekazywaną przez zagłuszany kanał (II_JAM) odniesioną do kanału bez zakłóceń (II_REF), tj. dla I = 0. Dla przykładu, zastosowanie zakłócenia 100 razy silniejszego od sygnału w łączu pracującym normalnie przy stosunku S/N równym 100, zmniejsza ilość przekazywanej informacji prawie do zera.



Rysunek 6. Maksymalna ilość informacji jaką kanał telekomunikacyjny może przenieść maleje ze wzrostem mocy sygnału zakłócającego.

Atak niszczący

Taki atak elektromagnetyczny ma na celu trwałe zniszczenie elementów fizycznej infrastruktury. W szeregu krajów prowadzone są od wielu lat badania nad rozwojem narzędzi służących do takiego ataku jak i sposobów ochrony przed nim[49]. Jak wspomniano zagłuszanie nie powoduje trwałych uszkodzeń sprzętu; ma ono na celu jedynie „zniszczenie" przekazywanej informacji. Jest ono tym bardziej skuteczne im większa jest moc zakłóceń. Przy zwiększaniu tej mocy, osiąga się stan, w którym wrażliwe elementy zagłuszanego systemu ulegają nieodwracalnemu uszkodzeniu. Rysunek 7 pokazuje typową zależność wejście – wyjście odbiornika informacji. Obszar normalnej jego pracy rozciąga się pomiędzy poziomem szumów własnych a poziomem związanym ze szkodliwymi nieliniowymi zjawiskami w elementach systemu. Przy dalszym zwiększaniu energii na wejściu występuje trwale uszkodzenie jednego lub więcej elementów. Skutki takie wywołać może atak elektromagnetyczny.



Rysunek 7. Typowa charakterystyka wejście-wyjście układu elektronicznego. Przy dużej mocy sygnału, następuje nieodwracalne uszkodzenie układu.

Oczywiście z niszczącym atakiem elektromagnetycznym należy się liczyć w przypadku otwartej wojny, jednak coraz częściej spotyka się w literaturze informacje o możliwych atakach elektromagnetycznych w celach terrorystycznych. Jednym z najbardziej znanych sposobów trwałego niszczenia infrastruktury przeciwnika jest eksplozja ładunku nuklearnego nad ziemią [50].

[49] US/UK Non-Lethal Weapons (NLW)/ Urban Operations Executive Seminar, 30 Nov.2000, London; http://www.sunshine-project.org/incapacitants/jnlwdpdf/usukassess.pdf

[50] Definicja według słownika ATIS Telecom Glossary 2007: Electromagnetic pulse (EMP): 1. The electromagnetic radiation from a nuclear explosion caused by Compton-recoil elctrons and photoelectrons from photons scattered in the materials of the nuclear device or in a surrounding medium. The resulting electric and magnetic fields may couple with electrical/electronic systems to produce damaging current and voltage surges. May also be caused by

EMP

Impuls elektromagnetyczny o dużej energii (EMP – Electromagnetic Pulse; NEMP – Nuclear Electromagnetic Pulse) towarzyszący wybuchowi nuklearnemu zaobserwowano już przy pierwszych próbach broni jądrowej w 1945, jednak dopiero w 1954 r. opublikowano jego teorię[51]. Badania w tym obszarze były przez długi czas ograniczone do urządzeń i instalacji wojskowych, które są dziś w wielu krajach uodpornione na impuls elektromagnetyczny. W międzyczasie terroryzm przesunął obszar zagrożeń z obiektów wojskowych na obiekty cywilne w centrach miast a postęp wiedzy doprowadził do tego, że (według prasy codziennej) recepty na budowę generatora potężnych narażeń elektromagnetycznych w „warunkach domowych" krążą w Internecie. Dla zapewnienia bezpieczeństwa ludności, agencje rządowe w wielu krajach podjęły badania skutków ewentualnego terrorystycznego ataku elektromagnetycznego. Ich celem jest ocena rzeczywistej wrażliwości cywilnej infrastruktury państwa na atak elektromagnetyczny, wykrycie słabych punktów i zwiększenie odporności na taki atak w podobny sposób jak wcześniej uodporniona została infrastruktura wojskowa. Nawiązano współpracę międzynarodowa w tej dziedzinie[52]. Międzynarodowa Unia Nauk Radiowych (URSI – Union Radio-Scientifique Internationale) na XXV Zgromadzeniu Plenarnym (Toronto 1999) przyjęła rezolucję zatytułowaną „Criminal Activities using Electromagnetic Tools". Zdefiniowano w niej zamierzone zakłócenia elektromagnetyczne (IEMI – Intentional Electromagnetic Interference) jako

> *„Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing, or damaging these systems for terrorist or criminal purposes".*

Powstał nowy termin: „EM Terrorism"[53]. Wspomniane wyżej badania łączą teoretyczne metody symulacyjne z testami urządzeń i sieci[54]. Dla przykładu, na Rysunku 11 pokazano wyniki symulacji, zaczerpnięte z opublikowanego w 2008 r. raportu [12]. Pokazana tam mapa części Stanów Zjednoczonych ilustruje zasięg uszkodzeń powodowanych impulsem elektromagnetycznym o dużej energii. Kolory oznaczają stopień narażenia. W odróżnieniu od Stanów Zjednoczonych, podobne badania nie były prowadzone w kraju i stopień zagrożenia infrastruktury Polski nie jest znany. Dla celów orientacyjnych na Rysunku 6, na mapę Stanów Zjednoczonych nałożono mapę konturową Polski. Widać, że pojedynczy taki impuls może spowodować poważne szkody na terenie całego kraju (przy założeniu identycznego środowiska elektromagnetycznego w obu krajach).

---

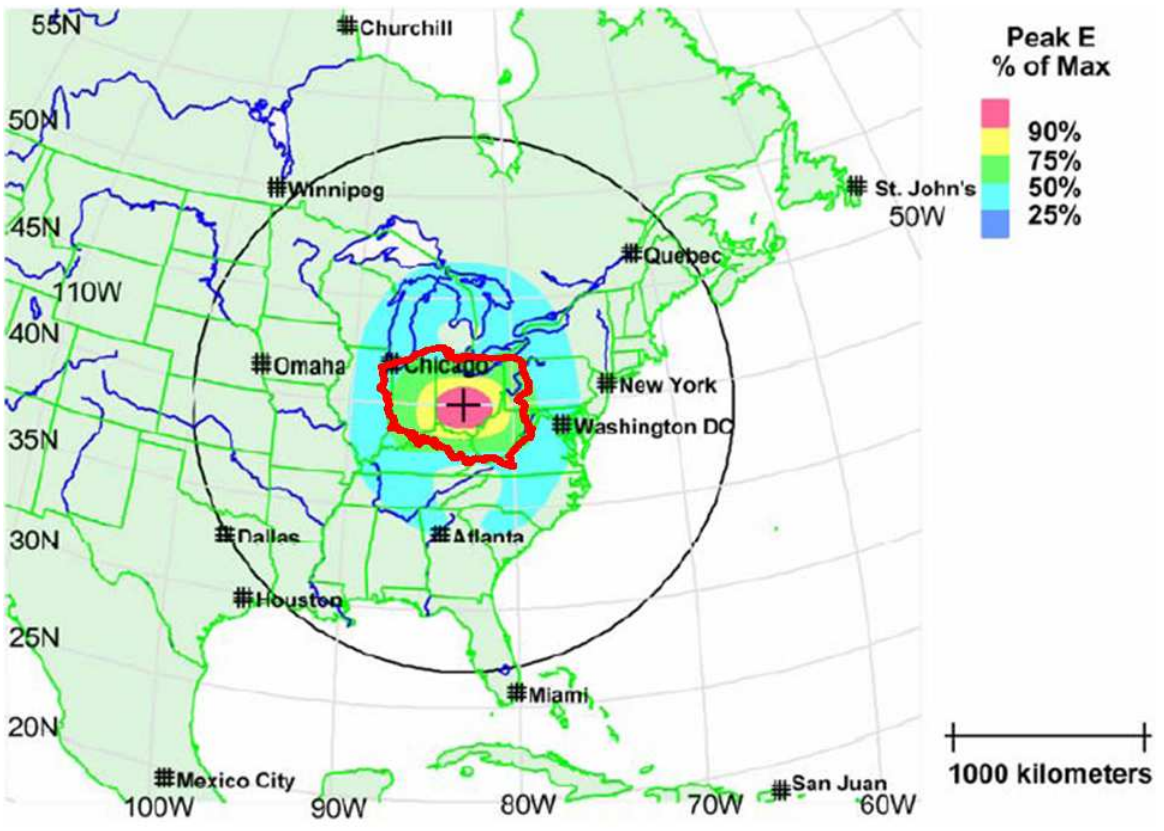
nonnuclear means. [JP1] 2. A broadband, high-intensity, short-duration burst of electromagnetic energy. (188) *Note:* In the case of a nuclear detonation, the electromagnetic pulse consists of a continuous frequency spectrum. Most of the energy is distributed throughout the lower frequencies between 3 Hz and 30 kHz.

[51] Degauque P, Hamelin J: Electromagnetic Compatibility; Oxford University Press 1993 ISBN 0-19-856375-2

[52] Wik M.W., Radasky W.A.: Intentional Electromagnetic Interference (IEMI): Background and Status of the Standardization Work in the International Electrotechnical Commission (IEC); The Radio Science Bulletin, No 299, Dec.2001, pp. 13-18

[53]Definicja według slownika ATIS Telecom Glossary 2007: Electronic warfare (EW): Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. ATIS Telecom Glossary 2007

[54] Ianoz M., Wipf H.: Modeling and simulation methods to assess EM terrorism effects; Electromagnetic Compatibility 1999. Proceedings of 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, 1999

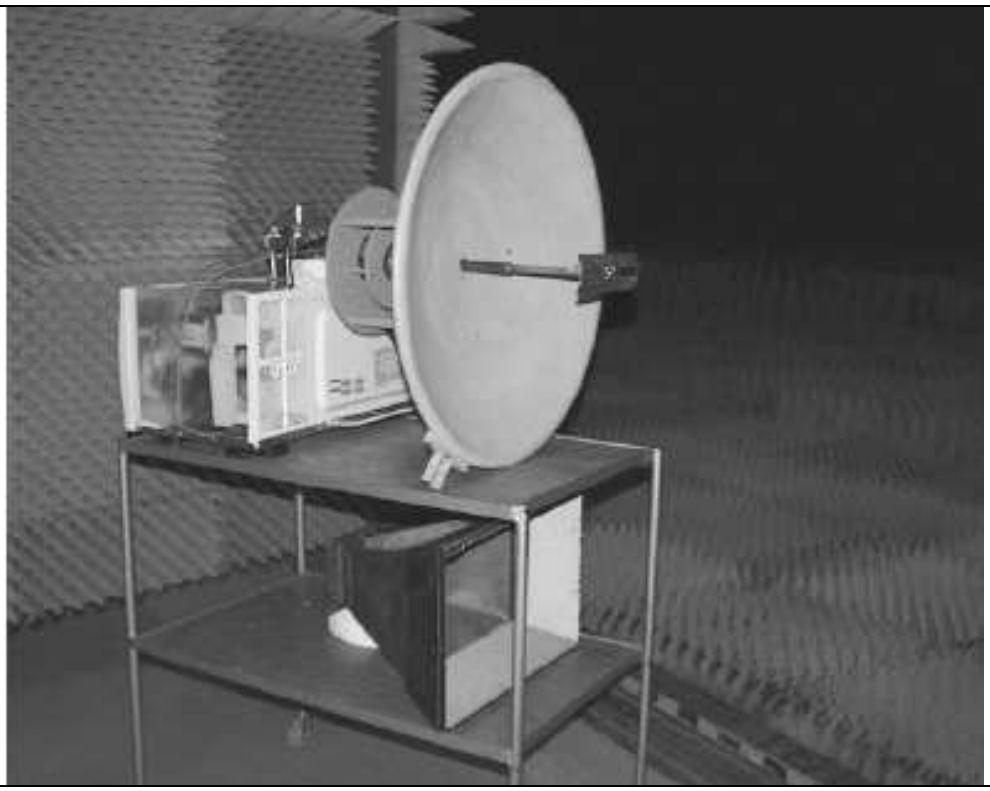


Rysunek 8. Zasięg zniszczeń spowodowanych w Stanach Zjednoczonych AP impulsem elektromagnetycznym o dużej energii. Dla porównania, na mapę Stanów Zjednoczonych nałożono konturową mapę Polski w tej samej skali. Źródło: Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Volume 1: Executive Report 2004;* http://www.empcommission.org/docs/empc_exec_rpt.pdf.

Uszkodzeniu ulęgają elementy i zasoby infrastruktury państwa wrażliwe na narażenia: w pierwszym rzędzie teleinformatyka i energetyka. Wzajemne powiązania powodują, że dysfunkcja jednego elementu może prowadzić uszkodzenia kolejnych, prowadząc do ogólnej katastrofy (efekt domina). Zasoby te obejmują m.in. systemy i sieci użytkowane przez administrację rządową, organy władzy ustawodawczej, władzy sądowniczej, samorządu terytorialnego, a także strategiczne z punktu widzenia bezpieczeństwa państwa podmioty gospodarcze działające w obszarze telekomunikacji, energii, gazu, bankowości, ochrony zdrowia i inne[26].

HPM

HMP to skrót od High Power Microwaves, taniej alternatywy dla impulsu elektromagnetycznego EMP. W literaturze ukazują się informacje o urządzeniach mikrofalowych, które można wykorzystać do trwałego uszkodzenia elementów infrastruktury cywilnej na odległość. Co ważniejsze, takie urządzenia można stosunkowo łatwo, bezpiecznie, i niewielkim kosztem wytworzyć w prymitywnych warunkach, „w garażu” i ta łatwość budzi uzasadniony niepokój. Rysunek 9 pokazuje przykład takiego urządzenia.



Rysunek 9. Elementy domowej kuchni mikrofalowej i anteny do odbioru telewizji satelitarnej, które mogą być wykorzystane do budowy gneneratora HPM (Rysunek zaczerpnięty z pracy: Mats Bäckström: The Threat From Intentional Emi Against yhe Civil Technical Infrastructure; *Reprint from ESW2006, 3rd European Survivability Workshop, 16 – 19 May 2006, Toulouse, France.*

Urządzenie to składa się z elementów domowej kuchenki mikrofalowych i anteny do odbioru telewizji satelitarnej, które są łatwo dostępne na rynku bez żadnych ograniczeń. Wytwarza ono ciągłą fale elektromagnetyczną o mocy wystarczającej do zniszczenia wrażliwych elementów infrastruktury teleinformatycznej na odległość (na szczęście niewielką w porównaniu z zasięgiem nuklearnego impulsu elektromagnetycznego). Przykład takiego wykorzystania pokazano na rysunku 4. Tego typu urządzenia mogą uszkodzić układy scalone w telefonach komórkowych i stacjach bazowych, w odbiornikach systemów nawigacyjnych GPS, w sieciach WiFi, komputerach itd. Tablica 1 przedstawia przykładowe wyniki eksperymentów z komputerami osobistymi poddanymi narażeniom wytworzonym przez tego typu urządzenia.

Tablica 1. Wrażliwość komputerów osobistych na narażenia elektromagnetyczne

Typ PC	Opis narażenia EM			Efekty
	Częstotliwość nośna GHz	Natężenie pola V/m	Modulacja	
Pentium, Pentium II 133; 233 & 300 MHz	1,040 - 2,887	30 - 100	CW, AM	Błąd zapisu, Utrata danych, Reset, Utrata zasilania, Utrata dostępu

Źródło danych: Wik M.W., Radasky W.A.: Intentional Electromagnetic Interference (IEMI): Background and Status of the Standardization Work in the International Electrotechnical Commission (IEC); The Radio Science Bulletin, No 299, Dec.2001, p. 16

Symulacja a rzeczywistość

Rysunek 8 przedstawia wyniki symulacji i można mieć wątpliwości jak dalece odpowiadają one rzeczywistości. Dostępne są (ograniczone) informacje na temat wczesnych eksperymentów z niszczącym atakiem elektromagnetycznym. W 1962, Stany Zjednoczone AP przeprowadziły próbną eksplozję ładunku nuklearnego (1,4 megaton) na wysokości 400 km nad Pacyfikiem. Zanotowano wówczas uszkodzenia systemów alarmowych i oświetlenia ulicznego w Honolulu, w odległości około 1500 km od miejsca wybuchu. Zaobserwowano również przerwanie radiokomunikacji mikrofalowej. Niektóre satelity zostały uszkodzone w czasie testu i w okresie 6 miesięcy po nim, z powodu powstania wokół Ziemi nowych przejściowych obszarów intensywnego promieniowania.[55]. Podobny eksperyment w Związku Radzieckim (na Syberii) pokazał np., że kabel elektroenergetyczny zakopany na głębokości kilkudziesięciu centymetrów pod ziemią uległ zniszczeniu w zasięgu kilkuset kilometrów od miejsca wybuchu. Te eksperymenty dostarczyły danych do opracowania teorii i modeli symulacyjnych. Można spekulować, że ich celem było także zademonstrowanie najwyższym władzom skutków takiego ataku.

Te eksperymenty przeprowadzano nad obszarami niezamieszkałymi lub bardzo słabo zaludnionymi. Brak danych o skutkach takiego ataku na obszary uprzemysłowione i zurbanizowane. O skali szkód możliwych można jedynie wnioskować na podstawie raportów z katastrof naturalnych o znacznie mniejszej skali. Wspomniany raport komisji Kongresu cytuje jako przykład m. in. efekty krótkotrwałego zaniku zasilania energia elektryczną rafinerii w Pembroke (W Brytania). Przerwa w zasilaniu trwała zaledwie 0.4 sekundy (powstała w wyniku naturalnego wyładowania atmosferycznego o znacznie mniejszej energii niż omawiany tu impuls). W efekcie zakłócony został proces technologiczny powodując szereg niekontrolowanych zdarzeń, które doprowadziły do wybuchów i pożarów. Efekt końcowy to straty szacowane na 70 milionów dolarów USA, 4,5 miesiąca przymusowego postoju I spadek o 10% zdolności produkcyjnych całego krajowego przemysłu rafineryjnego.

4.3 Zagrożenia niezamierzone

Niezamierzone zagrożenia elektromagnetyczne mogą mieć takie same skutki jak atak elektromagnetyczny i w tym rozdziale omawiamy je krótko. Należy jednak podkreślić, ze w idealnym świecie nie powinno być zamierzonych zakłóceń i wszystkie oddziaływania elektromagnetyczne spełniają warunki kompatybilności. Przypomnijmy, że kompatybilność elektromagnetyczna odnosi się do stanu, w którym systemy i urządzenia elektromagnetyczne ani nie zakłócają środowiska (tj. działania innych systemów), ani nie odczuwają zakłóceń w sposób istotny. Świat realny jest jednak inny. Nawet przypadkowe oddziaływania elektromagnetyczne mogą powodować skutki równie poważne jak narażenia celowe i cyberatak, omawiane powyżej. Sprawę ilustrują następujące przykłady.

W czasie pracy w Międzynarodowym Doradczym Komitecie Radiokomunikacyjnym (CCIR- ITU) w Genewie, autorowi powierzono rozwiązanie następującego problemu. W jednym z krajów Ameryki Środkowej występowały powtarzające się sporadycznie uszkodzenia jedynej linii radiowej, koncentrującej wszystkie połączenia między wschodnią i zachodnią częścią kraju.

[55] Radasky WA. : 2007 Update on Intentional Electromagnetic Interference (IEMI) and High-altitude Electromagnetic Pulse (HEMP). ITEM- Interference Technology an online Guide to Electromagnetic Compatibility http://www.interferencetechnology.com/articles/articles/article/2007-update-on-intentional-electromagnetic-interference-iemi-and-high-altitude-electromagnetic-pul.html

Linia ta prowadziłam przez słabo zaludnione i trudno dostępne rejony górskie i naprawa uszkodzeń wymagała dużych nakładów sił, środków i czasu, co prowadziło do długotrwałych przerw łączności. Przeprowadzona analiza wstępna wykluczyła źródła zakłóceń podlegające jurysdykcji tego kraju. Prawdopodobną przyczyną były niezamierzone zakłócenia elektromagnetyczne spowodowane stacjami radaru dalekiego zasięgu pracującymi na okrętach obcego państwa, które przepływały obok (prawdopodobną, ponieważ nie udało się na drodze dyplomatycznej formalnie zidentyfikować źródła zakłóceń: po rozpoczęciu formalnej procedury mającej na celu wykrycie sprawcy, zakłócenia zanikły).

Inny przykład został opisany we wspomnianym Raporcie Grahama. W 1999 r. dwa duże przedsiębiorstwa, San Diego County Water Authority i San Diego Gas and Electric, zaopatrujące ludność w wodę i gaz zaobserwowały poważne zakłócenia w pracy zautomatyzowanych systemów rozdzielczych: zdalne sterowanie zaworów przestało funkcjonować. (San Diego County rozciąga się ponad 100 km w kierunku północ-południe i 200 km ze wschodu na zachód i liczy 3 milionów mieszkańców). Przedsiębiorstwa te były zmuszone wyłączyć automatyczne systemy kontroli i sterowania (SCADA) i wysłać personel w teren, aby ograniczyć straty i zapobiec ewentualnej katastrofie (przez ręczne ustawienie zaworów rozmieszczone w dużej odległości od siebie). Potencjalny efekt niesprawności sieci rozprowadzania wody to niekontrolowany wypływ tysięcy galonów[56] wody na minutę, przerwy usług, poważna powódź i znaczne szkody wyrządzone przedsiębiorstwom, organizacjom i osobom prywatnym. Przyczyna tych wydarzeń były niezamierzone zakłócenia elektromagnetyczne w systemach SCADA, spowodowane przypadkowym „naświetleniem" wiązką fal promieniowaną przez radar okrętu, z odległości 25 mil morskich[57], [12]. W tym samym raporcie opisana jest m.in. katastrofa, jaka wydarzyła się w 1980 r. w Holandii, w okolicy portu Den Helder. Miała tam miejsce awaria gazociągu o średnicy 36", która zakończyła się poważnym wybuchem gazu. Przyczyną były tu przypadkowe niezamierzone zakłócenia elektromagnetyczne systemu SCADA spowodowane radarem Inne pouczające przykłady można znaleźć np. w poradniku opublikowanym w 2008 r. w Anglii przez The Institution of Engineering and Technology[58]

Istnieją w każdym kraju systemy, których bezpieczeństwo jest szczególnie ważne. Jednym z nich jest system nawigacji lotniczej. Mimo wielu środków ostrożności nie można zapewnić jego działania bez zakłóceń. Np. w 2003 r. ukazała się informacja o niezamierzonych zakłóceniach elektromagnetycznych powodowanych w pobliżu lotnisk w Wielkiej Brytanii przez produkowane serynie urządzenie domowe[59].

Rysunek 10 pokazuje wyniki systematycznej rejestracji i analizy takich przypadkowych zakłóceń zaobserwowanych w korytarzach linii lotniczych nad Japonią w latach 1998 - 2006.[60] Przedstawia on miejsca występowania zakłóceń, wysokości i fazy lotu oraz najczęściej zakłócane urządzenia pokładowe. Systematyczne gromadzenie i analiza tego typu danych jest istotna dla zapobiegania katastrofom lotniczym, a także dla wyjaśniania ich przyczyn. Obecnie przyczyny te

[56] 1 galon = 3,78541178 litra

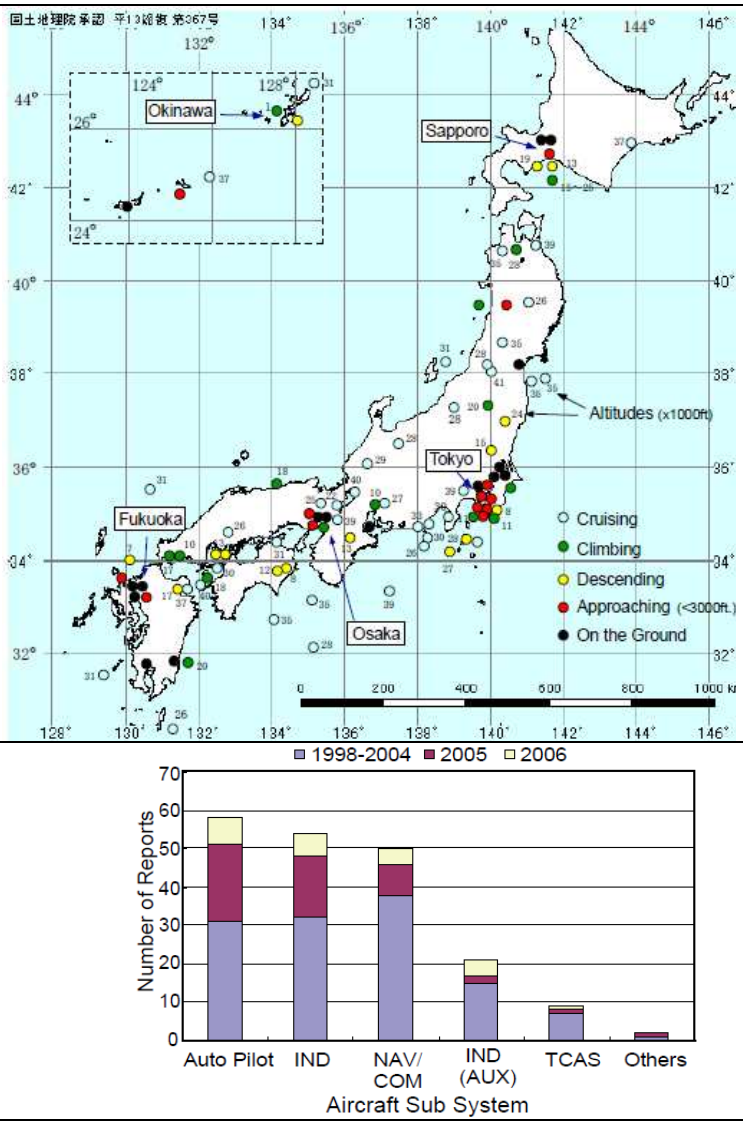
[57] 1 mila morska (NM) = 1 852 m

[58] IET Electromagnetic Compatibility for Functional Safety; IET, 2008 (www.theiet.org)

[59] http://www.ofcom.org.uk/static/archive/ra/topics/research/RAwebPages/Radiocomms/pages/interexpl/houseapp.htm#babyalarm (2003)

[60] Yamamoto, K. Yamada, K. Yonemoto, N.; PED Interference Reporting System in Japan ; Electromagnetic Compatibility and Electromagnetic Ecology, 2007 7th International Symposium on; Saint-Petersburg, 26-29 June 2007, pp. 220-223; ISBN: 978-1-4244-1270-9

są badane indywidualnie, od przypadku do przypadku. Bierze się pod uwagę szereg czynników, np. stan pogody, widoczność, itp., ale rzadko zwraca się uwagę na postronne sygnały i ewentualne zakłócenia elektromagnetyczne. Najczęściej uznaje się, że przyczyną katastrofy jest błąd pilota, co satysfakcjonuje opinię publiczną, organy kontrolne, producenta i właściciela statku powietrznego, ale czy na pewno zawsze odpowiada ono rzeczywistości?



Rys. 10. Niezamierzone zakłócenia w lotniczych systemach radioelektrycznych zarejestrowane w Japonii w latach 1998-2006: (a) Lokalizacje, fazy i wysokości lotu, przy których zarejestrowano zakłócenia. (Mapa wskazuje nie tylko stopień zagrożenia elektromagnetycznego, ale także rejony gdzie należy szukać źródła zagrożenia); (b) Podsystemy, których działanie było zakłócone (Pozwalają one ocenić stopień zagrożenia oraz zidentyfikować słabe punkty wyposażenia samolotów, które wymagają poprawy). Źródło: Yamamoto, K. Yamada, K. Yonemoto, N.: PED Interference Reporting System in Japan; Electromagnetic Compatibility and Electromagnetic Ecology, 2007 7th International Symposium on; Saint-Petersburg, 26-29 June 2007, pp. 220-223; ISBN: 978-1-4244-1270-9

Podobnie jak w lotnictwie, zakłócenia elektromagnetyczne występują w transporcie morskim i lądowym (drogowym i kolejowym) a także w innych systemach w każdym kraju, również w Polsce. Systematyczna obserwacja takich zakłóceń jest niezbędna dla racjonalnego planowania istotnych przedsięwzięć inwestycyjnych lub organizacyjnych mających na celu powiększenie bezpieczeństwa podróżnych. Zwykle jednak takie obserwacje nie są prowadzone, rejestrowane, gromadzone i analizowane, mimo, iż maja ona zasadnicze znaczenie. W Polsce

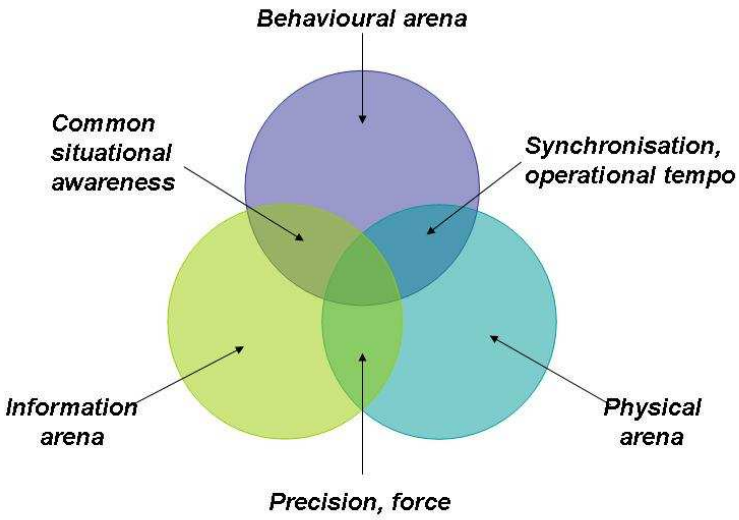
wspomniane wcześniej założenia do projektu rządowego nie przewidują żadnych przedsięwzięć w tym zakresie.

Te przykłady pokazują, że niezamierzone zakłócenia elektromagnetyczne mogą mieć taki sam efekt jak atak elektromagnetyczny lub cyberatak, jeżeli występują w elementach krytycznych systemu (np. w komputerach lub bazach danych).

5. Ochrona cyberprzestrzeni

Ochrona przestrzeni informacyjnej[61] to problem holistyczny, w którym przeplatają się elementy techniczne, organizacyjne, ekonomiczne i socjalne, jak również działania prewencyjne, przygotowawcze, ochronne i naprawcze (prevention, preparation, protection, and recovery), jak pokazano na Rysunku 14 i Rysunku 15.

Rysunek 11. Ochrona przed atakiem EM. Kolejne fazy: prewencja, przygotowanie, reakcja, naprawa szkód



Rysunek 12. Ochrona przed atakiem. Trzy areny ochrony: informacyjna, fizyczna i behawioralna (Zaadaptowane z : Wik M W: What is Network-Based Defence (NBD) and the Impact on the Future Defence? *Royal Swedish Academy of War Sciences, October 2003*)

[61] Definicja według slownika ATIS Telecom Glossary 2007: Information security, cyber security: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. ATIS Telecom Glossary 2007

System ochrony jest tak szybki jak jego najwolniejsze ogniwo i tak silny jak jego najsłabsze ogniwo. Należy podkreślić, że ochrona infrastruktury przed atakiem niszczącym jest kosztowna. Wymaga ona m.in. na zwiększenia odporności (”EMP hardening”) krytycznych urządzeń, instalacji, budynków itd. na narażenia elektromagnetyczne, lub ich wymiany na bardziej odporne i z reguły znacznie droższe. Z jednej strony stwarza to popyt na nowe urządzenia, instalacje i budynki, prace adaptacyjne i na związane z tym badania. Z drugiej strony pociąga to za sobą znaczne wydatki. Założenia do Programu Rządowego (cytowane w punkcie 2.5) ograniczają się do ochrony przed atakiem w cyberprzestrzeni. W poprzednich rozdziałach wykazaliśmy, że atak elektromagnetyczny na fizyczna infrastrukturę (EMP i HPM), oraz niezamierzone zakłócenia elektromagnetyczne, mogą powodować równie poważne, albo nawet większe, szkody. Wydaje się wiec, że program rządowy powinien być rozszerzony na ochronę przed takimi oddziaływaniami elektromagnetycznymi w przestrzeni fizycznej.

5.1 Zalecenia Komisji Grahama

Doraźne

Najważniejsze pilne zalecenie Komisji dotyczy zwiększenia i utrzymania niezawodności systemów i sieci teleinformatycznych w służbach awaryjnych takich jak pogotowie medyczne straż pożarna, służby porządkowe itd. Czytamy w jej raporcie:

> *“Command, control, communications, and information (C3I) systems for emergency responders are critical for coordinating their efforts and increasing the promptness and effectiveness of response. Unfortunately, such systems are extremely vulnerable to attack; currently many of them do not even use state-of the- art mechanisms for security and reliability. Since emergency-response organizations often do not have the expertise to review and revamp the telecommunications and computing technologies used for emergency response, it is necessary to provide them with authoritative knowledge and support. In addition, designated emergency-response agencies should use existing technology to achieve short-term improvements in the telecommunications and computing infrastructure for first responders. Unlike some other sectors of national importance, information technology is a sector in which the federal government has little leverage. Thus, constructively engaging the private sector by emphasizing market solutions seems a desirable and practical way for the government to stimulate advances that can strengthen the nation’s information technology infrastructure. The challenge for federal policy makers is to change the market dynamics by encouraging the private sector to pay more attention to security-related issues and by facilitating the adoption of effective security (e.g., through federally supported or incentivized research that makes better technologies available and reduces the costs of implementing security-related functionality).”*

Długofalowe

Komisja stwierdziła, ze obecne (2008) modele matematyczne niezbędne do oszacowania szkód w razie ataku elektromagnetycznego mają istotne ograniczenia i nie pozwalają na adekwatną ocenę skutków jednoczesnego uszkodzenia wielu powiązanych ze sobą dynamicznie elementów infrastruktury:

> *“The Commission recommends that research be conducted to better understand infrastructure system interdependencies and interactions, along with the effects of various EMP attack scenarios. In particular, the Commission recommends that such research*

include a strong component of interdependency modeling. Funding could be directed through a number of avenues, including through the National Science Foundation and the Department of Homeland Security. The Commission recognizes current interest in protecting SCADA systems from electronic cyber assault. The Commission recommends that such activities be expanded to address the vulnerability of SCADA systems to other forms of electronic assault, such as EMP."

Dalej, Komisja zaleca Rządowi prowadzenie multidyscyplinarnych badań naukowych w celu pełnego zrozumienia występujących tu problemów

"The federal government's efforts should focus on multidisciplinary problem oriented research that is applicable to both civilian and military users, yet is driven by a deep understanding and assessment of vulnerabilities to terrorism. To achieve long-term advances, the research must extend beyond improving existing systems and investigate new approaches to secure and reliable operation that do not directly evolve from the information technology of today."

Wspomniany wcześniej Raport Komisji Grahama zaleca w tym zakresie (miedzy innymi) następujące kroki:

- Systematycznie zbierać, analizować i rozpowszechniać istotne informacje na temat zagrożeń elektromagnetycznych i cyberataków
- Przeprowadzać testy w celu zidentyfikowania słabych ogniw w istniejących instalacjach i systemach
- Zapewnić sprawne funkcjonowanie infrastruktur łącznie sektora prywatnego, rządowego i samorządowego, zwłaszcza w sytuacjach krytycznych (krok wymagający ścisłej współpracy)
- Uwzględniać wymagania dot. zabezpieczenia przed narażeniami elektromagnetycznymi i cyberatakami w specyfikacji i wymaganiach stawianych każdej nowej sieci/ systemowi
- Monitorować na bieżąco technologie ataku elektromagnetycznego i cyberataku oraz przeciwdziałań zabezpieczających, rozumieć je i oceniać stopień zagrożenia; monitorować wczesne symptomy zagrożeń
- Prowadzić badania w celu udoskonalenia środków/ systemów obrony
- Promować popularyzacje problemów ochrony przed cyberatakiem i atakiem elektromagnetycznym
- Ustanowić i wdrożyć do praktyki standardy techniczne i operacyjne w zakresie ochrony przed cyberatakiem i atakiem elektromagnetycznym
- Ustanowić i wdrożyć kryteria oceny stopnia zagrożenia i stopnia odporności na atak [12].

5.2 Trudności

- Organizacje zaatakowane (lub poszkodowane w wyniku niezamierzonych oddziaływań), nie są zainteresowane dzieleniem się swoimi doświadczeniami. Przeciwnie, wolą ukrywać fakt ataku i jego efekty zasłaniając się prawem „trade secret", ponieważ upublicznienie niekorzystnych informacji może podkopać zaufanie publiczne, i zaszkodzić w karierze dyrektorów. Pracownicy i eksperci zewnętrzni są najczęściej związani tajemnicą służbową. Na przykład, za każdym napadem na bank z bronią w ręku ukazują się szczegółowe opisy tego wydarzenia

w prasie, radiu i telewizji, ale bardzo rzadko publikowane są informacje o kradzieży dokonanej na drodze elektronicznej. Stan taki utrudnia wymianę doświadczeń, systematyczne gromadzenie faktów i ich analizę oraz identyfikację słabych punktów i ich eliminowanie.

- System zabezpieczony przed atakiem oferuje użytkownikowi takie same funkcje jak system niezabezpieczony. Z tego powodu sektor prywatny poświęca minimum środków na bezpieczeństwo, tyle tylko ile można uzasadnić argumentami biznesowymi. Może to być znacznie mniej niż wynika to z potrzeb społecznych. To samo dotyczy agencji rządowych i samorządowych, które pracują w warunkach ograniczonego budżetu.
- Jak wspomniano wcześniej, kompleksowa ochrona obejmuje prewencję, przygotowania na wypadek ataku, uodpornienie i protekcję w czasie ataku oraz naprawę szkód po ataku. Działania te mogą być bardzo kosztowne i mimo to nie gwarantują pełnej, 100% ochrony. Przy ograniczonym budżecie powstaje pytanie, co jest bardziej korzystne: czy wydać więcej na działania prewencyjne czy na kuracyjne? Intuicja podpowiada, że istnieje optymalna kombinacja obu tych działań, która zapewnia określony stopień ochrony przy minimum kosztów.
- Sprawy bezpieczeństwa są chronicznie niedoinwestowane, ponieważ korzyści z bezpieczeństwa odnosi cale społeczeństwo a wydatki ponoszą indywidualne organizacje/ firmy[12].

> *„For economic reasons, systems are generally built out of commercial off-the-shelf components. These are not very secure because there isn't much market demand: Customers buy features and performance rather than security. The failure of the U.S. government's Orange Book program even within the federal marketplace is a striking example. The government demanded secure systems, industry produced them, and then government agencies refused to buy them because they were slower and less functional than other nonsecure systems available on the open market ".[Cybersecurity Today and Tomorrow: Pay Now or Pay Later, p. 7]*

5.3 Ochrona przed narażeniami niezamierzonymi

Systematyczne prace nad ochroną cywilnej przestrzeni informatycznej przed atakiem elektromagnetycznym nie były dotychczas w Polsce prowadzone. Były natomiast prowadzone z sukcesem prace nad ochroną sieci telekomunikacyjnych przed niezamierzonymi oddziaływaniami elektromagnetycznymi. Prace te rozpoczęto w Polsce w 1956 roku w Instytucie Łączności we Wrocławiu[62]. Doprowadziły do ustanowienia w Polsce systemu ochrony, opartego na przepisach prawnych i normach państwowych i organizacji zapewniającej ich przestrzeganie. Normy Polskie określają

- wymagania techniczne stawiane urządzeniom w zakresie dopuszczalnych emisji energii elektromagnetycznej,
- wymagania stawiane urządzeniom w zakresie odporności na niezamierzone narażenia elektromagnetyczne

[62] Struzak R et al.: Pół wieku innowacji – Prace Oddziału Instytutu Łaczności we Wrocławiu;. Telekomunikacja i Techniki Informacyjne nr 3-4, 2009, str. 68-82

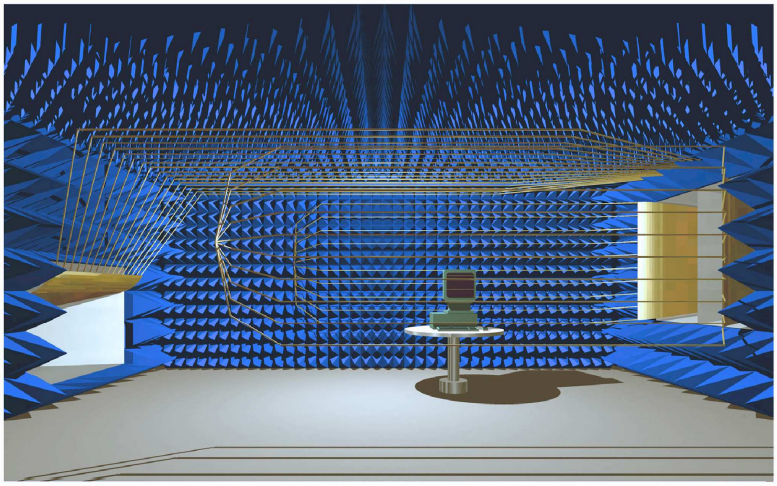
- wymagania stawiane specjalistycznej aparaturze kontrolno-pomiarowej
- standardowe warunki i metody kontroli urządzeń na zgodność z ww. wymaganiami dotyczącymi emisyjności i odporności
- standardowe warunki i metody badania skuteczności podzespołów stosowanych do zmniejszania emisyjności i wrażliwości na niezamierzone oddziaływania elektromagnetyczne.

Badania odporności na narażenia elektromagnetyczne prowadzone w Instytucie Łączności i innych laboratoriach w kraju są ograniczone do obiektów o stosunkowo niewielkich rozmiarach i nie obejmują badań niszczących, które wymagają stosowania dużych energii. W rezultacie, Polskie Normy (po kolejnych aktualizacjach) są zgodne z Dyrektywami Europejskimi i standardami międzynarodowymi nie uwzględniają możliwości ataku elektromagnetycznego. Podane w nich poziomy dopuszczalne narażeń elektromagnetycznych i wrażliwości na nie dotyczą standardowych (tj. przeciętnych) warunków eksploatacji. Ustalone one zostały na podstawie przeprowadzonych badań, obserwacji i danych zebranych w przeszłości, w konsultacji ze wszystkimi zainteresowanymi, biorąc pod zarówno aspekty kompatybilności elektromagnetycznej i stan środowiska elektromagnetycznego jak i aspekty ekonomiczne. Należy w tym miejscu dodać, że normy i przepisy legislacyjne reagują z opóźnieniem na nowe technologie i nowe zagrożenia. Tymczasem środowisko elektromagnetyczne zmienia się ciągle, w rezultacie wzrostu liczby urządzeń i systemów generujących energię elektromagnetyczną i wrażliwych na nią.

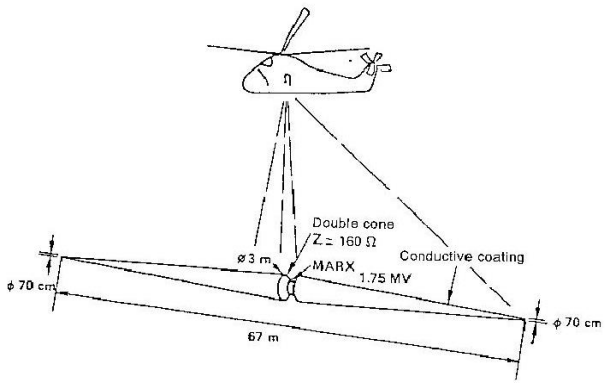
Oddział Instytutu Łączności we Wrocławiu był pierwszą i przez długi czas jedyną w Polsce placówką naukowo-badawczą, wyspecjalizowaną w problemach niezamierzonych narażeń elektromagnetycznych i odporności na nie. Jego prace uzupełniały akty prawne i organizacyjne takie jak Ustawa o Łączności, czy utworzenie kontrolnego organu rządowego z placówkami terenowymi i własnymi laboratoriami, którego funkcje pełni dzisiaj UKE – Urząd Komunikacji Elektronicznej. Stanowiły one również podstawy techniczne aktów prawnych i przepisów regulacyjnych oraz uzasadnienie merytoryczne stanowiska Polski w negocjacjach międzynarodowych dotyczących jednolitych przepisów zakresie kompatybilności elektromagnetycznej. W wyniku tych prac obok laboratoriów Zakładu Kompatybilności Elektromagnetycznej Instytutu Łączności we Wrocławiu powstał szereg laboratoriów kompatybilności elektromagnetycznej w Polsce. Oddział Instytutu Łączności we Wrocławiu, wspólnie z Politechniką Wrocławska, stały się ośrodkiem wiodącym i znanym za granicą. Niewątpliwie przyczyniło się do tego Międzynarodowe Wrocławskie Sympozjum Kompatybilności Elektromagnetycznej, najstarsze regularne sympozjum EMC w Europie, organizowane co dwa lata, począwszy od 1972 r.

Jak wspomniano wcześniej, wszystkie te prace te dotyczyły narażeń niezamierzonych, tj. o stosunkowo małej energii. W latach osiemdziesiątych planowano rozszerzenie prac prowadzonych w Instytucie Łączności we Wrocławiu na aspekty ochrony instalacji cywilnych i ich odporności na atak elektromagnetyczny. W tym celu w Zakładzie Kompatybilności Elektromagnetycznej zbudowano m.in. unikalną komorę narażeń elektromagnetycznych. Jest ona przedstawiona na Rysunku 14, a jej unikalność polega na możliwości kontroli polaryzacji wytwarzanych w niej narażeń (pola elektromagnetycznego TEM). Do tego służą widoczne na rysunku układy przewodów ułożonych w dwu płaszczyznach: poziomej (pod stropem komory) i pionowej (w głębi rysunku). W 1997 komora ta uległa uszkodzeniu w wyniku Powodzi Tysiąclecia. Brak zamówień na badania tego typu, spowodował, że uszkodzenia te nie zostały w pełni naprawione i jej unikalne właściwości dotychczas nie są w pełni wykorzystywane.

W latach siedemdziesiątych w Zakładzie Kompatybilności Elektromagnetycznej Instytutu Łączności zostało utworzone wielozadaniowe laboratorium kontrolno-pomiarowe na śmigłowcu.[63] Było ono wykorzystywane do różnych celów. Planowano wykorzystać go do zbudowania mobilnego generatora silnych narażeń elektromagnetycznych (podobnego do istniejącego od szeregu lat w Stanach Zjednoczonych AP[51]). Naśladowałby on atak elektromagnetyczny na różne obiekty w miejscu ich użytkowania w celu określenia ich odporności w normalnych warunkach pracy. Rysunek 13 przedstawia schematyczny rysunek oryginału amerykańskiego oraz fotografię śmigłowca Instytutu Łączności. Konstrukcja przymocowana do kadłuba to antena pomiarowa. Po prywatyzacji sektora telekomunikacyjnego w Polsce, Latające Laboratorium Instytutu Łączności zostało zlikwidowane z uwagi na brak zainteresowania (źródeł finansowania) i wysokie koszty amortyzacji. Plany podjęcia badan nad zwiększeniem odporności cywilnych instalacji teleinformatycznych na atak elektromagnetyczny zostały zawieszone. Nie zostały one podjęte dotychczas z uwagi na brak zainteresowania tak ze strony sektora prywatnego, jak i ze strony jednostek rządowych i samorządowych.



Rysunek 13. Komora narażeniowa Zakładu kompatybilności Elektromagnetycznej Instytutu Łączności we Wrocławiu umożliwiająca kontrole polaryzacji fali narażeniowej.

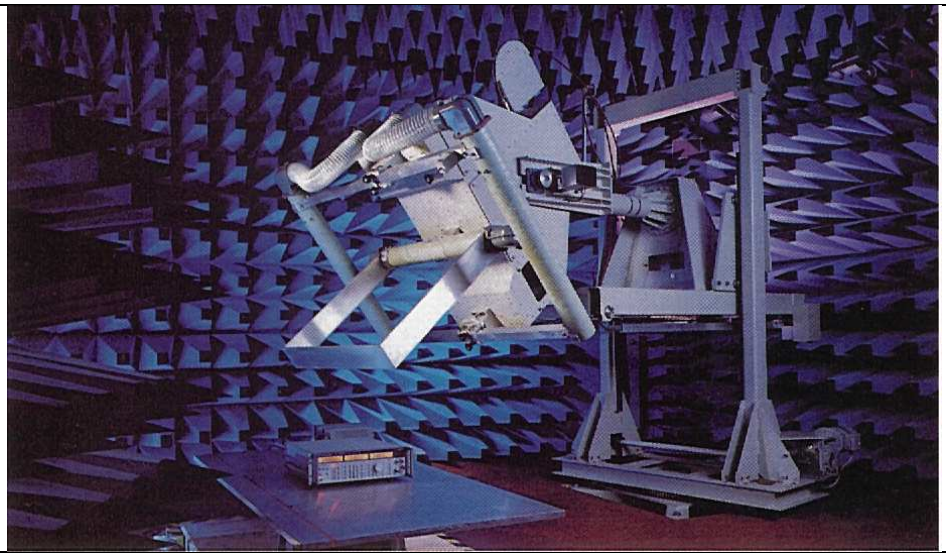


Rysunek 14. Mobilny generator impulsu elektromagnetycznego o dużej energii. Z prawej strony szkic generatora amerykańskiego (wg: Degauque P, Hamelin J:Electromagnetic Compatibility, ISBN 0-19-856375-2, str. 571). Z prawej strony śmigłowiec Instytutu Łączności przewidywany do przenoszenia takiego generatora. Element z lewej strony kadłuba to generator narażeń o niewielkiej energii (źródło: Strużak R, Żernicki E: Latające Laboratorium Instytutu łączności; *Przegląd Telekomunikacyjny*, 1981, Nr 9/10, p.258-262.

[63] Struzak R, Zernicki E: Latające Laboratorium Instytutu łączności; *Przeglad Telekomunikacyjny*, 1981, Nr. 9/10, p.258-282

5.4 Badania odporności na atak EM

W krajach rozwiniętych badania wrażliwości na narażenia elektromagnetyczne prowadzi się od lat. W Polsce nie ma obecnie laboratorium, które byłby w stanie ocenić na podstawie pomiarów stopień odporności istniejących urządzeń, instalacji i sieci na atak elektromagnetyczny o dużej energii. Brak również teoretycznych (obliczeniowych) modeli symulacyjnych. Istniejące normy krajowe nie uwzględniają badań związanych z atakiem elektromagnetycznym, zwłaszcza niszczących. Wyposażenie i utrzymanie laboratoriów narażeń elektromagnetycznych o dużej energii jest kosztowne z uwagi na unikalny charakter aparatury pomiarowej, produkowanej jednostkowo. Rysunki 14 do 21 przedstawiają kilka wybranych stanowisk pomiarowych do badania odporności na narażenia elektromagnetyczne za granicą.



Rysunek 15. Widok stanowiska pomiarowego w bezechowej kabinie ekranowanej do badania odporności małych urządzeń elektronicznych na narażenia elektromagnetyczne o dużej energii (źródło: materiały firmowe, Rohde & Schwarz)

Figure 1-4. EMP Simulator with Test Structures and Internal Electronics

Rysunek 16. Widok stanowiska pomiarowego w terenie do badania odporności małych urządzeń elektronicznych na narażenia elektromagnetyczne o dużej energii (źródło: Raport Komisji Grahama)

Figure 3-7. Testing at NOTES Facility

Figure 3-8 shows examples of some of the smaller items tested at the NOTES facility.

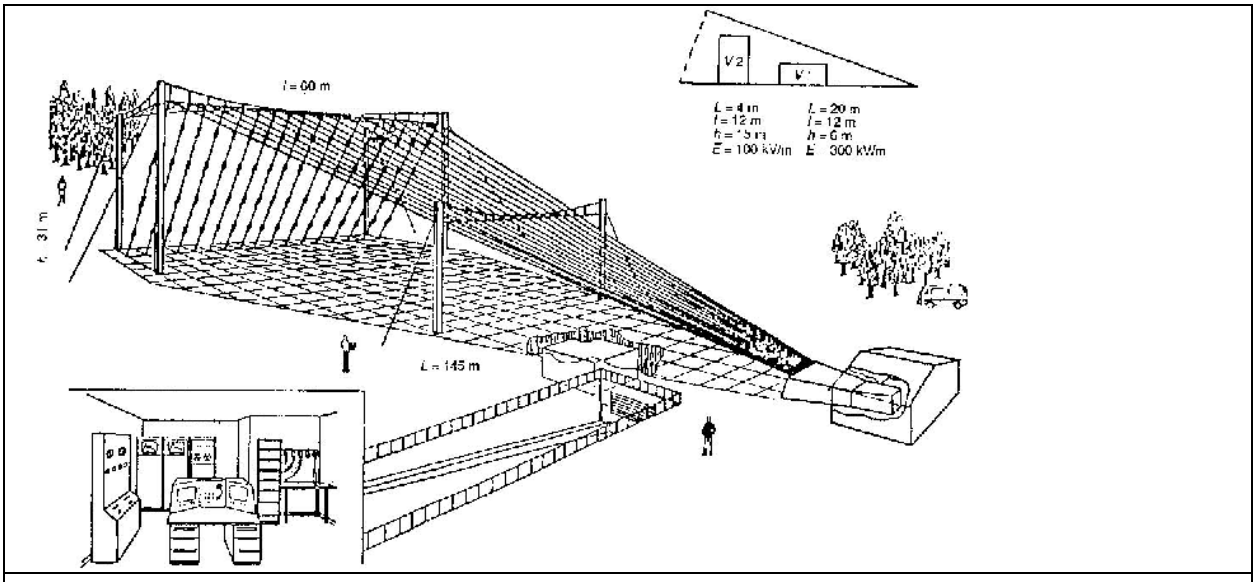
Rysunek 17. Widok stanowiska pomiarowego w terenie do badania odporności małych urządzeń elektronicznych na narażenia elektromagnetyczne o dużej energii – szczegóły (źródło: Raport Komisji Grahama)

Figure 3-6. Cellular Network Testing at INL

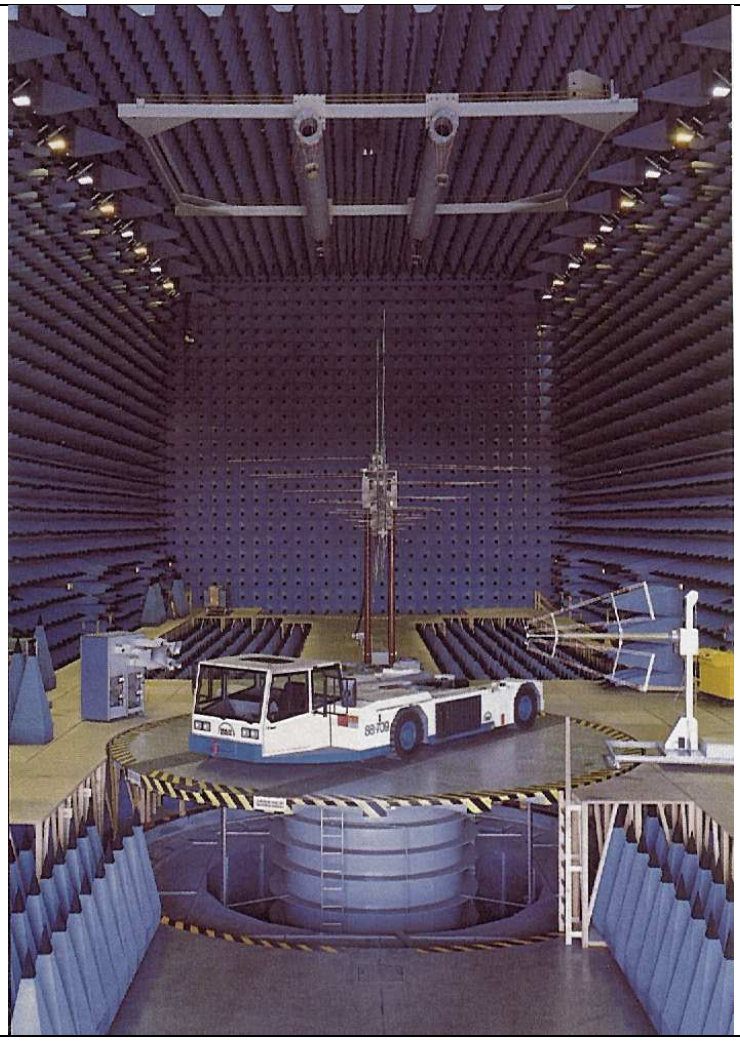
Rysunek 18. Widok stanowiska pomiarowego w terenie do badania odporności kontenerowych stacji bazowych telefonii komórkowej na narażenia elektromagnetyczne o dużej energii (źródło: Raport Komisji Grahama)

Rysunek 19. Widok stanowiska pomiarowego do badania odporności aparatury elektronicznej zainstalowanej w samolocie na narażenia elektromagnetyczne o dużej energii (Szwecja)

Rysunek 20. Widok stanowiska pomiarowego do badania odporności aparatury elektronicznej zainstalowanej w samolocie na narażenia elektromagnetyczne o dużej energii. Przedmiot widoczny nad samolotem wraz z siecią drutów, to generator narażeń. Źródła energii, aparatura pomiarowa i kontrolna nie są pokazane.
(Źródło: http://en.wikipedia.org/wiki/Electromagnetic_pulse (4.10.2009))



Rysunek 21. Schematyczny rysunek instalacji (długość 145 m, szerokość 60 m, wysokość 31 m) do badania odporności na narażenia elektromagnetyczne dużych obiektów (Francja) źródło Degauque & Hamelin



Rysunek 22. Widok stanowiska pomiarowego w bezechowej hali ekranowanej do badania odporności dużych urządzeń na narażenia elektromagnetyczne o dużej energii (źródło: materiały firmowe, Rohde & Schwarz)

6. Zakończenie

W pracy omówiono wybrane problemy oddziaływań elektromagnetycznych, przyjaznych i wrogich, celowych i niezamierzonych, w aspekcie programów rozwoju Społeczeństwa Informacyjnego i ochrony cyberprzestrzeni. Założenia programu rządowego dotyczące ochrony koncentrują się na ataku w przestrzeni wirtualnej (cyberataku). Problemy ochrony infrastruktury w przestrzeni fizycznej (urządzeń, instalacji, budynków) przed narażeniami elektromagnetycznymi są w tych założeniach pominięty milczeniem. Ta tematyka nie jest podjęta w Polsce, na co wskazuje pobieżny choćby przegląd materiałów zgłoszonych ostatnio na Krajowej Konferencji Radiokomunikacji, Radiofonii i Telewizji. W opracowaniu wykazano, że atak elektromagnetyczny stanowi rzeczywiste zagrożenie takie jak cyberatak, albo większe. W pewnych sytuacjach podobne szkody mogą powodować także niezamierzone oddziaływania elektromagnetyczne. Wspomniano o wcześniejszych pracach Instytutu Łączności we Wrocławiu, które łączą się merytorycznie z omawianym tematem.

Istnieje potrzeba strategicznych decyzji w sprawie ochrony przestrzeni informatycznej kraju przed atakiem elektromagnetycznym i przed niezamierzonymi oddziaływaniami elektromagnetycznymi. Decyzje te mogą wymagać znacznych nakładów finansowych i mieć duże znaczenie dla gospodarki kraju. Wobec niedostatku środków finansowych w okresie światowego kryzysu ekonomicznego, wydaje się potrzebna publiczna debata w tej sprawie, dla zapewnienia społecznego zrozumienia i poparcia dla podejmowanych decyzji. Z uwagi na możliwy konflikt interesów różnych grup socjalnych, w tej debacie powinni uczestniczyć wszyscy zainteresowani: użytkownicy, właściciele i operatorzy sieci teleinformatycznych, naukowcy i praktycy, producenci, wykonawcy i dostawcy urządzeń i instalacji, ekonomiści, finansiści oraz ludzie biznesu i polityki. Ważne problemy, co do których potrzebne jest wypracowanie wspólnej opinii są np. następujące:

- Jak należy traktować w Polsce problem narażeń elektromagnetycznych i wrażliwości na nie cywilnej infrastruktury teleinformatycznej?
- Jakie miejsce powinien ten problem zająć na liście priorytetów rządowych?
- Jakie niezbędne przedsięwzięcia należy podjąć i w jakiej kolejności?
- Jak należy ustawić współpracę z zagranicą z sąsiednimi krajami i z organizacjami międzynarodowymi, w tym europejskimi?
- Jaka powinna być rola rządu, sektora państwowego, sektora prywatnego, kapitału zagranicznego?
- Jaka powinna być rola Państwowych Instytutów Badawczych (w tym Instytutu Łączności) i wyższych uczelni?
- Jaki jest koszt i źródła finansowania niezbędnej działalności w tej dziedzinie?

Autor ma nadzieję, że niniejsze opracowanie stanowić będzie wystarczające wprowadzenie do takiej dyskusji.

Wykaz literatury

1. ATIS Telecom Glossary 2007, American National Standard; The Alliance for Telecommunications Industry Solutions; http://www.atis.org/glossary/foreword.aspx
2. Bonabeau E, Dorigo M, Theraulaz G: Swarm Intelligence. From Natural to Artificial Systems; Oxford University Press, 1999
3. Degauque P, Hamelin J:Electromagnetic Compatibility, Oxford University Press 1993, ISBN 0-19-856375-2, 652 p.
4. Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance. Basic EMC publication, IEC 61000-2-9; http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=cat-det.p&wartnum=020728
5. Fitzek F.H.P., Katz M.D.: Cognitive Wireless Networks; ISBN 978-1-4020-5978-0, Springer 2007
6. Fitzek F.H.P., Katz M.D: Cooperation in Wireless Networks: Principles and Applications; Springer 2006, ISBN 10-1-4020-4710-X (640 p.)
7. Graham R et at: Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Executive summary. http://www.empcommission.org/docs/empc_exec_rpt.pdf; Critical National Infrastructures, April 2008, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf
8. Ianoz M., Wipf H.: Modeling and simulation methods to assess EM terrorism effects; Electromagnetic Compatibility 1999. Proceedings of 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, 1999
9. IET Electromagnetic Compatibility for Functional Safety; IET, 2008 (www.theiet.org)
10. ITU International Telecommunication Union: International Telecommunication Convention; Geneva
11. ITU Internet Reports: The Internet of Things; Geneva, November 2005
12. ITU-T, Telecommunication Standardization Sector of ITU, Series K.78: Protection Against Interference. HEMP Immunity Guide For Telecommunication Centres (Approved 06-2009, to be published)
13. Kirby R , Struzak R: On Radio Spectrum, Competition and Collaboration; (Invited Paper), Proceedings of the 17-th General Assembly of the URSI, Tel-Aviv, Israel, 24 September - 2 Oct. 1987
14. Leese R, Hurley S (eds.): Methods and Algorithms for Radio Channel Assignment; (Struzak R: Introduction to Spectrum Management; p. 7 -21); Oxford University Press 2002, ISBN
15. National Research Council: Cybersecurity Today and Tomorrow; ISBN 0-300-50929-7, 50p. (2002)
16. National Research Council: Making the Nation Safer: The Role and Technology in Countering Terrorism; ISBN 0-309-55781-X- 4400p. (2002)
17. Radasky W.A: 2007 Update on Intentional Electromagnetic Interference (IEMI) and High-altitude Electromagnetic Pulse (HEMP). ITEM- Interference Technology an online Guide to Electromagnetic Compatibility;

http://www.interferencetechnology.com/articles/articles/article/2007-update-on-intentional-electromagnetic-interference-iemi-and-high-altitude-electromagnetic-pul.html

18. Radicella S (ed.) /Struzak R: Introduction to International Radio Regulations; International Centre for Theoretical Physics, ISBN 92-95003-23-3 (2003). Dostępna wersja elektroniczna: http://publications.ictp.it/lns/vol16.html.
19. Strategia Rozwoju Społeczeństwa Informacyjnego w Polsce do roku 2013, Projekt wersja 3.00 (październik 2008); http://www.mswia.gov.pl/strategia/
20. Strużak R, Żernicki E: Latające Laboratorium Instytutu Łączności; *Przeglad Telekomunikacyjny*, 1981, Nr 9/10, p.258-282
21. Strużak R: Emergency Telecommunications with and in the Field: Evaluation Report; United Nations New York and Geneva, July 2000; (tekst dostępny w Internecie: http://www.reliefweb.int/telecoms/evalu/evaluation.html)
22. Strużak R: Improved utilization of the radio spectrum respecting physical laws; (Invited paper), Proceedings of the URSI General Assembly, Chicago, Illinois, USA, 9-16 August 2008
23. Strużak R: Trends in Use of RF Spectrum; Journal of Telecommunications and Information Technology; No. 4/2009, pp. 1-6; ISSN 1509-4553
24. Wik M W., Radasky W.A.: Intentional Electromagnetic Interference (IEMI): Background and Status of the Standardization Work in the International Electrotechnical Commission (IEC); The Radio Science Bulletin, No 299, Dec.2001, pp. 13-18
25. Wik M W: Revolution in Information Affairs; Global Communications Americas 2000, Hanson Cooke Ltd, ISBN 1-902221-38-9, 2000
26. Wik M W: URSI statement - Nuclear electromagnetic pulse [EMP] and associated effects; Antennas and Propagation Society Newsletter, IEEE**,** Jun 1987, Vol. 29/3, pp 19- 23
27. Wik M W: What is Network-Based Defence (NBD) and the Impact on the Future Defence? *Royal Swedish Academy of War Sciences, October 2003*
28. Wik M.W: Global Information Infrastructure: Threats; Global Communications Interactive 1997, Hanson Cooke limited, ISBN: 0946 393 893 (tekst dostepny w Internecie www.intercomms.net/content/threats.php)
29. Yamamoto, K. Yamada, K. Yonemoto, N.; PED Interference Reporting System in Japan ; Electromagnetic Compatibility and Electromagnetic Ecology, 2007 7th International Symposium on**;** Saint-Petersburg, 26-29 June 2007, pp. 220-223; ISBN: 978-1-4244-1270-9
30. Założenia do Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011 (Data publikacji : dn.11 marca 2009) http://www.mswia.gov.pl/portal/pl/2/6966/Zalozenia_do_Rzadowego_programu_ochrony_cyberprzestrzeni_RP_na_lata_20092011.html

-ooOoo-